aws

用户指南

AWS CloudTrail

版本 1.0

AWS CloudTrail: 用户指南

Table of Contents

什么是 AWS CloudTrail？ 1
正在访问 CloudTrail 2
CloudTrail 控制台 2
AWS CLI 3
CloudTrail API 3
AWS 软件开发工具包 3
如何 CloudTrail 运作 3
CloudTrail 事件历史记录 4
CloudTrail 湖泊和事件数据存储 4
CloudTrail 步道 6
CloudTrail 洞察活动 10
CloudTrail 频道 11
概念 12
CloudTrail 事件 12
事件历史记录 26
跟踪 26
组织足迹 28
CloudTrail 湖泊和事件数据存储 29
CloudTrail 见解 30
标签 30
AWS Security Token Service 和 CloudTrail 30
全球服务事件 31
支持的区域 32
支持的服务和集成 35
AWS 与日志的服务集成 CloudTrail 36
CloudTrail 与亚马逊集成 EventBridge 38
CloudTrail 与集成 AWS Organizations 39
AWS 的服务主题 CloudTrail 39
不支持的服务 60
中的配额 AWS CloudTrail 61
CloudTrail 教程 66
授予使用权限 CloudTrail 66
查看事件历史记录 67
创建记录管理事件的跟踪 69

查看您的日志文件 74
后续步骤计划 75
为 S3 数据事件创建事件数据存储 76
将跟踪事件复制到 CloudTrail Lake 事件数据存储中 83
查看 CloudTrail 湖泊仪表板 90
查看和运行 CloudTrail Lake 示例查询 95
将 CloudTrail Lake 查询结果保存到 S3 存储桶中 97
查看 CloudTrail 成本和使用情况 101
其他 资源 103
处理 CloudTrail 事件历史记录 104
事件历史记录的限制 105
使用控制台查看最近的管理事件 105
在页面之间导航 107
自定义显示视图 107
筛选 CloudTrail 事件 108
查看事件的详细信息 110
下载事件 110
使用 AWS Config查看引用的资源 111
使用查看最近的管理事件 AWS CLI 111
先决条件 113
获取命令行帮助 113
查找事件 113
指定要返回的事件数目 115
按时间范围查找事件 115
按属性查找事件 115
指定下一页结果 117
从文件中获取 JSON 输入 118
查找输出字段 119
与 L CloudTrail ake 合作 121
CloudTrail 湖泊事件数据存储 121
CloudTrail 湖泊整合 122
CloudTrail 湖泊查询 122
其他 资源 123
CloudTrail 支持湖泊的区域 123
CloudTrail 湖泊的概念和术语 125
事件数据存储 125

集成 127
查询 127
控制面板 128
事件数据存储 129
使用控制台创建、更新和管理事件数据存储 130
使用创建、更新和管理事件数据存储 AWS CLI 175
管理事件数据存储生命周期 198
将跟踪事件复制到事件数据存储 199
联合事件数据存储 219
组织事件数据存储 228
集成 232
使用控制台创建与 CloudTrail 合作伙伴的集成 234
创建与控制台的自定义集成 236
使用 Lake 创建、更新和管理 CloudTrail Lake 集成 AWS CLI 239
有关集成合作伙伴的其他信息 247
CloudTrail 湖泊集成事件架构 248
查看 Lake 控制面板 255
限制 255
先决条件 256
选择控制面板 256
根据日期或时间范围筛选控制面板 257
查看控制面板小组件的查询 258
查询 122
查询编辑器工具 259
查看示例查询 259
创建或编辑查询 261
运行查询并保存查询结果 263
查看查询结果 267
下载已保存的查询结果 269
验证已保存的查询结果 271
使用运行和管理 CloudTrail Lake 查询 AWS CLI 284
CloudTrail 湖泊 SQL 限制 288
支持的函数、条件和联接运算符 289
高级多表查询支持 290
支持的事件数据存储的 SQL 架构 291
CloudTrail 事件记录字段支持的架构 291

Ins CloudTrail ights 事件记录字段支持的架构 295
AWS Config 配置项目记录字段支持的架构 296
AWS Audit Manager 证据记录字段支持的架构 298
非AWS 事件字段支持的架构 299
控制用户权限 300
管理 CloudTrail 湖泊成本 301
事件数据存储定价选项 301
了解 CloudTrail Lake 费用 302
关于如何降低成本的建议 304
可帮助管理成本的工具 305
另请参阅 306
支持的 CloudWatch 指标 306
处理 CloudTrail 轨迹 309
为您创建路线 AWS 账户 310
使用控制台创建和更新跟踪 311
使用创建、更新和管理跟踪 AWS CLI 351
为组织创建跟踪 379
从成员账户跟踪转移到组织跟踪 382
准备为您的组织创建跟踪 382
在控制台中为您的组织创建跟踪 386
使用为组织创建跟踪 AWS Command Line Interface 402
故障排除 408
查看路径的 CloudTrail Insights 事件 410
在 CloudTrail 控制台中查看跟踪的 CloudTrail Insights 事件 411
使用查看路径的 CloudTrail Insights 事件 AWS CLI 419
将追踪事件复制到 CloudTrail湖中 430
复制跟踪事件的注意事项 431
复制跟踪事件所需的权限 432
使用 CloudTrail 控制台将跟踪事件复制到现有的事件数据存储中 436
获取和查看您的 CloudTrail 日志文件 439
正在查找您的 CloudTrail 日志文件 439
正在下载您的 CloudTrail 日志文件 441
配置 Amazon SNS 通知 CloudTrail 442
配置 CloudTrail 为发送通知 442
关于管理跟踪记录的提示 444
管理 CloudTrail 跟踪成本 444

命名要求 446
创建多个跟踪 448
控制用户权限 450
支持的 VPC 端点 450
可用性 451
为创建 VPC 终端节点 CloudTrail 452
共享子网 452
AWS 账户 封闭和步道 452
配置 CloudTrail 设置 454
组织的委托管理员 454
指定委托管理员所需的权限 457
添加 CloudTrail 委派管理员 457
移除 CloudTrail 委派的管理员 458
服务相关通道 459
使用控制台查看服务相关通道 459
使用查看与服务相关的频道 AWS CLI 459
了解 CloudTrail 事件 463
管理事件 463
数据事件 466
洞察活动 480
管理事件 483
管理事件 483
读取和写入事件 485
使用 AWS Command Line Interface记录事件 485
使用 AWS 开发工具包记录事件 496
向 Amazon CloudWatch 日志发送事件 496
数据事件 496
数据事件 498
只读和只写事件 513
使用记录数据事件 AWS Management Console 514
使用记录数据事件 AWS Command Line Interface 537
使用高级事件选择器筛选数据事件 548
记录 AWS Config 合规性的数据事件 568
使用 AWS SDK 记录数据事件 569
向 Amazon CloudWatch 日志发送事件 569
洞察活动 569

了解 Insights 事件传输情况 570
使用记录见解事件 AWS Management Console 571
使用记录见解事件 AWS Command Line Interface 573
使用 AWS SDK 记录事件 578
跟踪的其他信息 578
CloudTrail 录制内容 585
Insights 事件的记录字段 594
示例 sharedEventID 595
CloudTrail 用户身份元素 596
示例 597
字段 598
具有 SAML 和网络联合身份验证 AWS STS 的 API 的值 604
AWS STS 来源身份 605
见解 insightDetails 元素 608
示例 insightDetails 数据块 613
捕获的非 API 事件 CloudTrail 616
AWS 服务事件 616
AWS Management Console 登录事件 617
CloudTrail 日志文件 632
接收来自多个区域的 CloudTrail 日志文件 633
管理数据一致性 634
使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件 635
将事件发送到 CloudWatch 日志 636
为 CloudTrail 事件创建 CloudWatch 警报：示例 643
停止 CloudTrail 向 CloudWatch 日志发送事件 650
CloudWatch 的日志组和日志流命名 CloudTrail 650
使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档 651
接收来自多个账户的 CloudTrail 日志文件 653
为其他账户调用的数据事件修订存储桶拥有者账户 ID 654
设置适用于多个账户的存储桶策略 655
在其他账户中创建跟踪 657
在 AWS 账户之间共享 CloudTrail 日志文件 658
通过代入角色在账户之间共享日志文件 659
验证 CloudTrail 日志文件完整性 668
为什么使用它？ 668
工作方式 668

为启用日志文件完整性验证 CloudTrail 669
CloudTrail 使用验证日志文件的完整性 AWS CLI 670
CloudTrail 摘要文件结构 677
CloudTrail 日志文件完整性验证的自定义实现 684
CloudTrail 日志文件示例 695
CloudTrail 日志文件名格式 695
日志文件示例 695
使用 CloudTrail 处理库 708
最低要求 709
处理 CloudTrail 日志 709
高级主题 714
其他 资源 720
安全性 721
数据保护 721
Identity and Access Management 723
受众 723
使用身份进行身份验证 724
使用策略管理访问 726
如何 AWS CloudTrail 与 IAM 配合使用 728
基于身份的策略示例 735
基于资源的策略示例 750
适用于 Amazon S3 存储桶的政策 CloudTrail 753
适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略 759
Amazon SNS 主题政策 CloudTrail 762
故障排除 769
使用服务相关角色 772
AWS 托管策略 774
合规性验证 776
韧性 777
基础设施安全性 778
防止跨服务混淆代理 778
安全最佳实操 779
CloudTrail 侦探安全最佳实践 779
CloudTrail 预防性安全最佳实践 781
使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS) 784
启用日志文件加密 785

授予创建 KMS 密钥的权限 786
为以下各项配置 AWS KMS 密钥策略 CloudTrail 787
更新资源以使用 KMS 密钥 801
使用启用和禁用 CloudTrail 日志文件加密 AWS CLI 804
文档历史记录 808
早期更新 842
AWS 术语表 858
..... dccclix

什么是 AWS CloudTrail？

AWS CloudTrail 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。用户、角色或 AWS 服务采取的操作将作为事件记录在中 CloudTrail。事件包括在 AWS Management Console、、AWS Command Line Interface、 AWS 软件开发工具包和 API 中执行的操作。

CloudTrail AWS 账户 当你创建它时，它在你的中处于活动状态。当您的活动发生在您的活动时 AWS 账户，该活动就会记录在 CloudTrail 事件中。

CloudTrail 提供了三种记录事件的方法：

- 事件历史记录 – 事件历史记录提供对 AWS 区域中过去 90 天发生的管理事件的可查看、可搜索、可下载和不可变记录。您可以依单个属性筛选事件，从而搜索事件。创建账户时，您自动获得对事件历史记录的访问权限。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。

  查看活动历史记录不 CloudTrail 收取任何费用。

- CloudTrail L a AWS CloudTrail ke — La ke 是一个托管数据湖，用于捕获、存储、访问和分析用户和 API 活动， AWS 用于审计和安全目的。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件被聚合到事件数据存储，是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。如果您选择一年可延期保留定价选项，则可以将事件数据在事件数据存储中最多保留 3653 天（大约 10 年）；如果您选择七年保留定价选项，则最多可以保留 2557 天（大约 7 年）。您可以使用为单个 AWS 账户 或多个 AWS 账户 事件创建事件数据存储 AWS Organizations。您可以将任何现有 CloudTrail 日志从 S3 存储桶导入现有或新的事件数据存储中。您还可以使用 La ke 仪表板可视化热门 CloudTrail 事件趋势。有关更多信息，请参阅 与 L AWS CloudTrail ake 合作。

  CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。在 Lake 中运行查询时，您需要按扫描的数据量付费。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

- T@@ rail s — T rail s 会捕获 AWS 活动记录，将这些事件传送并存储在 Amazon S3 存储桶中，还可以选择传送到 CloudWatch Logs 和 Amazon EventBridge。您可以将这些事件输入到您的安全监控解决方案中。您也可以使用自己的第三方解决方案或解决方案（例如 Amazon Athena）来搜索和分析您的日志。 CloudTrail 您可以使用为单条 AWS 账户 或多 AWS 账户 条轨迹创建跟踪 AWS Organizations。您可以记录 Insights 事件以分析您的管理事件，以查看 API 调用量和错误率中的异常行为。有关更多信息，请参阅 为您创建路线 AWS 账户。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到 S3 存储桶，但是 Amazon S3 会收取存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

AWS 账户活动的可见性是安全和运营最佳实践的关键方面。您可以使用 CloudTrail 查看、搜索、下载、存档、分析和响应 AWS 基础架构中的账户活动。您可以确定谁或什么采取了哪些行动、对哪些资源采取了行动、事件发生的时间以及其他详细信息，以帮助您分析和响应 AWS 账户中的活动。

您可以使用 API CloudTrail 集成到应用程序中，为您的组织自动创建跟踪或事件数据存储，检查您创建的事件数据存储和跟踪的状态，并控制用户查看 CloudTrail 事件的方式。

正在访问 CloudTrail

您可以通过以下任何一种方式使用 CloudTrail 。

主题

- CloudTrail 控制台
- AWS CLI
- CloudTrail API
- AWS 软件开发工具包

CloudTrail 控制台

登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。

CloudTrail 控制台提供了用于执行许多 CloudTrail 任务的用户界面，例如：

- 查看您 AWS 账户的近期活动和事件历史记录。
- 从事件历史记录中下载过去 90 天管理事件的筛选或完整文件。
- 创建和编辑 CloudTrail 路径。
- 创建和编辑 CloudTrail Lake 事件数据存储。
- 对事件数据存储运行查询。
- 配置 CloudTrail 跟踪，包括：
  - 选择用于跟踪的 Amazon S3 存储桶。

- 设置前缀。
- 配置向 CloudWatch 日志的传输。
- 使用 AWS KMS 密钥对跟踪数据进行加密。
- 为跟踪上的日志文件传送启用 Amazon SNS 通知。
- 为跟踪记录添加和管理标签。

- 配置 CloudTrail Lake 事件数据存储，包括：
  - 将事件数据存储与 CloudTrail 合作伙伴或您自己的应用程序集成，以记录来自外部来源的事件 AWS。
  - 联合事件数据存储以运行来自 Amazon Athena 的查询。
  - 使用 AWS KMS 密钥对事件数据存储数据进行加密。
  - 为您的事件数据存储添加和管理标签。

有关更多信息 AWS Management Console，请参阅AWS Management Console。

AWS CLI

AWS Command Line Interface 是一个统一的工具，可用于 CloudTrail 从命令行与之交互。有关更多信息，请参阅《AWS Command Line Interface 用户指南》。有关 CloudTrail CLI 命令的完整列表，请参阅《命令参考》中的 cloudtrail 和 cloudtrail-data。AWS CLI

CloudTrail API

除了控制台和 CLI 之外，您还可以使用 CloudTrail RESTful API CloudTrail 直接进行编程。有关更多信息，请参阅 AWS CloudTrail API 参考和 CloudTrail-Data API 参考。

AWS 软件开发工具包

除了使用 CloudTrail API 之外，您还可以使用其中一个 AWS SDK。每个软件开发工具包均包含适用于各种编程语言和平台的库和示例代码。这些软件开发工具包提供了一种便捷的方式来创建对的编程访问权限。 CloudTrail例如，您可以使用开发工具包以加密方式对请求进行签名，管理错误并自动重试请求。有关更多信息，请参阅 “构建工具 AWS” 页面。

如何 CloudTrail 运作

创建 CloudTrail 事件历史记录时，您可以自动访问事件历史记录 AWS 账户。事件历史记录提供对 AWS 区域中过去 90 天的已记录管理事件的可查看、可搜索、可下载和不可变记录。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrail Lake 事件数据存储。

主题

- CloudTrail 事件历史记录
- CloudTrail 湖泊和事件数据存储
- CloudTrail 步道
- CloudTrail 洞察活动
- CloudTrail 频道

CloudTrail 事件历史记录

您可以前往事件历史记录页面，在 CloudTrail 控制台中轻松查看最近 90 天的管理事件。您还可以通过运行 aws cloudtrail lookup-events 命令或 `LookupEvents` API 操作来查看事件历史记录。您可以针对单个属性筛选事件，来搜索 Event history（事件历史记录）中的事件。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。

事件历史记录与您账户中存在的任何跟踪或事件数据存储无关，也不会受到您对跟踪和事件数据存储所做的配置更改的影响。

查看事件历史记录页面或运行`lookup-events`命令不 CloudTrail 收取任何费用。

CloudTrail 湖泊和事件数据存储

您可以创建事件数据存储来记录CloudTrail 事件（管理事件、数据事件）、CloudTrailInsights 事件、AWS Audit Manager 证据、AWS Config 配置项目或外部的事件 AWS。

事件数据存储可以记录您 AWS 账户 AWS 区域 中当前 AWS 区域事件或全部事件。用于从外部记录集成事件的事件数据存储 AWS 必须仅用于单个区域；它们不能是多区域事件数据存储。

如果您在中创建了组织 AWS Organizations，则可以创建一个组织事件数据存储，用于记录该组织中所有 AWS 账户的所有事件。组织事件数据存储可以应用于所有 AWS 区域或当前区域。组织事件数据存储必须使用管理账户或委托管理员账户创建，并且在指定为应用于某个组织时，事件数据存储将自动应用于该组织中的所有成员账户。成员账户无法查看组织事件数据存储，也无法对其进行修改或删除。组织事件数据存储不能用于从外部收集事件 AWS。有关更多信息，请参阅 组织事件数据存储。

默认情况下，事件数据存储中的所有事件都由加密 CloudTrail。配置事件数据存储时，可以选择使用自己的数据存储 AWS KMS key。使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数

据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。有关更多信息，请参阅 使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)。

下表提供了有关可以在事件数据存储上执行的任务的信息。

任务	描述
查看湖泊仪表板	您可以使用 CloudTrail Lake 仪表板对收集管理事件、S3 数据事件或 Insights 事件的事件数据存储中的事件进行可视化。
日志管理事件	将事件数据存储配置为记录只读、只写或所有管理事件。默认情况下，事件数据存储日志管理事件。
记录数据事件	配置您的事件数据存储以记录数据事件。您可以使用高级事件选择器对、和`resources.ARN` 字段进行筛选 `eventName` `readOnly`，以仅记录那些感兴趣的事件。
记录见解事件	将事件数据存储配置为记录 Insights 事件，以帮助您识别和应对与管理 API 调用相关的异常活动。有关更多信息，请参阅 记录 Insights 事件。 将对 Insights 事件收取额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅 AWS CloudTrail 定价。
复制跟踪事件	您可以将跟踪事件复制到新的或现有的事件数据存储中，以创建记录到跟踪的事件的 point-in-time 快照。
在事件数据存储上启用联合	您可以联合事件数据存储以在数据目录中查看与事件数据存储相关的元数据，并使用 Amazon Athena 对事件数据运行 SQL 查询。 AWS Glue 存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。
在事件数据存储上停止或启动事件摄取	您可以在收集 CloudTrail 管理和数据事件或 AWS Config 配置项目的事件数据存储上停止和启动事件摄取。
与外部的事件源创建集成 AWS	您可以使用 La CloudTrail ke 集成从外部记录和存储来自混合环境中任何来源的 AWS用户活动数据，例如本地或云端托管的内部

任务	描述
	或 SaaS 应用程序、虚拟机或容器。有关可用集成合作伙伴的信息，请参阅 AWS CloudTrail Lake 集成。
在 CloudTrail 控制台中查看 Lake 示例查询	CloudTrail 控制台提供了许多示例查询，可以帮助您开始编写自己的查询。
创建或编辑查询	中的查询 CloudTrail 是用 SQL 编写的。您可以在 L CloudTrail ake E ditor 选项卡上生成查询，方法是从头开始用 SQL 编写查询，或者打开已保存的查询或示例查询并对其进行编辑。
将查询结果保存到 S3 存储桶	运行查询时，您可以将查询结果保存到 S3 存储桶。
下载已保存的查询结果	您可以下载包含已保存的 L CloudTrail ake 查询结果的 CSV 文件。
验证已保存的查询结果	在将 CloudTrail 查询结果 CloudTrail 传送到 S3 存储桶后，您可以使用查询结果完整性验证来确定查询结果是被修改、删除还是未更改。

有关 CloudTrail Lake 的更多信息，请参阅与 L AWS CloudTrail ake 合作。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。在 Lake 中运行查询时，您需要按扫描的数据量付费。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

CloudTrail 步道

跟踪是一种配置，可用于将事件传送到您指定的 Amazon S3 存储桶。您还可以使用 Amazon L CloudWatch ogs 和 Amazon 在跟踪中交付和分析事件 EventBridge。

Trails 可以记录 CloudTrail 管理事件、数据事件和 Insights 事件。

您可以为创建两种类型的跟踪 AWS 账户：多区域跟踪和单区域跟踪。

多区域跟踪

创建多区域跟踪时，会在您工作的AWS 分区 AWS 区域中 CloudTrail 记录所有事件，并将 CloudTrail 事件日志文件传送到您指定的 S3 存储桶。如果在创建多区域跟踪后添加了，则会自动包含该新区域，并记录该区域中的事件。 AWS 区域 推荐的最佳实践是创建多区域跟踪，因为您可记录您账户中的所有区域的活动。您使用 CloudTrail 控制台创建的所有跟踪都是多区域的。您可以使用将单区域跟踪转换为多区域跟踪。 AWS CLI有关更多信息，请参阅 在控制台中创建跟踪 和 将应用到一个区域的跟踪转换为应用到所有区域。

单区域跟踪

创建单区域跟踪时，仅 CloudTrail 记录该区域的事件。然后，它 CloudTrail 会将事件日志文件传送到您指定的 Amazon S3 存储桶。您只能使用 AWS CLI创建单区域跟踪。如果您创建其他单个跟踪，则可以让这些跟踪将 CloudTrail 事件日志文件传送到同一 S3 存储桶或单独的存储桶。这是您使用 AWS CLI 或 CloudTrail API 创建跟踪时的默认选项。有关更多信息，请参阅 使用创建、更新和管理跟踪 AWS CLI。

> **Note**
>
> 对于这两种类型的跟踪，您可以在任何区域中指定 Amazon S3 存储桶。

如果您在中创建了组织 AWS Organizations，则可以创建组织跟踪，记录该组织中所有 AWS 账户的所有事件。组织跟踪可以应用于所有 AWS 地区或当前区域。组织跟踪必须使用管理账户或委托管理员账户创建，并且在指定为应用于某个组织时，组织跟踪将自动应用于该组织中的所有成员账户。成员账户可以看到组织记录，但不能对其进行修改或删除。默认情况下，成员账户无权访问 Amazon S3 存储桶中组织跟踪的日志文件。

默认情况下，当您在 CloudTrail 控制台中创建跟踪时，您的事件日志文件将使用 KMS 密钥进行加密。如果您选择不启用 SSE-KMS 加密，则您的事件日志将使用 Amazon S3 服务器端加密 (SSE) 进行加密。您可以将日志文件在 存储桶中存储任意长的时间。您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。如果您想接收有关日志文件传送和验证的通知，可以设置 Amazon SNS 通知。

CloudTrail 每小时多次发布日志文件，大约每 5 分钟发布一次。这些日志文件包含来自支持账户中的服务的 API 调用 CloudTrail。有关更多信息，请参阅 CloudTrail 支持的服务和集成。

> **Note**
>
> CloudTrail 通常在 API 调用后的平均大约 5 分钟内传送日志。此时间并不能得到保证。有关更多信息，请参阅 AWS CloudTrail 服务等级协议。
> 如果您错误配置了跟踪（例如，无法访问 S3 存储桶），则 CloudTrail会尝试将日志文件重新传送到您的 S3 存储桶，持续 30 天，这些 attempted-to-deliver 事件将按标准费用收费。CloudTrail 为避免配置错误的跟踪产生费用，您需要删除跟踪。
> CloudTrail 捕获用户直接执行的操作或 AWS 服务代表用户执行的操作。例如， AWS CloudFormation `CreateStack`调用可能会导致对亚马逊 EC2、Amazon RDS、Amazon EBS 或 AWS CloudFormation 模板要求的其他服务进行额外的 API 调用。这是正常的，也是预期的行为。您可以通过 CloudTrail事件中的`invokedby`字段来识别操作是否由 AWS 服务机构执行。

下表提供了有关可以在跟踪上执行的任务的信息。

任务	描述
记录管理事件	将您的跟踪配置为记录只读、只写或所有管理事件。
记录数据事件	您可以使用高级事件选择器来创建精细的选择器，以仅记录那些感兴趣的数据事件。使用高级事件选择器时，您可以对该`eventName` 字段进行筛选，以包含或排除特定 API 调用的记录，这有助于控制成本。
记录见解事件	将跟踪记录配置为记录 Insights 事件，以帮助您识别和应对与管理 API 调用相关的异常活动。 将对 Insights 事件收取额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅AWS CloudTrail 定价。
查看洞察活动	在跟踪上启用 CloudTrail Insights 后，您可以使用 CloudTrail 控制台或查看最多 90 天的 Insights 事件 AWS CLI。

任务	描述
下载洞察活动	在跟踪上启用 CloudTrail Insights 后，您可以为跟踪下载包含最多 90 天的 Insights 事件的 CSV 或 JSON 文件。
将追踪事件复制到 CloudTrail Lake	您可以将现有跟踪事件复制到 CloudTrail Lake 事件数据存储中，以创建记录到跟踪的事件的 point-in-time 快照。
创建并订阅 Amazon SNS 主题	订阅主题以接收有关将日志文件传送至您的存储桶的通知。Amazon SNS 可通过多种方式通知您，包括使用 Amazon Simple Queue Service 以编程方式通知您。 **Note** 如果您要接收有关从所有区域传送日志文件的 SNS 通知，请为您的跟踪仅指定一个 SNS 主题。如果要以编程方式处理所有事件，请参阅 使用 CloudTrail 处理库。
查看您的日志文件	从 S3 存储桶中查找并下载您的日志文件。
使用 CloudWatch 日志监控事件	您可以将跟踪配置为向 L CloudWatch ogs 发送事件。然后，您可以使用 CloudWatch 日志来监控您的账户中是否有特定 API 调用和事件。 **Note** 如果您配置适用于所有区域的跟踪以将事件发送到 CloudWatch 日志日志组，则会将来自所有区域的事件 CloudTrail 发送到单个日志组。

任务	描述
启用日志加密	日志文件加密为您的日志文件提供额外的安全层。
启用日志文件完整性	日志文件完整性验证可帮助您验证日志文件自 CloudTrail 交付以来是否保持不变。
与其他人共享日志文件 AWS 账户	您可以在账户之间共享日志文件。
汇总来自多个账户的日志	您可以将多个账户中的日志文件聚合到单个存储桶中。
使用合作伙伴解决方案	使用与集成的合作伙伴解决方案分析您的 CloudTrail 产出 CloudTrail。合作伙伴解决方案提供了一组广泛的功能，例如，更改跟踪、故障排除和安全分析。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到 S3 存储桶，但是 Amazon S3 会收取存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 洞察活动

AWS CloudTrail Insights 通过持续分析 CloudTrail 管理事件，帮助 AWS 用户识别和响应与 API 调用和 API 错误率相关的异常活动。 CloudTrail Insights 会分析您的 API 调用量和 API 错误率的正常模式（也称为基线），并在呼叫量或错误率超出正常模式时生成 Insights 事件。针对 `write` 管理 API 生成的 API 调用量的 Insights 事件，以及针对 `read` 和 `write` 管理 API 生成的 API 错误率的 Insights 事件。

默认情况下， CloudTrail 跟踪和事件数据存储不记录 Insights 事件。您必须配置跟踪或事件数据存储以记录 Insights 事件。有关更多信息，请参阅 使用记录见解事件 AWS Management Console 和 使用记录见解事件 AWS Command Line Interface。

将对 Insights 事件收取额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅AWS CloudTrail 定价。

查看跟踪和事件数据存储的 Insights 事件

CloudTrail 跟踪和事件数据存储都支持 Insights 事件，但是，查看和访问 Insights 事件的方式存在一些差异。

查看跟踪的 Insights 事件

如果您在跟踪上启用了 Insights 事件并 CloudTrail 检测到异常活动，则 Insights 事件会记录到您的跟踪的目标 S3 存储桶中的其他文件夹或前缀。在 CloudTrail 控制台上查看 Insights 事件时，您还可以查看洞察类型和事件时间段。有关更多信息，请参阅 在 CloudTrail 控制台中查看跟踪的 CloudTrail Insights 事件。

首次在跟踪上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 36 小时 CloudTrail 才能交付第一个 Insights 事件。

查看事件数据存储的 Insights 事件

要在 L CloudTrail ake 中记录 Insights 事件，您需要一个用于记录 Insights 事件的目标事件数据存储和一个启用 Insights 并记录管理事件的源事件数据存储。有关更多信息，请参阅 使用控制台为 CloudTrail Insights 事件创建事件数据存储。

首次在源事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最多可能需要 7 天才能 CloudTrail 将第一个 Insights 事件传送到目标事件数据存储。

如果您在源事件数据存储上启用了 CloudTrail Insights 并 CloudTrail 检测到异常活动，则会将 Insigh CloudTrail ts 事件传送到您的目标事件数据存储。然后，您可以查询目标事件数据存储以获取有关您的 Insights 事件的信息，还可以选择将查询结果保存到 S3 存储桶中。有关更多信息，请参阅 创建或编辑查询 和 在 CloudTrail 控制台中查看示例查询。

您可以查看 Insights 事件控制面板，以可视化目标事件数据存储中的 Insights 事件。有关 Lake 控制面板的更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

CloudTrail 频道

CloudTrail 支持两种类型的频道：

CloudTrail Lake 与 Lake 以外的事件源集成的渠道 AWS

> CloudTrail Lake 使用渠道将与您合作的外部合作伙伴或您自己的来源的外部活动带 AWS CloudTrail入 CloudTrail Lake。在创建通道时，您可以选择一个或多个事件数据存储，用于存储来自通道来源的事件。只要将目标事件数据存储设置为记录活动事件，即可根据需要更改通道的目标事件数据存储。当您为来自外部合作伙伴的活动创建通道时，您需要向合作伙伴或来源应用程

序提供通道 ARN。附加到该通道的资源策略允许来源通过该通道传输事件。有关更多信息，请参阅《AWS CloudTrail API 参考》中的 与外部的事件源创建集成 AWS 和 `CreateChannel`。

服务相关通道

AWS 服务可以创建与服务相关的渠道来代表您接收 CloudTrail 事件。创建 AWS 服务相关频道的服务会为该频道配置高级事件选择器，并指定该频道是适用于所有区域还是适用于当前区域。

您可以使用CloudTrail 控制台或AWS CLI查看由 AWS 服务创建的任何 CloudTrail 服务相关频道的相关信息。

CloudTrail 概念

本节总结了与之相关的基本概念 CloudTrail。

概念：

- CloudTrail 事件
- 事件历史记录
- 跟踪
- 组织足迹
- CloudTrail 湖泊和事件数据存储
- CloudTrail 见解
- 标签
- AWS Security Token Service 和 CloudTrail
- 全球服务事件

CloudTrail 事件

中的事件 CloudTrail 是 AWS 账户中某项活动的记录。此活动可以是 IAM 身份或可由 CloudTrail监控的服务采取的操作。 CloudTrail事件提供通过 AWS Management Console、 AWS SDK、命令行工具和其他 AWS 服务进行的 API 和非 API 账户活动的历史记录。

CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序出现。

CloudTrail 记录三种类型的事件：

- 管理事件

- 数据事件
- 洞察活动

所有事件类型都使用 CloudTrail JSON 日志格式。

默认情况下，跟踪记录和事件数据存储将记录管理事件，但不记录数据事件或 Insights 事件。

有关如何与 AWS 服务 集成的信息 CloudTrail，请参阅AWS 的服务主题 CloudTrail。

管理事件

管理事件提供有关对您 AWS 账户中的资源执行的管理操作的信息。这些也称为控制层面操作。

示例管理事件包括：

- 配置安全性（例如， AWS Identity and Access Management `AttachRolePolicy`API 操作）。
- 注册设备（例如，Amazon EC2 `CreateDefaultVpc` API 操作）。
- 配置传送数据的规则（例如，Amazon EC2 `CreateSubnet` API 操作）。
- 设置日志记录（例如， AWS CloudTrail `CreateTrail`API 操作）。

管理事件还包括在您的账户中发生的非 API 事件。例如，当用户登录您的账户时，会 CloudTrail 记录该`ConsoleLogin`事件。有关更多信息，请参阅 捕获的非 API 事件 CloudTrail。

默认情况下，t CloudTrail rails 和 CloudTrail Lake 事件数据存储日志管理事件。有关记录管理事件的更多信息，请参阅记录管理事件。

数据事件

数据事件提供有关对在资源上或资源内执行的资源操作的信息。这些也称为数据层面操作。数据事件通常是高容量活动。

示例数据事件包括：

- 针@@ 对 S3 存储桶中对象的 Amazon S3 对象级 `PutObject` API 活动（例如`GetObject`、`DeleteObject`、和 API 操作）。
- AWS Lambda 函数执行活动（`Invoke`API）。
- CloudTrail `PutAuditEvents`用于记录外部事件的 L CloudTrail ake 频道上的活动 AWS。
- 针对主题的 Amazon SNS `Publish` 和 `PublishBatch` API 操作。

下表显示可用于跟踪和事件数据存储的数据事件类型。数据事件类型（控制台）列显示控制台中的相应选择。resources.typ **`resources.type`** e 值列显示您将使用或 API 指定的值，以便在跟踪或事件数据存储中包含该 AWS CLI 类型的数据事件。 CloudTrail

对于跟踪，您可以使用基本或高级事件选择器来记录 Amazon S3 对象、Lambda 函数和 DynamoDB 表（显示在表的前三行）的数据事件。您只能使用高级事件选择器来记录其余行中显示的数据事件类型。

对于事件数据存储，只能使用高级事件选择器来包含数据事件。

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon DynamoDB	表上的 Amazon DynamoDB 项目级 API 活动（例如`PutItem`、`DeleteItem`、`UpdateItem` 和 API 操作）。 **Note** 对于启用了流的表，数据事件中的 `resources` 字段同时包含 `AWS::DynamoDB::Stream` 和 `AWS::DynamoDB::Table`。如果您为 `resources.type` 指定 `AWS::DynamoDB::Tab`	DynamoDB	`AWS::DynamoDB::Table`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	le ，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName 在该字段上添加过滤器。		
AWS Lambda	AWS Lambda 函数执行活动（ InvokeAPI ）。	Lambda	AWS::Lambda::Function
Amazon S3	针@@ 对 S3 存储桶中对象的 Amazon S3 对象级 PutObject API 活动（例如GetObject DeleteObject 、和 API 操作）。	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 用于配置操作的 API 活动，例如对StartConfiguration Session 和的调用GetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS B2B 数据交换	用于转换器操作的 B2B 数据交换 API 活动，例如对 `GetTransformerJob` 和 `StartTransformerJob` 的调用。	B2B 数据交换	`AWS::B2BI::Transformer`
Amazon Bedrock	代理别名上的 Amazon Bedrock API 活动。	Bedrock 代理别名	`AWS::Bedrock::AgentAlias`
	知识库上的 Amazon Bedrock API 活动。	Bedrock 知识库	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront 在 a KeyValueStore上的 API 活动	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map 命名空间上的 API 活动。	AWS Cloud Map 命名空间	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map 服务上的 API 活动。	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` 用于记录外部事件的 L CloudTrail lake 频道上的活动 AWS。	CloudTrail 频道	`AWS::CloudTrail::Channel`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon CodeWhisperer	亚马逊 CodeWhisperer API 在自定义方面的活动。	CodeWhisperer 定制	`AWS::CodeWhisperer::Customization`
	个人资料上的亚马逊 CodeWhisperer API 活动。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	针对 Amazon Cognito 身份池的 Amazon Cognito API 活动。	Cognito 身份池	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	针对流的 Amazon DynamoDB API 活动	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) 直接 API，例如 Amazon EBS 快照上的 `PutSnapshotBlock` 、`GetSnapshotBlock` 和 `ListChangedBlocks` 。	Amazon EBS 直接 API	`AWS::EC2::Snapshot`
Amazon EMR	针对预写日志工作空间的 Amazon EMR API 活动。	EMR 预写日志工作空间	`AWS::EMRWAL::Workspace`
Amazon FinSpace	针对环境的 Amazon FinSpace API 活动	FinSpace	`AWS::FinSpace::Environment`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS Glue	AWS Glue 在 Lake Formation 创建的表格上的 API 活动。 **Note** AWS Glue 目前仅以下区域支持表的数据事件： • 美国东部（弗吉尼亚州北部） • 美国东部（俄亥俄州） • 美国西部（俄勒冈州） • 欧洲地区（爱尔兰） • Asia Pacific（Tokyo）Region	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	探测器的亚马逊 GuardDuty API 活动。	GuardDuty 探测器	`AWS::GuardDuty::Detector`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS HealthImaging	AWS HealthImaging 数据存储上的 API 活动。	医学成像数据存储	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT 证书上@@的 API 活动。	物联网证书	`AWS::IoT::Certificate`
	AWS IoT API 在事物上的活动。	物联网的东西	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	组件版本上来自 Greengrass 核心设备的 Greengrass API 活动。 **Note** Greengrass 不会记录被拒绝访问的事件。	物联网 Greengrass 组件版本	`AWS::GreengrassV2::ComponentVersion`
	部署时来自 Greengrass 核心设备的 Greengrass API 活动。 **Note** Greengrass 不会记录被拒绝访问的事件。	物联网 Greengrass 部署	`AWS::GreengrassV2::Deployment`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS IoT SiteWise	资产上的@@ 物联网 SiteWise API 活动。	物联网 SiteWise 资产	AWS::IoTSiteWise::Asset
	时间序列上的@@ 物联网 SiteWise API 活动。	物联网 SiteWise 时间序列	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	实体上的物联网 TwinMaker API 活动。	物联网 TwinMaker 实体	AWS::IoTTwinMaker::Entity
	工作空间上 TwinMaker 的 IoT API 活动。	物联网 TwinMaker 工作空间	AWS::IoTTwinMaker::Workspace
Amazon Kendra Intelligent Ranking	针对重新评分执行计划的 Amazon Kendra Intelligent Ranking API 活动。	Kendra 排名	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces（Apache Cassandra 兼容）	表上的 Amazon Keyspaces API 活动。	卡桑德拉桌	AWS::Cassandra::Table
Amazon Kinesis Data Streams	直播中的 Kinesis Data Streams API 活动。	Kinesis 直播	AWS::Kinesis::Stream
	Kinesis Data Streams 针对直播使用者的 API 活动。	Kinesis 直播消费者	AWS::Kinesis::StreamConsumer

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon Kinesis Video Streams	Kinesis Video Streams 视频流上的 API 活动，例如GetMedia对和的调用。PutMedia	Kinesis 视频流	AWS::KinesisVideo::Stream
Amazon Managed Blockchain	针对网络的 Amazon Managed Blockchain API 活动。	托管区块链网络	AWS::ManagedBlockchain::Network
	针对 Ethereum 节点的 Amazon Managed Blockchain JSON-RPC 调用，如 eth_getBalance 或 eth_getBlockByNumber 。	托管区块链	AWS::ManagedBlockchain::Node
Amazon Neptune 图形	Neptune Graph 上的数据 API 活动，例如查询、算法或向量搜索。	Neptune 图形	AWS::NeptuneGraph::Graph
AWS Private CA	AWS Private CA 活动目录 API 活动的连接器。	AWS Private CA 活动目录连接器	AWS::PCAConnectorAD::Connector
亚马逊 Q 应用程序	亚马逊 Q 应用程序上的数据 API 活动。	亚马逊 Q 应用程序	AWS::QApps:QApp
Amazon Q Business	应用程序上的 Amazon Q Business API 活动。	Amazon Q Business 应用程序	AWS::QBusiness::Application

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	数据来源上的 Amazon Q Business API 活动。	Amazon Q Business 数据来源	`AWS::QBusiness::DataSource`
	索引上的 Amazon Q Business API 活动。	Amazon Q Business 索引	`AWS::QBusiness::Index`
	Web 体验上的 Amazon Q Business API 活动。	Amazon Q Business Web 体验	`AWS::QBusiness::WebExperience`
Amazon RDS	数据库集群上的 Amazon RDS API 活动。	RDS 数据 API-数据库集群	`AWS::RDS::DBCluster`
Amazon S3	接入点上的 Amazon S3 API 活动。	S3 接入点	`AWS::S3::AccessPoint`
	Amazon S3 对象 Lambda 接入点 API 活动，例如对和的调用。`CompleteMultipartUpload` `GetObject`	S3 对象 Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 on Outposts 对象级别 API 活动。	S3 Outposts	`AWS::S3Outposts::Object`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon SageMaker	亚马逊在终端节点上的 SageMaker InvokeEndpointWithResponseStream 活动。	SageMaker 端点	AWS::SageMaker::Endpoint
	特色商店中的亚马逊 SageMaker API 活动。	SageMaker feature store	AWS::SageMaker::FeatureGroup
	Amazon SageMaker API 在实验试用组件上的活动。	SageMaker 指标实验试验组件	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	针对平台端点的 Amazon SNS Publish API 操作。	SNS 平台端点	AWS::SNS::PlatformEndpoint
	针对主题的 Amazon SNS Publish 和 PublishBatch API 操作。	SNS 主题	AWS::SNS::Topic
Amazon SQS	消息上的 Amazon SQS API 活动。	SQS	AWS::SQS::Queue
AWS Step Functions	Step Functions API 在状态机上的活动。	Step Functions 状态机	AWS::StepFunctions::StateMachine
AWS Supply Chain	AWS Supply Chain 实例上的 API 活动。	供应链	AWS::SCN::Instance

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon SWF	域名上的@@ 亚马逊 SWF API 活动。	SWF 域名	AWS::SWF::Domain
AWS Systems Manager	控制通道上的 Systems Manager API 活动。	Systems Manager (系统管理员)	AWS::SSMMessages::ControlChannel
	托管节点上的 Systems Manager API 活动。	Systems Manager 托管式节点	AWS::SSM::ManagedNode
Amazon Timestream	针对数据库的 Amazon Timestream Query API 活动。	Timestream 数据库	AWS::Timestream::Database
	针对表的 Amazon Timestream Query API 活动。	Timestream 表	AWS::Timestream::Table
Amazon Verified Permissions	针对策略存储的 Amazon Verified Permissions API 活动。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces 瘦客户机	WorkSpaces 设备上的瘦客户端 API 活动。	瘦客户端设备	AWS::ThinClient::Device
	WorkSpaces 环境中的瘦客户端 API 活动。	瘦客户端环境	AWS::ThinClient::Environment
AWS X-Ray	追踪上@@ 的 X-Ray API 活动。	X 射线追踪	AWS::XRay::Trace

默认情况下，在您创建跟踪或事件数据存储时，未记录数据事件。要记录 CloudTrail 数据事件，必须明确添加要为其收集活动的支持的资源或资源类型。有关记录事件数据的更多信息，请参阅 记录数据事件。

记录数据事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

洞察活动

CloudTrail Insights 事件通过分析 CloudTrail 管理活动来捕获您 AWS 账户中异常的 API 调用率或错误率活动。Insights 事件提供相关信息，例如关联的 API、错误代码、事件时间和统计数据，以帮助您了解异常活动并对其采取措施。与在 CloudTrail 跟踪或事件数据存储中捕获的其他类型的事件不同，Insights 事件仅在 CloudTrail 检测到您的账户 API 使用情况或错误率记录的变化与账户的典型使用模式明显不同时，才会记录 Insights 事件。

可能生成 Insights 事件的活动的示例包括：

- 您的账户通常每分钟记录不超过 20 次 Simple Storage Service（Amazon S3）`DeleteBucket` API 调用，但是您的账户一开始就平均每分钟记录 100 次 `DeleteBucket` API 调用。在异常活动开始时记录一个 Insights 事件，并记录另一个见解事件以标记异常活动的结束。
- 您的账户通常每分钟记录 20 次对 Amazon EC2 `AuthorizeSecurityGroupIngress` API 的调用，但是您的账户开始记录对 `AuthorizeSecurityGroupIngress` 的零次调用。在异常活动开始时记录一个 Insights 事件，10 分钟后，当异常活动结束时，将记录另一个 Insights 事件以标记异常活动的结束。
- 您的账户七天内对 AWS Identity and Access Management API、`DeleteInstanceProfile` 记录的 `AccessDeniedException` 错误通常不到一个。你的账户开始对 `DeleteInstanceProfile` API 调用每分钟平均记录 12 个 `AccessDeniedException` 错误。在异常错误率活动开始时记录一个 Insights 事件，并记录另一个 Insights 事件以标记异常活动的结束。

这些示例仅用于说明用途。根据您的使用案例，您的结果可能会有所不同。

要记录 CloudTrail Insights 事件，您必须在新的或现有的跟踪或事件数据存储上明确启用 Insights 事件。有关记录 Insights 事件的更多信息，请参阅 记录 Insights 事件。

将对 Insights 事件收取额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅AWS CloudTrail 定价。

查看跟踪和事件数据存储的 Insights 事件

CloudTrail 跟踪和事件数据存储都支持 Insights 事件，但是，查看和访问 Insights 事件的方式存在一些差异。

查看跟踪的 Insights 事件

如果您在跟踪上启用了 Insights 事件并 CloudTrail 检测到异常活动，则 Insights 事件会记录到您的跟踪的目标 S3 存储桶中的其他文件夹或前缀。在 CloudTrail 控制台上查看 Insights 事件时，您还可以查看洞察类型和事件时间段。有关更多信息，请参阅 在 CloudTrail 控制台中查看跟踪的 CloudTrail Insights 事件。

查看事件数据存储的 Insights 事件

要在 L CloudTrail ake 中记录 Insights 事件，您需要一个用于记录 Insights 事件的目标事件数据存储和一个启用 Insights 并记录管理事件的源事件数据存储。有关更多信息，请参阅 使用控制台为 CloudTrail Insights 事件创建事件数据存储。

如果您在源事件数据存储上启用了 CloudTrail Insights 并 CloudTrail 检测到异常活动，则会将 Insigh CloudTrail ts 事件传送到您的目标事件数据存储。然后，您可以查询目标事件数据存储以获取有关您的 Insights 事件的信息，还可以选择将查询结果保存到 S3 存储桶中。有关更多信息，请参阅 创建或编辑查询 和 在 CloudTrail 控制台中查看示例查询。

您可以查看 Insights 事件控制面板，以可视化目标事件数据存储中的 Insights 事件。有关更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

事件历史记录

CloudTrail 事件历史记录提供了过去 90 天中管理事件的可查看、可搜索、可下载且不可变的 CloudTrail 记录。 AWS 区域您可以使用此历史记录在、软件开发工具 AWS 包 AWS Management Console、命令行工具和其他 AWS 服务中查看您的 AWS 账户中执行的操作。您可以通过选择显示哪些列来自定义 CloudTrail 控制台中的事件历史记录视图。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。

跟踪

跟踪是一种配置，允许将 CloudTrail 事件传输到 S3 存储桶，也可以选择传送到 L CloudWatch ogs 和 A mazon EventBridge。您可以使用跟踪来选择要传送 CloudTrail 的事件，使用密 AWS KMS 钥加密 CloudTrail 事件日志文件，以及为日志文件传输设置 Amazon SNS 通知。有关如何创建和管理跟踪的更多信息，请参阅为您创建路线 AWS 账户。

多区域和单区域跟踪

您可以为创建两种类型的跟踪 AWS 账户：多区域跟踪和单区域跟踪。

多区域跟踪

创建多区域跟踪时，会在您工作的AWS 分区 AWS 区域中 CloudTrail 记录所有事件，并将 CloudTrail 事件日志文件传送到您指定的 S3 存储桶。如果在创建多区域跟踪后添加了，则会自动包含该新区域，并记录该区域中的事件。 AWS 区域 推荐的最佳实践是创建多区域跟踪，因为您可记录您账户中的所有区域的活动。您使用 CloudTrail 控制台创建的所有跟踪都是多区域的。您可以使用将单区域跟踪转换为多区域跟踪。 AWS CLI有关更多信息，请参阅 在控制台中创建跟踪 和 将应用到一个区域的跟踪转换为应用到所有区域。

单区域跟踪

创建单区域跟踪时，仅 CloudTrail 记录该区域的事件。然后，它 CloudTrail 会将事件日志文件传送到您指定的 Amazon S3 存储桶。您只能使用 AWS CLI创建单区域跟踪。如果您创建其他单个跟踪，则可以让这些跟踪将 CloudTrail 事件日志文件传送到同一 S3 存储桶或单独的存储桶。这是您使用 AWS CLI 或 CloudTrail API 创建跟踪时的默认选项。有关更多信息，请参阅 使用创建、更新和管理跟踪 AWS CLI。

> **Note**
>
> 对于这两种类型的跟踪，您可以在任何区域中指定 Amazon S3 存储桶。

多区域跟踪具有以下优点：

- 跟踪的配置设置一致地应用于所有轨迹 AWS 区域。
- 您可以在单个 Amazon S3 存储桶 AWS 区域 中接收来自所有 CloudTrail 事件的事件，也可以选择在 CloudWatch 日志日志组中接收事件。
- 您可以 AWS 区域 从一个位置管理所有人的跟踪配置。

将跟踪应用于所有 AWS 区域时， CloudTrail 使用您在特定区域中创建的跟踪，在您所在AWS 分区的所有其他区域中创建配置相同的跟踪。

这有以下影响：

- CloudTrail 将所有 AWS 区域的账户活动日志文件传输到您指定的单个 Amazon S3 存储桶，也可以传输到 CloudWatch 日志日志组。
- 如果您为跟踪配置了 Amazon SNS 主题，则有关所有 AWS 区域日志文件传输的 SNS 通知将发送到该单个 SNS 主题。

无论跟踪是多区域还是单区域，发送到 Ama EventBridge zon 的事件都会在每个区域的事件总线中接收，而不是在单个事件总线中接收。

每区域多个跟踪记录

如果您拥有不同但相关的用户组，例如开发人员、安全人员和 IT 审计人员，您可以为每个区域创建多个跟踪记录。这可使每个组均接收各自的日志文件副本。

CloudTrail 每个区域支持五条跟踪。多区域跟踪计为每个区域一条跟踪。

以下是包含五条轨迹的区域的示例：

- 您在美国西部（加利福尼亚北部）区域创建了两个仅适用于此区域的跟踪记录。
- 您又在美国西部（加利福尼亚北部）地区创建了两条多区域跟踪。
- 您在亚太地区（悉尼）地区创建另一条多区域跟踪。此跟踪也作为美国西部（加利福尼亚北部）区域中的跟踪存在。

您可以在 CloudTrail 控制台的 Trails 页面 AWS 区域 中查看跟踪列表。有关更多信息，请参阅 更新跟踪。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

组织足迹

组织跟踪是一种配置，允许将管理账户和 AWS Organizations 组织中所有成员账户中的 CloudTrail 事件传送到同一 Amazon S3 存储桶、 CloudWatch 日志和 Amazon EventBridge。创建组织跟踪可帮助您为组织定义统一的事件记录策略。

使用控制台创建的所有组织跟踪都是多区域组织跟踪，用于记录组织 AWS 区域 中每个成员账户中已启用的事件。要记录组织中所有 AWS 分区中的事件，请在每个分区中创建多区域组织跟踪。您可以使用创建单区域或多区域组织跟踪。 AWS CLI如果您创建单区域跟踪，则只能在该跟踪 AWS 区域 （也称为主区域）中记录活动。

尽管大多数区域默认 AWS 区域 处于启用状态 AWS 账户，但您必须手动启用某些区域（也称为可选区域）。有关默认启用哪些区域的信息，请参阅AWS Account Management 参考指南中的启用和禁用区域之前的注意事项。有关 CloudTrail支持的区域列表，请参阅CloudTrail 支持的区域。

创建组织跟踪时，将在属于您的组织的成员账户中创建带有您指定名称的跟踪副本。

- 如果组织跟踪适用于单区域，而跟踪的主区域不是 Opt-Region，则会在组织跟踪的主区域的每个成员账户中创建跟踪的副本。

- 如果组织跟踪是针对单区域的，而跟踪的主区域是选择区域，则会在组织跟踪的主区域中在启用该区域的成员账户中创建该跟踪的副本。
- 如果组织跟踪是多区域，并且跟踪的主区域不是可选区域，则会在每个成员账户中启用的 AWS 区域每个跟踪中创建一个跟踪副本。当成员账户启用可选区域时，将在该区域的激活完成后，在新选择的区域中为该成员账户创建多区域跟踪的副本。
- 如果组织跟踪是多区域，而主区域是可选区域，则成员账户将不会向组织跟踪发送活动，除非他们选择进入创建多区域跟踪 AWS 区域 的地方。例如，如果您创建了多区域跟踪并选择欧洲（西班牙）地区作为跟踪的主区域，则只有为其账户启用了欧洲（西班牙）地区的成员账户才会将其账户活动发送到组织跟踪。

> **Note**
>
> CloudTrail 即使资源验证失败，也会在成员账户中创建组织跟踪。验证失败的示例包括：
>
> - Amazon S3 存储桶策略不正确
> - 不正确的 Amazon SNS 主题政策
> - 无法传送到 CloudWatch 日志组
> - 权限不足，无法使用 KMS 密钥进行加密
>
> 拥有 CloudTrail 权限的成员账户可以通过在 CloudTrail 控制台上查看跟踪的详细信息页面或运行 AWS CLI get-trail-status命令来查看组织跟踪的任何验证失败。

拥有成员账户 CloudTrail 权限的用户在从自己的账户登录 AWS CloudTrail 控制台时或运行诸如（尽管成员 AWS 账户在使用时必须使用 ARN 而不是名称）之类的 AWS CLI 命令时，他们将能够看到组织跟踪`describe-trails`（包括跟踪 ARN）。 AWS CLI但是，成员账户中的用户将没有足够的权限删除组织跟踪、开启或关闭日志记录、更改记录的事件类型或以任何方式更改组织跟踪。有关 AWS Organizations的更多信息，请参阅 Organizations 术语和概念。有关创建和使用组织跟踪记录的更多信息，请参阅为组织创建跟踪。

CloudTrail 湖泊和事件数据存储

CloudTrail Lake 允许您对事件运行基于 SQL 的精细查询，并记录来自外部 AWS来源（包括您自己的应用程序）以及与之集成的合作伙伴的事件。 CloudTrail您无需在账户中配置跟踪即可使用 CloudTrail Lake。

事件被聚合到事件数据存储，是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。如果您选择一年可延期保留定价选项，则可以将事件数据在事件数据存储中最多保留 3653 天（大约 10 年）；如果您选择七年保留定价选项，则最多可以保留 2557 天（大约 7 年）。您可以保存 Lake 查询以供将来使用，并查看最多七天的查询结果。您也可以将查询结果保存到 S3 存储桶中。 CloudTrail Lake 还可以将来自组织的事件存储 AWS Organizations 在事件数据存储中，或者存储来自多个区域和账户的事件。 CloudTrail Lake 是审计解决方案的一部分，可帮助您进行安全调查和故障排除。有关更多信息，请参阅 与 L AWS CloudTrail ake 合作 和 CloudTrail 湖泊的概念和术语。

CloudTrail 见解

CloudTrail Insights 通过持续分析 CloudTrail 管理事件，帮助 AWS 用户识别和响应异常数量的 API 调用或 API 调用中记录的错误。Insights 事件是异常级别的 `write` 管理 API 活动，或管理 API 活动返回的异常错误级别。默认情况下，跟踪和事件数据存储不记录 CloudTrail Insights 事件。在控制台中，您可以选择在创建或更新跟踪或事件数据存储时记录 Insights 事件。使用 CloudTrail API 时，您可以通过使用 `PutInsightSelectors`API 编辑现有跟踪或事件数据存储的设置来记录 Insights 事件。记录 CloudTrail Insights 事件需要支付额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅 记录 Insights 事件 和 AWS CloudTrail 定价。

标签

标签是客户定义的密钥和可选值，可以分配给 AWS 资源，例如 CloudTrail 跟踪、事件数据存储和频道、用于存储 CloudTrail 日志文件的 S3 存储桶、 AWS Organizations 组织和组织单位等等。通过向跟踪和用于存储跟踪日志文件的 S3 存储桶中添加相同的标签，您可以更轻松地管理、搜索和筛选这些资源。AWS Resource Groups您可以实施标记策略以帮助您持续、高效且轻松地查找和管理您的资源。有关更多信息，请参阅为AWS 资源添加标签的最佳实践。

AWS Security Token Service 和 CloudTrail

AWS Security Token Service (AWS STS) 是一项具有全局终端节点的服务，还支持特定于区域的终端节点。终端节点是作为 Web 服务请求入口点的 URL。例如，`https://cloudtrail.us-west-2.amazonaws.com`是该 AWS CloudTrail 服务的美国西部（俄勒冈）区域入口点。区域性终端节点可帮助减少应用程序中的延迟。

当您使用 AWS STS 特定于区域的终端节点时，该区域中的跟踪仅传送该区域中发生 AWS STS 的事件。例如，如果您使用终端节点 `sts.us-west-2.amazonaws.com`，则 us-west-2 中的跟踪仅传输源自 us-west-2 的 AWS STS 事件。有关 AWS STS 区域终端节点的更多信息，请参阅 IAM 用户指南 AWS STS 中的在 AWS 区域中激活和停用。

有关 AWS 区域终端节点的完整列表，请参阅中的AWS 区域和终端节点AWS 一般参考。有关来自全局 AWS STS 终端节点的事件的详细信息，请参阅全球服务事件。

全球服务事件

> **Important**
>
> 自 2021 年 11 月 22 日起， AWS CloudTrail 更改了跟踪捕获全球服务事件的方式。现在，事件由 Amazon 创建 CloudFront AWS Identity and Access Management，并 AWS STS 记录在创建这些事件的区域，即美国东部（弗吉尼亚北部）区域 us-east-1。这使得如何 CloudTrail 对待这些服务与其他 AWS 全球服务保持一致。要继续接收美国东部（弗吉尼亚州北部）以外的全球服务事件，请务必将使用美国东部（弗吉尼亚州北部）以外全球服务事件的单区域跟踪转换为多区域跟踪。如需有关捕获全球服务事件的更多信息，请参阅本章节后面部分的启用和禁用全球服务事件记录。
> 相比之下， CloudTrail 控制台中的事件历史记录和aws cloudtrail lookup-events命令将显示这些事件的发生 AWS 区域 地点。

对于大多数服务，事件被记录在发生操作的区域。对于诸如 AWS Identity and Access Management (IAM) 和 Amazon 之类的全球服务 CloudFront，事件会发送到包含全球服务的任何跟踪。 AWS STS

对于大多数全球服务，事件记录为发生在美国东部（弗吉尼亚州北部）区域，但有些全球服务事件记录为发生在其他区域，例如美国东部（俄亥俄州）区域或美国西部（俄勒冈州）区域。

要避免接收重复的全球服务事件，请注意：

- 默认情况下，全局服务事件会传递到使用 CloudTrail 控制台创建的跟踪。事件传输到跟踪的存储桶中。
- 如果您有多个单区域跟踪记录，可考虑将跟踪配置为只在其中一个跟踪记录中传输全球服务事件。有关更多信息，请参阅 启用和禁用全球服务事件记录。
- 如果将跟踪配置从记录所有区域改为只记录单个区域，则会自动为该跟踪关闭全球服务事件日志记录。同理，如果将跟踪配置从记录单个区域改为记录所有区域，则会自动为该跟踪打开全球服务事件日志记录。

  有关更改跟踪的全球服务事件日志记录的更多信息，请参阅 启用和禁用全球服务事件记录。

示例：

1. 您可以在 CloudTrail 控制台中创建跟踪。默认情况下，此跟踪将记录全球服务事件。
2. 您有多个单区域跟踪记录。
3. 您不需要为单区域跟踪记录包含全球服务。全球服务事件会提交给第一个跟踪。有关更多信息，请参阅 使用创建、更新和管理跟踪 AWS CLI。

> **Note**
>
> 使用 AWS CLI、 AWS SDK 或 CloudTrail API 创建或更新跟踪时，您可以指定是包含还是排除跟踪的全局服务事件。您无法从 CloudTrail 控制台配置全局服务事件日志。

CloudTrail 支持的区域

> **Note**
>
> 有关 CloudTrail Lake 支持的区域的信息，请参阅CloudTrail 支持湖泊的区域。
> 有关数据平面端点的信息，请参阅中的数据平面端点AWS 一般参考。

区域名称	区域	控制平面端点	协议	支持日期
美国东部（弗吉尼亚州北部）	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	11/13/2013
美国东部（俄亥俄州）	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	10/17/2016
美国西部（北加利福尼亚）	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	05/13/2014
美国西部（俄勒冈州）	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	11/13/2013

区域名称	区域	控制平面端点	协议	支持日期
非洲（开普敦）	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	2020 年 4 月 22 日
亚太地区（香港）	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	04/24/2019
亚太地区（海得拉巴）	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	11/22/2022
亚太地区（雅加达）	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	12/13/2021
亚太地区（墨尔本）	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	2023 年 1 月 23 日
亚太地区（孟买）	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	06/27/2016
亚太地区（大阪）	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	2018 年 2 月 12 日
亚太地区（首尔）	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	01/06/2016
亚太地区（新加坡）	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	06/30/2014
亚太地区（悉尼）	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	05/13/2014
亚太地区（东京)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	06/30/2014
加拿大（中部）	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	12/08/2016

区域名称	区域	控制平面端点	协议	支持日期
加拿大西部（卡尔加里）	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	2023 年 12 月 20 日
中国（北京）	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	03/01/2014
中国（宁夏）	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	12/11/2017
欧洲地区（法兰克福）	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	10/23/2014
欧洲地区（爱尔兰）	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	05/13/2014
欧洲地区（伦敦）	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	12/13/2016
欧洲地区（米兰）	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	04/27/2020
欧洲地区（巴黎）	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	12/18/2017
欧洲（西班牙）	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	11/16/2022
欧洲地区（斯德哥尔摩）	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	12/11/2018
欧洲（苏黎世）	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022

区域名称	区域	控制平面端点	协议	支持日期
以色列（特拉维夫）	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	07/31/2023
中东（巴林）	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	07/29/2019
中东（阿联酋）	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	08/30/2022
南美洲（圣保罗）	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	06/30/2014
AWS GovCloud（美国东部）	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	11/12/2018
AWS GovCloud（美国西部）	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	08/16/2011

有关 CloudTrail 在中使用的更多信息 AWS GovCloud (US) Regions，请参阅AWS GovCloud (US) 用户指南中的服务终端节点。

有关 CloudTrail 在中国（北京）区域使用的更多信息，请参阅AWS 中的中国终端节点和 ARN。Amazon Web Services 一般参考

CloudTrail 支持的服务和集成

CloudTrail 支持记录许多事件 AWS 服务。您可以在每种受支持的服务的指南中找到该服务的具体信息。有关特定于服务的主题列表，请参阅AWS 的服务主题 CloudTrail。此外，有些还 AWS 服务 可用于分析和处理 CloudTrail 日志中收集的数据。

> **Note**
>
> 要查看每个服务支持的区域列表，请参阅《Amazon Web Services 一般参考》中的 Service endpoints and quotas。

主题

- AWS 与日志的服务集成 CloudTrail
- CloudTrail 与亚马逊集成 EventBridge
- CloudTrail 与集成 AWS Organizations
- AWS 的服务主题 CloudTrail
- CloudTrail 不支持的服务

AWS 与日志的服务集成 CloudTrail

> **Note**
>
> 您还可以使用 CloudTrail Lake 来查询和分析您的事件。 CloudTrail 与事件历史记录或运行**LookupEvents**中的简单键和值查找相比，Lake 查询提供了更深入、更可自定义的事件视图。 CloudTrail Lake 用户可以在一个 CloudTrail 事件中跨多个字段运行复杂的标准查询语言 (SQL) 查询。有关更多信息，请参阅 与 L AWS CloudTrail ake 合作 和 将追踪事件复制到 CloudTrail湖中。
> CloudTrail 湖泊事件数据存储和查询会产生 CloudTrail 费用。有关 CloudTrail Lake 定价的更多信息，请参阅AWS CloudTrail 定价。

您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅以下主题。

AWS 服务	主题	描述
Amazon Athena	查询 AWS CloudTrail 日志	将 Athena CloudTrail 与日志配合使用是增强服务活动分析 AWS 的有力方法。例如，您可以使用查询来确定趋势，并根

AWS 服务	主题	描述
		据属性（如源 IP 地址或用户）进一步隔离活动。 您可以直接从 CloudTrail 控制台自动创建用于查询日志的表，并使用这些表在 Athena 中运行查询。有关更多信息，请参阅 Amazon Athen a 用户 CloudTrail指南中的在控制台中创建 CloudTrail 日志表。 **Note** 在 Amazon Athena 中运行查询会产生额外成本。有关更多信息，请参阅 Amazon Athena 定价。

AWS 服务	主题	描述
Amazon CloudWatch 日志	使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件	您可以配置 CloudWatch 日志 CloudTrail 来监控您的跟踪日志，并在发生特定活动时收到通知。例如，您可以定义 CloudWatch 日志指标过滤器，这些过滤器将在触发 CloudWatch 警报时触发警报并向您发送通知。 **Note** Amazon CloudWatch 和 Amazon CloudWatch Logs 的标准定价适用。有关更多信息，请参阅 Amazon CloudWatch 定价。

CloudTrail 与亚马逊集成 EventBridge

Amazon EventBridge 是一项提供近乎实时的系统事件流的 AWS 服务，这些事件描述了 AWS 资源的变化。在中 EventBridge，您可以创建响应所记录的事件的规则 CloudTrail。有关更多信息，请参阅在 Amazon 中创建规则 EventBridge。

通过使用 EventBridge 控制台创建规则，您可以将您在跟踪中订阅的事件发送到 EventBridge 该事件。

在 EventBridge 控制台上：

- 选择要交付 CloudTrail 数据和管理事件的`AWS API Call via CloudTrail`详细信息类型。`eventType` `AwsApiCall`要记录详细类型值为的事件`AWS API Call via CloudTrail`，您必须有一个当前正在记录管理事件或数据事件的跟踪。
- 选择要发送AWS Management Console 登录`AWS Console Sign In via CloudTrail`事件的详细信息类型。要记录详细信息类型为的事件`AWS Console Sign In via CloudTrail`，您必须有一个当前正在记录管理事件的跟踪。

- 选择要发布洞察AWS Insight via CloudTrail事件的详细信息类型。要记录详细类型值为的事件AWS Insight via CloudTrail，您必须有一个当前正在记录 Insights 事件的跟踪。有关记录 Insights 事件的信息，请参阅 记录 Insights 事件。

有关如何创建跟踪的更多信息，请参阅 创建跟踪。

CloudTrail 与集成 AWS Organizations

AWS Organizations 组织的管理账户可以添加委派管理员来管理该组织的 CloudTrail 资源。您可以在管理账户或委托管理员账户中为组织创建组织跟踪或组织事件数据，以收集 AWS Organizations中组织内所有 AWS 账户的所有事件数据。创建组织跟踪可帮助您为组织定义统一的事件记录策略。

组织跟踪会自动应用于组织中的每个 AWS 账户。成员账户中的用户可以看到这些跟踪记录但无法修改它们，并且默认情况下看不到为组织跟踪记录创建的日志文件。有关更多信息，请参阅 为组织创建跟踪。

AWS 的服务主题 CloudTrail

您可以详细了解如何将各个 AWS 服务的事件记录在 CloudTrail 日志中，包括在日志文件中记录该服务的示例事件。有关特定 AWS 服务如何与之集成的更多信息 CloudTrail，请参阅该服务的个人指南中有关集成的主题。

仍处于预览阶段、尚未发布正式上市 (GA) 的服务或没有公共 API 的服务均不被视为受支持。
CloudTrail 目前不记录特定于 Amazon VPC 终端节点策略的事件。

> **Note**
>
> 要查看每个服务支持的区域列表，请参阅《Amazon Web Services 一般参考》中的 Service endpoints and quotas。
> 有关哪些服务记录数据事件的信息，请参阅 数据事件。

AWS 服务	CloudTrail 话题	支持开始时间
Amazon API Gateway	使用记录对 Amazon API Gateway 的 API 管理调用 AWS CloudTrail	07/09/2015

AWS 服务	CloudTrail 话题	支持开始时间
Amazon AppFlow	使用记录亚马逊 AppFlow API 调用 AWS CloudTrail	2020 年 4 月 22 日
亚马逊 AppStream 2.0	使用记录亚马逊 AppStream 2.0 API 调用 AWS CloudTrail	04/25/2019
Amazon Athena	使用记录亚马逊 Athena API 调用 AWS CloudTrail	05/19/2017
Amazon Aurora	监控 Amazon Aurora API 调用 AWS CloudTrail	08/31/2018
Amazon Bedrock	使用记录亚马逊 Bedrock API 调用 AWS CloudTrail	2023 年 10 月 23 日
Amazon Braket	使用 Amazon Braket API 进行登录 CloudTrail	08/12/2020
Amazon Chime	使用记录 Amazon Chime 管理通话 AWS CloudTrail	09/27/2017
Amazon Cloud Directory	使用记录 Cloud Directory API 调用 AWS CloudTrail	01/26/2017
Amazon CloudFront	使用 AWS CloudTrail 捕获发送到 CloudFront API 的请求	05/28/2014
Amazon CloudSearch	使用记录亚马逊 CloudSearch 配置服务调用 AWS CloudTrail	10/16/2014
Amazon CloudWatch	记录亚马逊 CloudWatch API 调用 AWS CloudTrail	04/30/2014
Amazon CloudWatch 日志	记录 Amazon CloudWatch 记录 API 调用 AWS CloudTrail	03/10/2016

AWS 服务	CloudTrail 话题	支持开始时间
Amazon CodeCatalyst	使用在连接中记录 CodeCatalyst API 调 AWS 账户 用 AWS CloudTrail	12/01/2022
Amazon CodeGuru Reviewer	使用记录 Amazon CodeGuru Reviewer API 调用 AWS CloudTrail	12/02/2019
Amazon CodeWhisperer	AWS CloudTrail 和 CodeWhisperer API	04/13/2023
Amazon Cognito	使用记录亚马逊 Cognito API 调用 AWS CloudTrail	02/18/2016
Amazon Comprehend	使用记录亚马逊 Comprehend API 调用 AWS CloudTrail	01/17/2018
Amazon Comprehend Medical	透过使用 AWS CloudTrail记录 Amazon Comprehend Medical API 调用	11/27/2018
Amazon Connect	使用 AWS CloudTrail记录 Amazon Connect API 调用	12/11/2019
Amazon Data Firehose	使用监控亚马逊数据 Firehose API 调用 AWS CloudTrail	03/17/2016
Amazon Data Lifecycle Manager	使用记录亚马逊数据生命周期管理器 API 调用 AWS CloudTrail	07/24/2018
Amazon Detective	使用 AWS CloudTrail记录 Amazon Detective API 调用	03/31/2020
Amazon DevOps Guru	使用记录 Amazon DevOps Guru API 调用 AWS CloudTrail	05/04/2021

AWS 服务	CloudTrail 话题	支持开始时间
Amazon DocumentDB（与 MongoDB 兼容）	使用 AWS CloudTrail记录 Amazon DocumentDB API 调用	01/09/2019
Amazon DynamoDB	使用记录 DynamoDB 操作 AWS CloudTrail	05/28/2015
Amazon EC2	使用记录亚马逊 EC2 API 调用 AWS CloudTrail	11/13/2013
Amazon EC2 Auto Scaling	使用记录 Auto Scaling API 调用 CloudTrail	07/16/2014
Amazon EC2 容量块	记录容量阻止 API 调用 AWS CloudTrail	2023 年 10 月 31 日
Amazon EC2 Image Builder	使用记录 EC2 Image Builder API 调用 CloudTrail	12/02/2019
Amazon Elastic Block Store（Amazon EBS） EBS 直接 API	使用记录 API 调用 AWS CloudTrail 使用 AWS CloudTrail记录 EBS Direct API 的 API 调用	Amazon EBS：11/13/2013 EBS 直接 API：2020 年 6 月 30 日
Amazon Elastic Container Registry (Amazon ECR)	使用记录亚马逊 ECR API 调用 AWS CloudTrail	12/21/2015
Amazon Elastic Container Service (Amazon ECS)	使用记录亚马逊 ECS API 调用 AWS CloudTrail	04/09/2015
Amazon Elastic File System (Amazon EFS)	使用记录亚马逊 EFS API 调用 AWS CloudTrail	06/28/2016
Amazon Elastic Kubernetes Service(Amazon EKS)	使用记录亚马逊 EKS API 调用 AWS CloudTrail	06/05/2018

AWS 服务	CloudTrail 话题	支持开始时间
Amazon Elastic Transcoder	使用记录亚马逊 Elastic Transcoder API 调用 AWS CloudTrail	10/27/2014
Amazon ElastiCache	使用记录亚马逊 ElastiCache API 调用 AWS CloudTrail	09/15/2014
Amazon EMR	登录 Amazon EMR API 调用 AWS CloudTrail	04/04/2014
Amazon EMR on EKS	使用 AWS CloudTrail记录 Amazon EMR on EKS API 调用	12/09/2020
Amazon EventBridge	使用记录亚马逊 EventBridge API 调用 AWS CloudTrail	07/11/2019
Amazon FinSpace	查询 AWS CloudTrail 日志	10/18/2022
Amazon Forecast	使用记录亚马逊 Forecast API 调用 AWS CloudTrail	11/28/2018
Amazon Fraud Detector	使用 AWS CloudTrail记录 Amazon Fraud Detector API 调用	01/09/2020
Amazon FSx for Lustre	使用以下方式记录亚马逊 FSx for Lustre API 调用 AWS CloudTrail	01/11/2019
Amazon FSx for Windows File Server	使用监控 AWS CloudTrail	11/28/2018
Amazon GameLift	使用记录亚马逊 GameLift API 调用 AWS CloudTrail	01/27/2016

AWS 服务	CloudTrail 话题	支持开始时间
Amazon GuardDuty	使用记录亚马逊 GuardDuty API 调用 AWS CloudTrail	2018 年 2 月 12 日
Amazon Inspector	使用记录亚马逊 Inspector API 调用 AWS CloudTrail	11/29/2021
Amazon Inspector Classic	使用记录 Amazon Inspector 经典 API 调用 AWS CloudTrail	04/20/2016
Amazon Inspector 扫描	Amazon Inspector 扫描中的信息 CloudTrail	11/27/2023
Amazon Interactive Video Service	使用 AWS CloudTrail记录 Amazon IVS API 调用	07/15/2020
Amazon Kendra	使用@@ 日志记录亚马逊 Kendra API 调用 AWS CloudTrail并使用日志记录亚马逊 Kendra 智能排名 API 调用 AWS CloudTrail	05/11/2020
Amazon Keyspaces（Apache Cassandra 兼容）	使用 AWS CloudTrail记录 Amazon Keyspaces API 调用	01/13/2020
适用于 Apache Flink 的亚马逊托管服务	记录适用于 Apache 的托管服务 Flink API 调用 AWS CloudTrail	03/22/2019
Amazon Kinesis Data Streams	使用记录亚马逊 Kinesis Data Streams API 调用 AWS CloudTrail	04/25/2014
Amazon Kinesis Video Streams	使用记录 Kinesis Video Streams 的 API 调用 AWS CloudTrail	05/24/2018

AWS 服务	CloudTrail 话题	支持开始时间
Amazon Lex	使用记录 Amazon Lex API 调用 CloudTrail	08/15/2017
Amazon Lightsail	使用记录 Lightsail API 调用 AWS CloudTrail	12/23/2016
Amazon Location Service	使用 AWS CloudTrail进行日志记录和监控	12/15/2020
Amazon Lookout for Equipment	监控亚马逊 Lookout for Equipment	12/01/2020
Amazon Lookout for Metrics	在中查看 Amazon Lookout for Metrics API 活动 AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	使用 AWS CloudTrail记录 Amazon Lookout for Vision 调用	12/01/2020
Amazon Machine Learning	使用记录亚马逊 ML API 调用 AWS CloudTrail	12/10/2015
Amazon Macie	使用 AWS CloudTrail记录 Amazon Macie API 调用	05/13/2020
Amazon Managed Blockchain	使用 AWS CloudTrail记录 Amazon Managed Blockchain API 调用 使用 AWS CloudTrail记录用于 Managed Blockchain 的 Ethereum API 调用（预览版）	04/01/2019
Amazon Managed Grafana	使用 AWS CloudTrail记录 Amazon Managed Grafana API 调用	12/15/2020

AWS 服务	CloudTrail 话题	支持开始时间
Amazon Managed Service for Prometheus	使用 AWS CloudTrail记录 Amazon Managed Service for Prometheus API 调用	12/15/2020
Amazon Managed Streaming for Apache Kafka	使用记录 API 调用 AWS CloudTrail	12/11/2018
Amazon Managed Workflows for Apache Airflow	查看审核日志 AWS CloudTrail	11/24/2020
适用于 Redis 的 Amazon MemoryDB	使用记录适用于 Redis 的 Amazon MemoryDB API 调用 AWS CloudTrail	08/19/2021
Amazon MQ	使用记录亚马逊 MQ API 调用 AWS CloudTrail	07/19/2018
Amazon Neptune	使用记录亚马逊 Neptune API 调用 AWS CloudTrail	05/30/2018
Amazon Nimble Studio	使用记录 Nimble Studio 通话 AWS CloudTrail	06/19/2023
Amazon One Enterprise	使用记录亚马逊 One 企业 API 调用 AWS CloudTrail	11/27/2023
亚马逊 OpenSearch 服务	使用监控亚马逊 OpenSearch 服务 API 调用 AWS CloudTrail	10/01/2015
Amazon Personalize	使用记录亚马逊个性化 API 调用 AWS CloudTrail	11/28/2018
Amazon Pinpoint	使用记录亚马逊 Pinpoint API 调用 AWS CloudTrail	02/06/2018
Amazon Pinpoint SMS and Voice API	使用记录亚马逊 Pinpoint API 调用 AWS CloudTrail	11/16/2018

AWS 服务	CloudTrail 话题	支持开始时间
Amazon Polly	使用记录 Amazon Polly API 调用 AWS CloudTrail	11/30/2016
Amazon Q（商业用途）	使用记录 Amazon Q API 调用 AWS CloudTrail	11/28/2023
Amazon Q（供 AWS 建筑商使用）	使用记录 Amazon Q API 调用 AWS CloudTrail	11/28/2023
Amazon Quantum Ledger Database (Amazon QLDB)	使用 AWS CloudTrail记录 Amazon QLDB API 调用	09/10/2019
Amazon QuickSight	使用记录操作 CloudTrail	04/28/2017
Amazon Relational Database Service (Amazon RDS)	使用记录 Amazon RDS API 调用 AWS CloudTrail	11/13/2013
Amazon RDS 性能详情	使用记录 Amazon RDS API 调用 AWS CloudTrail Amazon RDS Performance Insights API 是 Amazon RDS API 的子集。	06/21/2018
Amazon Redshift	使用记录亚马逊 Redshift API 调用 AWS CloudTrail	06/10/2014
Amazon Rekognition	使用记录亚马逊 Rekognition API 调用 AWS CloudTrail	04/6/2018
Amazon Route 53	使用 AWS CloudTrail 捕获已发送到 Route 53 API 的请求	02/11/2015
Amazon Route 53 应用程序恢复控制器	使用记录 Amazon Route 53 应用程序恢复控制器 API 调用 AWS CloudTrail	07/27/2021

AWS 服务	CloudTrail 话题	支持开始时间
Amazon S3	使用记录亚马逊 S3 API 调用 AWS CloudTrail	管理事件：09/01/2015 数据事件：11/21/2016
Amazon S3 Glacier	使用记录 S3 Glacier API 调用 AWS CloudTrail	12/11/2014
Amazon SageMaker	使用记录亚马逊 SageMaker API 调用 AWS CloudTrail	01/11/2018
Amazon Security Lake	使用记录亚马逊安全湖 API 调用 CloudTrail	05/30/2023
Amazon Simple Email Service（Amazon SES）	使用记录亚马逊 SES API 调用 AWS CloudTrail	05/07/2015
Amazon Simple Notification Service (Amazon SNS)	使用记录亚马逊 SNS API 调用 AWS CloudTrail	10/09/2014
Amazon Simple Queue Service(Amazon SQS)	使用记录亚马逊 SQS API 操作 AWS CloudTrail	07/16/2014
Amazon Simple Workflow Service (Amazon SWF)	使用录制 API 调用 AWS CloudTrail	管理层活动：2014 年 5 月 13 日 数据事件：2024 年 2 月 14 日
Amazon Textract	使用记录亚马逊 Textract API 调用 AWS CloudTrail	05/29/2019
Amazon Timestream	使用记录时间流 API 调用 AWS CloudTrail	09/30/2020
Amazon Transcribe	使用记录 Amazon Transcribe API 调用 AWS CloudTrail	06/28/2018
Amazon Translate	使用 AWS CloudTrail记录 Amazon Translate API 调用	04/04/2018

AWS 服务	CloudTrail 话题	支持开始时间
Amazon Verified Permissions	使用记录亚马逊已验证的权限 API 调用 AWS CloudTrail	06/13/2023
Amazon Virtual Private Cloud (Amazon VPC)	使用记录 API 调用 AWS CloudTrail Amazon VPC API 是 Amazon EC2 API 的子集。	11/13/2013
Amazon VPC Lattice	CloudTrail 日志	03/31/2023
Amazon VPC Reachability Analyzer	使用记录 Reachability Analyzer API 调用 AWS CloudTrail	11/27/2023
Amazon WorkDocs	使用记录亚马逊 WorkDocs API 调用 AWS CloudTrail	08/27/2014
Amazon WorkMail	使用记录亚马逊 WorkMail API 调用 AWS CloudTrail	12/12/2017
Amazon WorkSpaces	使用记录亚马逊 WorkSpaces API 调用 CloudTrail	04/09/2015
Amazon WorkSpaces 瘦客户机	使用记录亚马逊 WorkSpaces 瘦客户端 API 调用 AWS CloudTrail	11/26/2023
Amazon WorkSpaces Web	使用记录亚马逊 WorkSpaces Web API 调用 AWS CloudTrail	11/30/2021
Application Auto Scaling	使用记录应用程序 Auto Scaling API 调用 AWS CloudTrail	10/31/2016
AWS Amplify	使用 AWS CloudTrail记录 Amplify API 调用	11/30/2020

AWS 服务	CloudTrail 话题	支持开始时间
AWS App Mesh	使用 AWS CloudTrail记录 App Mesh API 调用	AWS App Mesh 2019 年 10 月 30 日 App Mesh Envoy 管理服务 03/18/2022
AWS App Runner	使用记录 App Runner API 调用 AWS CloudTrail	05/18/2021
AWS AppConfig	使用记录 AWS AppConfig API 调用 AWS CloudTrail	管理层活动：2020 年 7 月 31 日 数据事件：2024 年 4 月 1 日
AWS AppFabric	使用记录 AWS AppFabric API 调用 AWS CloudTrail	06/27/2023
AWS 应用程序成本分析器	AWS 应用程序成本分析器 API 参考	05/13/2021
AWS Application Discovery Service	使用 AWS CloudTrail记录 Application Discovery Service API 调用	05/12/2016
AWS 应用程序转换服务	（ AWS 工具使用的后端服务，例如适用于.NET 的 AWS 微服务提取器）	08/26/2023
AWS AppSync	使用记录 AWS AppSync API 调用 AWS CloudTrail	02/13/2018
AWS Artifact	使用记录 AWS Artifact API 调用 AWS CloudTrail	01/27/2023
AWS Audit Manager	使用记录 AWS Audit Manager API 调用 AWS CloudTrail	12/07/2020

AWS 服务	CloudTrail 话题	支持开始时间
AWS Auto Scaling	使用记录 AWS Auto Scaling API 调用 CloudTrail	08/15/2018
AWS B2B 数据交换	使用记录 AWS B2B 数据交换 API 调用 AWS CloudTrail	12/01/2023
AWS Backup	使用记录 AWS Backup API 调用 AWS CloudTrail	02/04/2019
AWS Batch	使用记录 AWS Batch API 调用 AWS CloudTrail	1/10/2018
AWS Billing and Cost Management	使用记录 AWS Billing and Cost Management API 调用 AWS CloudTrail	06/07/2018
AWS Billing Conductor	使用记录 AWS Billing Conductor API 调用 AWS CloudTrail	03/12/2024
AWS BugBust	使用记录 BugBust API 调用 CloudTrail	06/24/2021
AWS Certificate Manager	使用 AWS CloudTrail	03/25/2016
AWS Clean Rooms	使用记录 AWS Clean Rooms API 调用 AWS CloudTrail	03/21/2023
AWS Cloud Map	使用记录 AWS Cloud Map API 调用 AWS CloudTrail	11/28/2018
AWS Cloud9	使用记录 AWS Cloud9 API 调用 AWS CloudTrail	01/21/2019
AWS CloudFormation	记录 AWS CloudFormation API 调用 AWS CloudTrail	04/02/2014

AWS 服务	CloudTrail 话题	支持开始时间
AWS CloudHSM	使用记录 AWS CloudHSM API 调用 AWS CloudTrail	01/08/2015
AWS CloudShell	登录和监控 AWS CloudShell	12/15/2020
AWS CloudTrail	AWS CloudTrail API 参考（所有 CloudTrail API 调用均由记录 CloudTrail。）	11/13/2013
AWS CodeArtifact	使用记录 CodeArtifact API 调用 AWS CloudTrail	06/10/2020
AWS CodeBuild	使用记录 AWS CodeBuild API 调用 AWS CloudTrail	12/01/2016
AWS CodeCommit	使用记录 AWS CodeCommit API 调用 AWS CloudTrail	01/11/2017
AWS CodeDeploy	使用监控部署 AWS CloudTrail	2014/12/16
AWS CodePipeline	使用记录 CodePipeline API 调用 AWS CloudTrail	07/09/2015
AWS CodeStar	使用记录 AWS CodeStar API 调用 AWS CloudTrail	06/14/2017
AWS CodeStar 通知	使用记录 AWS CodeStar 通知 API 调用 AWS CloudTrail	11/05/2019
AWS Config	通过以下方式记录 AWS Config API 调用 AWS CloudTrail	02/10/2015
AWS 控制目录	使用日志 AWS 控制目录 API 调用 AWS CloudTrail	04/08/2024
AWS Control Tower	使用记录 AWS Control Tower 操作 AWS CloudTrail	08/12/2019

AWS 服务	CloudTrail 话题	支持开始时间
AWS Data Pipeline	使用记录 AWS Data Pipeline API 调用 AWS CloudTrail	12/02/2014
AWS Database Migration Service (AWS DMS)	使用记录 AWS Database Migration Service API 调用 AWS CloudTrail	02/04/2016
AWS DataSync	使用记录 AWS DataSync API 调用 AWS CloudTrail	11/26/2018
AWS 截止日期云	使用记录通话 CloudTrail	04/02/2024
AWS Device Farm	使用记录 AWS Device Farm API 调用 AWS CloudTrail	07/13/2015
AWS Direct Connect	记录 AWS Direct Connect API 调用 AWS CloudTrail	03/08/2014
AWS Directory Service	使用记录 AWS Directory Service API 调用 CloudTrail	05/14/2015
AWS Elastic Beanstalk（Elastic Beanstalk）	将 Elastic Beanstalk API 调用与 AWS CloudTrail	03/31/2014
AWS Elastic Disaster Recovery	使用记录 AWS Elastic Disaster Recovery API 调用 AWS CloudTrail	11/17/2021
AWS Elemental MediaConnect	使用记录 AWS Elemental MediaConnect API 调用 AWS CloudTrail	11/27/2018
AWS Elemental MediaConvert	使用记录 AWS Elemental MediaConvert API 调用 CloudTrail	11/27/2017

AWS 服务	CloudTrail 话题	支持开始时间
AWS Elemental MediaLive	使用记录 MediaLive API 调用 AWS CloudTrail	01/19/2019
AWS Elemental MediaPackage	使用记录 AWS Elemental MediaPackage API 调用 AWS CloudTrail	12/21/2018
AWS Elemental MediaStore	使用记录 AWS Elemental MediaStore API 调用 CloudTrail	11/27/2017
AWS Elemental MediaTailor	使用记录 AWS Elemental MediaTailor API 调用 AWS CloudTrail	02/11/2019
AWS 实体分辨率	使用 A 记录 AWS 实体解析 API 调用AWS CloudTrail	07/26/2023
AWS Fault Injection Service	使用记录 API 调用 AWS CloudTrail	03/15/2021
AWS Firewall Manager	使用记录 AWS Firewall Manager API 调用 AWS CloudTrail	04/05/2018
AWS Global Accelerator	使用记录 AWS 全球加速器 API 调用 AWS CloudTrail	11/26/2018
AWS Glue	使用记录 AWS Glue 操作 AWS CloudTrail	11/07/2017
AWS Ground Station	使用记录 AWS Ground Station API 调用 AWS CloudTrail	05/31/2019
AWS Health	使用记录 AWS Health API 调用 AWS CloudTrail	11/21/2016

AWS 服务	CloudTrail 话题	支持开始时间
AWS Health Dashboard	使用记录 AWS Health API 调用 AWS CloudTrail	12/01/2016
AWS HealthImaging	使用记录 AWS HealthImaging API 调用 AWS CloudTrail	07/26/2023
AWS HealthLake	使用记录 AWS HealthLake API 调用 AWS CloudTrail	12/07/2020
AWS HealthOmics	使用记录 AWS HealthOmics API 调用 AWS CloudTrail	11/29/2022
AWS IAM Identity Center	使用记录 IAM 身份中心 API 调用 AWS CloudTrail	12/07/2017
AWS Identity and Access Management (IAM)	使用记录 IAM 事件 AWS CloudTrail	11/13/2013
AWS IoT	使用记录 AWS IoT API 调用 AWS CloudTrail	04/11/2016
AWS IoT 1-Click	使用记录 AWS IoT 1-Click API 调用 AWS CloudTrail	05/14/2018
AWS IoT 分析	使用记录 AWS IoT 分析 API 调用 AWS CloudTrail	04/23/2018
AWS IoT 活动	使用记录 AWS IoT 事件 API 调用 AWS CloudTrail	06/11/2019
AWS IoT Greengrass	使用记录 AWS IoT Greengrass API 调用 AWS CloudTrail	10/29/2018
AWS IoT Greengrass V2	使用记录 AWS IoT Greengrass V2 API 调用 AWS CloudTrail	12/14/2020
AWS IoT SiteWise	使用记录 AWS IoT SiteWise API 调用 AWS CloudTrail	04/29/2020

AWS 服务	CloudTrail 话题	支持开始时间
AWS Key Management Service (AWS KMS)	使用记录 AWS KMS API 调用 AWS CloudTrail	11/12/2014
AWS Lake Formation	使用记录 AWS Lake Formation API 调用 AWS CloudTrail	08/09/2019
AWS Lambda	使用记录 AWS Lambda API 调用 AWS CloudTrail	管理事件：04/09/2015 数据事件：11/30/2017
AWS Launch Wizard	使用记录 AWS Launch Wizard API 调用 AWS CloudTrail	11/08/2023
AWS License Manager	AWS 使用记录 License Manager API 调用 AWS CloudTrail	03/01/2019
AWS Mainframe Modernization	使用记录 AWS Mainframe Modernization API 调用 AWS CloudTrail	06/08/2022
AWS Managed Services	AMS Accelerate 中的日志管理	12/21/2016
AWS Marketplace 协议	使用记录协议 API 调用 AWS CloudTrail	09/01/2023
AWS Marketplace 部署服务	使用记录 AWS Marketplace 部署服务调用 CloudTrail	11/29/2023
AWS Marketplace 发现	使用记录 AWS Marketplace 发现 API 调用 AWS CloudTrail	2022 年 12 月 15 日
AWS Marketplace 计量服务	使用记录 AWS Marketplace API 调用 AWS CloudTrail	08/22/2018
AWS Migration Hub	使用记录 M AWS igration Hub API 调用 AWS CloudTrail	08/14/2017

AWS 服务	CloudTrail 话题	支持开始时间
AWS Network Firewall	使用记录对 AWS Network Firewall API 的调用 AWS CloudTrail	11/17/2020
AWS OpsWorks for Chef Automate	使用记录 AWS OpsWorks for Chef Automate API 调用 AWS CloudTrail	07/16/2018
AWS OpsWorks for Puppet Enterprise	使用登录 OpsWorks Puppet 企业 API 调用 AWS CloudTrail	07/16/2018
AWS OpsWorks Stacks	使用记录 AWS OpsWorks Stacks API 调用 AWS CloudTrail	06/04/2014
AWS Organizations	使用记录 AWS Organizations API 调用 AWS CloudTrail	02/27/2017
AWS Outposts	使用记录 AWS Outposts API 调用 AWS CloudTrail	02/04/2020
AWS Panorama	AWS Panorama API Reference	10/20/2021
AWS Payment Cryptography	使用记录 AWS Payment Cryptography API 调用 AWS CloudTrail	06/08/2023
AWS 专用 5G	使用记录 AWS 私有 5G API 调用 AWS CloudTrail	08/11/2022
AWS Private Certificate Authority (AWS Private CA)	使用 CloudTrail	04/04/2018
AWS Proton	登录和监控 AWS Proton	06/09/2021

AWS 服务	CloudTrail 话题	支持开始时间
AWS re:Post 私人	使用记录 AWS re:Post 私有 API 调用 AWS CloudTrail	11/26/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	使用记录 AWS RAM API 调用 AWS CloudTrail	11/20/2018
AWS 资源探索器	使用记录 AWS 资源探索器 API 调用 AWS CloudTrail	11/07/2022
AWS Resource Groups	在 Resource Groups 中记录和监控	06/29/2018
AWS RoboMaker	使用记录 AWS RoboMaker API 调用 AWS CloudTrail	01/16/2019
AWS Secrets Manager	监控您的 AWS Secrets Manager 机密的使用情况	04/05/2018
AWS Security Hub	使用记录 AWS Security Hub API 调用 AWS CloudTrail	11/27/2018
AWS Security Token Service (AWS STS)	使用记录 IAM 事件 AWS CloudTrail IAM 主题包含有关的信息 AWS STS。	11/13/2013
AWS Serverless Application Repository	使用记录 AWS Serverless Application Repository API 调用 AWS CloudTrail	02/20/2018
AWS Service Catalog	使用记录 Service Catalog API 调用 AWS CloudTrail	07/06/2016
AWS Shield	使用记录 Shield 高级 API 调用 AWS CloudTrail	02/08/2018

AWS 服务	CloudTrail 话题	支持开始时间
AWS Snowball 边缘	使用记录 AWS Snowball 边缘 API 调用 AWS CloudTrail	01/25/2019
AWS Step Functions	使用记录 AWS Step Functions API 调用 AWS CloudTrail	12/01/2016
AWS Storage Gateway	使用记录 Storage Gateway API 调用 AWS CloudTrail	2014/12/16
AWS Support	使用记录 AWS Support API 调用 AWS CloudTrail	04/21/2016
AWS Support 推荐（预览）	使用记录 AWS Support 推荐 API 调用 AWS CloudTrail	05/22/2024
AWS Systems Manager	使用记录 AWS Systems Manager API 调用 AWS CloudTrail	11/29/2017
AWS Systems Manager Incident Manager	使用记录 AWS Systems Manager 事件管理器 API 调用 AWS CloudTrail	05/10/2021
AWS 电信网络生成器 (AWS TNB)	使用记录 AWS 电信网络生成器 API 调用 AWS CloudTrail	02/21/2023
AWS Transfer for SFTP	使用记录 AWS Transfer for SFTP API 调用 AWS CloudTrail	01/08/2019
AWS Transit Gateway	使用 AWS CloudTrail记录 Transit Gateway 的 API 调用	11/26/2018
AWS Trusted Advisor	使用记录 AWS Trusted Advisor 控制台操作 AWS CloudTrail	10/22/2020

AWS 服务	CloudTrail 话题	支持开始时间
AWS Verified Access	使用记录 AWS Verified Access API 调用 AWS CloudTrail	04/27/2023
AWS WAF	使用记录 AWS WAF API 调用 AWS CloudTrail	04/28/2016
AWS Well-Architected Tool	使用记录 AWS Well-Architected Tool API 调用 AWS CloudTrail	12/15/2020
AWS X-Ray	使用记录 AWS X-Ray API 调用 CloudTrail	04/25/2018
Elastic Load Balancing	AWS CloudTrail 登录 Classic 负载均衡器并AWS CloudTrail 记录应用程序负载均衡器	04/04/2014
FreeRTOS 无线更新 (OTA)	使用记录 AWS IoT OTA API 调用 AWS CloudTrail	05/22/2019
服务限额	使用记录 Service Quotas API 调用 AWS CloudTrail	06/24/2019

CloudTrail 不支持的服务

仍处于预览阶段、尚未发布公开发行（GA）或没有公共 API 的服务均不被视为受支持。

此外，不支持以下 AWS 服务和事件：

- AWS Import/Export
- Amazon VPC 端点策略特定事件

有关支持的 AWS 服务的列表，请参阅AWS 的服务主题 CloudTrail。

中的配额 AWS CloudTrail

下表描述了其中的配额（以前称为限制） CloudTrail。 CloudTrail 没有可调整的配额。有关中其他配额的信息 AWS，请参阅AWS 服务配额。

资源	默认限额	注释
每区域的跟踪数	5	无法提高此配额。
获取、描述并列出 API	每秒 10 个事务 (TPS)	在不受限制的情况下，每秒可发出的操作请求的最大数目。CancelQuery 、、LookupEvents ListInsightsMetricData PutAuditEvents 、和 StartQuery API 不包含在此类别中。
CancelQuery， StartQuery API	每秒 3 个事务 (TPS)	在不受限制的情况下，每秒可发出的操作请求的最大数目。 无法提高此配额。
LookupEvents API	每秒 2 个事务 (TPS)。	在不受限制的情况下，每秒可发出的操作请求的最大数目。 无法提高此配额。
ListInsightsMetricData API	每秒 1 个事务 (TPS)	在不受限制的情况下，每秒可发出的操作请求的最大数目。 无法提高此配额。
PutAuditEvents API	每秒 100 个事务 (TPS)	在不受限制的情况下，每秒可发出的操作请求的最大数目。 无法提高此配额。

资源	默认限额	注释
所有其他 API	每秒 1 个事务 (TPS)	在不受限制的情况下，每秒可发出的操作请求的最大数目。 无法提高此配额。
事件数据存储	10	您可以在任何单个 AWS 区域中拥有的最大事件数据存储数量。这包括该区域的单区域事件数据存储以及所有 AWS 区域区域中的任何多区域事件数据存储。这包括任何生命周期阶段的事件数据存储。 无法提高此配额。
渠道	25	此配额适用于用于与 CloudTrail Lake 以外的事件源集成的频道 AWS，不适用于与服务相关的频道。 无法提高此配额。
并发查询	10	您可以在 La CloudTrail ke 中同时运行的已排队或正在运行的最大查询数。 无法提高此配额。
每个 PutAuditEvents 请求的事件	100	每个 `PutAuditEvents` 请求最多可以添加 100 个活动事件（或最多 1MB）。 无法提高此配额。
事件选择器	每个跟踪 5 个	无法提高此配额。

资源	默认限额	注释
高级事件选择器	跨所有高级事件选择器的 500 个条件	如果跟踪或事件数据存储使用高级事件选择器，则所有高级事件选择器中允许的所有条件的总数最多为 500。除非跟踪或事件数据存储记录所有资源（如所有 S3 存储桶或所有 Lambda 函数）上的数据事件，否则您将被限制为 250 个数据资源。数据资源可以在事件选择器之间分配，但总数不能超过 250 个。 无法提高此配额。

资源	默认限额	注释
事件选择器中的数据资源	一个跟踪中的所有事件选择器中共 250 个	如果您选择使用事件选择器或高级事件选择器限制数据事件，则跟踪中所有事件选择器的数据资源总数不能超过 250。单个事件选择器上的资源的数量限制可配置为最多 250 个。仅当所有事件选择器中的数据资源的总数不超过 250 个时才允许此上限。 示例： • 允许一个跟踪包含 5 个事件选择器，每个选择器配置为包含 50 个数据资源。(5*50=250) • 还允许一个跟踪包含 5 个事件选择器，其中 3 个选择器配置为包含 50 个数据资源，1 个选择器配置为包含 99 个数据资源，剩余的 1 个选择器配置为包含 1 个数据资源。((3*50)+1+99=250) • 不允许一个跟踪配置为包含 5 个事件选择器，所有选择器均配置为包含 100 个数据资源。(5*100=500) 事件选择器仅适用于跟踪。对于事件数据存储，您必须使用高级事件选择器。 无法提高此配额。

资源	默认限额	注释
		如果选择在所有资源（例如，所有 S3 存储桶或所有 Lambda 函数）上记录数据事件，则不适用此限额。
事件大小	所有事件版本：不能将超过 256 KB 的事件发送到 CloudWatch 日志 事件版本 1.05 及更高版本：事件总大小限制为 256 KB	Amaz CloudWatch on Logs 和 Amazon EventBridge 各允许的最大事件大小为 256 KB。CloudTrail 不会向 CloudWatch 日志发送超过 256 KB 的事件或 EventBridge。 从事件版本 1.05 开始，事件的大小最大值为 256 KB。这是为了帮助防止恶意行为者利用这些漏洞，并允许其他 AWS 服务（例如 L CloudWatch ogs 和）使用事件 EventBridge。
CloudTrail 发送到 Amazon S3 的文件大小	50MB ZIP 文件，压缩后	对于管理事件和数据事件，CloudTrail 将事件以最多 50 MB（压缩）的 ZIP 文件形式发送到 S3。 如果在跟踪中启用，则在 CloudTrail 将 ZIP 文件发送到 S3 之后，Amazon SNS 会发送日志传输通知。

AWS CloudTrail 教程入门

如果您不熟悉 AWS CloudTrail，这些教程可以帮助您学习如何使用其功能。

主题

- 授予使用权限 CloudTrail
- 查看事件历史记录
- 创建记录管理事件的跟踪
- 为 S3 数据事件创建事件数据存储
- 将跟踪事件复制到 CloudTrail Lake 事件数据存储中
- 查看 CloudTrail 湖泊仪表板
- 查看和运行 CloudTrail Lake 示例查询
- 将 CloudTrail Lake 查询结果保存到 S3 存储桶中

授予使用权限 CloudTrail

要创建、更新和管理跟踪、事件数据存储和频道等 CloudTrail 资源，您需要授予使用权限 CloudTrail。本节提供有关可用的托管策略的信息 CloudTrail。

> **Note**
>
> 您授予用户执行 CloudTrail 管理任务的权限与将日志文件传输到 Amazon S3 存储桶或向 Amazon SNS 主题发送通知 CloudTrail 所需的权限不同。有关这些权限的更多信息，请参阅适用于 Amazon S3 存储桶的政策 CloudTrail。
>
> 如果您配置与 Amazon CloudWatch Logs 的集成，则 CloudTrail 还需要一个可以代入的角色来向 Amazon Lo CloudWatch gs 日志组传送事件。您必须创建 CloudTrail 使用的角色。有关更多信息，请参阅 授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限 和 将事件发送到 CloudWatch 日志。

以下 AWS 托管策略可用于 CloudTrail：

- AWSCloudTrail_FullAccess— 此政策提供对 CloudTrail 资源 CloudTrail 操作的完全访问权限，例如跟踪、事件数据存储和频道。此策略提供创建、更新和删除 CloudTrail跟踪、事件数据存储和频道所需的权限。

该策略还提供管理 Amazon S3 存储桶、日志日志组和 CloudWatch 跟踪的 Amazon SNS 主题的权限。但是，AWSCloudTrail_FullAccess托管策略不提供删除 Amazon S3 存储桶、日志组或 Amazon SNS 主题的权限。 CloudWatch 有关其他 AWS 服务的托管策略的信息，请参阅《AWS 托管策略参考指南》。

> **Note**
>
> 本AWSCloudTrail_FullAccess政策不打算在您之间广泛共享 AWS 账户。拥有此角色的用户能够关闭或重新配置他们的 AWS 账户账户中最敏感且最重要的审计功能。因此，您只能将此策略应用于账户管理员。您必须严格控制和监控此策略的使用。

- AWSCloudTrail_ReadOnlyAccess— 此策略授予查看 CloudTrail 控制台的权限，包括最近的事件和事件历史记录。此策略还支持查看现有跟踪、事件数据存储和通道。拥有此策略的角色和用户可以下载事件历史记录，但他们无法创建或更新跟踪、事件数据存储或通道。

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

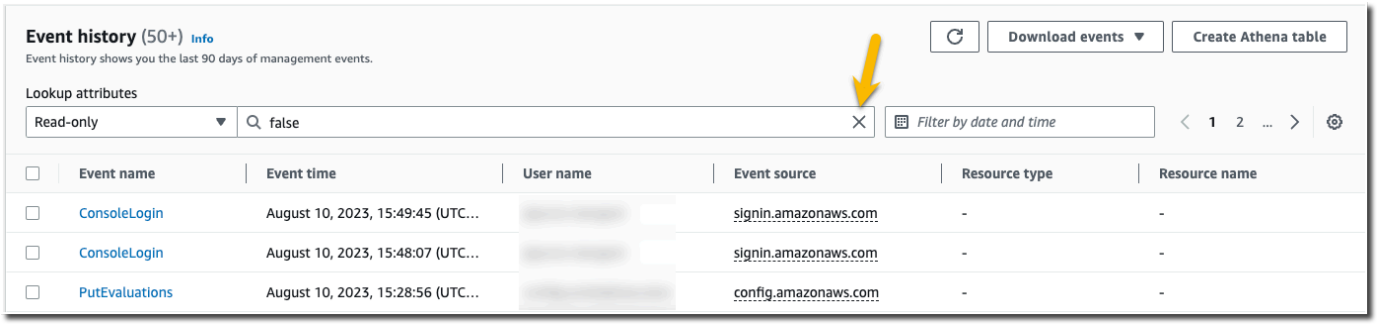
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

查看事件历史记录

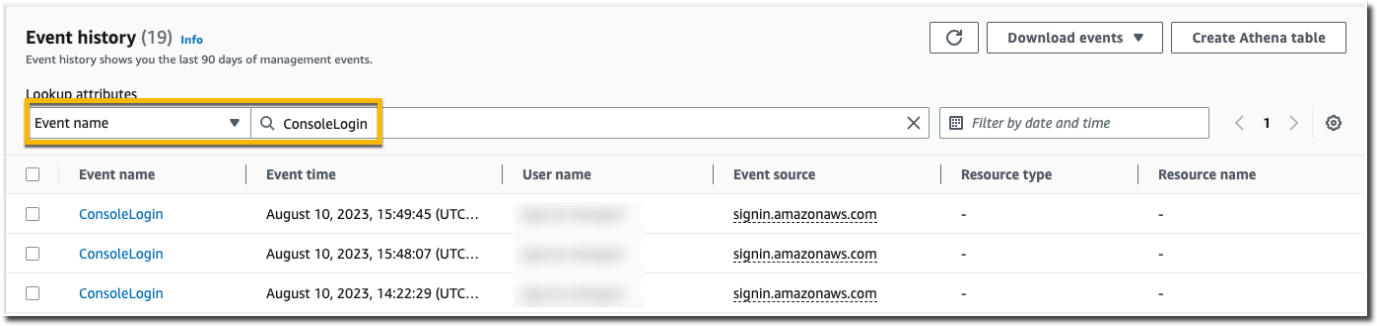
本节介绍如何使用 CloudTrail 控制台上的 CloudTrail 事件历史记录页面查看您 AWS 账户 当前最近 90 天的管理事件 AWS 区域。

查看活动历史记录

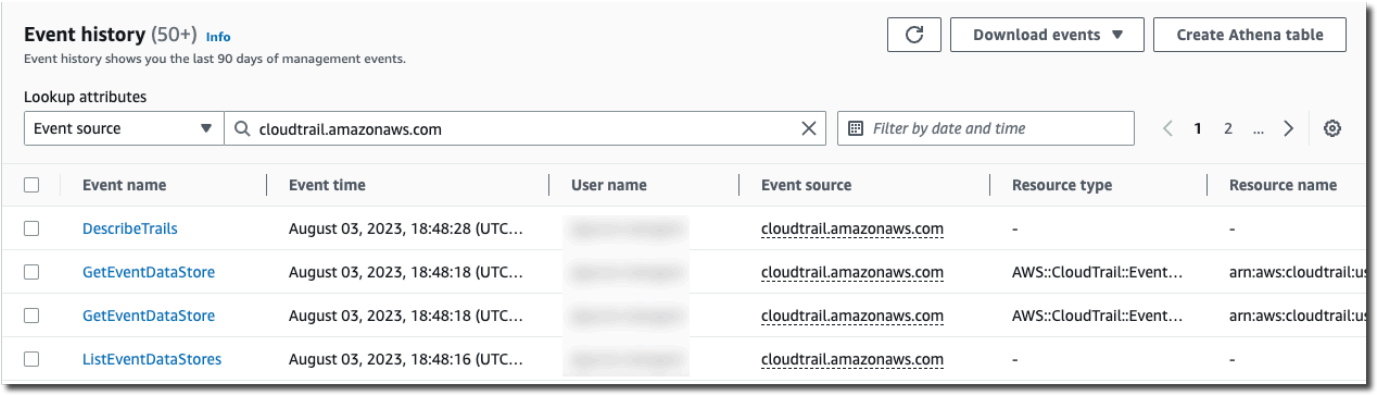
1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择事件历史记录。您会看到一个筛选的事件列表，最新的事件显示在最前面。事件的默认筛选条件是只读的，设置为 false。您可以选择筛选条件右上角的 X 以清除该筛选条件。您可以针对单个属性筛选事件，以搜索事件历史记录中的事件。



3. 选择要筛选的属性，然后输入该属性的完整值。 CloudTrail 无法筛选部分值。例如，要查看所有控制台登录事件，请选择事件名称过滤器，然后指定ConsoleLogin属性值。



或者，要查看最近的 CloudTrail 管理事件，请选择事件源并指定`cloudtrail.amazonaws.com`。



4. 要查看特定管理事件，请选择事件名称。在事件详细信息页面上，您可以查看事件详细信息、任何引用的资源以及事件记录。
5. 比较事件时，可以通过填充 Event history（事件历史记录）表左侧边缘的复选框选择最多五个事件。您可以在比较事件详细信息表 side-by-side 中查看所选事件的详细信息。
6. 您可以采用 CSV 或 JSON 格式的文件进行下载来保存事件历史记录。下载事件历史记录可能需要几分钟。

有关更多信息，请参阅 处理 CloudTrail 事件历史记录。

创建记录管理事件的跟踪

对于您的第一个跟踪，我们建议您创建一个记录所有 AWS 区域的所有管理事件且不记录任何数据事件的跟踪。管理事件的示例包含安全事件（如 IAM `CreateUser` 和 `AttachRolePolicy` 事件）、资源事件（如 `RunInstances` 和 `CreateBucket`），等等。在控制台中创建跟踪的过程中，您将创建一个 Amazon S3 存储桶，用于存储跟踪的 CloudTrail 日志文件。

> **Note**
>
> 本教程假定您创建您的第一个跟踪。根据您 AWS 账户中的跟踪数量以及这些跟踪的配置方式，以下过程可能会产生费用，也可能不会产生费用。 CloudTrail 将日志文件存储在 Amazon S3 存储桶中，这会产生成本。有关定价的更多信息，请参阅 AWS CloudTrail 定价和 Simple Storage Service（Amazon S3）定价。

创建跟踪

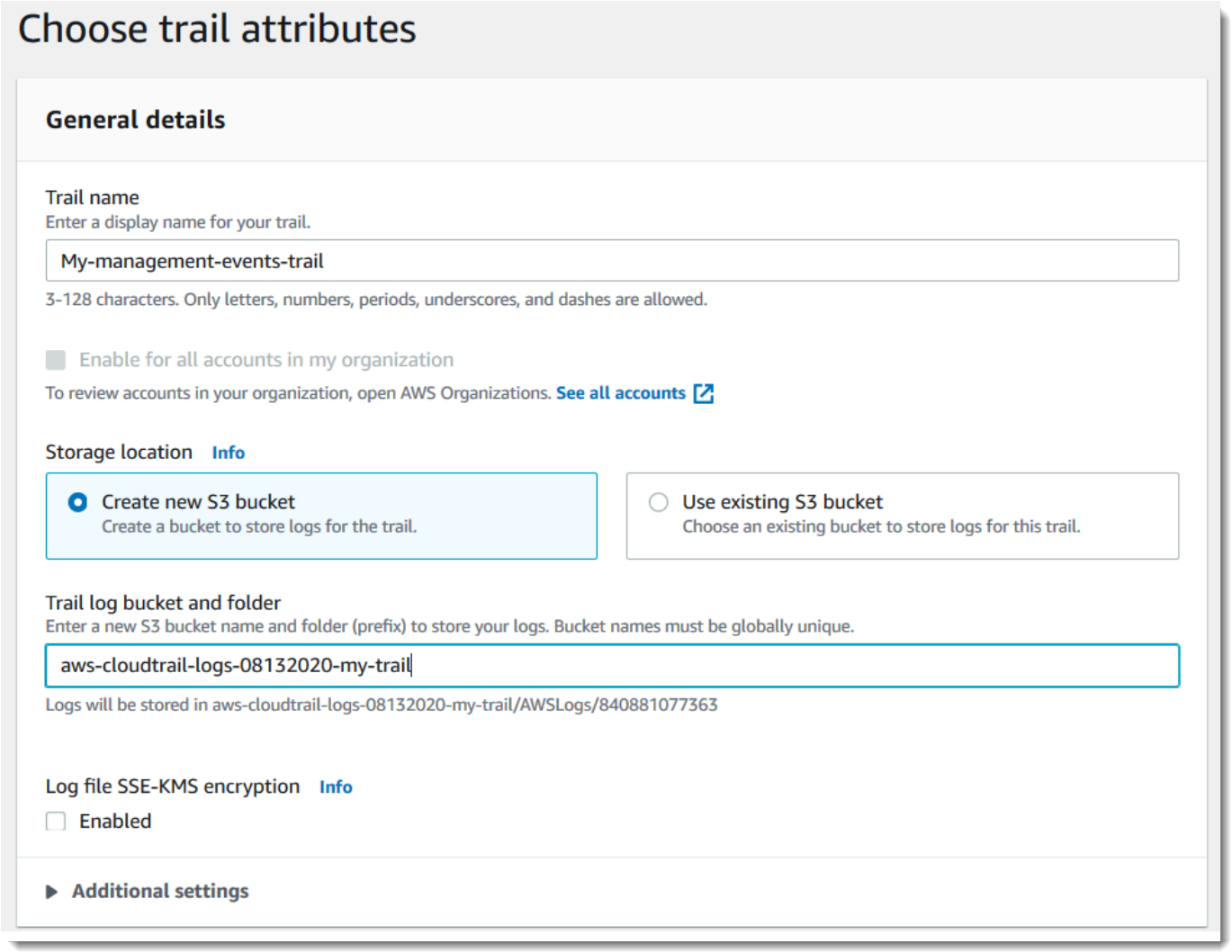
1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在区域选择器中，选择要在其中创建跟踪的 AWS 区域。这是跟踪的主区域。

> **Note**
>
> 即使跟踪记录了所有 AWS 区域的事件，主区域也是您在创建跟踪后可以查看和更新跟踪的唯一 AWS 区域。

3. 在 CloudTrail 服务主页、“跟踪” 页面或 “控制面板” 页面的 “跟踪” 部分，选择 “创建跟踪”。
4. 在 Trail name (跟踪名称) 中，为您的跟踪提供一个名称，如 *My-Management-Events-Trail*。作为最佳实践，请使用可快速识别跟踪用途的名称。在这种情况下，您正在创建的跟踪将记录管理事件。
5. 保留为我的组织中的所有账户启用的默认设置。除非您在 Organizations 中配置了账户，否则此选项将不能进行更改。
6. 对于 Storage location（存储位置，选择 Create new S3 bucket（创建 S3 存储桶）以创建存储桶。创建存储桶时， CloudTrail 会创建并应用所需的存储桶策略。如果您选择创建新的 S3 存储桶，则您的 IAM 策略需要包含`s3:PutEncryptionConfiguration`操作权限，因为默认情况下，该存储桶已启用服务器端加密。为您的存储桶指定一个便于识别的名称。

   为了便于查找日志，请在现有存储桶中创建一个新文件夹（也称为前缀）来存储 CloudTrail 日志。

   > **Note**
   >
   > Simple Storage Service（Amazon S3）存储桶的名称必须是全局唯一的。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶命名规则。

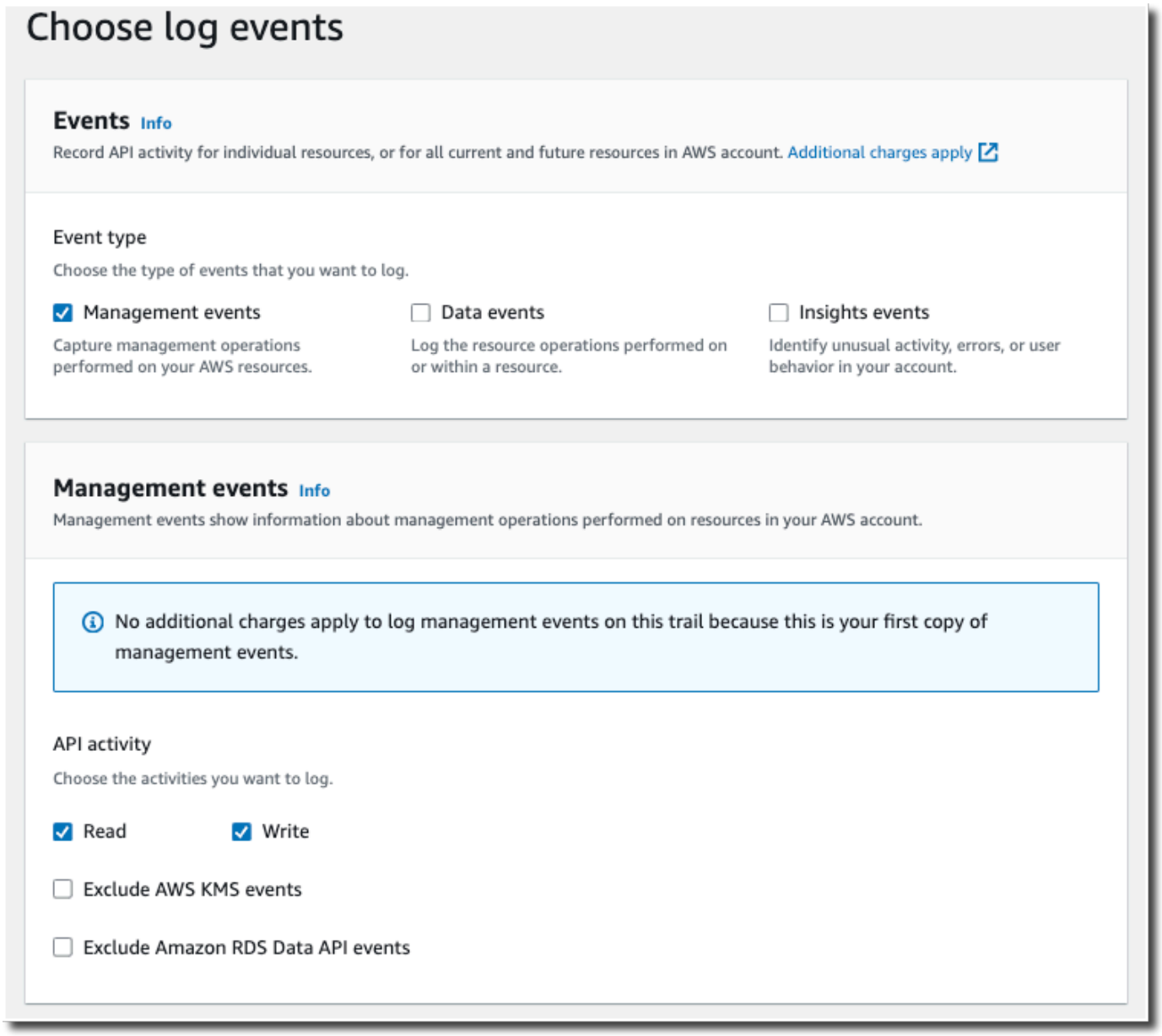


7. 清除此复选框可禁用 Log file SSE-KMS encryption（日志文件 SSE-KMS 加密）。默认情况下，您将使用 SSE-S3 加密法加密日志文件。有关此设置的更多信息，请参阅对 Amazon S3 托管密钥使用服务器端加密 (SSE-S3)。
8. 在 Additional settings（其他设置）中保留默认设置。
9. 保留CloudWatch 日志的默认设置。目前，不要向 Amazon Logs 发送 CloudWatch 日志。
10. （可选）在标签中，将一个或多个自定义标签（键值对）添加到跟踪中。标签可以帮助您识别您的 CloudTrail 跟踪和其他资源，例如包含 CloudTrail 日志文件的 Amazon S3 存储桶。例如，您可以附加名称为 **`Compliance`**、值为 **`Auditing`** 的标签。

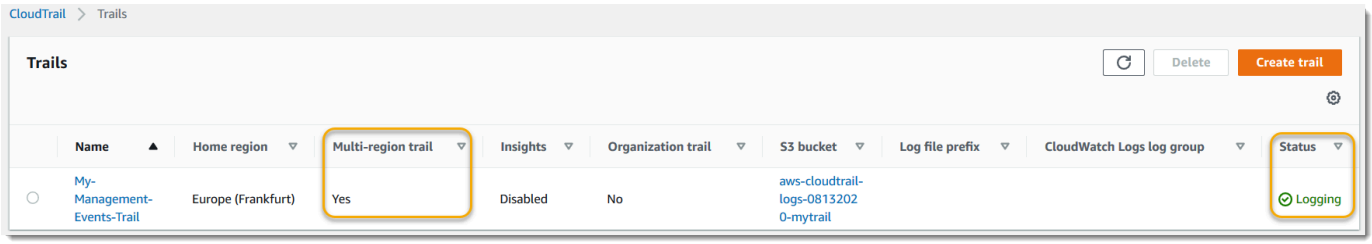
> **Note**
>
> 尽管您可以在 CloudTrail 控制台中创建跟踪时向其添加标签，也可以创建 Amazon S3 存储桶在控制台中存储日志文件，但您无法从 CloudTrail 控制台向 Amazon S3 存储桶添加标签。 CloudTrail 有关查看和更改 Simple Storage Service（Amazon S3）存储桶属性（包括向存储桶添加标签）的更多信息，请参阅 Simple Storage Service（Amazon S3）用户指南。

完成标签创建后，选择 Next（下一步）。

11. 在 Choose log events（选择日志事件）页面中，选择要记录的事件类型。对于此跟踪，请保留默认值 Management events（管理事件）。在 Management events（管理事件）区域中，如果尚未选择，则选择以记录 Read（读取）和 Write（写入）两类事件。将排除 AWS KMS 事件和排除 Amazon RDS 数据 API 事件复选框留空，以记录所有管理事件。



12. 保留数据事件和 Insights 事件的默认设置。此跟踪不会记录任何数据或 CloudTrail Insights 事件。选择下一步。
13. 在 Review and create（审核和创建）页面上，审核您为跟踪选择的设置。对相关部分选择 Edit（编辑）以返回并进行更改。在准备好创建跟踪时，选择 Create trail（创建跟踪）。
14. Trails（跟踪）页面会在表中显示您的新跟踪记录。请注意，跟踪设置为 Multi-region trail（多区域跟踪），并且默认情况下为跟踪打开了日志记录。



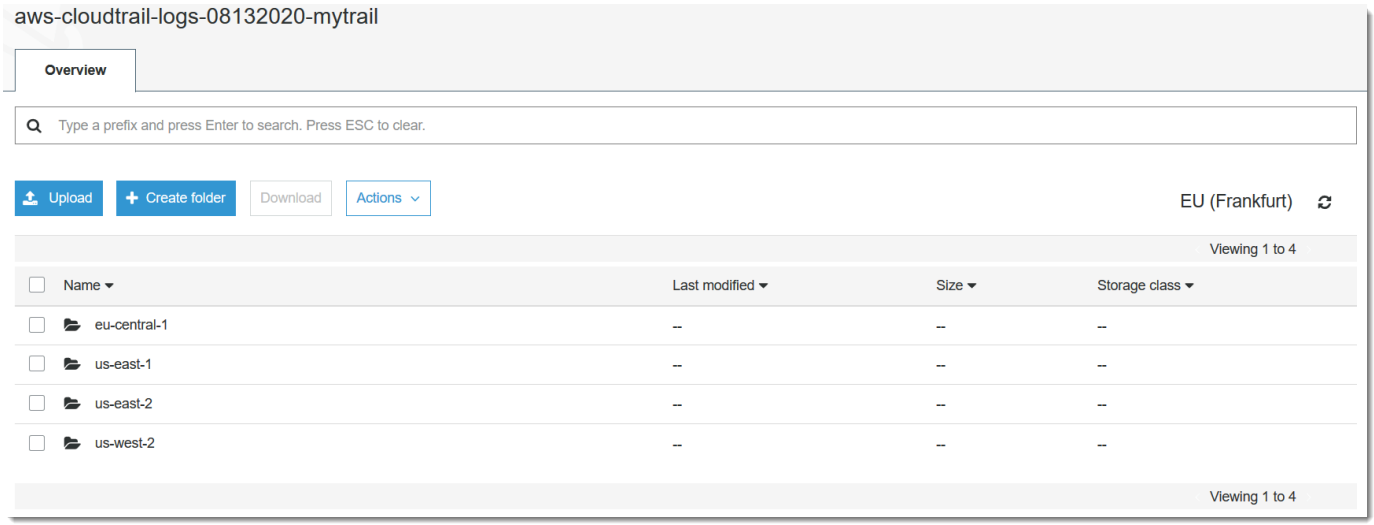
查看您的日志文件

在创建第一个跟踪后的平均大约 5 分钟内，会将第一组日志文件 CloudTrail 传送到您的跟踪的 Amazon S3 存储桶。您可以查看这些文件并了解它们包含的信息。

> **Note**
>
> CloudTrail 通常在 API 调用后的平均大约 5 分钟内传送日志。此时间并不能得到保证。有关更多信息，请参阅 AWS CloudTrail 服务等级协议。
> 如果您错误配置了跟踪（例如，无法访问 S3 存储桶），则 CloudTrail 会尝试将日志文件重新传送到您的 S3 存储桶，持续 30 天，这些 attempted-to-deliver 事件将按标准费用收费。CloudTrail 为避免配置错误的跟踪产生费用，您需要删除跟踪。

查看日志文件

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择 Trails（跟踪记录）。在 Trails（跟踪记录）页面上，查找您刚创建的跟踪记录的名称（在本例中为 *My-Management-Events-Trail*）。
3. 在跟踪行中，选择 S3 存储桶的值（在示例中为 *aws-cloudtrail-logs-08132020-*mytrail）。
4. Simple Storage Service（Amazon S3）控制台在日志文件的顶层打开并显示该存储桶。由于您创建了记录所有 AWS 区域事件的跟踪，因此显示屏将在显示每个区域文件夹的级别打开。*#### Amazon S3 ##############/AWS##/## ID/#* CloudTrail为要查看日志文件的 AWS 区域选择文件夹。例如，如果您希望查看美国东部（俄亥俄）区域的日志文件，请选择 us-east-2。



5. 将存储桶文件夹结构导航至您要查看该地区的活动日志的年、月和日。在这一天会有多个文件。文件名以您的 AWS 账户 ID 开头，并以扩展名结尾.gz。*#########ID # 123456789012################123456789012 _ _ us-east-2 _ 20190610t1255abcdeExample .json.gz#CloudTrail*

   要查看这些文件，您可以下载它们，解压缩，然后在纯文本编辑器或 JSON 文件查看器中查看它们。有些浏览器还支持直接查看 .gz 和 JSON 文件。我们建议使用 JSON 查看器，因为它可以更轻松地解析 CloudTrail 日志文件中的信息。

后续步骤计划

现在您有了跟踪，就可以访问 AWS 账户中持续记录的事件和活动了。这种持续记录有助于您满足 AWS 账户的会计和审计需求。但是，你可以用 CloudTrail CloudTrail 数据做更多的事情。

- 为您的跟踪数据增加额外的安全性。 CloudTrail创建跟踪时会自动应用一定的安全级别。但是，您可以使用其他一些步骤来帮助您确保数据安全。
  - 默认情况下，您在创建跟踪时创建的 Amazon S3 存储桶已应用 CloudTrail 允许将日志文件写入该存储桶的策略。该存储桶不可公开访问，但如果您的 AWS 账户中的其他用户有权读取和写入您账户中的存储桶，则他们可能可以访问该存储桶。 AWS 查看存储桶的策略，如果必要，进行更改以限制访问。有关更多信息，请参阅 Simple Storage Service（Amazon S3）安全文档和用于保护存储桶的示例演练。
  - 传送 CloudTrail 到您的存储桶的日志文件通过亚马逊服务器端加密，使用亚马逊 S3 托管的加密密钥 (SSE-S3) 进行加密。要提供可直接管理的安全层，您可以改为使用带有 AWS KMS托管密钥 (SSE-KMS) 的服务器端加密来处理日志文件。 CloudTrail 要将 SSE-KMS 与配合使用

CloudTrail，您需要创建并管理 KMS 密钥，也称为。AWS KMS key有关更多信息，请参阅 使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)。

- 有关其他安全计划，请查看的安全最佳实践 CloudTrail。

- 创建跟踪以记录数据事件。如果您想记录何时在一个或多个 Amazon S3 存储桶中添加、检索和删除对象，在 DynamoDB 表中添加、更改或删除项目，或者调用一个或 AWS Lambda 多个函数时，这些都是数据事件。在本教程前面创建的管理事件跟踪不会记录这些类型的事件。您可以创建单独的跟踪，专门用于记录部分或全部支持的资源类型的数据事件。有关更多信息，请参阅 数据事件。

  > **Note**
  >
  > 记录数据事件将收取额外费用。有关更多信息，请参阅AWS CloudTrail 定价。

- 在您的跟踪中记录 CloudTrail 见解事件。 AWS CloudTrail Insights 通过持续分析 CloudTrail 管理事件，帮助 AWS 用户识别和响应与 API 调用和 API 错误率相关的异常活动。 CloudTrail Insights 使用数学模型来确定账户的 API 和服务事件活动的正常水平。它可识别正常模式之外的行为，生成 Insights 事件，并将这些事件传送到为跟踪记录选择的 S3 存储桶中的 `/CloudTrail-Insight` 文件夹。有关 CloudTrail Insights 的更多信息，请参阅记录 Insights 事件。

  > **Note**
  >
  > 记录 Insights 事件将收取额外费用。有关更多信息，请参阅AWS CloudTrail 定价。

- 设置 CloudWatch 日志警报，以便在发生某些事件时提醒您。 CloudWatch 日志允许您监控和接收捕获的特定事件的警报 CloudTrail。例如，您可以监控关键的安全和网络相关管理事件，例如安全组更改、失败的 AWS Management Console 登录事件或者对 IAM 策略的更改。有关更多信息，请参阅使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

- 使用分析工具来识别 CloudTrail 日志中的趋势。尽管事件历史记录中的筛选条件可帮助您查找近期活动中的特定事件或事件类型，但它不提供搜索更长时间段内的活动的功能。要进行更深入和更复杂的分析，您可以使用 Amazon Athena。有关更多信息，请参阅 Amazon Athena 用户指南中的查询 AWS CloudTrail 日志。

为 S3 数据事件创建事件数据存储

您可以创建事件数据存储来记录 CloudTrail 事件（管理事件、数据事件）、CloudTrail Insights 事件、AWS Audit Manager 证据、AWS Config 配置项目或非AWS 事件。

在为数据事件创建事件数据存储时，可以选择要记录数据事件的 AWS 服务 和资源类型。有关 AWS 服务 该日志数据事件的信息，请参阅数据事件。

本演练向您展示如何为 Amazon S3 数据事件创建事件数据存储。在本教程中，我们将选择自定义日志选择器模板来仅在从特定 S3 存储桶中删除对象时记录事件，而不记录所有 Amazon S3 数据事件。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

为 CloudTrail 数据事件创建事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在配置事件数据存储页面上，在常规详细信息中，为您的事件数据存储命名，例如 *s3-data-events-eds*。作为最佳实践，请使用可快速识别事件数据存储用途的名称。有关 CloudTrail 命名要求的信息，请参见命名要求。
5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。

7. （可选）在加密中，选择是否要使用自己的 KMS 密钥加密事件数据存储。默认情况下，事件数据存储中的所有事件都 CloudTrail 使用为您 AWS 拥有和管理的 KMS 密钥进行加密。

   要使用自己的 KMS 密钥进行加密，请选择使用我自己的 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail 日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

   > **Note**
   >
   > 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

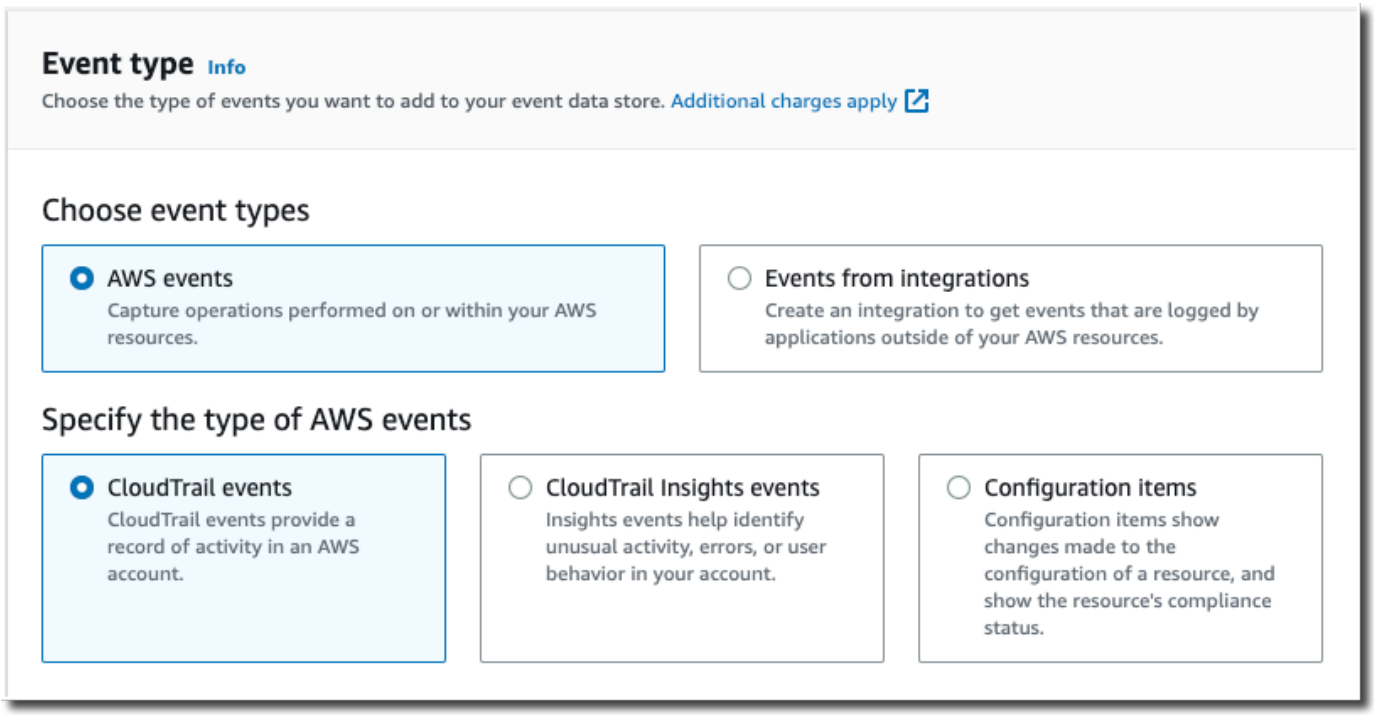
   b. 如果您在创建新角色，请输入名称来标识该角色。

   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

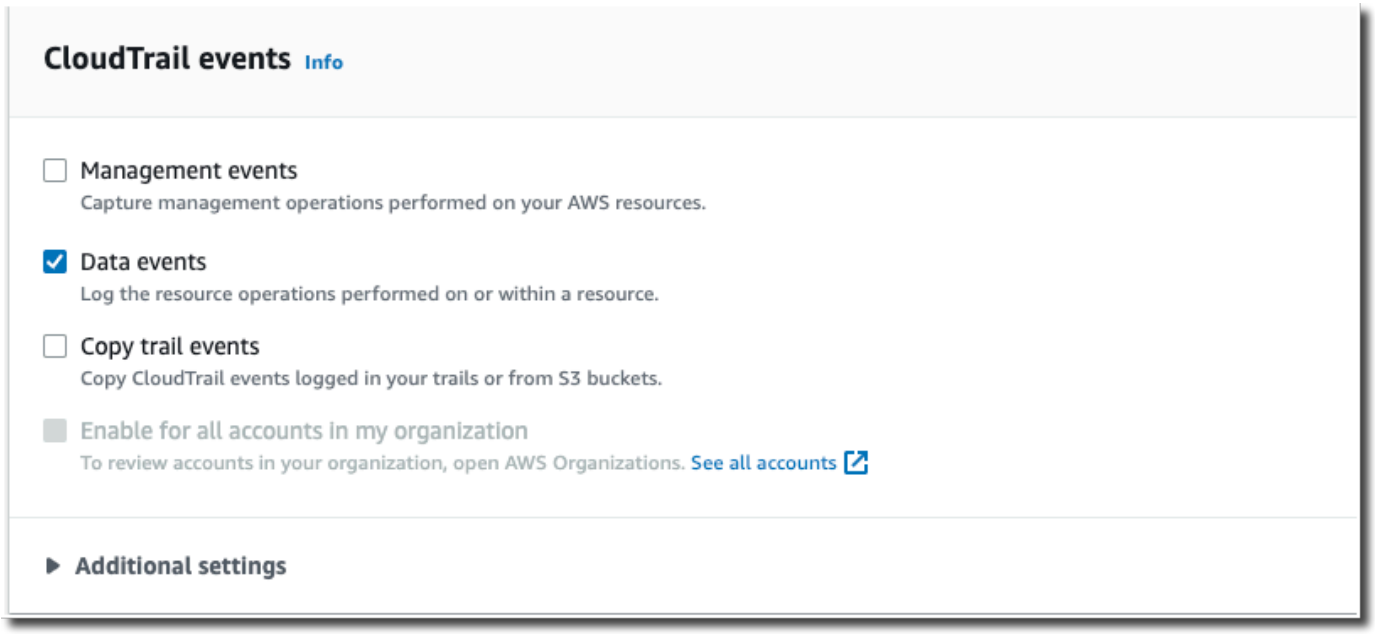
9. （可选）在标签中，将一个或多个自定义标签（键值对）添加到事件数据存储中。标签可以帮助您识别 CloudTrail 事件数据存储。例如，您可以附加名称为 **`stage`**、值为 **`prod`** 的标签。您可以使用标签来限制对事件数据存储的访问。您还可以使用标签来跟踪事件数据存储的查询和摄取成本。

有关如何使用标签跟踪成本的信息，请参阅 为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签。有关如何使用 IAM 策略根据标签授权对事件数据存储的访问，请参阅 示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。
11. 在选择事件页面上，保留事件类型的默认选择。



12. 对于CloudTrail 事件，请选择数据事件并取消选择管理事件。有关数据事件的更多信息，请参阅记录数据事件。

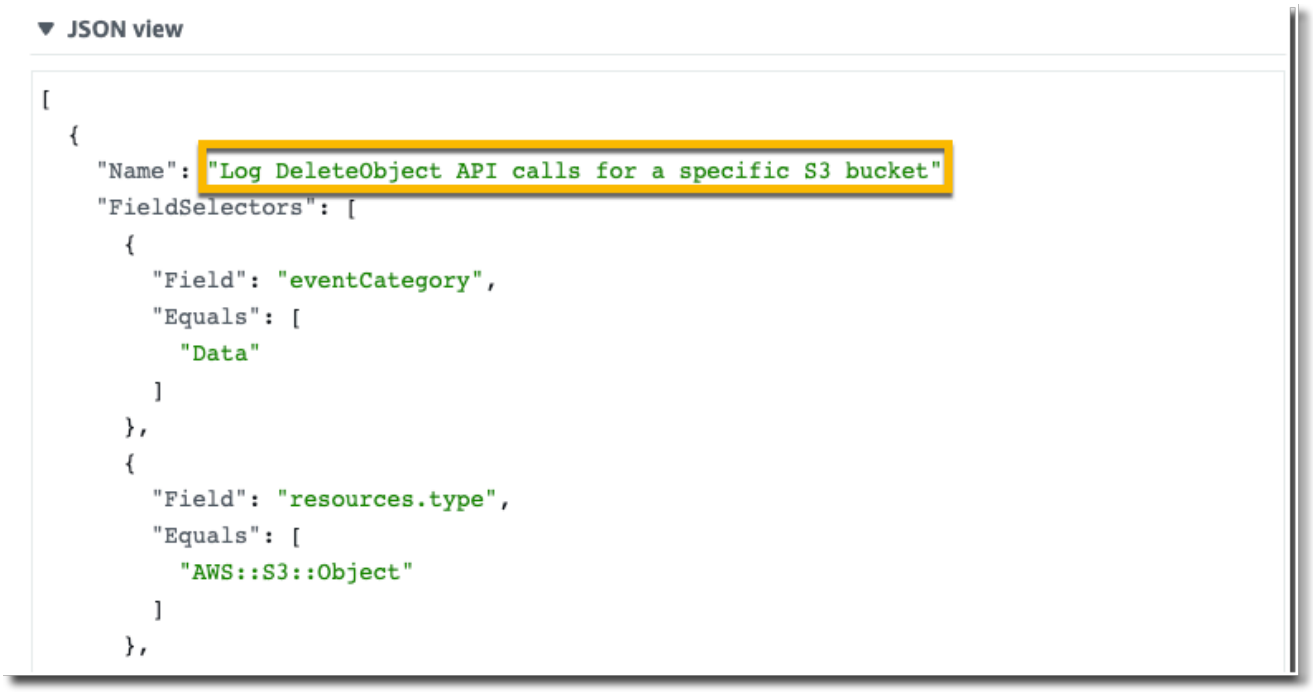


13. 保留复制跟踪事件的默认设置。您可以使用此选项将现有的跟踪事件复制到事件数据存储。有关更多信息，请参阅 将跟踪事件复制到事件数据存储。
14. 如果这是组织事件数据存储，请选择为我组织中的所有账户启用。除非您在 AWS Organizations中配置了账户，否则此选项将不能进行更改。
15. 对于其他设置，请保留默认选择。默认情况下，事件数据存储会收集所有人的事件， AWS 区域并在创建事件时开始摄取事件。
16. 对于数据事件，请进行下列选择：

    a. 在数据事件类型中，选择 S3。数据事件类型用于标识记录数据事件的 AWS 服务 和资源。

    b. 在日志选择器模板中，选择自定义。选择自定义可定义自定义事件选择器来按 `eventName`、`resources.ARN` 和 `readOnly` 字段进行筛选。有关这些字段的信息，请参阅 AWS CloudTrail API 参考AdvancedFieldSelector中的。

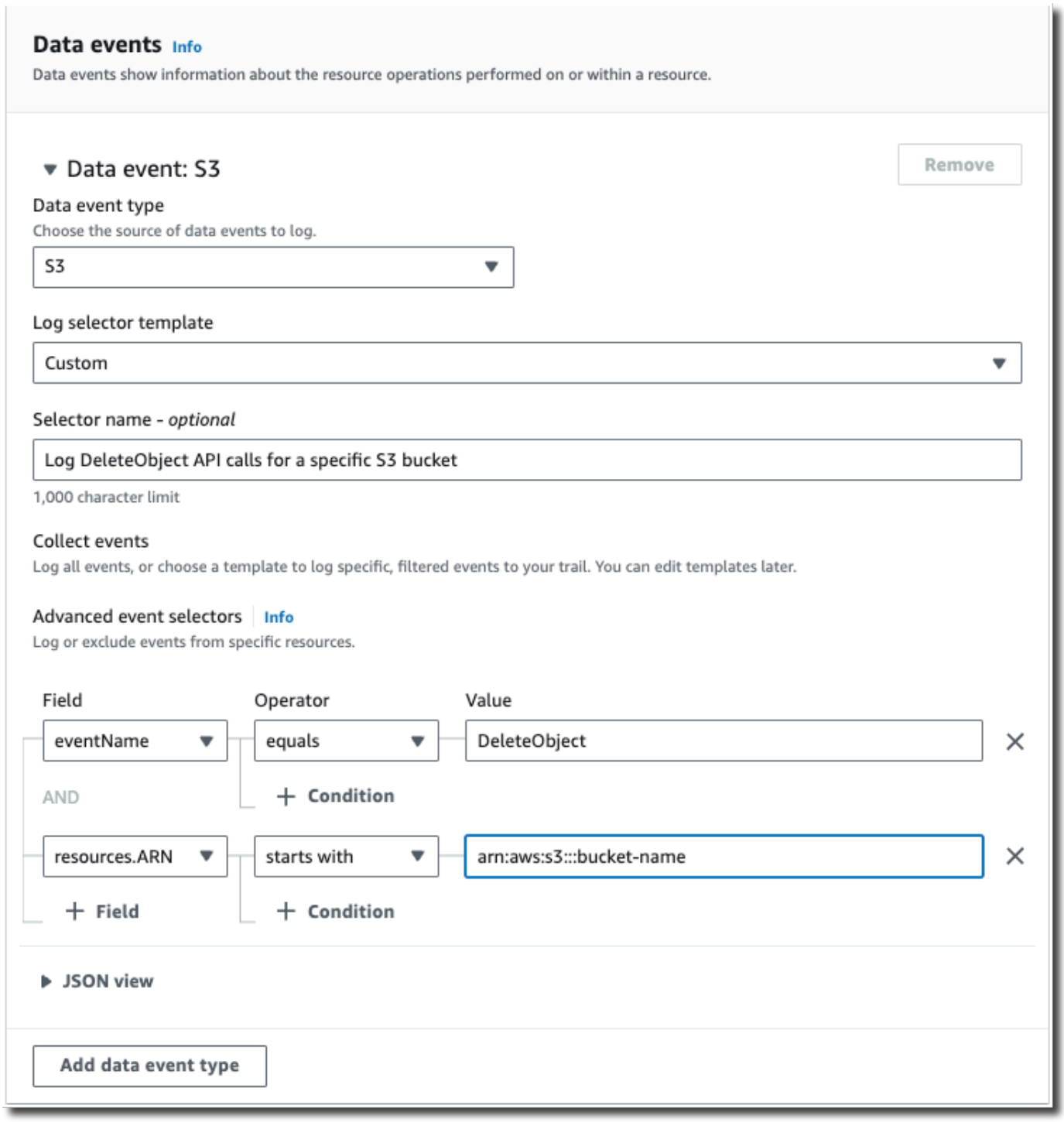
    c. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如 “记录特定 S3 存储桶 DeleteObject 的 API 调用”。选择器名称在高级事件选择器中列为 `Name`，展开 JSON 视图即可查看该名称。



d. 在高级事件选择器中，我们将构建自定义事件选择器来筛选`eventName`和`resources.ARN`字段。事件数据存储的高级事件选择器的工作方式与应用于跟踪记录的高级事件选择器相同。有关如何构建高级事件选择器的详细信息，请参阅使用高级事件选择器记录数据事件。

   i. 对于字段，选择 eventName。对于运算符，选择 equals。对于值，请输入 **`DeleteObject`**。选择 + 字段可筛选其他字段。

   ii. 对于字段，选择 resources.ARN。对于 “操作员”，选择StartsWith。对于值，输入存储桶的 ARN（例如 *`arn:aws:s3:::bucket-name`*）。有关如何获取 ARN 的信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 资源。



17. 选择 Next（下一步）以查看您的选择。
18. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
19. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

从现在开始，事件数据存储将捕获与其高级事件选择器匹配的事件。除非选择复制现有跟踪事件，否则在创建事件数据存储之前发生的事件不会出现在该事件数据存储中。

现在，您可以对事件数据存储运行查询。有关如何查看和运行示例查询的信息，请参阅 查看和运行 CloudTrail Lake 示例查询。

将跟踪事件复制到 CloudTrail Lake 事件数据存储中

本演练向您展示了如何将跟踪事件复制到新的 CloudTrail Lake 事件数据存储中以进行历史分析。有关复制跟踪事件的更多信息，请参阅 将跟踪事件复制到事件数据存储。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

将跟踪事件复制到 CloudTrail Lake 事件数据存储时，会根据事件数据存储提取的未压缩数据量产生费用。

将跟踪事件复制到 CloudTrail Lake 时， CloudTrail 解压缩以 gzip（压缩）格式存储的日志，然后将日志中包含的事件复制到您的事件数据存储中。未压缩数据的大小可能大于 S3 的实际存储大小。要对未压缩数据的大小进行总体估计，可以将 S3 存储桶中日志的大小乘以 10。

您可以通过为复制的事件指定更窄的时间范围来降低成本。如果您计划仅使用事件数据存储来查询复制的事件，则可以关闭事件摄取，以免对将来的事件产生费用。有关费用的更多信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

将跟踪事件复制到新的事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 “配置事件数据存储” 页面的 “常规详细信息” 中，为您的事件数据存储命名，例如*my-management-events-eds*。作为最佳实践，请使用可快速识别事件数据存储用途的名称。有关 CloudTrail 命名要求的信息，请参见命名要求。

5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。

   > **Note**
   >
   > 如果您要将跟踪事件复制到此事件数据存储中，则 CloudTrail 不会复制超过指定保留期的事件。`eventTime`要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`*）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。

7. （可选）在加密中，选择是否要使用自己的 KMS 密钥加密事件数据存储。默认情况下，事件数据存储中的所有事件都 CloudTrail 使用为您 AWS 拥有和管理的 KMS 密钥进行加密。

   要使用自己的 KMS 密钥进行加密，请选择使用我自己的 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail 日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

> **Note**
>
> 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在标签中，将一个或多个自定义标签（键值对）添加到事件数据存储中。标签可以帮助您识别 CloudTrail 事件数据存储。例如，您可以附加名称为 **`stage`**、值为 **`prod`** 的标签。您可以使用标签来限制对事件数据存储的访问。您还可以使用标签来跟踪事件数据存储的查询和摄取成本。

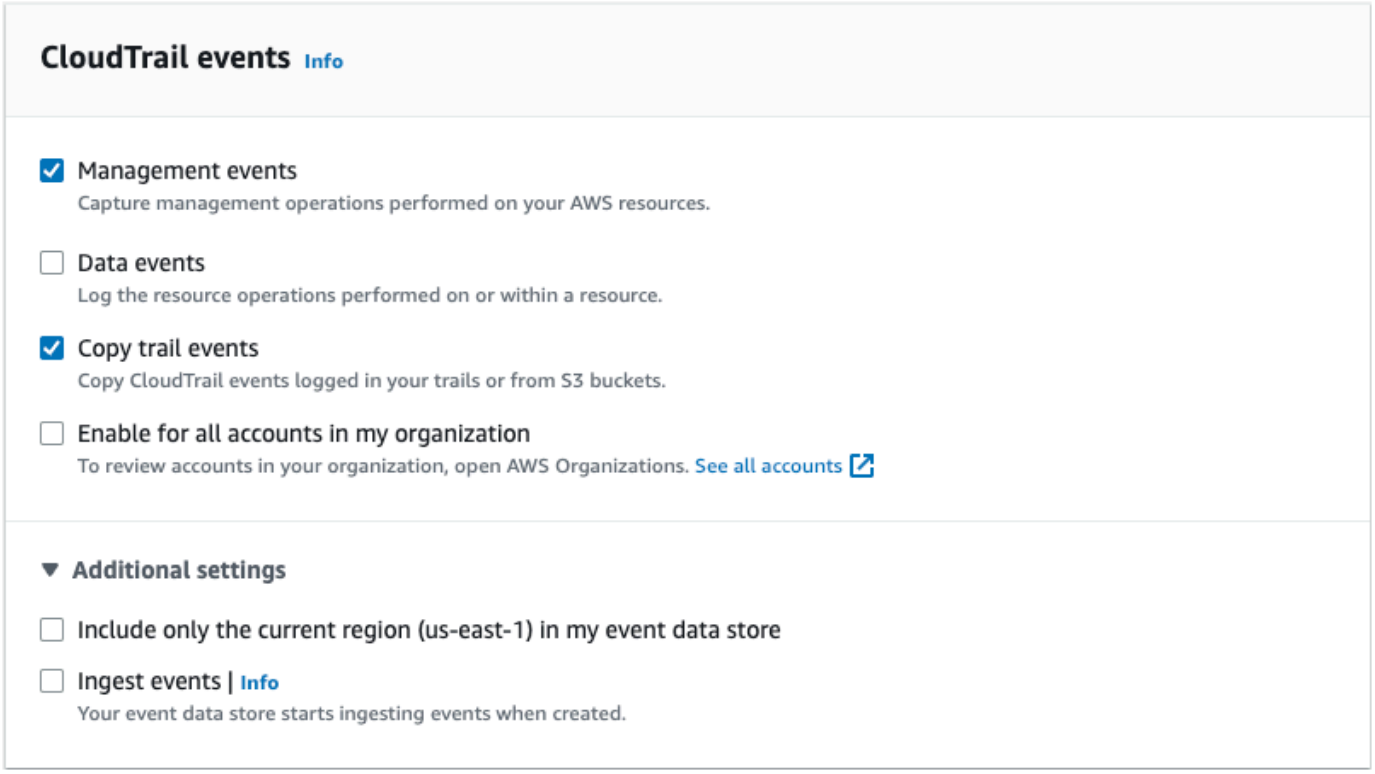
   有关如何使用标签跟踪成本的信息，请参阅 为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签。有关如何使用 IAM 策略根据标签授权对事件数据存储的访问，请参阅 示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

11. 在选择事件页面上，保留事件类型的默认选择。

12. 对于CloudTrail 事件，我们将选中 “管理” 事件，然后选择 “复制跟踪事件”。在此示例中，我们并不关心事件类型，因为我们仅使用事件数据存储来分析过去的事件，而不是摄取未来的事件。

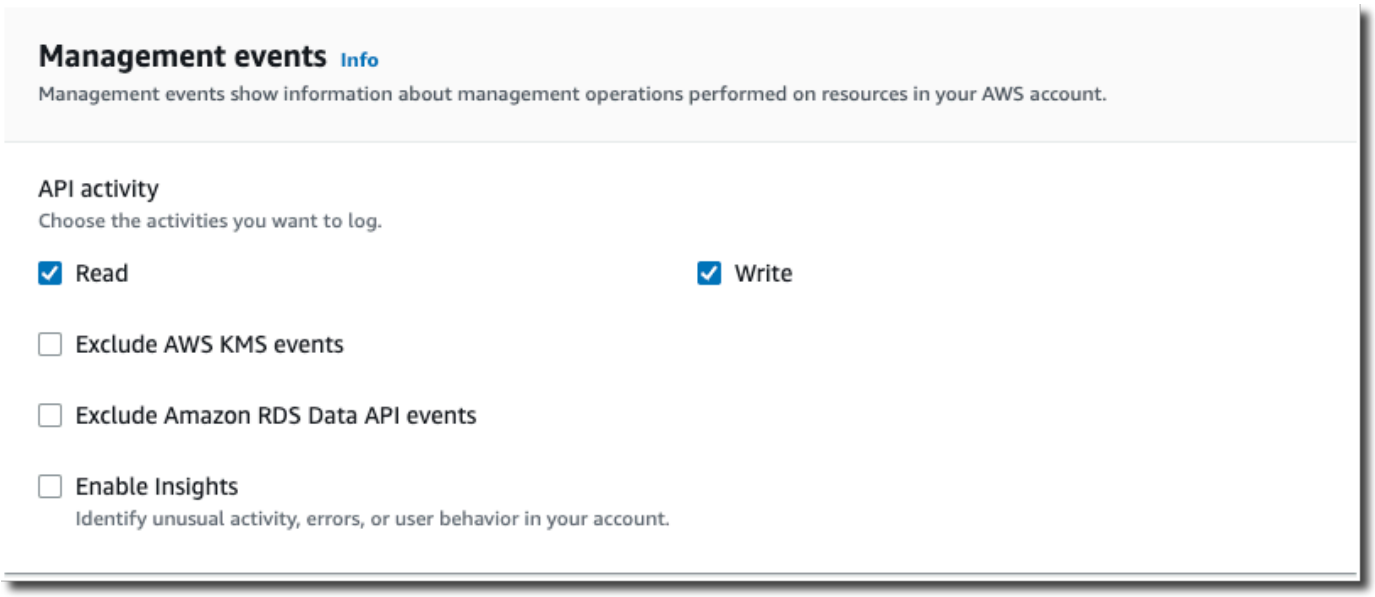
如果您要创建事件数据存储来替换现有的跟踪，请选择与您的跟踪相同的事件选择器，以确保事件数据存储具有相同的事件覆盖范围。



13. 如果这是组织事件数据存储，请选择为我组织中的所有账户启用。除非您在 AWS Organizations中配置了账户，否则此选项将不能进行更改。

> **Note**
>
> 如果您要创建组织事件数据存储，则必须使用组织的管理账户登录，因为只有管理账户才能将跟踪事件复制到组织事件数据存储。

14. 对于其他设置，我们将取消选择摄取事件，因为在此示例中，我们不希望事件数据存储摄取任何未来事件，我们只对查询复制的事件感兴趣。默认情况下，事件数据存储会收集所有人的事件，AWS 区域 并在创建事件时开始摄取事件。
15. 对于管理事件，我们将保留默认设置。



16. 在复制跟踪事件区域中，完成以下步骤。

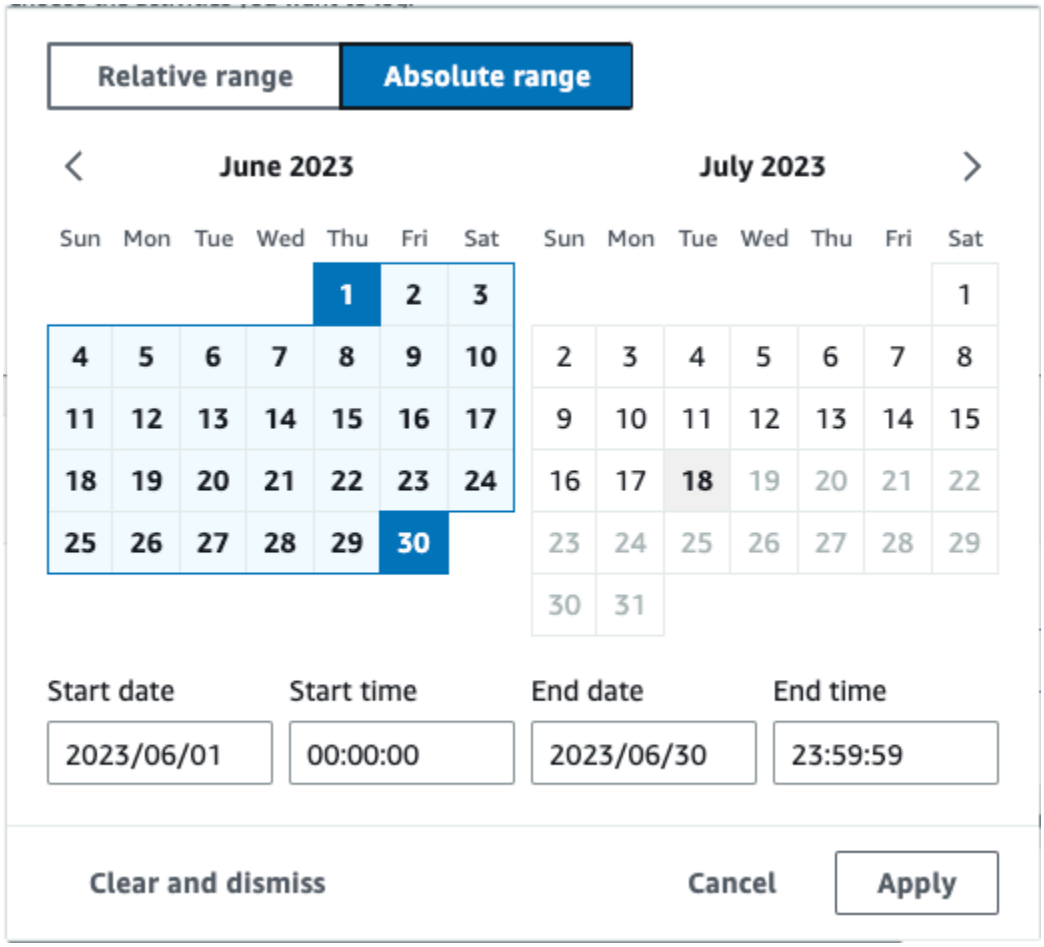
    a. 选择要复制的跟踪。在此示例中，我们将选择一个名为 *management-events* 的跟踪。

    默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的前缀，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，请选择 Enter S3 URI，然后选择 Browse S3 浏览到该前缀。如果跟踪的源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密数据。如果您的源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。有关更新 KMS 密钥政策的更多信息，请参阅 用于解密源 S3 存储桶中数据的 KMS 密钥政策。

    b. 选择复制事件的时间范围。 CloudTrail 在尝试复制跟踪事件之前，请检查前缀和日志文件名以验证该名称是否包含所选开始日期和结束日期之间的日期。您可以选择 Relative range（相对范围）或者 Absolute range（绝对范围）。为避免源跟踪和目标事件数据存储之间存在重复事件，请选择一个早于事件数据存储创建时间的时间范围。

    - 如果选择 “相对范围”，则可以选择复制过去 6 个月、1 年、2 年、7 年或自定义范围内记录的事件。 CloudTrail 复制选定时间段内记录的事件。
    - 如果选择 “绝对范围”，则可以选择特定的开始和结束日期。 CloudTrail 复制在所选开始日期和结束日期之间发生的事件。

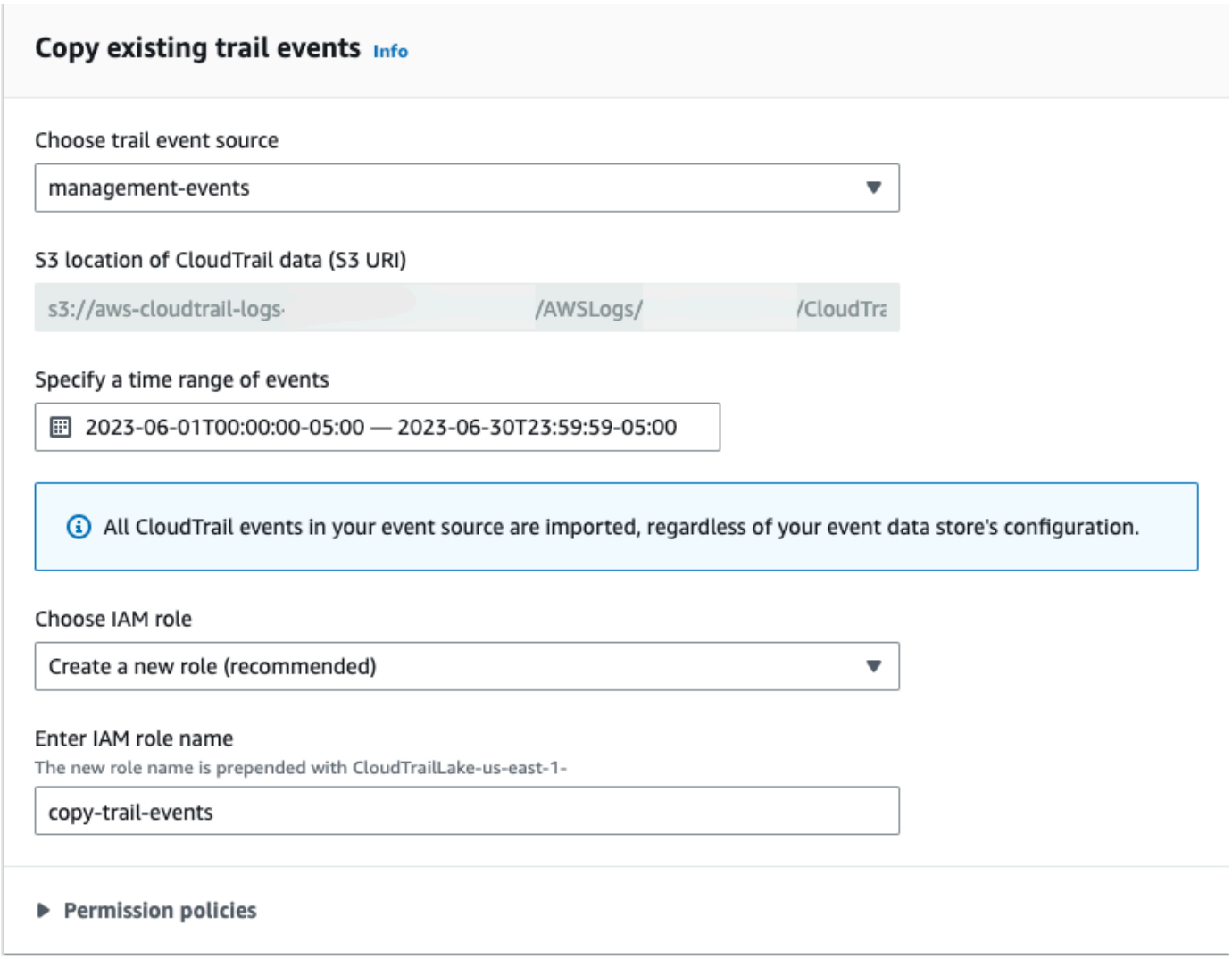
    在此示例中，我们将选择绝对范围，然后选择整个 6 月份。



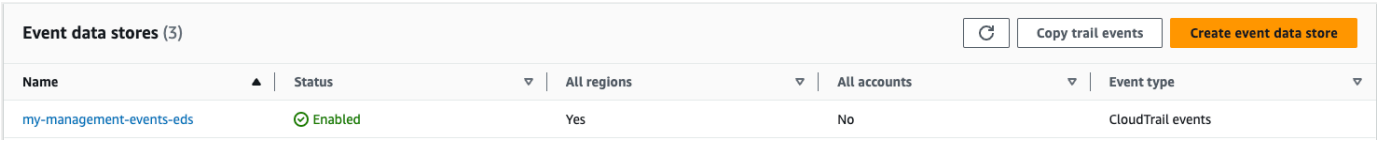
c. 对于 Permissions（权限），请从以下 IAM 角色选项中进行选择。如果您选择现有的 IAM 角色，请验证 IAM 角色策略是否提供了必要的权限。有关更新 IAM 角色权限的更多信息，请参阅 复制跟踪事件所需的 IAM 权限。

- 选择 Create a new role (recommended)（创建新角色（推荐））以创建新的 IAM 角色。在输入 IAM 角色名称中，输入角色的名称。 CloudTrail会自动为这个新角色创建必要的权限。
- 选择使用自定义 IAM 角色 ARN 以使用未列出的自定义 IAM 角色。对于 Enter IAM role ARN（输入 IAM 角色 ARN），输入 IAM ARN。
- 从下拉列表中选择现有的 IAM 角色。

在此示例中，我们将选择新建角色（推荐）并提供名称 **`copy-trail-events`**。

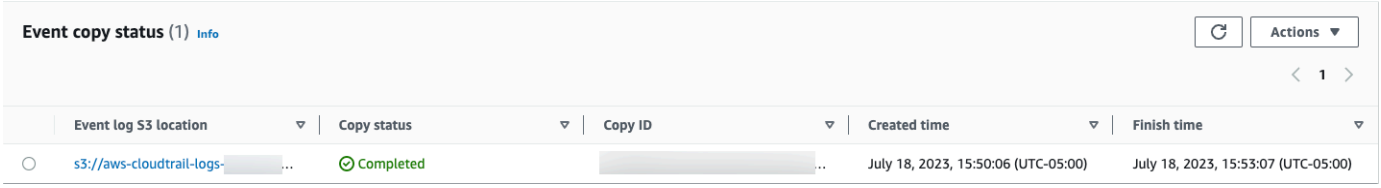


17. 选择 Next（下一步）以查看您的选择。
18. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
19. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

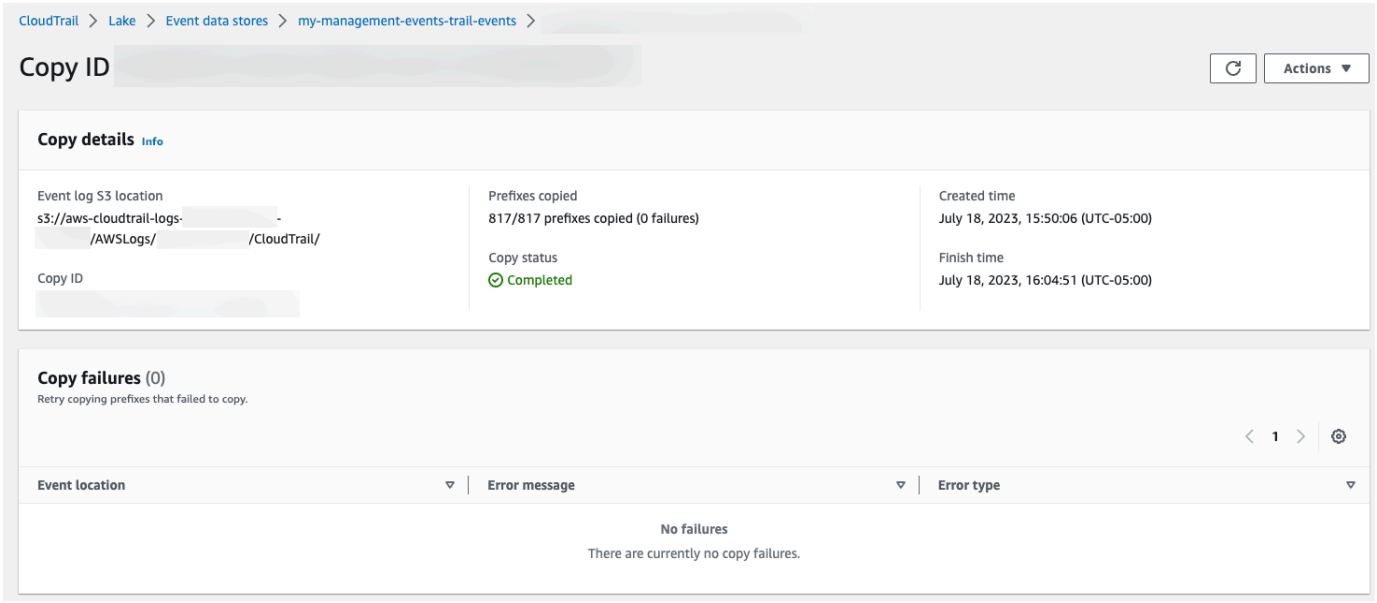


20. 选择事件数据存储名称以查看其详细信息页面。详细信息页面显示事件数据存储的详细信息以及复制状态。事件复制状态显示在事件复制状态区域中。

    跟踪事件复制完成后，如果复制未出错，则 Copy status（复制状态）将设置为 Completed（已完成），否则如果出错了，则设置为 Failed（失败）。



21. 要查看有关复制的更多详细信息，请在事件日志 S3 位置列中选择复制名称，或从操作菜单中选择查看详细信息选项。有关查看跟踪事件复制详细信息的更多信息，请参阅 事件复制详细信息。



22. 复制失败区域显示复制跟踪事件时发生的所有错误。如果 Copy status（复制状态）为 Failed（失败），则要先修复 Copy failures（复制失败）中显示的所有错误，然后选择 Retry copy（重试复制）。当您重试复制时，会在出现故障的位置 CloudTrail 恢复副本。

查看 CloudTrail 湖泊仪表板

本演练向您展示了如何查看 CloudTrail Lake 仪表板。CloudTrailLake 仪表板允许您可视化事件数据存储中的事件，并查看趋势，例如热门用户和热门错误。

每个控制面板由多个小组件组成，每个小组件代表一个 SQL 查询。要填充控制面板，请 CloudTrail 运行系统生成的查询。您需按所扫描的数据量为查询付费。

> **Note**
>
> 目前，控制面板仅适用于收集 CloudTrail管理事件、Amazon S3 数据事件和 Insights 事件的事件数据存储。

查看 Lake 控制面板

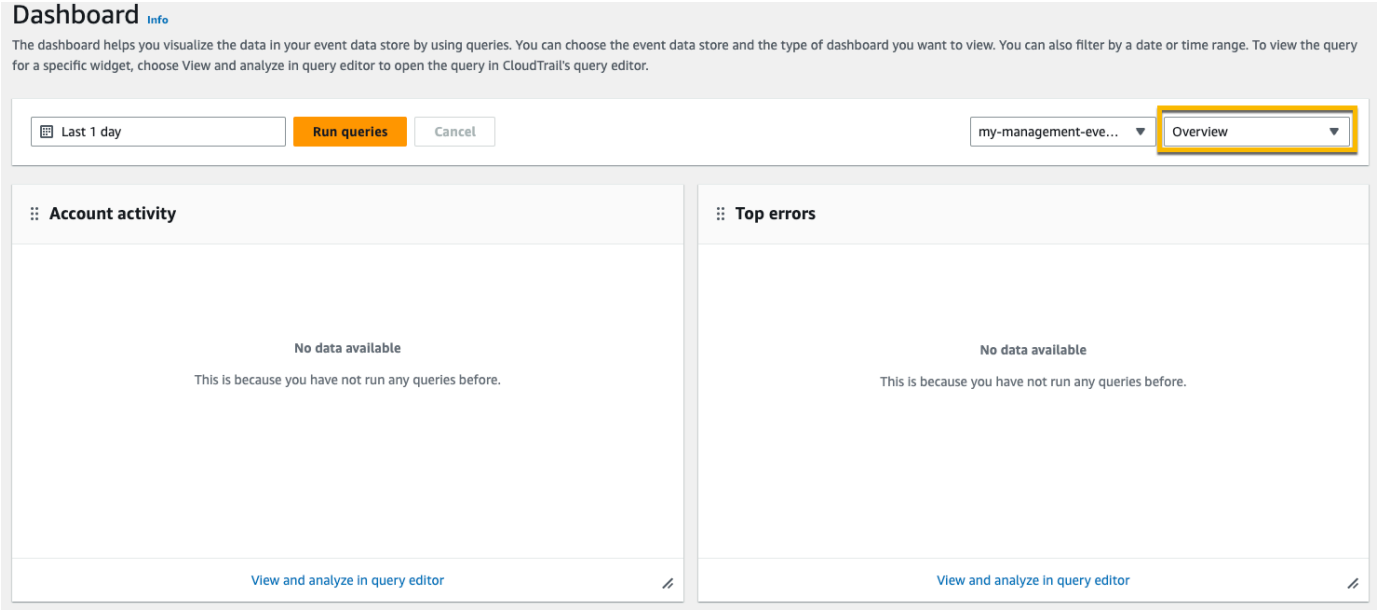
1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择控制面板。
3. 首次查看 “控制面板” 页面时， CloudTrail 会要求您确认与运行查询相关的费用。选择我同意以确认运行查询的费用。您只需确认此操作一次。有关 CloudTrail 定价的更多信息，请参阅CloudTrail 定价。
4. 从列表中选择事件数据存储，然后选择要查看的控制面板类型。

   以下是可能的控制面板类型。

   - 概览仪表板- AWS 服务 按事件计数显示最活跃的用户和事件。 AWS 区域您还可以查看有关 `read` 和 `write` 管理事件活动、最受限制的事件以及最常出现的错误的信息。此控制面板可用于收集管理事件的事件数据存储。
   - 管理事件控制面板 – 按用户显示控制台登录事件、访问被拒事件、破坏性操作和最常出现的错误。您还可以按用户查看有关 TLS 版本和过时的 TLS 调用的信息。此控制面板可用于收集管理事件的事件数据存储。
   - S3 数据事件控制面板 – 显示 S3 账户活动、访问次数最多的 S3 对象、排名靠前的 S3 用户和排名靠前的 S3 操作。此控制面板可用于收集 Amazon S3 数据事件的事件数据存储。
   - Insights 事件控制面板 - 按 Insights 类型显示 Insights 事件的总体比例、按 Insights 类型显示主要用户的服务的 Insights 事件比例以及每天的 Insights 事件数量。控制面板还包括一个小部件，可最多列出 30 天的 Insights 事件。此控制面板仅可用于收集 Insights 事件的事件数据存储。

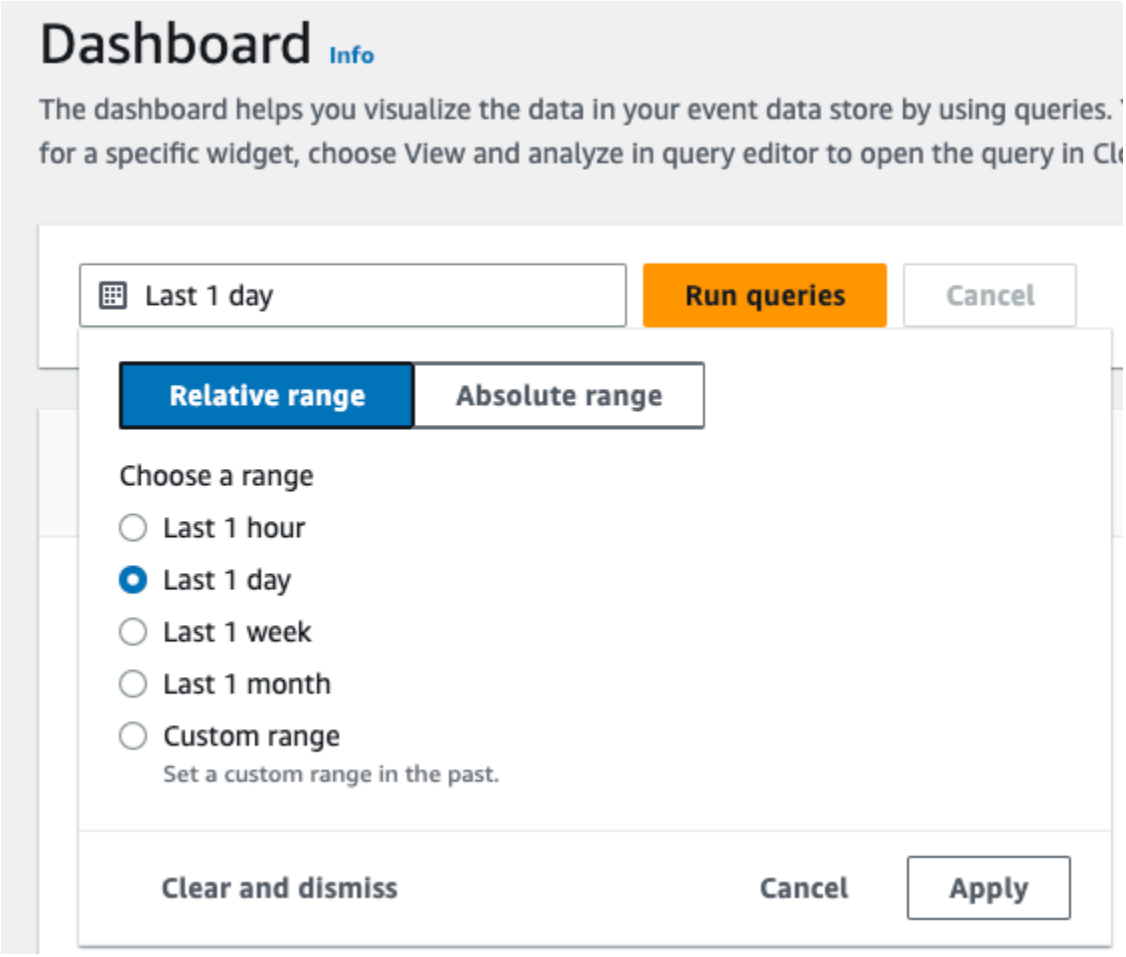
   > **Note**
   >
   > - 首次在源事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。有关更多信息，请参阅 了解 Insights 事件传输情况。
   > - Insights 事件控制面板仅显示有关选定事件数据存储收集的 Insights 事件的信息，这些信息由源事件数据存储的配置决定。例如，如果您将源事件数据存储配置为在 `ApiCallRateInsight` 上启用 Insights 事件，而不是 `ApiErrorRateInsight`，则您将不会看到有关 `ApiErrorRateInsight` 上的 Insights 事件的信息。

   在此示例中，我们选择了概览控制面板。



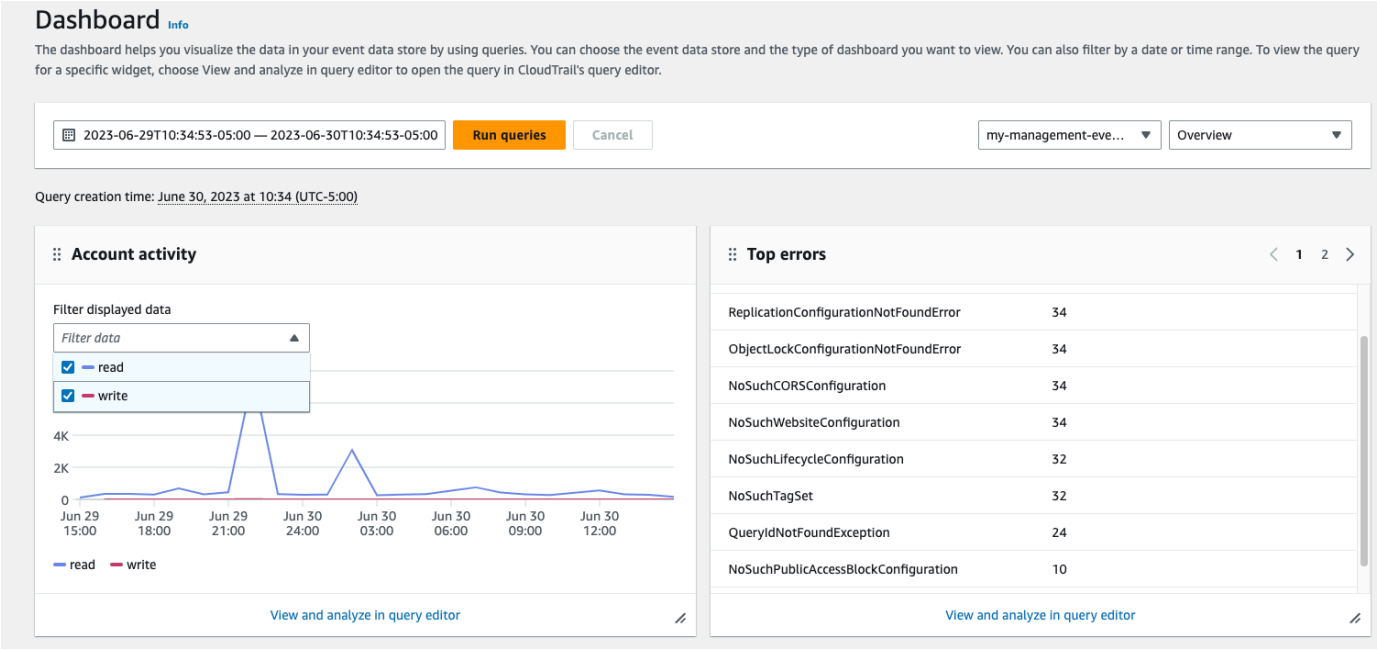
5. 选择要按时间范围筛选的日期字段，然后选择应用。选择绝对范围，以选择特定的日期和时间范围。选择相对范围，以选择预定义的时间范围或自定义范围。默认情况下，控制面板显示过去 24 小时的事件数据。

> **Note**
>
> 由于 CloudTrail 查询是根据扫描的数据量收取费用的，因此您可以通过在较窄的时间范围内进行筛选来降低成本。

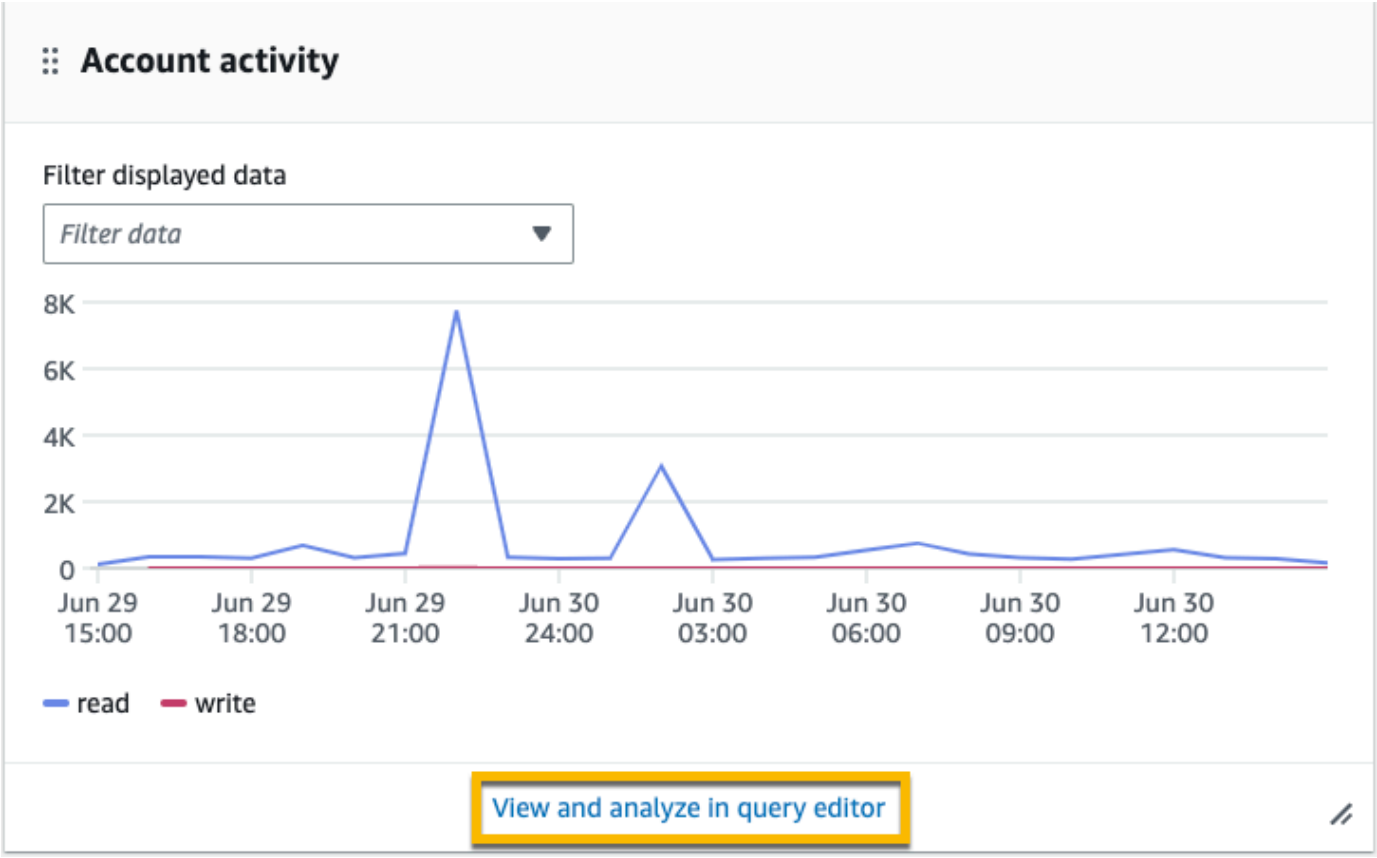


6. 选择运行查询以填充控制面板。每个小组件分别显示其关联查询的状态，并在查询完成时显示数据。

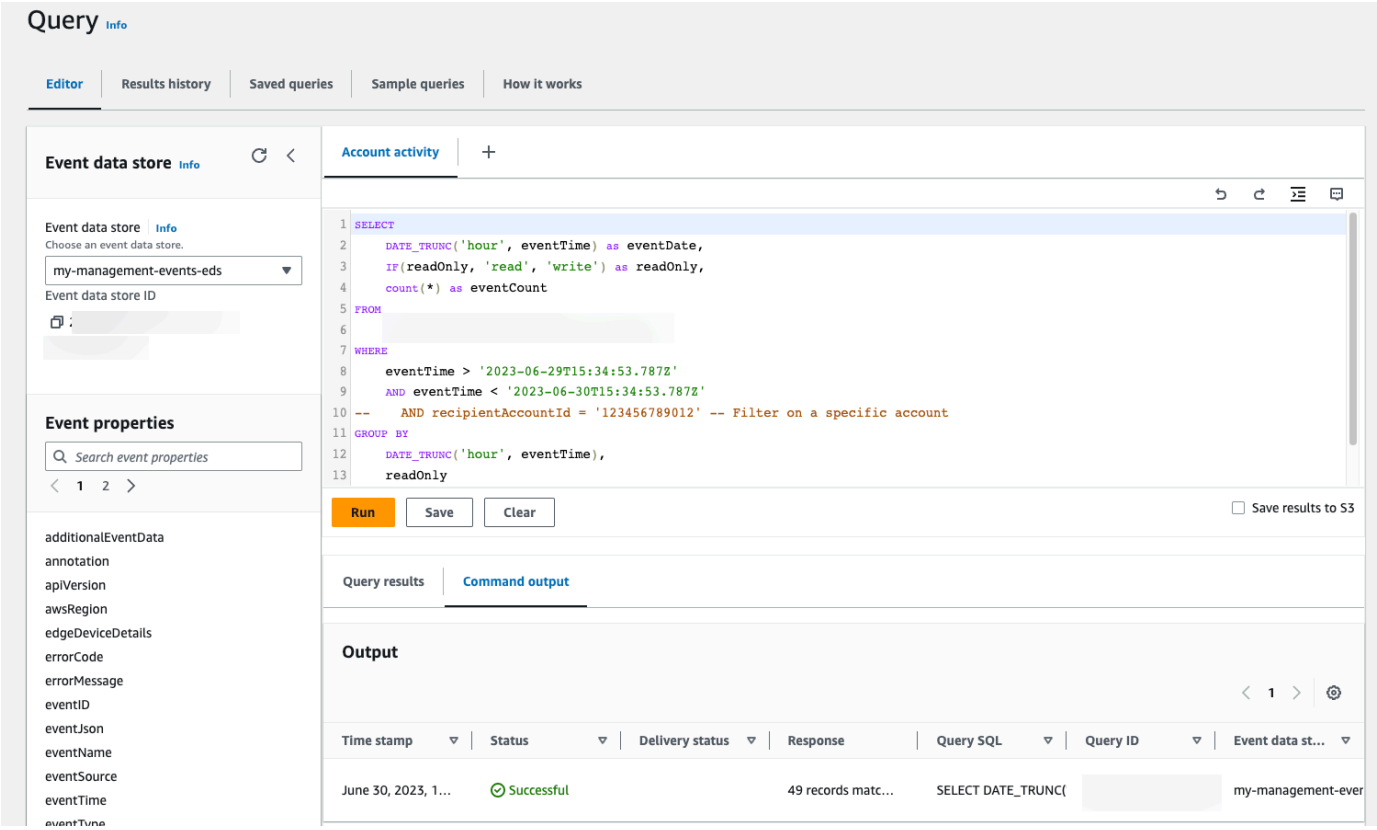
   您可以对某些小组件进行额外筛选，例如账户活动，它允许您按 `read` 和 `write` 事件活动进行筛选。



7. 要查看小组件的查询，请选择在查询编辑器中查看和分析。



选择 “在查询编辑器中查看和分析” 会在 CloudTrail Lake 的查询编辑器中打开查询，这样您就可以在仪表板之外进一步分析查询结果。有关编辑查询的更多信息，请参阅 创建或编辑查询。有关运行查询和保存查询结果的更多信息，请参阅 运行查询并保存查询结果。



有关控制面板的更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

查看和运行 CloudTrail Lake 示例查询

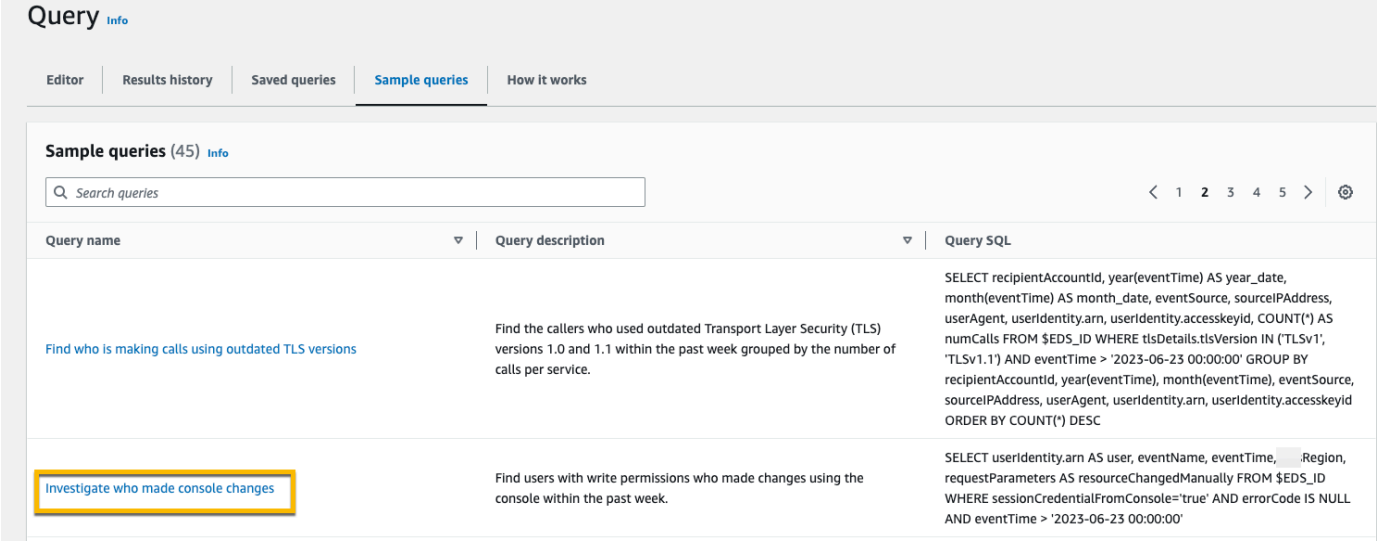
CloudTrail Lake 提供了许多示例查询，可以帮助您开始编写自己的查询。本演练向您展示如何选择和运行示例查询。

CloudTrail 查询会根据扫描的数据量收取费用。为了帮助控制成本，我们建议您通过为查询添加开始和结束 `eventTime` 时间戳，来限制查询。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

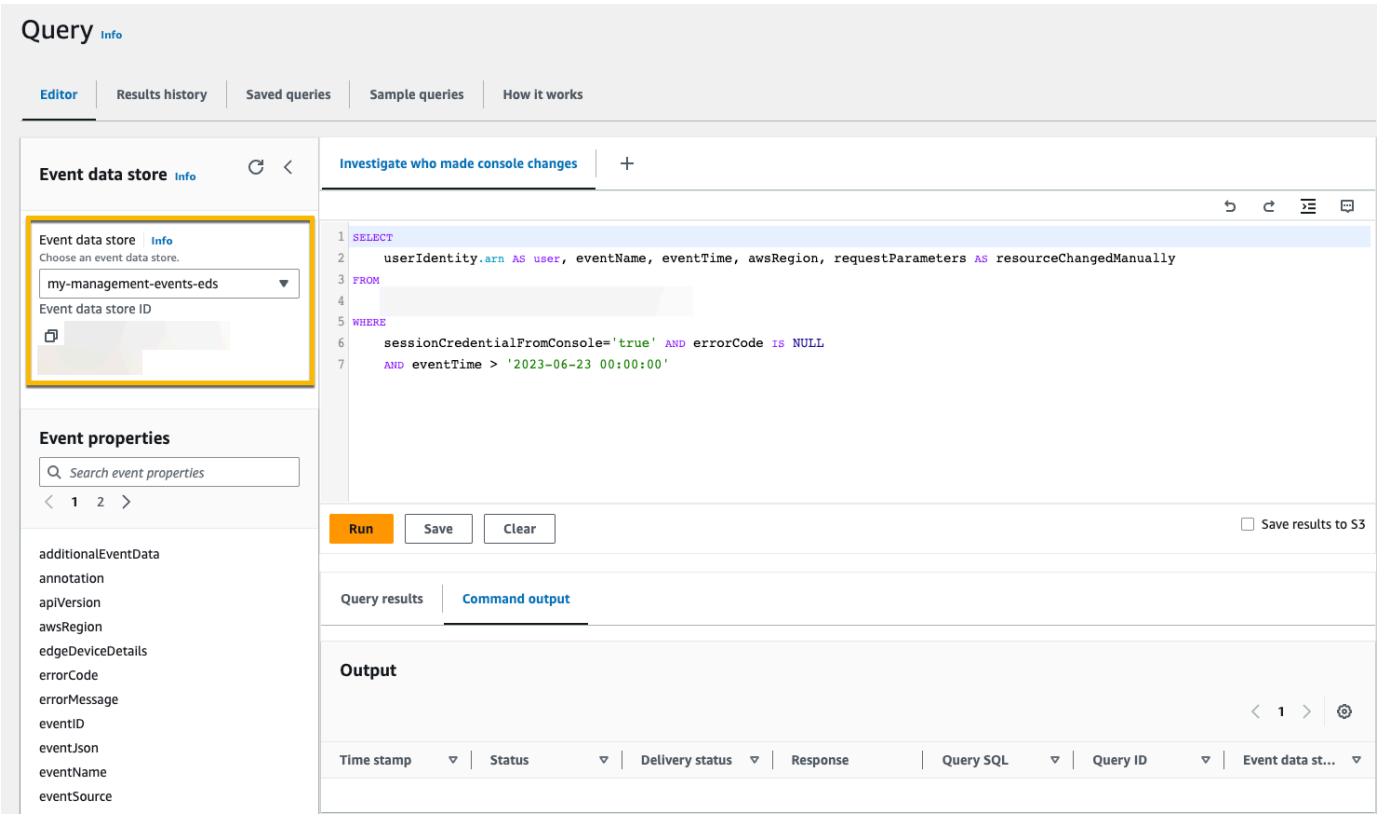
查看和运行示例查询

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。

2. 在导航窗格中，在 Lake 下，选择查询。
3. 在 Query（查询）页面上，选择 Sample queries（示例查询）选项卡。
4. 从列表中选择示例查询或搜索查询以筛选列表。在此示例中，我们将通过选择查询名称来打开调查谁对控制台进行了更改查询。这将在 Editor（编辑器）选项卡中打开此查询。

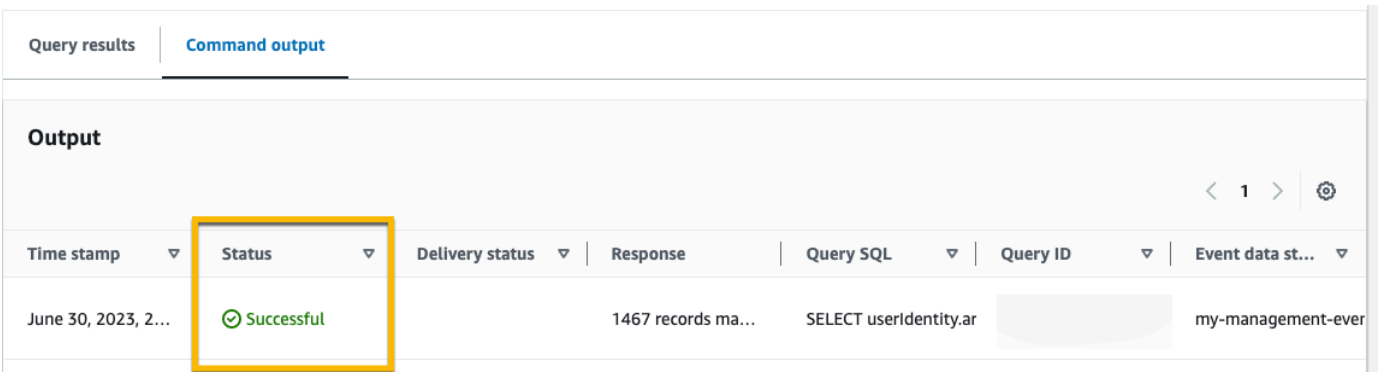


5. 在编辑器选项卡上，选择要为其运行查询的事件数据存储。当您从列表中选择事件数据存储时，CloudTrail 会在查询编辑器的FROM行中自动填充事件数据存储 ID。

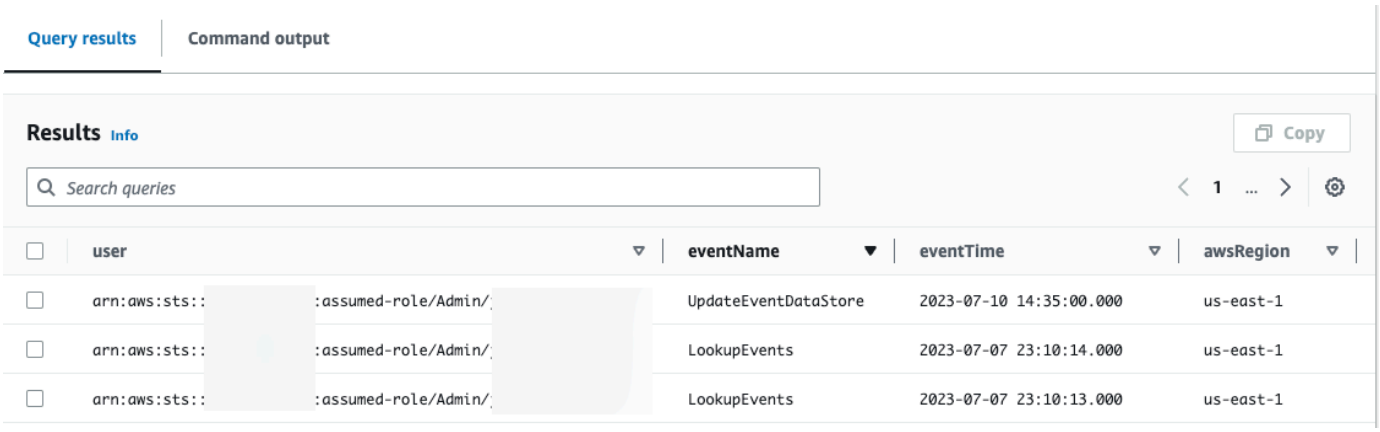


6. 选择运行以运行查询。

命令输出选项卡显示有关查询的元数据，例如查询是否成功、匹配的记录数量以及查询的运行时间。



查询结果选项卡显示选定事件数据存储中与查询匹配的事件数据。



有关编辑查询的更多信息，请参阅 创建或编辑查询。有关运行查询和保存查询结果的更多信息，请参阅 运行查询并保存查询结果。

将 CloudTrail Lake 查询结果保存到 S3 存储桶中

本演练展示了如何将 CloudTrail Lake 查询结果保存到 S3 存储桶中，然后下载这些查询结果。

在 CloudTrail Lake 中运行查询时，会根据查询扫描的数据量产生费用。将查询结果保存到 S3 存储桶不会产生额外的 CloudTrail Lake 费用，但会收取 S3 存储费用。有关 S3 定价的更多信息，请参阅 Amazon S3 定价。

保存查询结果时，查询结果可能会先显示在 CloudTrail 控制台中，然后才能在 S3 存储桶中查看，因为查询扫描完成后才会 CloudTrail 提供查询结果。虽然大多数查询会在几分钟内完成，但根据事件数据存储的大小，将查询结果传送 CloudTrail 到 S3 存储桶可能需要更长的时间。 CloudTrail 以压缩的

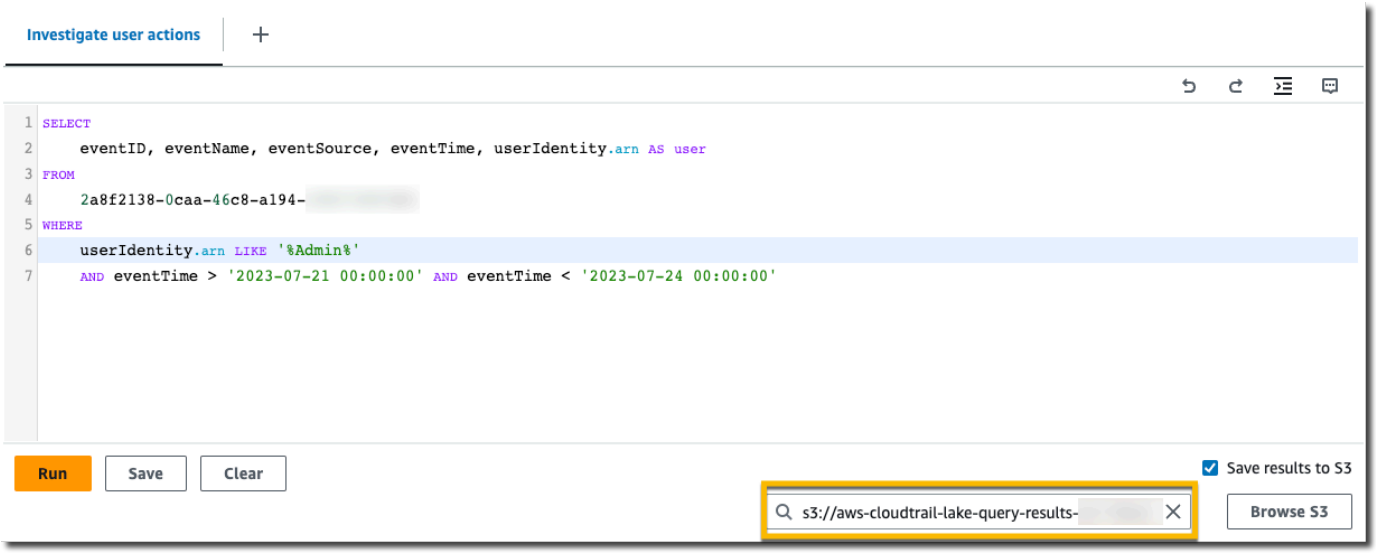
gzip 格式将查询结果传送到 S3 存储桶。平均而言，查询扫描完成后，传送到 S3 存储桶的每 GB 数据预计将出现 60 至 90 秒的延迟。

将查询结果保存到 Amazon S3 存储桶中

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择查询。
3. 在示例查询或已保存的查询选项卡上，通过选择查询名称来选择要运行的查询。在此示例中，我们将选择名为调查用户操作的示例查询。
4. 在 Editor（编辑器）选项卡的 Event data store（事件数据存储）中，从下拉列表中选择事件数据存储。从列表中选择事件数据存储时， CloudTrail 会自动填充`From`行中的事件数据存储 ID。
5. 在此示例查询中，我们将编辑 `userIdentity.ARN` 值以指定名为 `Admin` 的用户，并保留 `eventTime` 的默认值。运行查询时，您需要按扫描的数据量付费。为了帮助控制成本，我们建议您通过为查询添加开始和结束 `eventTime` 时间戳，来限制查询。

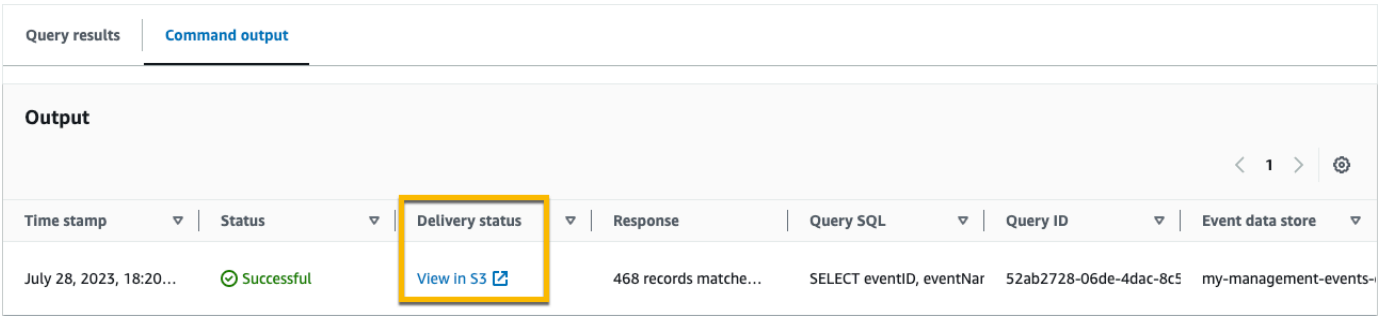
6. 选择将结果保存到 S3 中以将查询结果保存到 S3 存储桶中。当您选择默认 S3 存储桶时，CloudTrail 会创建并应用所需的存储桶策略。如果您选择默认 S3 存储桶，则您的 IAM 策略需要包含`s3:PutEncryptionConfiguration`操作权限，因为默认情况下，该存储桶已启用服务器端加密。有关保存查询结果的更多信息，请参阅 有关已保存查询结果的其他信息。在此示例中，我们将使用默认的 S3 存储桶。

> **Note**
>
> 要使用其他存储桶，请指定存储桶名称，或选择 Browse S3（浏览 S3）以选择存储桶。存储桶策略必须授予向存储桶传送查询结果的 CloudTrail 权限。有关手动编辑存储桶策略的信息，请参阅适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略。

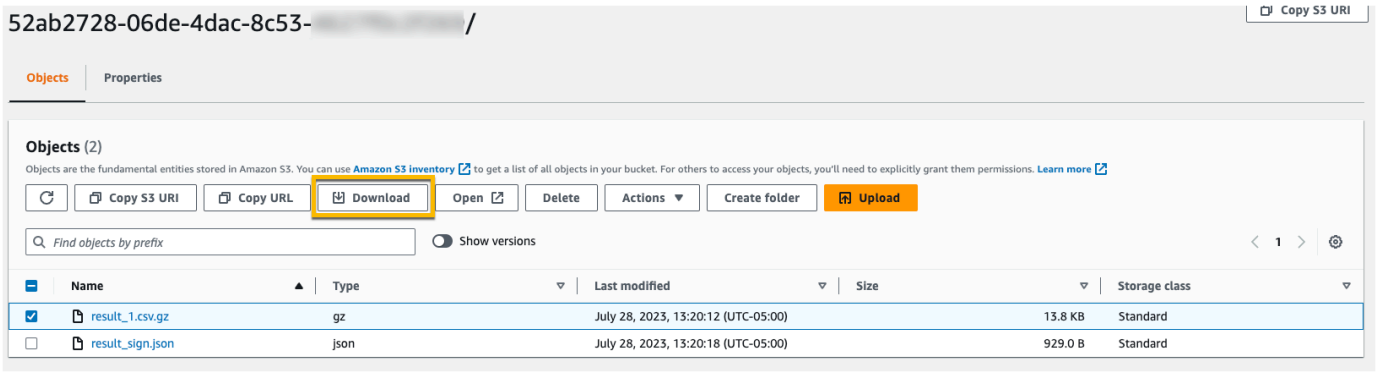


7. 选择运行。根据事件数据存储的大小及其包含的数据天数，运行查询可能需要几分钟时间。Command output（命令输出）选项卡用于显示查询的状态以及查询是否已完成运行。在完成运行查询后，打开 Query results（查询结果）选项卡，以查看活跃查询（编辑器中当前显示的查询）的结果表。
8. 将保存的查询结果传送到您的 S3 存储桶 CloudTrail 后，“交付状态” 列将提供指向 S3 存储桶的链接，其中包含您保存的查询结果文件以及可用于验证保存的查询结果的签名文件。选择在 S3 中查看以查看 S3 存储桶中的查询结果文件和签名文件。

> **Note**
>
> 保存查询结果时，查询结果可能会先显示在 CloudTrail 控制台中，然后才能在 S3 存储桶中查看，因为查询扫描完成后才会 CloudTrail 提供查询结果。虽然大多数查询会在几分钟内完成，但根据事件数据存储的大小，将查询结果传送 CloudTrail 到 S3 存储桶可能需要更长的时间。 CloudTrail 以压缩的 gzip 格式将查询结果传送到 S3 存储桶。平均而言，查询扫描完成后，传送到 S3 存储桶的每 GB 数据预计将出现 60 至 90 秒的延迟。



9. 要下载查询结果，请选择查询结果文件（在此示例中为 `result_1.csv.gz`），然后选择下载。



有关验证保存的查询结果的信息，请参阅 [验证已保存的查询结果](#)。

通过查看您的 CloudTrail 成本和使用情况 AWS Cost Explorer

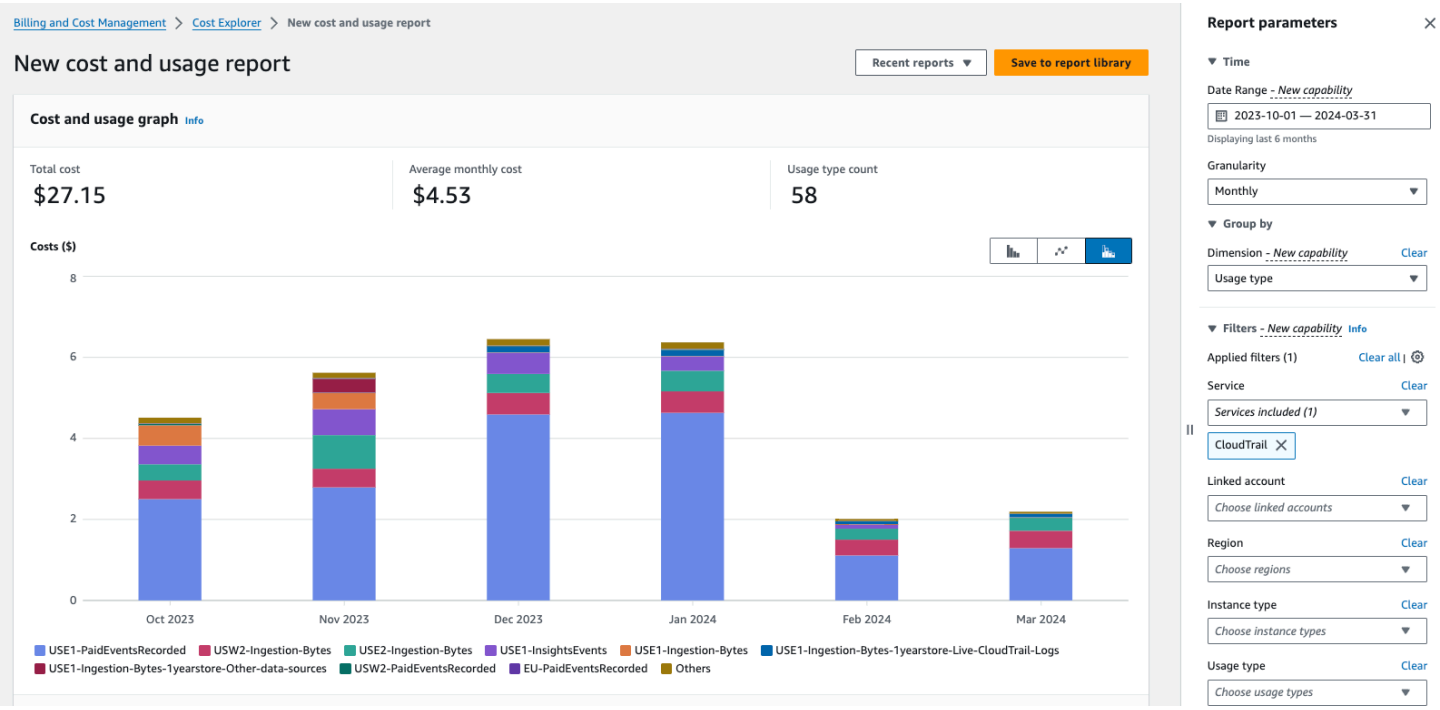
本节介绍如何使用查看 CloudTrail 费用和使用情况AWS Cost Explorer。Cost Explorer 使您能够可视化、了解和管理一段时间内的 AWS 成本和使用情况。

有关 CloudTrail 定价的详细信息，请参阅AWS CloudTrail 定价。

使用 Cost Explorer 查看 CloudTrail 成本和使用情况

1. 登录 AWS Management Console 并打开 Cost Explorer 控制台，网址为 https://console.aws.amazon.com/cost-management/home#/custom。
2. 在“时间”下，选择要分析的日期范围。
3. 在“分组依据”下，为“维度”选择“使用类型”。
4. 在“筛选器”下的“服务”中，选择CloudTrail。

下图显示了按使用类型筛选 CloudTrail 和分组的成本报告的示例。



查看使用类型以查看哪些 CloudTrail 功能产生的费用最高。每种使用类型都以费用 AWS 区域 发生地的代码开头。

下表描述了每项 CloudTrail 功能的 CloudTrail 使用类型。

CloudTrail 特征	使用情况类型	描述
CloudTrail 步道	*region*-FreeEventsRecorded	管理活动的第一份副本免费提供给 AWS 区域.
	region-PaidEventsRecorded	向某人发送管理事件的额外副本的费用 AWS 区域。
	region-DataEventsRecorded	向某人传送数据事件的费用 AWS 区域。数据事件总是会产生费用。
CloudTrail 湖	*region*-Ingestion-Bytes	使用七年保留定价选项将事件摄取到 CloudTrail Lake 事件数据存储中的费用。摄取定价基于采集的数据量，所有事件类型均相同。
	region-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	使用为期一年的可延期保留定价选项将 CloudTrail 数据事件和管理事件提取到 CloudTrail Lake 事件数据存储中的费用。
	region-Ingestion-Bytes-1yearstore-Other-data-sources	使用一年可延期保留定价选项将其他事件源提取到 CloudTrail Lake 事件数据存储中

CloudTrail 特征	使用情况类型	描述
		的费用。这包括 CloudTrail Insights 事件、来自的配置项目 AWS Config、来自的证据 AWS Audit Manager、从 S3 导入的（未压缩）历史 CloudTrail 日志以及外部的事件。 AWS
	region-QueryScanned-Bytes	运行 CloudTrail Lake 查询的费用。在 CloudTrail Lake 中运行查询时，会根据扫描的优化和压缩数据量收取费用。
CloudTrail 见解	*region*-InsightsEvents	CloudTrail Insights 事件的费用。对于 Insights 事件，您需要根据每种 Insight 类型分析的管理事件数量收取费用。

其他 资源

- AWS CloudTrail 定价
- 管理 CloudTrail 跟踪成本
- 管理 CloudTrail 湖泊成本

处理 CloudTrail 事件历史记录

CloudTrail 默认情况下，您的 AWS 账户已启用，并且您可以自动访问 CloudTrail 活动历史记录。事件历史记录提供对 AWS 区域中过去 90 天发生的管理事件的可查看、可搜索、可下载和不可变记录。这些事件捕获通过 AWS Management Console、、 AWS Command Line Interface、 AWS SDK 和 API 进行的活动。事件历史记录记录了事件 AWS 区域 发生地的事件。查看活动历史记录不 CloudTrail 收取任何费用。

您可以通过查看事件历史记录页面，在 CloudTrail 控制台中按地区查找与创建、修改或删除资源（例如 IAM 用户或 Amazon EC2 实例）相关的事件。 AWS 账户 您也可以通过运行 aws cloudtrail lookup-events 命令或使用 `LookupEvents` API 来查找这些事件。

您可以使用 CloudTrail 控制台中的事件历史记录页面来查看、搜索、下载、存档、分析和响应 AWS 基础架构中的账户活动。选择要在每个页面上显示的事件数量以及要在控制台中显示或隐藏的具体列，您就可以自定义事件历史记录 的视图 。您还可以在事件历史记录中比较事件的详细信息 side-by-side。您可以使用软件开发工具 AWS 包或以编程方式查找事件。 AWS Command Line Interface

> **Note**
>
> 随着时间的推移， AWS 服务 可能会添加其他事件。 CloudTrail 将这些事件记录在事件历史记录中，但是包含已添加事件的 90 天完整活动记录要等到添加事件 90 天后才可用。
> 事件历史记录与您为账户创建的任何跟踪或事件数据存储不相关。对事件数据存储或跟踪所做的更改不会对事件历史记录产生影响。

以下各节介绍如何使用 CloudTrail 控制台和查找最近的管理事件 AWS CLI，并介绍如何下载事件文件。有关使用 `LookupEvents` API 从 CloudTrail 事件中检索信息的信息，请参阅 AWS CloudTrail API 参考LookupEvents中的。

主题

- 事件历史记录的限制
- 使用控制台查看最近的管理事件
- 使用查看最近的管理事件 AWS CLI

事件历史记录的限制

以下限制适用于事件历史记录。

- CloudTrail 控制台上的事件历史记录页面仅显示管理事件。它不显示数据事件或 Insights 事件。
- 事件历史记录仅限于过去 90 天的事件。要持续记录您的事件 AWS 账户，请创建事件数据存储或跟踪。
- 当您从 CloudTrail 控制台的事件历史记录页面下载事件时，可以在单个文件中下载多达 200,000 个事件。如果您达到 200,000 个事件上限，则 CloudTrail 主机将提供下载其他文件的选项。
- 事件历史记录不提供组织级别的事件聚合。要记录整个组织的事件，请创建组织事件数据存储或跟踪。
- 一次事件历史搜索仅限于单个事件 AWS 账户，只能返回单个事件中的事件 AWS 区域，并且不能查询多个属性。您只能应用一个属性筛选条件和一个时间范围筛选条件。

  您可以创建 CloudTrail Lake 事件数据存储来查询多个属性和 AWS 区域。您也可以跨组织 AWS 账户 中的多个 AWS Organizations 组织进行查询。在 CloudTrail Lake 中，您可以查询多种事件类型，包括管理事件、数据事件、Insights 事件、 AWS Config 配置项目、Audit Manager 证据和非 AWS 事件。 CloudTrail 与事件历史记录或运行**`LookupEvents`**中的简单键和值查找相比，Lake 查询提供了更深入、更可自定义的事件视图。有关更多信息，请参阅 与 L AWS CloudTrail ake 合作 和使用控制台为事件创建 CloudTrail事件数据存储。
- 您不能从事件历史记录中排除 AWS KMS 或 Amazon RDS Data API 事件；您应用于跟踪或事件数据存储的设置不适用于事件历史记录。

使用控制台查看最近的管理事件

您可以使用 CloudTrail 控制台中的事件历史记录页面来查看最近 90 天的管理事件 AWS 区域。您也可以下载一个包含该信息的文件，或者根据您选择的筛选条件和时间范围下载一小部分信息。选择要在每个页面上显示的事件数量以及要在控制台中显示的具体列，您就可以自定义事件历史记录的视图。您也可以查找适用于特定服务的事件并按资源类型筛选这些事件。您最多可以在赛事历史记录中选择五个事件并比较它们的详细信息 side-by-side。

Event history（事件历史记录）不显示数据事件。要查看数据事件，请创建事件数据存储或跟踪。

90 天后，事件将不再显示在 Event history (事件历史记录) 中。您不能从 Event history (事件历史记录) 中手动删除事件。

您可以通过查阅特定服务的文档，详细了解如何 CloudTrail 记录该服务的事件的详细信息。有关更多信息，请参阅 AWS 的服务主题 CloudTrail。

> **Note**
>
> 要持续记录过去 90 天的活动和事件，请创建事件数据存储或跟踪。

查看事件历史记录

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择事件历史记录。您会看到一个筛选的事件列表，最新的事件显示在最前面。事件的默认筛选条件是只读的，设置为 false。您可以选择筛选条件右上角的 X 以清除该筛选条件。
3. 您可以根据单个属性筛选事件，您可以从下拉列表中进行选择。要筛选某个属性，请从下拉列表中选择该属性，然后输入该属性的完整值。例如，要查看所有控制台登录事件，请选择事件名称过滤器，然后指定ConsoleLogin。或者，要查看最近的 S3 管理事件，请选择事件源筛选器并指定`s3.amazonaws.com`。
4. 要查看特定管理事件，请选择事件名称。在事件详细信息页面上，您可以查看事件详细信息、任何引用的资源以及事件记录。
5. 比较事件时，可以通过填充 Event history（事件历史记录）表左侧边缘的复选框选择最多五个事件。您可以在比较事件详细信息表 side-by-side 中查看所选事件的详细信息。
6. 您可以采用 CSV 或 JSON 格式的文件进行下载来保存事件历史记录。下载事件历史记录可能需要几分钟。

目录

- 在页面之间导航
- 自定义显示视图
- 筛选 CloudTrail 事件
- 查看事件的详细信息
- 下载事件
- 使用 AWS Config查看引用的资源

在页面之间导航

您可以选择要查看的页面，在事件历史记录的页面之间导航。您还可以在事件历史记录中查看下一页和上一页。

选择 < 可查看事件历史记录的上一页。

选择 > 可查看事件历史记录的下一页。

自定义显示视图

您可以从以下首选项中进行选择，在 CloudTrail 控制台中自定义事件历史记录的视图。

- 页面大小 – 选择要在每页上显示 10 个、25 个还是 50 个事件。
- 换行 – 让文本换行，以便您可以看到每个事件的所有文本。
- 条纹行 – 在表中每隔一行加上阴影。
- 事件时间显示 – 选择是以 UTC 还是本地时区显示事件时间。
- 选择可见列 – 选择要显示的列。默认情况下，将显示以下列：
  - 事件名称
  - 事件时间
  - 用户名
  - 事件源
  - 资源类型
  - 资源名称

> **Note**
>
> 您不能更改列的顺序，也不能从 Event history (事件历史记录) 中手动删除事件。

自定义显示内容

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择事件历史记录。
3. 选择齿轮图标。
4. 在页面大小字段中，选择要在页面上显示的事件数。

5. 选择换行，可查看每个事件的所有文本。
6. 选择条纹行，可在表中每隔一行加上阴影。
7. 在事件时间显示字段中，选择是以 UTC 还是本地时区显示事件时间。默认选择 UTC。
8. 在 Select visible columns（选择可见列）中，选择要显示的列。关闭您不想显示的列。
9. 完成更改后，选择确认。

筛选 CloudTrail 事件

Event history (事件历史记录) 中的事件的默认显示使用属性筛选条件排除已显示事件列表中的只读事件。此属性筛选条件名为 Read only（只读），并且设置为 false。您可以删除此筛选条件以同时显示读取和写入事件。要仅查看 Read（读取）事件，您可以将筛选条件值更改为 true。还可以按其他属性筛选事件。可以按时间范围进一步进行筛选。

> **Note**
>
> 您只能应用一个属性筛选条件和一个时间范围筛选条件。您无法应用多个属性筛选条件。

AWS 访问密钥

用于签署请求的 AWS 访问密钥 ID。如果已使用临时安全证书发出请求，则为临时证书的访问密钥 ID。

事件 ID

事件的 CloudTrail ID。每个事件都有唯一的 ID。

事件名称

事件名称。例如，您可以筛选 IAM 事件（例如 `CreatePolicy`）或 Amazon EC2 事件（例如 `RunInstances`）。

事件源

向其发出请求的 AWS 服务，例如`iam.amazonaws.com`或`s3.amazonaws.com`。在选择 Event source 筛选条件后，您可以滚动浏览事件源的列表。

只读

读取类型的事件。事件分为读取事件或写入事件。如果设置为 false，则已显示事件的列表中不包含读取事件。默认情况下，系统会应用此属性筛选条件并将值设置为 false。

资源名称

事件引用的资源的名称或 ID。例如，Auto Scaling 组的资源名称可能是 “auto-scaling-test-group”，对于 EC2 实例，资源名称可能是 “i-12345678910”。

资源类型

事件引用的资源的类型。例如，资源类型可以是 `Instance` (适用于 EC2) 或 `DBInstance` (适用于 RDS)。每项 AWS 服务的资源类型各不相同。

时间范围

要筛选事件的时间范围。您可以选择相对范围或者绝对范围。您可以筛选最近 90 天的事件。

用户名称

事件引用的身份。例如，这可以是用户、角色名称或服务角色。

如果对于所选属性或时间没有记录事件，结果列表将为空。除时间范围之外，您只能另外应用一个属性筛选条件。如果您选择另一个属性筛选条件，则将保留指定的时间范围。

以下步骤介绍如何按属性筛选。

按属性筛选

1. 要按属性筛选结果，请从 Lookup attributes（查找属性）下拉列表中选择属性，然后在文本框中键入或选择值。
2. 要删除属性筛选条件，请选择该属性筛选条件框右侧的 X。

以下步骤介绍如何按开始日期和时间与结束日期和时间筛选。

按开始日期和时间与结束日期和时间筛选

1. 要缩小您要查看的事件的时间范围，请在时间范围栏中选择时间范围。您可以选择相对范围或者绝对范围。

   选择相对范围从预设值中进行选择，或者选择自定义范围。预设值为 30 分钟、1 小时、12 小时或 1 天。要指定自定义时间范围，请选择 Custom（自定义）。

   选择绝对范围指定明确的开始和结束时间。您还可以在 UTC 和本地时区之间切换。
2. 要删除时间范围筛选条件，请在时间范围栏中选择清除并关闭。

查看事件的详细信息

1. 选择结果列表中的事件以显示其详细信息。
2. 事件中引用的资源显示在事件详细信息页面的 Resources referenced（引用的资源）表格中。
3. 一些引用的资源具有链接。选择该链接可打开此资源的控制台。
4. 滚动到详细信息页面上的 Event record（事件记录）以查看 JSON 事件记录，又称为事件负载。
5. 在页面导航中选择 Event history（事件历史记录）以关闭事件详细信息页面，然后返回 Event history（事件历史记录）。

下载事件

您可以采用 CSV 或 JSON 格式的文件形式下载记录的事件历史记录。你可以在一个文件中下载多达 200,000 个事件。如果您达到 200,000 个事件上限，则 CloudTrail 主机将提供下载其他文件的选项。使用筛选条件和时间范围可减小您下载的文件的大小。

> **Note**
>
> CloudTrail 事件历史文件是包含可由个人用户配置的信息（例如资源名称）的数据文件。有些数据在用来读取和分析该数据的程序中有可能被解释为命令 (CSV 注入)。例如，将 CloudTrail 事件导出为 CSV 并导入到电子表格程序时，该程序可能会警告您注意安全问题。应该选择禁用此内容以保证系统安全。应始终禁用来自下载的事件历史记录文件中的链接或宏。

1. 添加事件的筛选条件和时间范围添加到您要下载的 Event history（事件历史记录）。例如，您可以指定事件名称 `StartInstances`，并指定时间范围为过去 3 天的活动。
2. 选择 Download events（下载事件），然后选择 Download as CSV（下载为 CSV）或 Download as JSON（下载为 JSON）。下载操作会立即开始。

   > **Note**
   >
   > 您的下载可能需要一点时间才能完成。要想更快地获得结果，在开始下载过程前，可使用更加具体的筛选条件或更短的时间范围来缩小结果范围。您可以取消下载。如果取消下载，则在本地计算机上可能会有仅包含某些事件数据的部分下载。要下载完整的事件历史记录，请重新开始下载。

3. 下载完成后，打开文件以查看您指定的事件。

4. 要取消下载，请选择 Cancel（取消），然后选择 Cancel download（取消下载）进行确认。如果您需要重新开始下载，请等到先前的下载完成取消。

使用 AWS Config查看引用的资源

AWS Config 记录配置详细信息、关系以及对 AWS 资源的更改。

在引用资源窗格上，选择AWS Config 资源时间轴列中的，以在 AWS Config 控制台中查看资源。

如果 图标为灰色、 AWS Config 未开启或未记录资源类型。选择图标进入 AWS Config 控制台以开启服务或开始记录该资源类型。有关更多信息，请参阅《AWS Config 开发人员指南》中的 AWS Config 使用控制台进行设置。

如果链接不可用显示在列中，则资源无法查看，原因可能是以下之一：

- AWS Config 不支持该资源类型。有关更多信息，请参阅 AWS Config 开发人员指南中的支持的资源、配置项和关系。
- AWS Config 最近增加了对资源类型的支持，但 CloudTrail 控制台尚未提供该支持。您可以在 AWS Config 控制台中查找资源以查看资源的时间表。
- 该资源归他人所有 AWS 账户。
- 该资源归其他资源所有 AWS 服务，例如托管 IAM 策略。
- 资源创建后被立即删除。
- 资源是最近创建的或在最近更新过。

要授予用户在 AWS Config 控制台中查看资源的只读权限，请参阅授予在 CloudTrail 控制台上查看 AWS Config 信息的权限。

有关的更多信息 AWS Config，请参阅《AWS Config 开发人员指南》。

使用查看最近的管理事件 AWS CLI

您可以使用aws cloudtrail lookup-events命令查找最近 90 天内当前 AWS 区域 的 CloudTrail 管理事件。该aws cloudtrail lookup-events命令显示事件发生 AWS 区域 的地点。

Lookup 支持管理事件的以下属性：

- AWS 访问密钥
- 事件 ID
- 事件名称
- 事件源
- 只读
- 资源名称
- 资源类型
- 用户名称

所有属性是可选的。

lookup-events 命令包含以下选项：

- `--max-items` *<integer>* – 命令的输出中要返回的项目总数。如果可用的总项目数超过指定的值，则命令的输出中会提供 NextToken。要恢复分页，请在后续命令的 starting-token 参数中提供 NextToken 值。请勿在 AWS CLI之外直接使用 NextToken 响应元素。
- `--start-time` *<timestamp>* – 指定仅返回在指定时间之时或之后发生的事件。如果指定的开始时间晚于指定的结束时间，则将返回错误。
- `--lookup-attributes` *<integer>* – 包含查找属性列表。目前，列表只能包含一个项目。
- `--generate-cli-skeleton` *<string>* – 在不发送 API 请求的情况下将 JSON 框架打印到标准输出。如果未提供任何值或值输入，则打印一个可用作 `--cli-input-json` 参数的示例输入 JSON。同理，如果提供了 yaml 输入，则打印一个可与 `--cli-input-yaml` 一起使用的示例输入 YAML。如果提供了值输出，则验证命令输入并返回该命令的示例输出 JSON。生成的 JSON 框架在各版本之间不稳定， AWS CLI 并且生成的 JSON 框架中没有向后兼容性保证。
- `--cli-input-json` *<string>* – 从提供的 JSON 字符串中读取参数。JSON 字符串遵循 `--generate-cli-skeleton` 参数提供的格式。如果命令行中提供了其他参数，这些值会覆盖 JSON 提供的值。无法使用 JSON 提供的值传递任意二进制值，因为会按字面意思处理字符串。这不能与 `--cli-input-yaml` 参数一起指定。

有关使用 AWS 命令行界面的一般信息，请参阅《AWS Command Line Interface 用户指南》。

目录

- 先决条件

- 获取命令行帮助
- 查找事件
- 指定要返回的事件数目
- 按时间范围查找事件
- 按属性查找事件
  - 属性查找示例
- 指定下一页结果
- 从文件中获取 JSON 输入
- 查找输出字段

先决条件

- 要运行 AWS CLI 命令，必须安装 AWS CLI。有关信息，请参阅入门 AWS CLI。
- 确保您的 AWS CLI 版本高于 1.6.6。要验证 CLI 版本，请在命令行上运行 aws --version。
- 要为会 AWS CLI 话设置帐户 AWS 区域、和默认输出格式，请使用aws configure命令。有关更多信息，请参阅配置 AWS 命令行界面。

> **Note**
>
> 这些 CloudTrail AWS CLI 命令区分大小写。

获取命令行帮助

要查看 `lookup-events` 的命令行帮助，请键入以下命令：

```
aws cloudtrail lookup-events help
```

查找事件

> **Important**
>
> 每个区域每个账户查找请求的速率限制为每秒两次。如果超过此限制，则会出现节流错误。

要查看最新的 10 个事件，请键入以下命令：

```
aws cloudtrail lookup-events --max-items 10
```

返回的事件看起来类似于以下虚构示例（为便于阅读，该示例已经过格式编排）：

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
                  \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                  \"eventType\":\"AwsApiCall\",
                  \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```

有关输出中与查找相关的字段的说明，请参阅本文档后面的查找输出字段部分。有关 CloudTrail 事件中字段的说明，请参阅CloudTrail 录制内容。

指定要返回的事件数目

要指定要返回的事件数目，请键入以下命令：

```
aws cloudtrail lookup-events --max-items <integer>
```

可能的值介于 1 和 50 之间。以下示例返回一个事件。

```
aws cloudtrail lookup-events --max-items 1
```

按时间范围查找事件

可查找过去 90 天发生的事件。要指定时间范围，请键入以下命令：

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time <timestamp>` 指定仅返回在指定时间或之后（采用 UTC）发生的事件。如果指定的开始时间晚于指定的结束时间，则将返回错误。

`--end-time <timestamp>` 指定仅返回在指定时间或之前（采用 UTC）发生的事件。如果指定的结束时间早于指定的开始时间，则将返回错误。

默认开始时间为过去 90 天内提供数据的最早日期。默认结束时间为在最接近当前时间发生事件的时间。

所有时间戳均采用 UTC 显示。

按属性查找事件

要按属性进行筛选，请键入以下命令：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

您只能为每个 lookup-events 命令指定一个属性密钥/值对。`AttributeKey` 的有效值如下所示。值的名称区分大小写。

- AccessKeyId
- EventId
- EventName
- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

的最大长度AttributeValue为 2000 个字符。在 2000 个字符限制中，以下字符（_ ,'、'\\n '、'、'）算作两个字符。

属性查找示例

以下示例命令返回 AccessKeyId 值为 AKIAIOSFODNN7EXAMPLE 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

以下示例命令返回指定的事件 CloudTrailEventId。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

以下示例命令返回 EventName 值为 RunInstances 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

以下示例命令返回 EventSource 值为 iam.amazonaws.com 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

以下示例命令返回写入事件。它不包含读取事件（如 GetBucketLocation 和 DescribeStream）。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

以下示例命令返回 ResourceName 值为 CloudTrail_CloudWatchLogs_Role 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

以下示例命令返回 ResourceType 值为 AWS::S3::Bucket 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

以下示例命令返回 Username 值为 root 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

指定下一页结果

要从 lookup-events 命令获取下一页结果，请键入以下命令：

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

其中，*<token>* 的值来自于上一个命令输出的第一个字段。

在命令中使用 --next-token 时，您必须使用与上一个命令中相同的参数。例如，假设您运行以下命令：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

要获取下一页结果，您的下一个命令将如下所示：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

从文件中获取 JSON 输入

AWS CLI 对于某些 AWS 服务，有两个参数，即--generate-cli-skeleton和--cli-input-json，可用于生成 JSON 模板，您可以修改该模板并将其用作--cli-input-json参数的输入。本部分介绍如何将这些参数和 aws cloudtrail lookup-events 结合使用。有关更多常规信息，请参阅AWS CLI 骨架和输入文件。

通过从文件中获取 JSON 输入来查找 CloudTrail 事件

1. 通过将 lookup-events 输出重定向到文件来创建与 --generate-cli-skeleton 结合使用的输入模板，如以下示例所示。

```
aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
```

生成的模板文件（在本例中为 LookupEvents .txt）如下所示：

```
{
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. 可使用文本编辑器根据需要修改 JSON。JSON 输入只能包含指定的值。

> **Important**
>
> 必须先从模板中删除所有空值，然后才能使用该模板。

以下示例指定一个时间范围和要返回的结果的最大数目。

```
{
```

```
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. 要将编辑后的文件用作输入，请使用语法 `--cli-input-json file://<filename>` ，如以下示例所示：

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> 您可在 `--cli-input-json` 所在的命令行中使用其他参数。

查找输出字段

事件

基于查找属性和已指定的时间范围的查找事件的列表。该事件列表按时间进行排序，最新的事件排在第一位。每个条目都包含有关查找请求的信息，并包含检索到 CloudTrail 的事件的字符串表示形式。

以下条目描述每个查找事件中的字段。

CloudTrailEvent

一个包含已返回事件的对象表示形式的 JSON 字符串。有关已返回的每个元素的信息，请参阅记录正文内容。

EventId

一个包含已返回事件的 GUID 的字符串。

EventName

一个包含已返回事件的名称的字符串。

EventSource

向其发出请求的 AWS 服务。

EventTime

事件的日期和时间（采用 UNIX 时间格式）。

资源

由已返回的事件引用的资源列表。每个资源条目指定一个资源类型和一个资源名称。

ResourceName

一个包含由事件引用的资源名称的字符串。

ResourceType

一个包含由事件引用的资源类型的字符串。如果无法确定资源类型，则返回 null。

用户名

一个包含已返回事件的账户用户名称的字符串。

NextToken

用于从上一个 `lookup-events` 命令获取下一页结果的字符串。要使用该令牌，参数必须与原始命令中的参数相同。如果输出中未显示任何 `NextToken` 条目，则不再返回结果。

与 L AWS CloudTrail ake 合作

AWS CloudTrail Lake 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件被聚合到事件数据存储，是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。如果您选择一年可延期保留定价选项，则可以将事件数据在事件数据存储中最多保留 3653 天（大约 10 年）；如果您选择七年保留定价选项，则最多可以保留 2557 天（大约 7 年）。您应用于事件数据存储的选择器控制哪些事件会持续存在并可供您查询。 CloudTrail Lake 是一种审计解决方案，可以补充您的合规堆栈，并帮助您进行近乎实时的故障排除。

CloudTrail 湖泊事件数据存储

在创建事件数据存储时，您可以选择要包括在事件数据存储中的事件的类型。您可以创建事件数据存储以包含来自外部CloudTrail 的事件、CloudTrail Insights 事件、AWS Config 配置项目、AWS Audit Manager 证据或事件 AWS。每个事件数据存储只能包含一个特定的事件类别（例如， AWS Config 配置项目），因为事件架构对于事件类别是唯一的。您可以将来自组织的事件存储 AWS Organizations 在组织事件数据存储中，包括来自多个区域和账户的事件。您还可以使用受支持的 SQL JOIN 关键字跨多个事件数据存储运行 SQL 查询。有关跨多个事件数据存储运行查询的信息，请参阅 高级多表查询支持。

您可以将跟踪事件复制到新的或现有的事件数据存储中，以创建记录到跟踪的事件的 point-in-time 快照。有关更多信息，请参阅 将跟踪事件复制到事件数据存储。

您可以联合事件数据存储以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并使用 Amazon Athena 对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

默认情况下，事件数据存储中的所有事件都由加密 CloudTrail。配置事件数据存储时，可以选择使用自己的 AWS Key Management Service 密钥。使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

您可以通过使用基于标签的授权来控制对事件数据存储的操作的访问。有关更多信息和示例，请参阅本指南中的示例：拒绝基于标签创建或删除事件数据存储的访问权限。

您可以使用 CloudTrail Lake 仪表板对事件数据存储中的数据进行可视化。每个控制面板由多个小组件组成，每个小组件代表一个 SQL 查询。有关 Lake 控制面板的更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

CloudTrail Lake 支持 Amazon CloudWatch 指标，这些指标提供有关摄取的数据和存储字节的信息。有关支持的 CloudWatch 指标的更多信息，请参阅支持的 CloudWatch 指标。

> **Note**
>
> CloudTrail 通常在 API 调用后平均大约 5 分钟内传送事件。此时间并不能得到保证。

CloudTrail 湖泊整合

您可以使用 La CloudTrail ke 集成来记录和存储来自外部的用户活动数据 AWS；这些数据来自混合环境中的任何来源，例如本地或云端托管的内部或 SaaS 应用程序、虚拟机或容器。在 CloudTrail Lake 中创建事件数据存储并创建用于记录活动事件的通道后，您可以调用 `PutAuditEvents` API 将您的应用程序活动引入其中 CloudTrail。然后，您可以使用 CloudTrail Lake 来搜索、查询和分析从您的应用程序中记录的数据。

集成还可以将来自十几个 CloudTrail合作伙伴的事件记录到您的事件数据存储中。在合作伙伴集成中，您可以创建目标事件数据存储、通道和资源策略。在您创建集成后，即可向合作伙伴提供通道 ARN。有两种类型的集成：直接集成和解决方案集成。通过直接集成，合作伙伴可以调用 `PutAuditEvents` API 将事件传送到您 AWS 账户的事件数据存储。通过解决方案集成，应用程序将在您的 AWS 账户中运行，应用程序会调用 `PutAuditEvents` API 将事件传送到您 AWS 账户的事件数据存储。

有关集成的更多信息，请参阅与外部的事件源创建集成。 AWS

CloudTrail 湖泊查询

CloudTrail 与事件历史记录或运行**`LookupEvents`**中的简单键和值查找相比，Lake 查询提供了更深入、更可自定义的事件视图。一次事件历史搜索仅限于单个事件 AWS 账户，只能返回单个事件中的事件 AWS 区域，并且不能查询多个属性。相比之下，L CloudTrail ake 用户可以跨多个事件字段运行复杂的 SQL 查询。 CloudTrail Lake 支持所有有效的 Presto `SELECT` 语句和函数。如需详细了解支持的 SQL 函数和运算符，请参阅 Presto 文档网站中的函数和运算符。

您可以保存 CloudTrail Lake 查询以备将来使用，还可以查看查询结果最长七天。运行查询时，您可以将查询结果保存到 Amazon S3 存储桶。

CloudTrail 控制台提供了许多示例查询，可以帮助您开始编写自己的查询。有关更多信息，请参阅 在 CloudTrail 控制台中查看示例查询。

CloudTrail 湖泊查询会产生费用。在 Lake 中运行查询时，您需要按扫描的数据量付费。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

其他 资源

以下资源可以帮助您更好地了解 CloudTrail Lake 是什么以及如何使用它。

- 使用 L CloudTrail ake 实现审计日志管理现代化（YouTube 视频）
- 记录来自 AWS CloudTrail 湖中非AWS 来源的活动事件（YouTube 视频）
- 使用 La AWS CloudTrail ke 和 Amazon Athen YouTube a 分析活动日志（视频）
- 查看员工和客户身份的活动日志（AWS 博客）
- 使用 L AWS CloudTrail ake 识别与 AWS 服务终端节点的较旧 TLS 连接（AWS 博客）
- Arcti@@ c Wolf 如何使用 AWS CloudTrail Lake 来简化安全和运营（AWS 博客）
- CloudTrail 湖泊常见问题
- AWS CloudTrail API 引用
- AWS CloudTrail 数据 API 参考
- AWS CloudTrail 合作伙伴入职指南

CloudTrail 支持湖泊的区域

目前，以下方面支持 L CloudTrail ake AWS 区域：

区域名称	区域
美国东部（弗吉尼亚州北部）	us-east-1
美国东部（俄亥俄州）	us-east-2
美国西部 (加利福尼亚北部)	us-west-1
美国西部（俄勒冈州）	us-west-2
非洲（开普敦）	af-south-1

区域名称	区域
亚太地区（香港）	ap-east-1
亚太地区（海得拉巴）	ap-south-2
亚太地区（雅加达）	ap-southeast-3
亚太地区（孟买）	ap-south-1
亚太地区（大阪）	ap-northeast-3
亚太地区（首尔）	ap-northeast-2
亚太地区（新加坡）	ap-southeast-1
亚太地区（悉尼）	ap-southeast-2
亚太地区（东京)	ap-northeast-1
加拿大（中部）	ca-central-1
欧洲地区（法兰克福）	eu-central-1
欧洲地区（爱尔兰）	eu-west-1
欧洲地区（伦敦）	eu-west-2
欧洲地区（米兰）	eu-south-1
欧洲地区（巴黎）	eu-west-3
欧洲（西班牙）	eu-south-2
欧洲地区（斯德哥尔摩）	eu-north-1
欧洲（苏黎世）	eu-central-2
以色列（特拉维夫）	il-central-1
中东（巴林）	me-south-1

区域名称	区域
中东（阿联酋）	me-central-1
南美洲（圣保罗）	sa-east-1
AWS GovCloud （美国东部）	us-gov-east-1
AWS GovCloud （美国西部）	us-gov-west-1

有关 CloudTrail 服务终端节点的信息，请参阅AWS CloudTrail 终端节点和配额。

有关 CloudTrail 在中使用的更多信息 AWS GovCloud (US) Regions，请参阅AWS GovCloud (US) 用户指南中的服务终端节点。

CloudTrail 湖泊的概念和术语

本节介绍可帮助您使用 L AWS CloudTrail ake 的关键概念和术语。

概念和术语

- 事件数据存储
- 集成
- 查询
- 控制面板

事件数据存储

事件被聚合到事件数据存储，是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。

您可以创建事件数据存储来记录CloudTrail 管理事件和数据事件、CloudTrail Insights 事件、AWS Audit Manager 证据、AWS Config 配置项目或外部的事件 AWS。

高级事件选择器

> 高级事件选择器决定在事件数据存储中包含哪些事件。高级事件选择器通过仅记录对您来说很重要的事件来帮助您控制成本。

对于管理事件和数据事件，您可以使用高级事件选择器来筛选事件。例如，如果您要创建事件数据存储来收集管理事件，则可以筛选出 AWS Key Management Service (AWS KMS) 或亚马逊关系数据库服务 (Amazon RDS) 数据 API 事件。通常，诸如`Encrypt`、`Decrypt`和之类的 AWS KMS 操作`GenerateDataKey`会生成超过 99% 的事件。

对于 AWS Config 配置项目、Audit Manager 证据或之外的事件 AWS，高级事件选择器仅用于在事件数据存储中包含该类型的事件。

联合身份验证

通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并使用 Amazon Athena 对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。

启用 Lake 查询联合后，将代表您 CloudTrail 创建联合资源并向注册这些资源AWS Lake Formation。启用 Lake 联合身份验证后，您可以直接在 Athena 中查询事件数据，而无需执行任何其他步骤。有关更多信息，请参阅 联合事件数据存储。

定价选项

创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关定价的信息，请参阅 AWS CloudTrail 定价和 管理 CloudTrail 湖泊成本。

保留期

事件数据存储的保留期决定了事件数据在事件数据存储中保存多长时间。 CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。

默认保留期

事件数据存储的默认保留期是事件数据在事件数据存储中保留的默认天数。在事件数据存储的默认保留期内，存储包含在摄取定价中，没有额外费用。在默认保留期过后，存储定价为 pay-as-you-go。

最长保留期

事件数据存储的最长保留期代表您可以在事件数据存储中保留数据的最高天数。

终止保护

默认情况下，事件数据存储将启用终止保护，以防止事件数据存储被意外删除。要删除启用了终止保护的事件数据存储，请从事件数据存储详细信息页面的操作菜单中，选择更改终止保护。然后，您可以继续删除事件数据存储。有关更多信息，请参阅 使用控制台更改终止保护。

集成

您可以使用 CloudTrail Lake 集成来记录和存储来自以下来源的用户活动数据：

- 在外面 AWS
- 混合环境中的任何来源，如本地或云中托管的内部或软件即服务（SaaS）应用程序、虚拟机或容器

集成需要一个通道来传输事件，需要一个事件数据存储来接收事件。设置集成后，调用 PutAuditEventsAPI 操作将您的应用程序活动引入其中 CloudTrail。然后，您可以使用 CloudTrail Lake 来搜索、查询和分析从您的应用程序中记录的数据。有关更多信息，请参阅 与外部的事件源创建集成 AWS。

集成类型

有两种类型的集成：直接集成和解决方案集成。通过直接集成，合作伙伴将调用 `PutAuditEvents` API 操作以将事件传输到您的 AWS 账户的事件数据存储中。通过解决方案集成，应用程序将在您的中运行 AWS 账户 ，应用程序会调用 `PutAuditEvents` API 操作将事件传送到您的 AWS 账户事件数据存储中。

渠道

通过使用渠道将与 CloudTrail您合作的外部合作伙伴或您自己的来源的事件引入 CloudTrail Lake，从而将来自工作之外来源的活动带入 Lake。 AWS 在创建通道时，您可以选择一个或多个事件数据存储，用于存储来自通道来源的事件。只要将目标事件数据存储设置为记录 `eventCategory="ActivityAuditLog"` 事件，即可根据需要更改通道的目标事件数据存储。当您为来自外部合作伙伴的活动创建通道时，您需要向合作伙伴或来源应用程序提供通道 Amazon 资源名称（ARN）。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。附加到该通道的基于资源的策略允许来源通过该通道传输事件。如果通道没有资源策略，则只有通道所有者可以针对该通道调用 `PutAuditEvents` API 操作。有关更多信息，请参阅 AWS CloudTrail 基于资源的策略示例。

查询

La CloudTrail ke 中的@@ 查询是用 SQL 编写的。您可以在 L CloudTrail ake E ditor 选项卡上生成查询，方法是从头开始用 SQL 编写查询，或者打开已保存的查询或示例查询并对其进行编辑。您无法用更改覆盖已包含的示例查询，但可以将其另存为新查询。有关更多信息，请参阅 创建或编辑查询。

CloudTrail Lake 支持所有有效的PrestoSELECT语句和函数。如需详细了解支持的 SQL 函数和运算符，请参阅 Presto 文档网站中的函数和运算符。

控制面板

通过使用 CloudTrail Lake 控制面板，您可以可视化事件数据存储中的事件，并查看事件趋势，例如热门事件 AWS 服务、用户和错误。有关更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

控制面板类型

可用于事件数据存储的控制面板类型取决于事件数据存储的高级事件选择器配置。例如，如果仪表板类型显示有关 CloudTrail 管理事件的信息，则只有当当前选定的事件数据存储收集 CloudTrail 管理事件时，您才能选择该仪表板。

以下是可以的控制面板类型：

- 概述仪表板- AWS 服务 按事件计数显示最活跃的用户。 AWS 区域您还可以查看有关 `read` 和 `write` 管理事件活动、最受限制的事件以及最常出现的错误的信息。此控制面板可用于收集管理事件的事件数据存储。
- 管理事件控制面板 – 按用户显示控制台登录事件、访问被拒事件、破坏性操作和最常出现的错误。您还可以按用户查看有关 TLS 版本和过时的 TLS 调用的信息。此控制面板可用于收集管理事件的事件数据存储。
- S3 数据事件控制面板 – 显示 Amazon S3 账户活动、访问次数最多的 S3 对象、排名靠前的 S3 用户和排名靠前的 S3 操作。此控制面板可用于收集 Amazon S3 数据事件的事件数据存储。
- Insights 事件控制面板 - 按 Insights 类型显示 Insights 事件的总体比例、按 Insights 类型显示主要用户的服务的 Insights 事件比例以及每天的 Insights 事件数量。控制面板还包括一个小部件，可最多列出 30 天的 Insights 事件。此控制面板仅可用于收集 Insights 事件的事件数据存储。

> **Note**
>
> - 首次在源事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。有关更多信息，请参阅 了解 Insights 事件传输情况。
> - Insights 事件控制面板仅显示有关选定事件数据存储收集的 Insights 事件的信息，这些信息由源事件数据存储的配置决定。例如，如果您将源事件数据存储配置为在 `ApiCallRateInsight` 上启用 Insights 事件，而不是 `ApiErrorRateInsight`，则您将不会看到有关 `ApiErrorRateInsight` 上的 Insights 事件的信息。

小组件

小组件是构成控制面板并提供可视化效果的组件，例如折线图或条形图。每个小组件均代表一个基础查询。当您选择 “运行查询” 时，将 CloudTrail 运行系统生成的查询来填充每个小组件的数据。

CloudTrail 湖泊事件数据存储

事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。

在 CloudTrail Lake 中创建事件数据存储时，您可以选择要包含在事件数据存储中的事件类型。您可以创建事件数据存储以包含 CloudTrail数据或管理事件、 CloudTrail Insights 事件、 AWS Config 配置项目或外部的事件 AWS。每种事件数据存储类型只能包含特定的事件类别（例如， AWS Config 配置项目），因为事件架构对于事件类别是唯一的。您可以使用受支持的 SQL JOIN 关键字跨多个事件数据存储运行 SQL 查询。有关跨多个事件数据存储运行查询的信息，请参阅 高级多表查询支持。

下表显示了每种事件数据存储类型支持的事件类别。eventCategory 列显示您在高级事件选择器中指定的值，以收集该类型的事件。

事件类型（控制台）	eventCategory（API）	描述
CloudTrail 事件	`Management` `Data`	此事件数据存储类型可以收集 CloudTrail 管理和数据事件。有关更多信息，请参阅为事件创建事件数据存 CloudTrail 储。
CloudTrail 洞察活动	`Insight`	此事件数据存储类型可以收集 CloudTrail Insights 事件。要接收 Insights 事件，您需要一个用于记录 CloudTrail 管理事件并启用 Insights 的源事件数据存储。有关创建源和目标事件数据存储的信息，请参阅为 CloudTrail Insights 事件创建事件数据存储。
配置项	`ConfigurationItem`	此事件数据存储类型可以收集 AWS Config 配置项目。有关更多信息，请参阅为 AWS Config 配置项目创建事件数据存储。

事件类型（控制台）	eventCategory（API）	描述
来自集成的事件	`ActivityAuditLog`	此事件数据存储类型可以从集成中收集非AWS事件。有关更多信息，请参阅为之外的事件创建事件数据存储 AWS。

您也可以使用 Audit Manager 控制台创建用于 AWS Audit Manager 证据的事件数据存储。有关使用 Audit Manager 在 CloudTrail Lake 中汇总证据的更多信息，请参阅AWS Audit Manager 用户指南中的了解证据查找器如何与 CloudTrail Lake 配合使用。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

以下各节介绍如何创建、更新和管理事件数据存储。

主题

- 使用控制台创建、更新和管理事件数据存储
- 使用创建、更新和管理事件数据存储 AWS CLI
- 管理事件数据存储生命周期
- 将跟踪事件复制到事件数据存储
- 联合事件数据存储
- 组织事件数据存储

使用控制台创建、更新和管理事件数据存储

您可以使用 CloudTrail 控制台创建、更新和管理您的事件数据存储。您还可以在事件数据存储上启动和停止事件提取，并使用控制台启用 Lake 查询联合。

使用 CloudTrail 控制台创建或更新事件数据存储具有以下优势：

- 如果这是您第一次创建事件数据存储，则使用 CloudTrail 控制台可以查看可用的功能和选项。
- 如果您正在配置事件数据存储以记录数据事件，则使用 CloudTrail 控制台可以查看可用的数据类型。有关更多信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储 和 记录数据事件。

- 如果您正在配置事件数据存储以记录外部的事件 AWS，则使用 CloudTrail 控制台可以查看有关可用合作伙伴的信息。有关更多信息，请参阅 使用控制台为外部的事件创建事件数据存储 AWS。

主题

- 使用控制台为事件创建 CloudTrail事件数据存储
- 使用控制台为 CloudTrail Insights 事件创建事件数据存储
- 使用控制台为 AWS Config 配置项目创建事件数据存储
- 使用控制台为外部的事件创建事件数据存储 AWS
- 使用控制台更新事件数据存储
- 使用控制台停止和启动事件提取
- 使用控制台更改终止保护
- 使用控制台删除事件数据存储
- 使用控制台恢复事件数据存储

使用控制台为事件创建 CloudTrail事件数据存储

事件 CloudTrail 的事件数据存储可以记录 CloudTrail 管理和数据事件。如果您选择一年可延期保留定价选项，则可以将事件数据在事件数据存储中最多保留 3653 天（大约 10 年）；如果您选择七年保留定价选项，则最多可以保留 2557 天（大约 7 年）。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

为 CloudTrail 管理事件或数据事件创建事件数据存储

使用此过程创建用于记录 CloudTrail 管理事件、数据事件或同时记录管理和数据事件的事件数据存储。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 Configure event data store（配置事件数据存储）页面上的 General details（一般细节）中，输入事件数据存储的名称。名称为必填项。

5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天

6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。

   > **Note**
   >
   > 如果您要将跟踪事件复制到此事件数据存储中，则 CloudTrail 不会复制超过指定保留期的事件。`eventTime`要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`*）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。

7. （可选）要使用启用加密 AWS Key Management Service，请选择使用我自己的加密 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

> **Note**
>
> 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在 Tags（标签）部分中，您最多可以添加 50 个标签键对，以帮助您对事件数据存储的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

11. 在 “选择事件” 页面上，选择AWS 事件，然后选择CloudTrail事件。

12. 对于CloudTrail 事件，请至少选择一种事件类型。默认情况下，已选中 Management events（管理事件）。您可以将管理事件和数据事件添加到事件数据存储中。有关管理事件的更多信息，请参阅 记录管理事件。有关数据事件的更多信息，请参阅 记录数据事件。

13. （可选）如果要从现有跟踪中复制事件以对过往事件运行查询，请选择 Copy trail events（复制跟踪事件）。要将跟踪事件复制到组织事件数据存储，必须使用该组织的管理账户。委托管理员账户无法将跟踪事件复制到组织事件数据存储。有关复制跟踪事件注意事项的更多信息，请参阅 复制跟踪事件的注意事项。

14. 要让您的事件数据存储收集 AWS Organizations 企业中所有账户的事件，请选择 Enable for all accounts in my organization（为我的企业中的所有账户启用）。您必须登录到组织的管理账户或委托管理员账户，才能创建为组织收集事件的事件数据存储。

    > **Note**
    >
    > 要复制跟踪事件或启用 Insights 事件，您必须登录组织的管理账户。

15. 展开其他设置以选择是希望事件数据存储收集所有 AWS 区域事件还是仅收集当前事件 AWS 区域，并选择事件数据存储是提取事件。默认情况下，您的事件数据存储会收集您账户中所有区域的事件，并在事件创建后开始摄取事件。

    a. 选择在我的事件数据存储中仅包含当前区域，以便仅包含在当前区域中记录的事件。如果不选择此选项，则您的事件数据存储将包含来自所有区域的事件。

    b. 如果您不希望事件数据存储开始摄取事件，请取消选择摄取事件。例如，如果您要复制跟踪事件并且不希望事件数据存储包含任何未来事件，则可能需要取消选择摄取事件。默认情况下，事件数据存储会在创建事件时开始摄取事件。

16. 如果您的事件数据存储包括管理事件，您可以从以下选项中进行选择。有关管理事件的更多信息，请参阅 记录管理事件。

    a. 选择是要包括读取事件、写入事件，还是两者兼而有之。至少需要选择一个选项。

    b. 选择是从您的事件数据存储中排除 AWS Key Management Service Amazon RDS 数据 API 事件。

    c. 选择是否启用 Insights。要启用 Insights，您需要设置目标事件数据存储来将根据该事件数据存储中的管理事件活动收集 Insights 事件。

       如果您选择启用 Insights，请执行以下操作。

       i. 在启用 Insights 中，选择将记录 Insights 事件的目标事件存储。目标事件数据存储将根据该事件数据存储中的管理事件活动收集 Insights 事件。有关如何创建目标事件数据存储的信息，请参阅 要创建记录 Insights 事件的目标事件数据存储。

       ii. 选择 Insights 类型。您可以选择 API 调用率、API 错误率或同时选择此两者。您必须记录写入管理事件，以针对 API 调用率记录 Insights 事件。您必须记录读取或写入管理事件，以针对 API 错误率记录 Insights 事件。

17. 要在事件数据存储中包含数据事件，请执行以下操作。

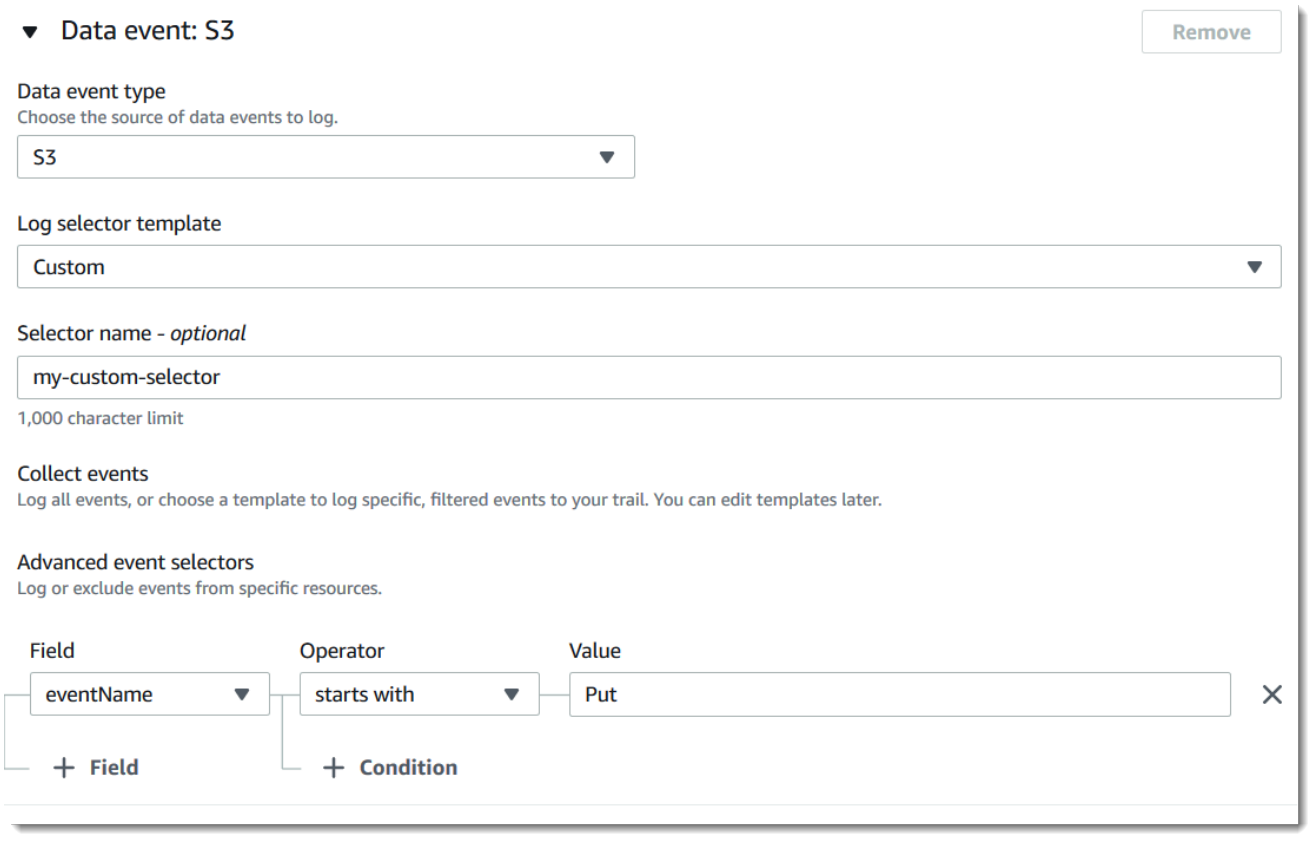
a. 选择数据事件类型。这是记录数据事件的 AWS 服务 和资源。要记录由 Lake Formation 创建的 AWS Glue 表的数据事件，请为数据类型选择 Lake Formation。

b. 在 Log selector template（日志选择器模板）中，选择一个模板。您可以选择记录所有数据事件、`readOnly` 事件、`writeOnly` 事件，或者通过 Custom（自定义）来构建自定义日志选择器。

c. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 `Name`，展开 JSON 视图即可查看该名称。

d. 在 Advanced event selectors（高级事件选择器）中，通过为 Field（字段）、Operator（运算符）和 Value（值）选择值来构建表达式。事件数据存储的高级事件选择器的工作方式与应用于跟踪记录的高级事件选择器相同。有关如何构建高级事件选择器的更多信息，请参阅[使用高级事件选择器筛选数据事件]。

   以下示例使用 Custom（自定义）日志选择器模板，以从 S3 对象中选择仅以 `Put` 开头的事件名称，例如 `PutObject`。由于高级事件选择器不包括或排除任何其他事件类型或资源 ARN，因此以 `Put` 开头的所有 S3 数据事件（包括读取和写入），均存储在事件数据存储中。



> **Important**
>
> 要使用 S3 存储桶 ARN 排除或包括高级事件选择器中的数据事件，请始终使用 Starts with 运算符。

e. 或者，展开 JSON 视图将您的高级事件选择器作为 JSON 数据块查看。

f. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。重复步骤 a 至此步骤，为数据事件类型配置高级事件选择器。

18. 要将现有跟踪事件复制到您的事件数据存储，请执行以下操作。

a. 选择要复制的跟踪。默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的前缀，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，请选择 Enter S3 URI，然后选择 Browse S3 浏览到该前缀。如果跟踪的源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密数据。如果您的源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。有关更新 KMS 密钥政策的更多信息，请参阅[用于解密源 S3 存储桶中数据的 KMS 密钥政策](#)。

b. 选择复制事件的时间范围。 CloudTrail 在尝试复制跟踪事件之前，请检查前缀和日志文件名以验证该名称是否包含所选开始日期和结束日期之间的日期。您可以选择 Relative range（相对范围）或者 Absolute range（绝对范围）。为避免源跟踪和目标事件数据存储之间存在重复事件，请选择一个早于事件数据存储创建时间的时间范围。

> **Note**
>
> CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。例如，如果事件数据存储的保留期为 90 天，则 CloudTrail 不会复制任何`eventTime`超过 90 天的跟踪事件。

- 如果选择 “相对范围”，则可以选择复制过去 6 个月、1 年、2 年、7 年或自定义范围内记录的事件。 CloudTrail 复制选定时间段内记录的事件。
- 如果选择 “绝对范围”，则可以选择特定的开始和结束日期。 CloudTrail 复制在所选开始日期和结束日期之间发生的事件。

c. 对于 Permissions（权限），请从以下 IAM 角色选项中进行选择。如果您选择现有的 IAM 角色，请验证 IAM 角色策略是否提供了必要的权限。有关更新 IAM 角色权限的更多信息，请参阅[复制跟踪事件所需的 IAM 权限](#)。

- 选择 Create a new role (recommended)（创建新角色（推荐））以创建新的 IAM 角色。在输入 IAM 角色名称中，输入角色的名称。 CloudTrail 会自动为这个新角色创建必要的权限。
- 选择使用自定义 IAM 角色 ARN 以使用未列出的自定义 IAM 角色。对于 Enter IAM role ARN（输入 IAM 角色 ARN），输入 IAM ARN。
- 从下拉列表中选择现有的 IAM 角色。

19. 选择 Next（下一步）以查看您的选择。
20. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
21. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

    从现在开始，事件数据存储将捕获与其高级事件选择器匹配的事件（如果保持选中摄取事件选项）。除非选择复制现有跟踪事件，否则在创建事件数据存储之前发生的事件不会出现在该事件数据存储中。

现在，您可以对新的事件数据存储运行查询。Sample queries（示例查询）选项卡提供了示例查询，以帮助您入门。有关创建和编辑查询的更多信息，请参阅创建或编辑查询。

您还可以查看 CloudTrail Lake 仪表板以可视化事件数据存储中的事件。有关 Lake 控制面板的更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

示例：为管理事件创建事件数据存储

本演练向您展示了如何创建事件数据存储，该存储可以记录所有 AWS 区域的所有管理事件，并且不记录任何数据事件。管理事件的示例包含安全事件（如 IAM `CreateUser` 和 `AttachRolePolicy` 事件）、资源事件（如 `RunInstances` 和 `CreateBucket`），等等。

为管理事件创建事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 “配置事件数据存储” 页面的 “常规详细信息” 中，为您的事件数据存储命名，例如*`my-management-events-eds`*。作为最佳实践，请使用可快速识别事件数据存储用途的名称。有关 CloudTrail 命名要求的信息，请参见命名要求。

5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。
7. （可选）在加密中，选择是否要使用自己的 KMS 密钥加密事件数据存储。默认情况下，事件数据存储中的所有事件都 CloudTrail 使用为您 AWS 拥有和管理的 KMS 密钥进行加密。

   要使用自己的 KMS 密钥进行加密，请选择使用我自己的 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail 日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

> **Note**
>
> 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

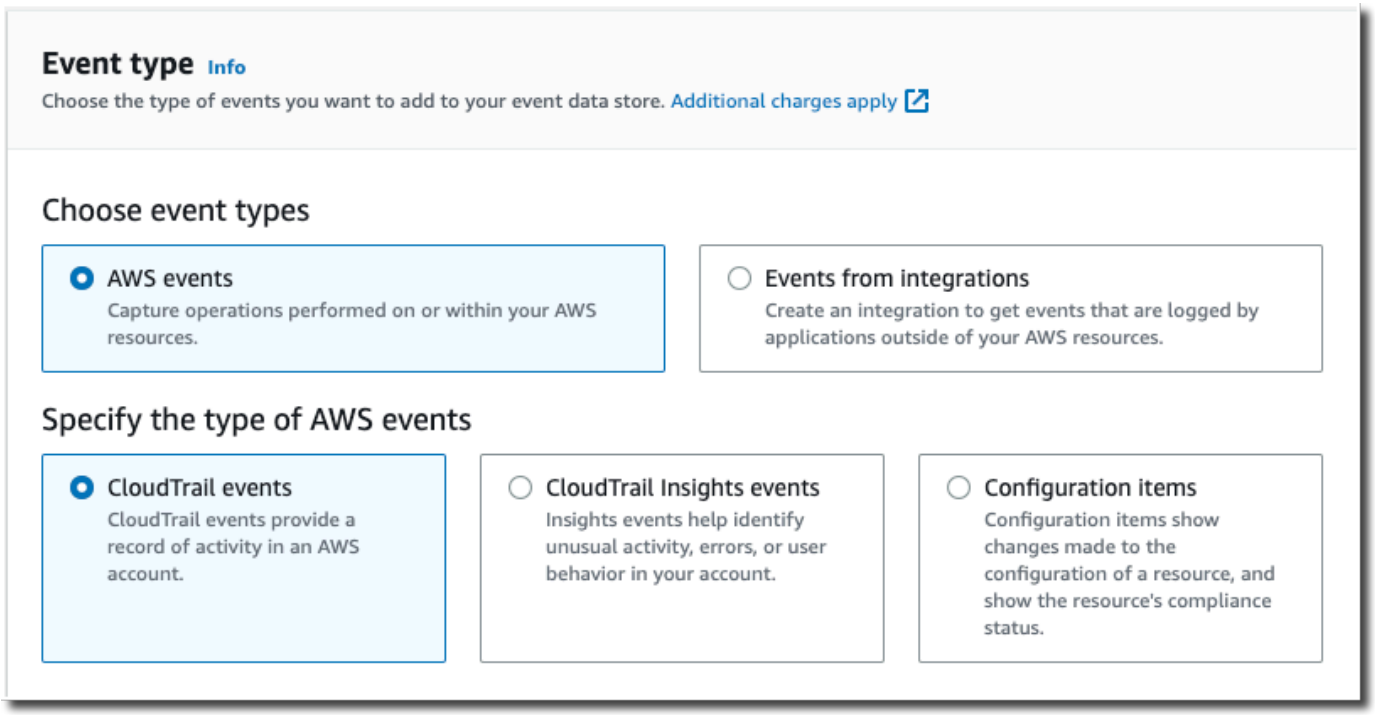
   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在标签中，将一个或多个自定义标签（键值对）添加到事件数据存储中。标签可以帮助您识别您的 CloudTrail 事件数据存储。例如，您可以附加名称为 **`stage`**、值为 **`prod`** 的标签。您可以使用标签来限制对事件数据存储的访问。您还可以使用标签来跟踪事件数据存储的查询和摄取成本。

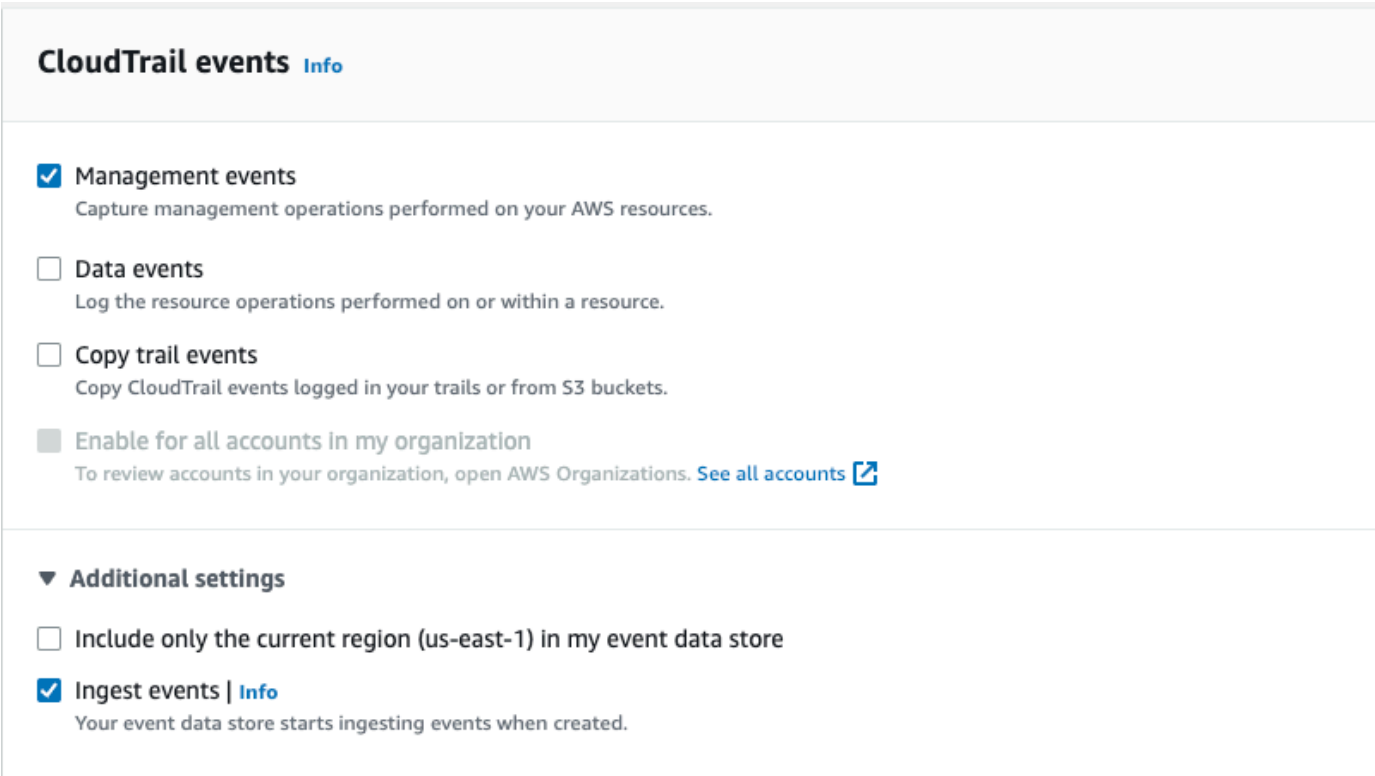
   有关如何使用标签跟踪成本的信息，请参阅 为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签。有关如何使用 IAM 策略根据标签授权对事件数据存储的访问，请参阅 示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

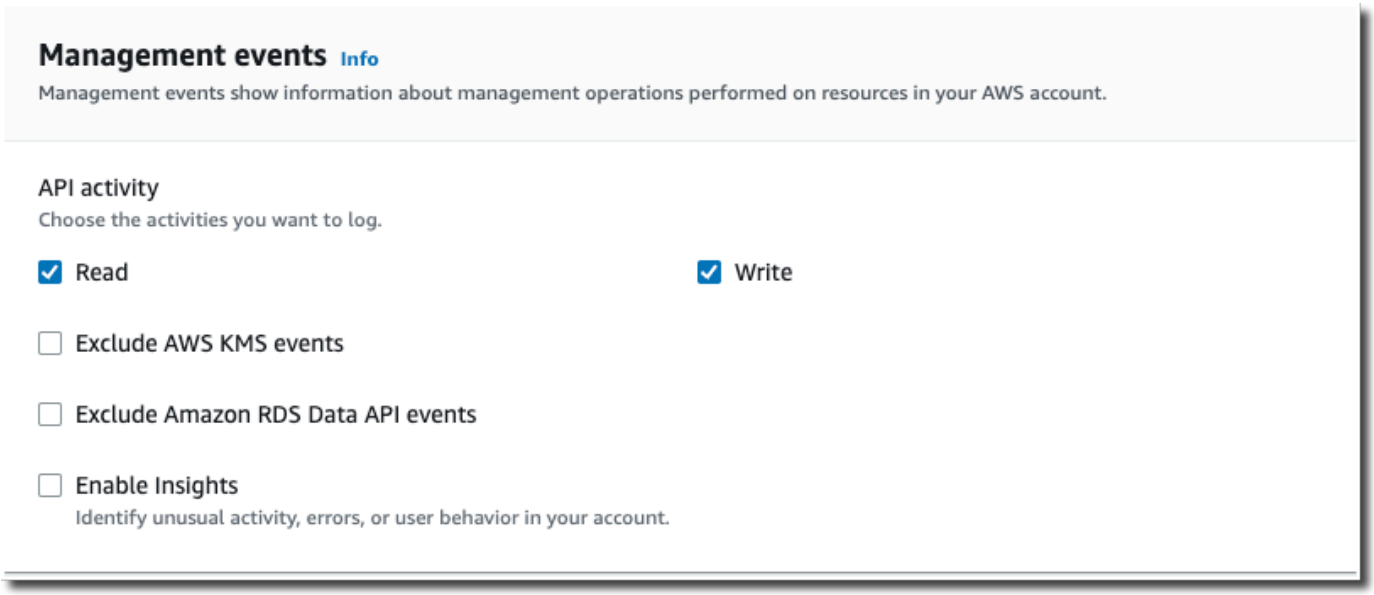
11. 在选择事件页面上，保留事件类型的默认选择。



12. 对于CloudTrail 事件，请保留默认选项。默认情况下， CloudTrail 事件数据存储会收集管理事件，而不收集数据事件。有关管理事件的更多信息，请参阅 记录管理事件。有关数据事件的更多信息，请参阅 记录数据事件。



13. 保留复制跟踪事件的默认设置。您可以使用此选项将现有的跟踪事件复制到事件数据存储。有关更多信息，请参阅 将跟踪事件复制到事件数据存储。
14. 如果这是组织事件数据存储，请选择为我组织中的所有账户启用。除非您在 AWS Organizations中配置了账户，否则此选项将不能进行更改。
15. 对于其他设置，请保留默认选择。默认情况下，事件数据存储会收集所有人的事件， AWS 区域并在创建事件时开始摄取事件。
16. 对于管理事件，选择同时收集读取与写入事件。将 “排除 AWS KMS 事件” 和 “排除 Amazon RDS 数据 API 事件” 复选框留空，以收集所有管理事件。将启用 Insights 事件复选框留空。



17. 选择 Next（下一步）以查看您的选择。
18. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
19. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

    从现在开始，事件数据存储将捕获与其高级事件选择器匹配的事件。除非选择复制现有跟踪事件，否则在创建事件数据存储之前发生的事件不会出现在该事件数据存储中。

示例：为 S3 数据事件创建事件数据存储

本演练向您展示如何为 Amazon S3 数据事件创建事件数据存储。在这种情况下，我们将不记录所有 Amazon S3 数据事件，而是选择自定义日志选择器模板来仅在从特定 S3 存储桶中删除对象时记录事件。

为 CloudTrail 数据事件创建事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在配置事件数据存储页面上，在常规详细信息中，为您的事件数据存储命名，例如 *s3-data-events-eds*。作为最佳实践，请使用可快速识别事件数据存储用途的名称。有关 CloudTrail 命名要求的信息，请参见命名要求。
5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。
7. （可选）在加密中，选择是否要使用自己的 KMS 密钥加密事件数据存储。默认情况下，事件数据存储中的所有事件都 CloudTrail 使用为您 AWS 拥有和管理的 KMS 密钥进行加密。

   要使用自己的 KMS 密钥进行加密，请选择使用我自己的 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail 日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

> **Note**
>
> 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

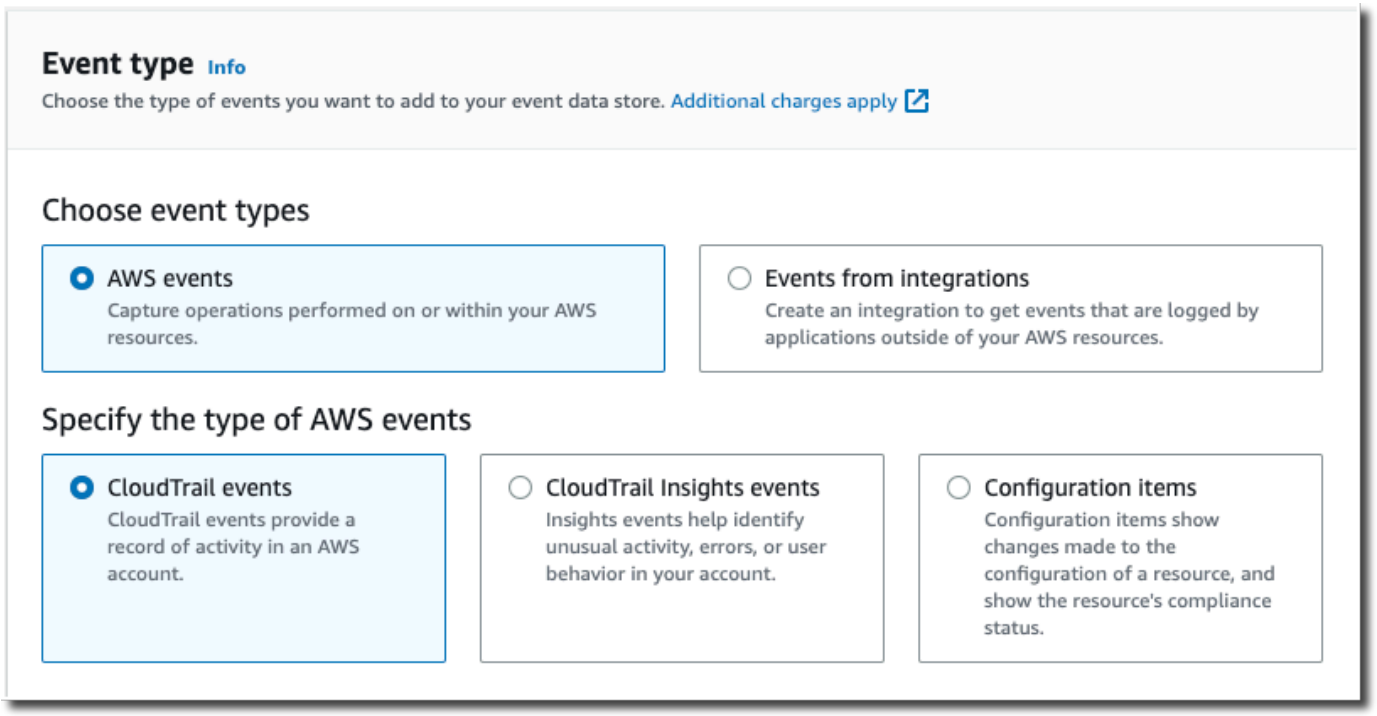
   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在标签中，将一个或多个自定义标签（键值对）添加到事件数据存储中。标签可以帮助您识别您的 CloudTrail 事件数据存储。例如，您可以附加名称为 **`stage`**、值为 **`prod`** 的标签。您可以使用标签来限制对事件数据存储的访问。您还可以使用标签来跟踪事件数据存储的查询和摄取成本。

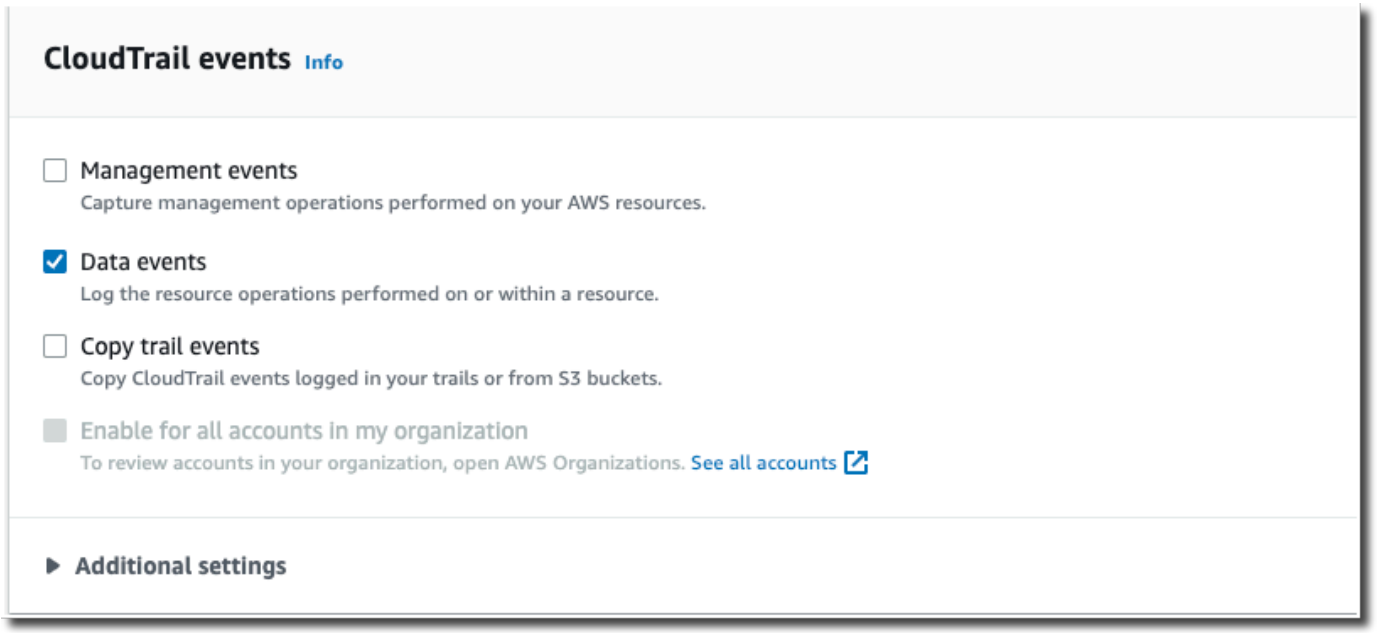
   有关如何使用标签跟踪成本的信息，请参阅 为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签。有关如何使用 IAM 策略根据标签授权对事件数据存储的访问，请参阅 示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

11. 在选择事件页面上，保留事件类型的默认选择。



12. 对于CloudTrail 事件，请选择数据事件并取消选择管理事件。有关数据事件的更多信息，请参阅记录数据事件。



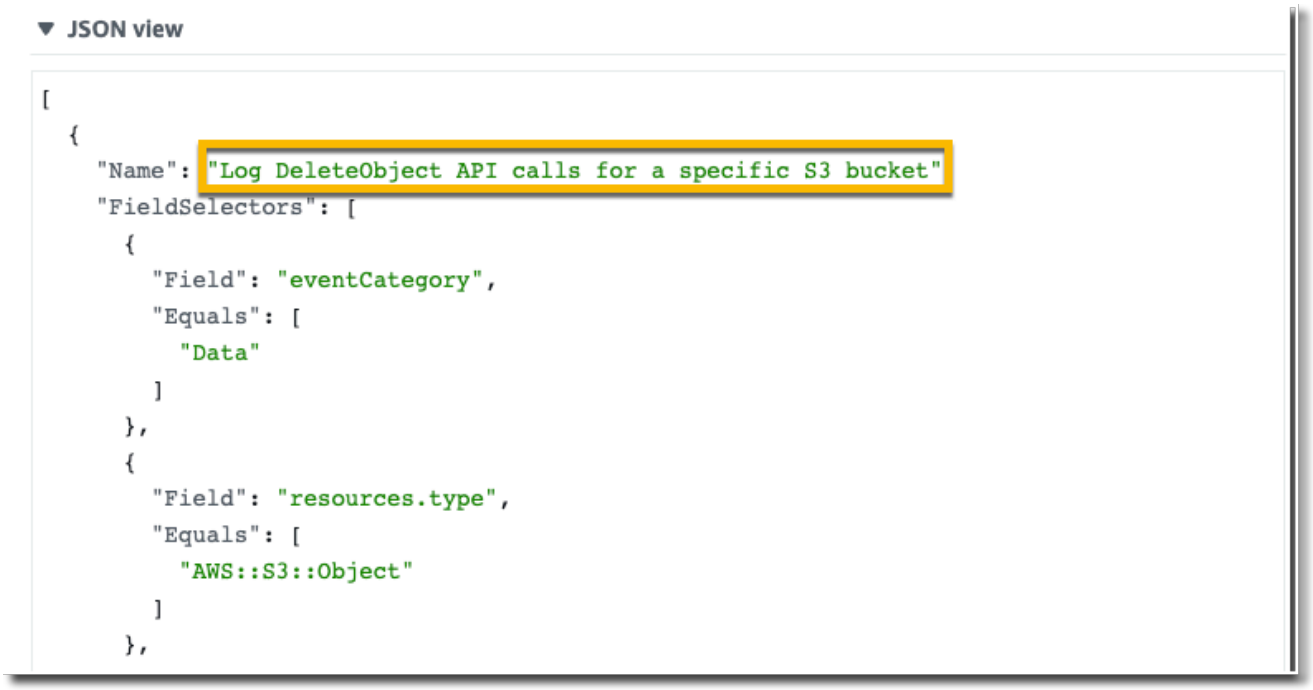
13. 保留复制跟踪事件的默认设置。您可以使用此选项将现有的跟踪事件复制到事件数据存储。有关更多信息，请参阅 将跟踪事件复制到事件数据存储。
14. 如果这是组织事件数据存储，请选择为我组织中的所有账户启用。除非您在 AWS Organizations中配置了账户，否则此选项将不能进行更改。

15. 对于其他设置，请保留默认选择。默认情况下，事件数据存储会收集所有人的事件， AWS 区域并在创建事件时开始摄取事件。
16. 对于数据事件，请进行下列选择：

    a. 在数据事件类型中，选择 S3。数据事件类型用于标识记录数据事件的 AWS 服务 和资源。

    b. 在日志选择器模板中，选择自定义。选择自定义可定义自定义事件选择器来按 `eventName`、`resources.ARN` 和 `readOnly` 字段进行筛选。有关这些字段的信息，请参阅 AWS CloudTrail API 参考AdvancedFieldSelector中的。

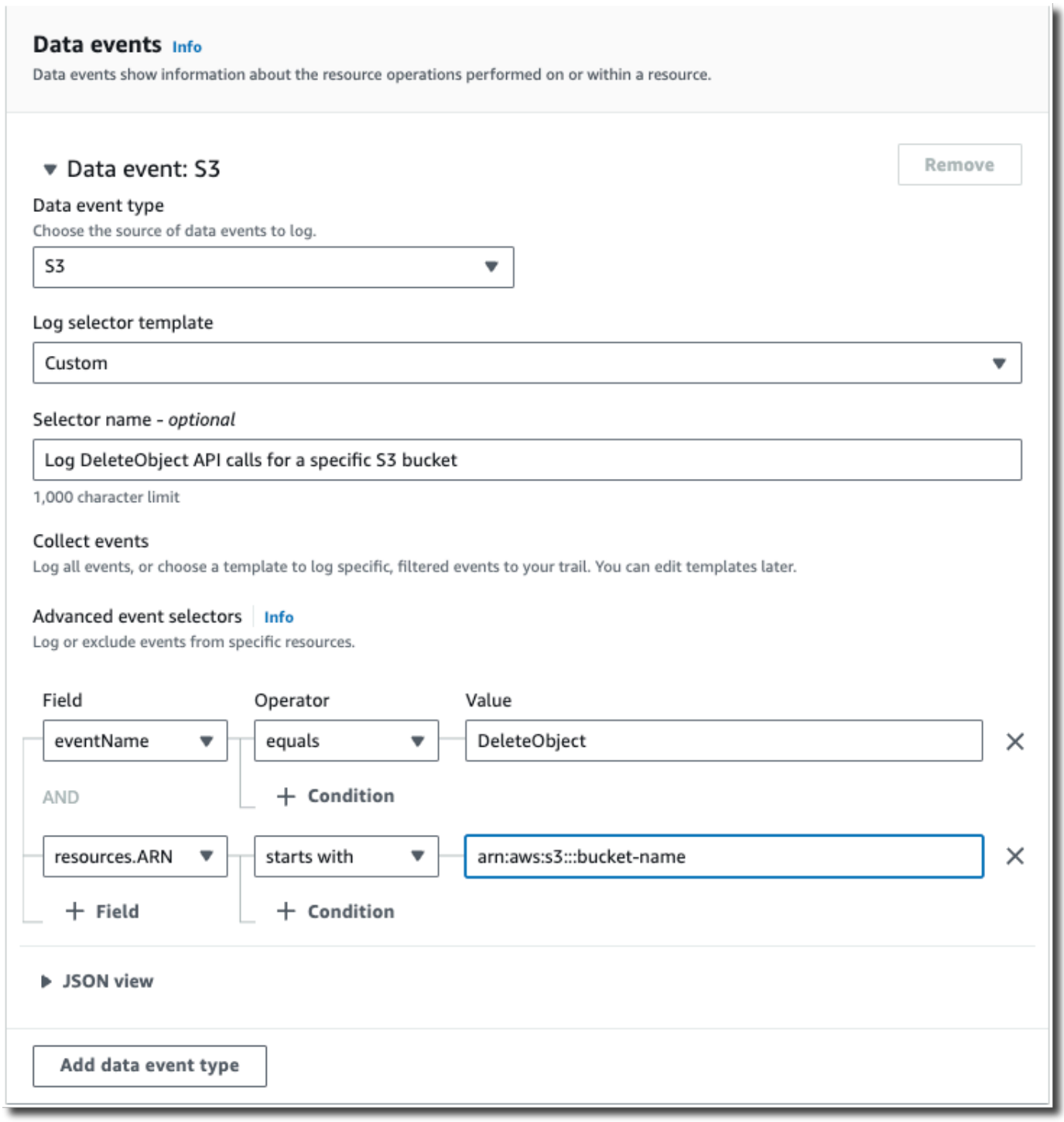
    c. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如 “记录特定 S3 存储桶 DeleteObject 的 API 调用”。选择器名称在高级事件选择器中列为 `Name`，展开 JSON 视图即可查看该名称。



    d. 在高级事件选择器中，我们将构建自定义事件选择器来筛选`eventName`和`resources.ARN`字段。事件数据存储的高级事件选择器的工作方式与应用于跟踪记录的高级事件选择器相同。有关如何构建高级事件选择器的详细信息，请参阅使用高级事件选择器记录数据事件。

        i. 对于字段，选择 eventName。对于运算符，选择 equals。对于值，请输入 **`DeleteObject`**。选择 + 字段可筛选其他字段。

        ii. 对于字段，选择 resources.ARN。对于 “操作员”，选择StartsWith。对于值，输入存储桶的 ARN（例如 *`arn:aws:s3:::bucket-name`*）。有关如何获取 ARN 的信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 资源。



17. 选择 Next（下一步）以查看您的选择。
18. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
19. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

从现在开始，事件数据存储将捕获与其高级事件选择器匹配的事件。除非选择复制现有跟踪事件，否则在创建事件数据存储之前发生的事件不会出现在该事件数据存储中。

使用控制台为 CloudTrail Insights 事件创建事件数据存储

AWS CloudTrail Insights 通过持续分析 CloudTrail 管理事件，帮助 AWS 用户识别和响应与 API 调用和 API 错误率相关的异常活动。 CloudTrail Insights 会分析您的 API 调用量和 API 错误率的正常模式（也称为基线），并在呼叫量或错误率超出正常模式时生成 Insights 事件。针对 `write` 管理 API 生成的 API 调用量的 Insights 事件，以及针对 `read` 和 `write` 管理 API 生成的 API 错误率的 Insights 事件。

要在 L CloudTrail ake 中记录 Insights 事件，您需要一个用于记录 Insights 事件的目标事件数据存储和一个启用 Insights 并记录管理事件的源事件数据存储。

> **Note**
>
> 要针对 API 调用量记录 Insights 事件，源事件数据存储必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，源事件数据存储必须记录 `read` 或 `write` 管理事件。

如果您在源事件数据存储上启用了 CloudTrail Insights 并 CloudTrail 检测到异常活动，则会将 Insigh CloudTrail ts 事件传送到您的目标事件数据存储。与事件数据存储中捕获的其他类型的事件不同，Insights 事件仅在 CloudTrail 检测到您的账户 API 使用情况与账户的典型使用模式明显不同时，才会记录 Insights 事件。 CloudTrail

首次在事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。

CloudTrail Insights 分析发生在单个区域（而不是全球区域）的管理事件。 CloudTrail Insights 事件是在生成其支持管理事件的同一区域生成的。

对于组织事件数据存储， CloudTrail 分析来自每个成员账户的管理事件，而不是分析组织所有管理事件的聚合。

在 Lake 中 CloudTrail 收取 Insights 事件需要支付额外费用。如果您同时为路径和 CloudTrail 湖泊事件数据存储启用 Insights，则需要单独付费。有关 CloudTrail 定价的信息，请参阅AWS CloudTrail 定价。

主题

- 要创建记录 Insights 事件的目标事件数据存储
- 要创建启用 Insights 事件的源事件数据存储

要创建记录 Insights 事件的目标事件数据存储

创建 Insights 事件数据存储时，您可以选择用于记录管理事件的现有源事件数据存储，然后指定要接收的 Insights 类型。或者，您可以在创建 Insights 事件数据存储后在新的或现有的事件数据存储上启用 Insights，然后选择此事件数据存储作为目标事件数据存储。

此过程向您演示如何创建记录 Insights 事件的目标事件数据存储。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，打开 Lake（湖）子菜单，然后选择 Event data stores（事件数据存储）。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 Configure event data store（配置事件数据存储）页面上的 General details（一般细节）中，输入事件数据存储的名称。名称为必填项。
5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期（以天为单位）。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。事件数据存储将保留指定天数内的事件数据。

7. （可选）要使用启用加密 AWS Key Management Service，请选择使用我自己的加密 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/MyAliasName`。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

   > **Note**
   >
   > 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在 Tags（标签）部分中，您最多可以添加 50 个标签键对，以帮助您对事件数据存储的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

11. 在 “选择事件” 页面上，选择AWS 事件，然后选择 CloudTrailInsights 事件。

12. 在 CloudTrail Insights 事件中，执行以下操作。

a. 如果您要向组织的委托管理员授予对此事件数据存储的访问权限，请选择允许委托管理员访问权。只有当您使用 AWS Organizations 组织的管理账户登录时，此选项才可用。

b. （可选）选择用于记录管理事件的现有源事件数据存储，并指定要接收的 Insights 类型。

要添加源事件数据存储，请执行以下操作。

i. 选择添加源事件数据存储。

ii. 选择源事件数据存储。

iii. 选择要接收的 Insights 类型。

- `ApiCallRateInsight` – `ApiCallRateInsight` Insights 类型根据基准 API 调用量分析每分钟汇总的只写管理 API 调用。要接收关于 `ApiCallRateInsight` 的 Insights，源事件数据存储必须记录写入管理事件。
- `ApiErrorRateInsight` – `ApiErrorRateInsight` Insights 类型分析生成错误代码的管理 API 调用。如果 API 调用不成功，就会显示错误。要接收关于 `ApiErrorRateInsight` 的 Insights，源事件数据存储必须记录写入或读取管理事件。

iv. 重复前两个步骤（ii 和 iii），以添加您想要接收的任何其他 Insights 类型。

13. 选择 Next（下一步）以查看您的选择。
14. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
15. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。
16. 如果您没有在步骤 10 中选择源事件数据存储，请按照 要创建启用 Insights 事件的源事件数据存储 中的步骤创建源事件数据存储。

要创建启用 Insights 事件的源事件数据存储

此过程向您演示如何创建启用 Insights 事件和记录管理事件的源事件数据存储。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，打开 Lake（湖）子菜单，然后选择 Event data stores（事件数据存储）。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 Configure event data store（配置事件数据存储）页面上的 General details（一般细节）中，输入事件数据存储的名称。名称为必填项。

5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。
7. （可选）要使用启用加密 AWS Key Management Service，请选择使用我自己的加密 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

   > **Note**
   >
   > 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。
8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元

数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

b. 如果您在创建新角色，请输入名称来标识该角色。

c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在 Tags（标签）部分中，您最多可以添加 50 个标签键对，以帮助您对事件数据存储的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

11. 在 “选择事件” 页面上，选择AWS 事件，然后选择CloudTrail事件。

12. 在CloudTrail 事件中，将管理事件保留为选中状态。

13. 要让您的事件数据存储收集 AWS Organizations 企业中所有账户的事件，请选择 Enable for all accounts in my organization（为我的企业中的所有账户启用）。您必须登录组织的管理账户，才能创建启用 Insights 解的事件数据存储。

14. 展开其他设置以选择是希望事件数据存储收集所有 AWS 区域事件还是仅收集当前事件 AWS 区域，并选择事件数据存储是提取事件。默认情况下，您的事件数据存储会收集您账户中所有区域的事件，并在事件创建后开始摄取事件。

    a. 如果您想要仅包含在当前区域中记录的事件，选择在我的事件数据存储中仅包含当前区域。如果不选择此选项，则您的事件数据存储将包含来自所有区域的事件。

    b. 将摄取事件保留为选中状态。

15. 选择要包含在事件数据存储中的管理事件的类型。您可以选择读取、写入或同时选择此两者。至少需要选择一个选项。

> **Note**
>
> 要针对 API 调用量记录 Insights 事件，事件数据存储必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，事件数据存储必须记录 `read` 或 `write` 管理事件。

16. 您可以选择从事件数据存储中排除 AWS Key Management Service Amazon RDS 数据 API 事件。有关这些选项的详细信息，请参阅 记录管理事件。
17. 选择启用 Insights。
18. 在启用 Insights 中，选择将记录 Insights 事件的目标事件存储。目标事件数据存储将根据该事件数据存储中的管理事件活动收集 Insights 事件。有关如何创建目标事件数据存储的信息，请参阅 要创建记录 Insights 事件的目标事件数据存储。
19. 选择 Insights 类型。您可以选择 API 调用率、API 错误率或同时选择此两者。您必须记录写入管理事件，以针对 API 调用率记录 Insights 事件。您必须记录读取或写入管理事件，以针对 API 错误率记录 Insights 事件。
20. 选择 Next（下一步）以查看您的选择。
21. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
22. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

    从现在开始，事件数据存储将捕获与其高级事件选择器匹配的事件。首次在源事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最多可能需要 7 天才能 CloudTrail 将第一个 Insights 事件传送到目标事件数据存储。

    您可以查看 CloudTrail Lake 仪表板以可视化目标事件数据存储中的 Insights 事件。有关 Lake 控制面板的更多信息，请参阅 查看 CloudTrail 湖泊仪表板。

在 Lake 中 CloudTrail 收取 Insights 事件需要支付额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关 CloudTrail 定价的信息，请参阅AWS CloudTrail 定价。

使用控制台为 AWS Config 配置项目创建事件数据存储

您可以创建事件数据存储以包含 AWS Config 配置项目，并使用事件数据存储来调查对生产环境的不合规更改。通过事件数据存储，您可以将不合规的规则与跟更改相关的用户和资源关联起来。配置项目表示您的账户中存在的受支持 AWS 资源的属性的 point-in-time 视图。 AWS Config 每当它检测到正在记录的资源类型发生变化时，都会创建一个配置项目。 AWS Config 还会在捕获配置快照时创建配置项目。

您可以同时使用 AWS Config 和 CloudTrail Lake 来对您的配置项目运行查询。您可以使用 AWS Config 基于单个 AWS 账户 和或多个账户和 AWS 区域区域的配置属性查询 AWS 资源的当前配置状态。相比之下，您可以使用 CloudTrail Lake 跨不同的数据源进行查询，例如 CloudTrail 事件、配置项目和规则评估。 CloudTrail Lake 查询涵盖所有 AWS Config 配置项目，包括资源配置和合规性历史记录。

为配置项目创建事件数据存储不会影响现有的 AWS Config 高级查询或任何已配置的 AWS Config 聚合器。您可以继续使用运行高级查询 AWS Config，并 AWS Config 继续将历史文件传送到您的 S3 存储桶。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

限制

以下限制适用于配置项目的事件数据存储。

- 不支持自定义配置项目
- 不支持使用高级事件选择器筛选事件

先决条件

在创建事件数据存储之前，请为所有账户和地区设置 AWS Config 记录。您可以使用 “快速设置”（一项功能）来快速创建由提供支持的配置记录器 AWS Config。 AWS Systems Manager

> **Note**
>
> AWS Config 开始记录配置时，您需要支付服务使用费。有关定价的更多信息，请参阅 AWS Config 定价。有关管理配置记录器的信息，请参阅《AWS Config 开发人员指南》中的管理配置记录器。

此外，建议执行以下操作，但这些操作不是创建事件数据存储所必需的。

- 设置 Amazon S3 桶以接收配置快照（按需）和配置历史记录。有关快照的更多信息，请参阅《AWS Config 开发人员指南》中的 Managing the Delivery Channel（管理传送通道）和 Delivering Configuration Snapshot to an Amazon S3 Bucket（将配置快照传送到 Amazon S3 桶）。
- 指定要 AWS Config 用来评估所记录资源类型的合规性信息的规则。 CloudTrail Lake 的几个 Lake 示例查询 AWS Config AWS Config 规则 需要评估 AWS 资源的合规性状态。有关更多信息 AWS Config 规则，请参阅《AWS Config 开发人员指南》 AWS Config 规则中的使用评估资源。

为配置项目创建事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 Configure event data store（配置事件数据存储）页面上的 General details（一般细节）中，输入事件数据存储的名称。名称为必填项。
5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。
7. （可选）要使用启用加密 AWS Key Management Service，请选择使用我自己的加密 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

> **Note**
>
> 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在 Tags（标签）部分中，您最多可以添加 50 个标签键对，以帮助您对事件数据存储的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择下一步。

11. 在选择事件页面上，选择 AWS 事件，然后选择配置项目。

12. CloudTrail 将事件数据存储资源存储在您创建该资源的区域中，但默认情况下，在数据存储中收集的配置项目来自您账户中所有启用了录制的区域。（可选）您可以选择 Include only the current region in my event data store（在我的事件数据存储中仅包含当前区域），以便仅包含在当前区域中捕获的配置项目。如果不选择此选项，则您的事件数据存储将包含所有已启用记录的所在区域中的配置项目。

13. 要让您的事件数据存储收集组织中所有账户的配置项目，请选择 “为我的 AWS Organizations 组织中的所有帐户启用”。您必须登录到组织的管理账户或委托管理员账户，才能创建为组织收集配置项目的事件数据存储。

14. 选择 Next（下一步）以查看您的选择。
15. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
16. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。

    从此时开始，事件数据存储将捕获配置项目。在创建事件数据存储之前出现的配置项目不会在该事件数据存储中。

示例查询

现在，您可以对新的事件数据存储运行查询。 CloudTrail 控制台上的 “示例查询” 选项卡提供了示例查询供您入门。以下是一些可以针对配置项目事件数据存储运行的示例查询。

描述	查询
通过将配置项目事件数据存储加入事件数据存储，找出哪位用户执行了导致不合规状态的 CloudTrail 操作。	`SELECT element_at(config1.eventData.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventData.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM config_event_data_store_ID as config1 JOIN config_event_data_store_ID as config2 on element_at(config1.eventData.configuration, 'targetResourceId') = config2.eventData.resourceId JOIN cloudtrail_event_data_store_ID as cloudtrail on config2.eventData.arn = element_at(cloudtrail.resources, 1).arn WHERE`

描述	查询
	element_at(config1.eventDat a.configuration, 'configRuleList') is not null AND element_at(config1.eventDat a.configuration, 'complianceType') = 'NON_COMPLIANT' AND cloudtrail.eventTime > '2022-11- 14 00:00:00' AND config2.eventData.resourceType = 'AWS::DynamoDB::Table'

描述	查询
查找所有 AWS Config 规则并返回过去一天内生成的配置项目的合规性状态。	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceName, eventData.resourceCreationTime, element_at(eventData.configuration,'complianceType') AS complianceType, element_at(eventData.configuration, 'configRuleList') AS configRuleList, element_at(eventData.configuration, 'resourceId') AS resourceId, element_at(eventData.configuration, 'resourceType') AS resourceType FROM config_event_data_store_ID WHERE eventData.resourceType = 'AWS::Config::ResourceCompliance' AND eventTime > '2022-11-22 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10`

描述	查询

查找按 AWS Config 资源类型、账户 ID 和地区分组的资源总数。	SELECT
	    eventData.resourceType, eventData
	.awsRegion, eventData.accountId,
	COUNT (*) AS resourceCount
	FROM
	    config_event_data_store_ID
	WHERE
	    eventTime > '2022-11-22 00:00:00'
	GROUP BY
	    eventData.resourceType, eventData
	.awsRegion, eventData.accountId

查找在特定日期生成的所有 AWS Config 配置项目的资源创建时间。	SELECT
	    eventData.configuration,
	 eventData.accountId,
	    eventData.awsRegion, eventData
	.resourceId,
	    eventData.resourceName, eventData
	.resourceType,
	    eventData.availabilityZone,
	 eventData.resourceCreationTime
	FROM
	    config_event_data_store_ID
	WHERE
	    eventTime > '2022-11-16 00:00:00'
	AND
	    eventTime < '2022-11-17 00:00:00'
	
	ORDER BY
	    eventData.resourceCreationTime
	DESC
	    limit 10;

有关创建和编辑查询的更多信息，请参阅创建或编辑查询。

配置项目架构

下表描述了与配置项目记录中的架构元素相匹配的必需和可选架构元素。的eventData内容由您的配置项目提供；其他字段由摄取 CloudTrail 后提供。

CloudTrail 中对事件记录内容进行了更详细的描述CloudTrail 录制内容。

- 摄取 CloudTrail 后提供的字段
- 由您的事件提供的字段

摄取 CloudTrail 后提供的字段

字段名称	输入类型	要求	描述
eventVersion	字符串	必需	AWS 事件格式的版本。
eventCategory	字符串	必需	事件类别。对于配置项目，有效值为 ConfigurationItem 。
eventType	字符串	必需	事件类型。对于配置项目，有效值为 AwsConfigurationItem 。
eventID	字符串	必需	事件的唯一 ID。
eventTime	字符串	必需	采用通用协调时间（UTC）的事件时间戳，格式为 yyyy-MM-DDTHH:mm:ss 。
awsRegion	字符串	必需	AWS 区域 要将事件分配给哪个。

字段名称	输入类型	要求	描述
recipientAccountId	字符串	必需	表示收到此事件的 AWS 账户 ID。
附录	附录	可选	显示有关事件延迟原因的信息。如果现有事件中缺少信息，则附录块将包含缺失的信息，以及缺失信息的原因。

eventData 中的字段由您的配置项目提供

字段名称	输入类型	要求	描述
eventData	-	必需	eventData 中的字段由您的配置项目提供。
• configurationItemVersion	字符串	可选	来自其来源的配置项目的版本。
• configurationItemCapture时间	字符串	可选	开始配置记录的时间。
• configurationItemStatus	字符串	可选	配置项目状态。有效值为 OK、ResourceDiscovered 、ResourceNotRecorded 、ResourceDeleted 和 ResourceDeletedNotRecorded 。
• accountId	字符串	可选	与资源关联 AWS 账户的 12 位数字 ID。

字段名称	输入类型	要求	描述
• resourceType	字符串	可选	AWS 资源的类型。有关有效资源类型的更多信息，请参阅 AWS Config API 参考ConfigurationItem中的。
• resourceId	字符串	可选	资源的 ID（例如，sg-*xxxxxx*）。
• resourceName	字符串	可选	资源的自定义名称（如果可用）。
• arn	字符串	可选	与资源关联的 Amazon 资源名称（ARN）。
• awsRegion	字符串	可选	资源 AWS 区域 所在的位置。
• availabilityZone	字符串	可选	与资源关联的可用区。
• resourceCreationTime	字符串	可选	创建资源时的时间戳。
• 配置	JSON	可选	资源配置的描述。
• supplementaryConfiguration	JSON	可选	为某些资源类型 AWS Config 返回的配置属性，用于补充为配置参数返回的信息。
• relatedEvents	字符串	可选	CloudTrail 事件 ID 列表。
• relationships	-	可选	相关 AWS 资源列表。

字段名称	输入类型	要求	描述
• • name	字符串	可选	与相关资源的关系的类型。
• • resourceType	字符串	可选	相关资源的资源类型。
• • resourceId	字符串	可选	相关资源的 ID（例如，sg-*xxxxxx*）。
• • resourceName	字符串	可选	相关资源的自定义名称（如果可用）。
• 标签	JSON	可选	与资源关联的键值标签的映射。

以下示例显示了与配置项目记录中的架构元素匹配的架构元素的层次结构。

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
```

```
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
       JSON
     }
    }
  }
}
```

使用控制台为外部的事件创建事件数据存储 AWS

您可以创建事件数据存储以包含外部的事件 AWS，然后使用 CloudTrail Lake 搜索、查询和分析应用程序中记录的数据。

您可以使用 La CloudTrail ke 集成来记录和存储来自外部的用户活动数据 AWS；这些数据来自混合环境中的任何来源，例如本地或云端托管的内部或 SaaS 应用程序、虚拟机或容器。

在为集成创建事件数据存储时，您还会创建一个通道，并将资源策略附加到该通道。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

为之外的事件创建事件数据存储 AWS

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。

2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 Configure event data store（配置事件数据存储）页面上的 General details（一般细节）中，输入事件数据存储的名称。名称为必填项。
5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。
7. （可选）要使用启用加密 AWS Key Management Service，请选择使用我自己的加密 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

> **Note**
>
> 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

   a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

   b. 如果您在创建新角色，请输入名称来标识该角色。

   c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

9. （可选）在 Tags（标签）部分中，您最多可以添加 50 个标签键对，以帮助您对事件数据存储的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

10. 选择 Next（下一步）以配置事件数据存储。

11. 在 Choose events（选择事件）页面上，选择 Events from integrations（来自集成的事件）。

12. 在 Events from integration（来自集成的事件）中，选择来源以将事件传送到事件数据存储。

13. 提供一个名称，用于标识集成的通道。该名称可以包含 3-128 个字符。只允许使用字母、数字、句点、下划线和短划线。

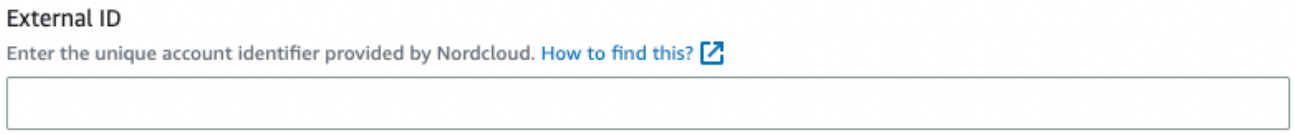
14. 在 Resource policy（资源策略）中，为集成的通道配置资源策略。资源策略是 JSON 策略文档，它们指定了指定主体可在资源上执行的操作，以及在什么条件下执行操作。在资源策略中定义为主体的账户可以调用 `PutAuditEvents` API，以向您的通道传送事件。如果资源所有者的 IAM policy 允许 `cloudtrail-data:PutAuditEvents` 操作，则资源所有者将拥有对资源的隐式访问权限。

该策略所需的信息由集成类型决定。对于方向集成， CloudTrail 会自动添加合作伙伴的 AWS 账户 ID，并要求您输入合作伙伴提供的唯一外部 ID。对于解决方案集成，您必须将至少一个 AWS 账户 ID 指定为委托人，并且可以选择输入外部 ID 以防止副手感到困惑。

> **Note**
>
> 如果您没有为通道创建资源策略，则只有通道所有者可以针对该通道调用 `PutAuditEvents` API。

a. 对于直接集成，请输入您的合作伙伴提供的外部 ID。集成合作伙伴将提供唯一的外部 ID（如账户 ID 或随机生成的字符串）用于集成，以防范混淆代理。合作伙伴负责创建和提供唯一的外部 ID。

   您可以选择 How to find this?（如何查找？），以查看描述如何查找外部 ID 的合作伙伴文档。



> **Note**
>
> 如果资源策略包括外部 ID，则针对 `PutAuditEvents` API 的所有调用都必须包括该外部 ID。但是，如果策略未定义外部 ID，合作伙伴仍然可以调用 `PutAuditEvents` API，并指定 `externalId` 参数。

b. 对于解决方案集成，请选择添加 AWS 账户以指定要作为委托人添加到策略中的每个 AWS 账户 ID。

15. 选择 Next（下一步）以查看您的选择。
16. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。
17. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。
18. 向合作伙伴应用程序提供通道 Amazon 资源名称（ARN）。有关向合作伙伴应用程序提供通道 ARN 的说明，可在合作伙伴文档网站上找到。有关更多信息，请在 Integrations（集成）页面的 Available sources（可用来源）选项卡上，选择与合作伙伴相对应的 Learn more（了解更多）链接，以便在 AWS Marketplace中打开合作伙伴的页面。

当您、合作伙伴或合作伙伴应用程序在渠道上调用 PutAuditEvents API 时，事件数据存储会开始 CloudTrail 通过集成的渠道将合作伙伴事件提取到该渠道中。

使用控制台更新事件数据存储

本部分介绍如何使用 AWS Management Console更新事件数据存储的设置。有关如何使用更新事件数据存储的信息 AWS CLI，请参阅使用更新事件数据存储 AWS CLI。

要更新事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择要更新的事件数据存储。此操作会打开事件数据存储的详细信息页面。
4. 在一般详细信息中，选择编辑以更改以下设置：

   - 事件数据存储名称 - 更改用于标识事件数据存储的名称。
   - 定价选项 - 对于使用七年期保留定价选项的事件数据存储，您可以选择改用一年可延期保留定价。对于每月摄取的事件数据少于 25TB 的事件数据存储，我们建议采用一年可延期保留定价。如果您在寻求最长 10 年的灵活保留期，我们也建议您采用一年可延期保留定价。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

     > **Note**
     >
     > 对于使用一年可延期保留定价的事件数据存储，您无法更改定价选项。如果您想使用七年期保留定价，请停止在当前事件数据存储上进行摄取。然后使用七年期保留定价选项创建新的事件数据存储。

   - 保留期 - 更改事件数据存储的保留期。保留期决定事件数据在事件数据存储中保存的时长。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

     > **Note**
     >
     > 如果您缩短了事件数据存储的保留期，则 CloudTrail 会删除所有保留期`eventTime`早于新保留期的事件。例如，如果之前的保留期为 365 天，而您将其缩短为 100 天，则 CloudTrail 会移除`eventTime`超过 100 天的事件。

- 加密 - 要使用自己的 KMS 密钥加密您的事件数据存储，请选择使用我自己的 AWS KMS key。默认情况下，事件数据存储中的所有事件都由加密 CloudTrail。使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。

  > **Note**
  >
  > 在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

- 要仅包含在当前 AWS 区域中记录的事件，请选择在我的事件数据存储中仅包含在当前区域中。如果不选择此选项，则您的事件数据存储将包含来自所有区域的事件。
- 要让您的事件数据存储收集组织中所有账户的事件，请为我的 AWS Organizations 组织中的所有账户选择 “启用”。只有当您使用组织的管理帐户登录并且事件数据存储的事件类型为CloudTrail事件或配置项目时，此选项才可用。

完成后，选择保存更改。

5. 在 Lake 查询联合身份验证中，选择编辑以启用或禁用 Lake 查询联合身份验证。启用 Lake 查询联合功能可让您在数据目录中查看事件数据存储的元 AWS Glue 数据，并使用 Amazon Athena 对事件数据运行 SQL 查询。禁用 Lake 查询联合会禁用与 AWS Glue AWS Lake Formation、和 Amazon Athena 的集成。禁用 Lake 查询联合身份验证后，您将无法再在 Athena 中查询数据。禁用联合后，不会删除任何 CloudTrail Lake 数据，并且您可以继续在 CloudTrail Lake 中运行查询。

   要启用联合身份验证，请执行以下操作：

   a. 请选择 启用。

   b. 选择是创建新的 IAM 角色还是使用现有角色。创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您使用现有角色，请确保该角色的策略提供所需的最低权限。

   c. 如果您在创建新的 IAM 角色，请为该角色输入名称。

   d. 如果您选择现有的 IAM 角色，请选择要使用的角色。角色必须存在于您的账户中。

   完成后选择保存更改。

6. 编辑您的事件类型的所有其他设置。

事件类型	可编辑的设置
CloudTrail 事件	您可以编辑以下 CloudTrail事件设置： • 要更改您的事件数据存储的日志事件，请选择在CloudTrail 事件中编辑。 • 在管理事件中，选择编辑以更改管理事件的设置。有关更多信息，请参阅 使用记录管理事件 AWS Management Console（步骤 3）。 • 在数据事件中，选择编辑以更改数据事件的设置。您可以选择要记录的数据事件类型，也可以选择要使用的日志选择器模板。有关更多信息，请参阅 更新现有的事件数据存储以记录数据事件 AWS Management Console。 完成后，选择保存更改。
来自集成的事件	在集成中，选择您的集成。然后选择编辑以更改以下设置： • 在集成详细信息中，更改标识集成通道的名称。 • 在事件传输位置中，选择事件的目的地。 • 在 Resource policy（资源策略）中，为集成的通道配置资源策略。 完成后，选择保存更改。 有关这些设置的更多信息，请参阅 与外部的事件源创建集成 AWS。

7. 要添加、更改或移除标签，请在标签中选择编辑。您最多可以添加 50 个标签键对，以帮助您对事件数据存储的访问进行识别、排序和控制。完成后，选择保存更改。

使用控制台停止和启动事件提取

默认情况下，事件数据存储被配置为摄取事件。您可以使用控制台、 AWS CLI或 API 来阻止事件数据存储提取事件。

“开始摄取” 和 “停止摄取” 选项仅适用于包含事件（管理和数据 CloudTrail 事件）或配置项目的事件数据存储。 AWS Config

当您停止对事件数据存储的摄取时，事件数据存储的状态将更改为 `STOPPED_INGESTION`。您仍然可以对事件数据存储中已存在的任何事件运行查询。您也可以将跟踪事件复制到事件数据存储中（如果它仅包含 CloudTrail 管理事件或数据事件）。

阻止事件数据存储摄取事件

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 在操作中，选择停止摄取。
5. 在提示您确认时，选择停止日志记录。事件数据存储将停止摄取实时事件。
6. 要恢复摄取，请选择开始摄取。

要重新启动事件摄取

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 从操作中，选择开始摄取。

使用控制台更改终止保护

默认情况下， AWS CloudTrail Lake 中的事件数据存储配置为启用终止保护。终止保护可防止事件数据存储被意外删除。如果要删除事件数据存储，您必须禁用终止保护。您可以使用 AWS Management Console AWS CLI、或 API 操作禁用终止保护。

要关闭终止保护

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 从操作中，选择更改终止保护。
5. 选择禁用。
6. 选择保存。现在，您可以删除事件数据存储。

要开启终止保护

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 从操作中，选择更改终止保护。
5. 要开启终止保护，请选择启用。
6. 选择保存。

使用控制台删除事件数据存储

本部分介绍如何使用 AWS CloudTrail 控制台删除事件数据存储。有关如何使用删除事件数据存储的信息 AWS CLI，请参阅使用删除事件数据存储 AWS CLI。

> **Note**
>
> 如果启用了终止保护或 Lake 查询联合身份验证，则无法删除事件数据存储。默认情况下，CloudTrail 启用终止保护以防止事件数据存储被意外删除。
> 要删除事件类型为集成中的事件的事件数据存储，必须先删除该集成的通道。您可以从集成的详细信息页面中或使用 aws cloudtrail delete-channel 命令删除通道。有关更多信息，请参阅删除频道以删除与的集成 AWS CLI。

要删除事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 对于 Actions (操作)，请选择 Delete (删除)。
5. 键入事件数据存储的名称以确认您要将其删除。
6. 选择删除。

在您删除事件数据存储后，事件数据存储的状态将更改为 PENDING_DELETION 并在该状态保留 7 天。在这 7 天的等待期内，您可以恢复事件数据存储。在 PENDING_DELETION 状态下，事件数据存储不可用于查询，除恢复操作之外，无法对事件数据存储执行其它操作。待删除的事件数据存储不会摄取事件，也不会产生成本。待删除的事件数据存储计入可以存在于一个事件数据存储的配额 AWS 区域。

使用控制台恢复事件数据存储

删除 AWS CloudTrail Lake 中的事件数据存储后，其状态将更改为该状态PENDING_DELETION并保持 7 天。在此期间，您可以使用 AWS Management Console AWS CLI、或 RestoreEventDataStoreAPI 操作恢复事件数据存储。

本部分介绍如何使用控制台恢复事件数据存储。有关如何使用恢复事件数据存储的信息 AWS CLI，请参阅使用恢复事件数据存储 AWS CLI。

要恢复事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 从操作中，选择恢复。

使用创建、更新和管理事件数据存储 AWS CLI

您可以使用 AWS CLI 来创建、更新和管理您的事件数据存储。使用时 AWS CLI，请记住您的命令在 AWS 区域 配置文件中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

事件数据存储的可用命令

用于在 La CloudTrail ke 中创建和更新事件数据存储的命令包括：

- create-event-data-store来创建事件数据存储。
- get-event-data-store返回有关事件数据存储的信息，包括为事件数据存储配置的高级事件选择器。
- update-event-data-store更改现有事件数据存储的配置。
- list-event-data-stores列出事件数据存储。
- delete-event-data-store删除事件数据存储。
- restore-event-data-store恢复待删除的事件数据存储。
- start-import开始将跟踪事件导入事件数据存储中，或者重试失败的导入。
- get-import返回有关特定导入的信息。
- stop-import停止将跟踪事件导入事件数据存储。
- list-imports返回有关所有导入的信息，或按ImportStatus或返回一组精选导入的信息Destination。
- list-import-failures列出指定导入的导入失败。
- stop-event-data-store-ingestion停止在事件数据存储上提取事件。
- start-event-data-store-ingestion在事件数据存储上重新启动事件摄取。
- enable-federation在事件数据存储上启用联合，以查询 Amazon Athena 中的事件数据存储。
- disable-federation在事件数据存储上禁用联合。禁用联合后，您将无法再在 Amazon Athena 中查询事件数据存储的数据。您可以继续在 L CloudTrail ake 中查询。
- put-insight-selectors为现有事件数据存储添加或修改 Insights 事件选择器，以及启用或禁用 Insights 事件。
- get-insight-selectors返回有关为事件数据存储配置的 Insights 事件选择器的信息。
- add-tags向现有的事件数据存储中添加一个或多个标签（键值对）。

- remove-tags从事件数据存储中移除一个或多个标签。
- list-tags返回与事件数据存储关联的标签列表。

有关可用于 La CloudTrail ke 查询的命令列表，请参阅可用于 L CloudTrail ake 查询的命令。

有关 La CloudTrail ke 集成的可用命令列表，请参阅L CloudTrail ake 集成的可用命令。

使用创建事件数据存储 AWS CLI

使用 create-event-data-store 命令创建事件数据存储。

创建事件数据存储时，唯一需要的参数是 --name，它用于标识事件数据存储。您可以配置其他可选参数，包括：

- --advanced-event-selectors - 指定要包括在事件数据存储中的事件的类型。默认情况下，事件数据存储会记录所有的管理事件。有关高级事件选择器的更多信息，请参阅 CloudTrail API 参考AdvancedEventSelector中的。
- --kms-key-id-指定用于加密传送的事件的 AWS KMS 密钥 ID CloudTrail。该值可以是前缀为 alias/ 的别名、别名的完全指定 ARN、密钥的完全指定 ARN 或全局唯一标识符。
- --multi-region-enabled-创建多区域事件数据存储，用于记录您账户 AWS 区域 中所有人的事件。默认情况下，即使未添加参数，也会设置 --multi-region-enabled。
- --organization-enabled - 启用事件数据存储，以收集组织中所有账户的事件。默认情况下，不会为组织中的所有账户启用事件数据存储。
- --billing-mode - 决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。

  有以下可能值。

  - EXTENDABLE_RETENTION_PRICING - 如果您每月摄取的事件数据少于 25TB，并且想要最长 3653 天（大约 10 年）的灵活保留期，则通常建议使用这种计费模式。此计费模式的默认保留期为 366 天。
  - FIXED_RETENTION_PRICING - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 2557 天（大约 7 年）的保留期，则建议采用此计费模式。此计费模式的默认保留期为 2557 天。

  默认值为 EXTENDABLE_RETENTION_PRICING。
- --retention-period - 事件在事件数据存储中保留的天数。如果 --billing-mode 为 EXTENDABLE_RETENTION_PRICING，则有效值为介于 7 和 3653 之间的整数；如果 --billing-mode 设置为 FIXED_RETENTION_PRICING，则有效值为介于 7 和 2557 之间的整数。如果未指定--retention-period，则 CloudTrail 使用默认的保留期--billing-mode。

- `--start-ingestion` - `--start-ingestion` 参数在其被创建时在事件数据存储上开始事件摄取。即使未添加该参数，也会设置此参数。

  如果您不希望事件数据存储摄取实时事件，请指定 `--no-start-ingestion`。例如，如果您要将事件复制到事件数据存储中，并且仅计划使用事件数据存储来分析过去的事件，则可能要设置此参数。仅当 `eventCategory` 为 `Management`、`Data` 或 `ConfigurationItem` 时，`--no-start-ingestion` 参数才有效。

以下示例演示了如何创建不同类型的事件数据存储。

主题

- 使用为 S3 数据事件创建事件数据存储 AWS CLI
- 使用为 AWS Config 配置项目创建事件数据存储 AWS CLI
- 使用为管理事件创建组织事件数据存储 AWS CLI
- 使用 Insights 事件创建事件数据存储 AWS CLI

使用为 S3 数据事件创建事件数据存储 AWS CLI

以下示例 AWS Command Line Interface (AWS CLI) create-event-data-store 命令创建一个名为的事件数据存储`my-event-data-store`，该存储选择所有 Amazon S3 数据事件，并使用 KMS 密钥进行加密。

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
    ]'
```

以下为响应示例。

```
{
```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

使用为 AWS Config 配置项目创建事件数据存储 AWS CLI

以下示例 AWS CLI create-event-data-store命令创建一个名为的事件数据存储库config-items-eds，用于选择 AWS Config 配置项目。要收集配置项目，请在高级事件选择器中指定 eventCategory 字段等于 ConfigurationItem。

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
```

```
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

使用为管理事件创建组织事件数据存储 AWS CLI

以下示例 AWS CLI create-event-data-store命令创建一个组织事件数据存储库，用于收集所有管理事件并将--billing-mode参数设置为FIXED_RETENTION_PRICING。

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

使用 Insights 事件创建事件数据存储 AWS CLI

要在 L CloudTrail ake 中记录 Insights 事件，您需要一个收集 Insights 事件的目标事件数据存储和一个启用 Insights 并记录管理事件的源事件数据存储。

此过程向您展示如何创建目标和源事件数据存储，然后启用 Insights 事件。

1. 运行 aws cloudtrail create-event-data-store 命令创建收集 Insights 事件的目标事件数据存储。eventCategory 的值必须为 Insight。*retention-period-days*替换为您希望在事件数据存储中保留事件的天数。如果 --billing-mode 为 EXTENDABLE_RETENTION_PRICING，则有效值为介于 7 和 3653 之间的整数；如果 --billing-mode 设置为 FIXED_RETENTION_PRICING，则有效值为介于 7 和 2557 之间的整数。如果未指定--retention-period，则 CloudTrail 使用默认的保留期--billing-mode。

   如果您使用 AWS Organizations 组织的管理账户登录，则如果要向委派的管理员授予对事件数据存储的访问权限，请添加--organization-enabled参数。

```
aws cloudtrail create-event-data-store \
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

   以下为响应示例。

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
```

```
                    "Field": "eventCategory",
                    "Equals": [
                        "Insight"
                      ]
                  }
              ]
          }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

您将使用响应中的 ARN（或 ARN 的 ID 后缀）作为步骤 3 中参数 `--insights-destination` 的值。

2. 请运行 aws cloudtrail create-event-data-store 命令以创建记录管理事件的源事件数据存储。默认情况下，事件数据存储会记录所有的管理事件。您无需指定任何高级事件选择器即可记录所有管理事件。*retention-period-days*替换为您希望在事件数据存储中保留事件的天数。如果 `--billing-mode` 为 EXTENDABLE_RETENTION_PRICING，则有效值为介于 7 和 3653 之间的整数；如果 `--billing-mode` 设置为 FIXED_RETENTION_PRICING，则有效值为介于 7 和 2557 之间的整数。如果未指定`--retention-period`，则 CloudTrail 使用默认的保留期`--billing-mode`。如果您正在创建组织事件数据存储，请包括 `--organization-enabled` 参数。

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
```

```
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

您将使用响应中的 ARN（或 ARN 的 ID 后缀）作为步骤 3 中参数 `--event-data-store` 的值。

3. 请运行 put-insight-selectors 命令以启用 Insights 事件。Insights 选择器值可以是 `ApiCallRateInsight` 和/或 `ApiErrorRateInsight`。对于 `--event-data-store` 参数，请指定记录管理事件并将启用 Insights 的源事件数据存储的 ARN（或 ARN 的 ID 后缀）。对于 `--insights-destination` 参数，请指定将记录 Insights 事件的目标事件数据存储的 ARN（或 ARN 的 ID 后缀）。

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

以下结果显示为事件数据存储配置的 Insights 事件选择器。

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
```

```
            {
               "InsightType": "ApiErrorRateInsight"
            },
            {
               "InsightType": "ApiCallRateInsight"
            }
        ]
}
```

首次在事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。

CloudTrail Insights 分析发生在单个区域（而不是全球区域）的管理事件。 CloudTrail Insights 事件是在生成其支持管理事件的同一区域生成的。

对于组织事件数据存储， CloudTrail 分析来自每个成员账户的管理事件，而不是分析组织所有管理事件的聚合。

在 Lake 中 CloudTrail 收取 Insights 事件需要支付额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关 CloudTrail 定价的信息，请参阅AWS CloudTrail 定价。

使用将跟踪事件导入到事件数据存储中 AWS CLI

在中 AWS CLI，您可以将跟踪事件导入到事件数据存储中。本部分中的过程演示如何通过运行 create-event-data-store 命令来创建和配置事件数据存储，然后使用 start-import 命令将事件导入该事件数据存储。有关导入跟踪事件的更多信息，包括有关注意事项和所需权限的信息，请参阅 将跟踪事件复制到事件数据存储。

正在准备导入跟踪事件

在导入跟踪事件之前，请做好以下准备工作。

- 确保您的角色具有将跟踪事件导入事件数据存储的所需权限。
- 确定您要为事件数据存储指定的 --billing-mode 值。`--billing-mode` 决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。

  将跟踪事件导入 CloudTrail Lake 时， CloudTrail 解压缩以 gzip（压缩）格式存储的日志。然后 CloudTrail 将日志中包含的事件复制到您的事件数据存储中。未压缩数据的大小可能大于 Amazon S3 的实际存储大小。要对未压缩数据的大小进行总体估计，将 S3 存储桶中日志的大小乘以 10。您可以使用此估算值为您的应用场景选择 `--billing-mode` 值。

- 确定您要为 `--retention-period` 指定的值。 CloudTrail 如果事件早于指定的保留期`eventTime`，则不会复制该事件。

  要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要将事件在事件数据存储中保留的天数之和，如以下公式所示：

  保留期限 = *oldest-event-in-days*+ *number-days-to-retain*

  例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。
- 决定是否要使用事件数据存储来分析任何未来的事件。如果您不想摄取任何未来事件，请在创建事件数据存储时包含 `--no-start-ingestion` 参数。默认情况下，事件数据存储会在创建事件时开始摄取事件。

要创建事件数据存储并将跟踪事件导入该事件数据存储

1. 运行 create-event-data-store 命令以创建新的事件数据存储。在此示例中，`--retention-period` 被设置为 `120` 是因为要复制的最早事件已有 90 天了，且我们希望将这些事件保留 30 天。之所以设置 `--no-start-ingestion` 参数，是因为我们不想摄取任何未来事件。在此示例中，`--billing-mode` 未设置，是因为我们使用的是默认值 `EXTENDABLE_RETENTION_PRICING`，因为我们预计摄取的事件数据少于 25TB。

   > **Note**
   >
   > 如果您正在创建事件数据存储来替换跟踪，我们建议将 `--advanced-event-selectors` 配置为与您的跟踪的事件选择器相匹配，以确保事件覆盖范围相同。默认情况下，事件数据存储会记录所有的管理事件。

   ```
   aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
    120 --no-start-ingestion
   ```

   以下为响应示例：

   ```
   {
       "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
   EXAMPLEa-4357-45cd-bce5-17ec652719d9",
       "Name": "import-trail-eds",
   ```

```
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

初始 Status 为 CREATED，因此我们将运行 get-event-data-store 命令来验证摄取是否已停止。

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

响应显示 Status 现在为 STOPPED_INGESTION，这表明事件数据存储未摄取实时事件。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
```

```
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. 运行 start-import 命令以将跟踪事件导入步骤 1 中创建的事件数据存储。将事件数据存储的 ARN（或 ARN 的 ID 后缀）指定为 `--destinations` 参数的值。对于 `--start-event-time`，请为要复制的最早的事件指定 `eventTime`，对于 `--end-event-time`，请指定要复制的最新事件的 `eventTime`。为包含您的跟踪日志的 S3 存储桶`--import-source`指定 S3 URI、S3 存储桶的，以及用于导入跟踪事件的角色的 ARN。 AWS 区域

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

以下为响应示例。

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
```

```
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
   "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
   "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. 运行 get-import 命令以获取有关导入的信息。

```
aws cloudtrail get-import --import-id import-id
```

以下为响应示例。

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
```

```
        "FailedEntries": 0
    }
}
```

如果没有故障，导入完成时 ImportStatus 显示为 COMPLETED，如果出现故障，则会显示 FAILED。

如果导入具有 FailedEntries，则可以运行 list-import-failures 命令以返回失败列表。

```
aws cloudtrail list-import-failures --import-id import-id
```

要重试失败的导入，请仅使用 --import-id 参数运行 start-import 命令。重试导入时，将在出现故障的位置 CloudTrail 恢复导入。

```
aws cloudtrail start-import --import-id import-id
```

使用获取事件数据存储 AWS CLI

以下示例 AWS CLI get-event-data-store命令返回有关由必需--event-data-store参数指定的事件数据存储的信息，该参数接受 ARN 或 ARN 的 ID 后缀。

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下为响应示例。创建时间和上次更新时间采用 timestamp 格式。

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
```

```
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::bucketName"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

列出账户中存储的所有事件数据 AWS CLI

以下示例 AWS CLI list-event-data-stores命令返回有关当前区域中账户中存储的所有事件数据的信息。可选参数包括 `--max-results`，以指定希望在单个页面上通过命令返回的最大结果数。如果结果数

超过指定的 --max-results 值，请再次运行命令，添加返回的 NextToken 值来获取下一页的结果。

```
aws cloudtrail list-event-data-stores
```

以下为响应示例。

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
}
```

使用更新事件数据存储 AWS CLI

以下示例演示如何更新事件数据存储。

主题

- 使用更新计费模式 AWS CLI
- 更新保留模式，启用终止保护，然后 AWS KMS key 使用指定 AWS CLI
- 使用禁用终止保护 AWS CLI

使用更新计费模式 AWS CLI

事件数据存储的 --billing-mode 决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。如果事件数据存储的 --billing-mode 设置为 FIXED_RETENTION_PRICING，

则可以将该值更改为 EXTENDABLE_RETENTION_PRICING。如果您的事件数据存储每月摄取的事件数据少于 25TB，并且您希望采用最多 3653 天的灵活保留期，则通常建议使用 EXTENDABLE_RETENTION_PRICING。有关定价的信息，请参阅 AWS CloudTrail 定价和 管理 CloudTrail 湖泊成本。

> **Note**
>
> 您不能将 --billing-mode 值从 EXTENDABLE_RETENTION_PRICING 更改为 FIXED_RETENTION_PRICING。如果事件数据存储的计费模式设置为 EXTENDABLE_RETENTION_PRICING，且您想改用 FIXED_RETENTION_PRICING，则可以停止对事件数据存储的摄取，并创建一个使用 FIXED_RETENTION_PRICING 的新事件数据存储。

以下示例 AWS CLI update-event-data-store命令将事件数据存储--billing-mode的命令从更改FIXED_RETENTION_PRICING为EXTENDABLE_RETENTION_PRICING。必要的 --event-data-store 参数值是 ARN（或 ARN 的 ID 后缀），且是必填项；其它参数是可选项。

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

以下为响应示例。

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
```

```
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

更新保留模式，启用终止保护，然后 AWS KMS key 使用指定 AWS CLI

以下示例 AWS CLI update-event-data-store命令更新事件数据存储以将其保留期更改为 100 天，并启用终止保护。必要的 `--event-data-store` 参数值是 ARN（或 ARN 的 ID 后缀），且是必填项；其它参数是可选项。在此示例中，添加了 `--retention-period` 参数，以将保留期限更改为 100 天。或者，您可以选择启用 AWS Key Management Service 加密并 AWS KMS key 通过在命令中添加并`--kms-key-id`指定 KMS 密钥 ARN 作为值来指定。 `--termination-protection-enabled`添加是为了在未启用终止保护的事件数据存储上启用终止保护。

AWS 无法更新记录外部事件的事件数据存储以记录 AWS 事件。同样，记录 AWS 事件的事件数据存储不能更新为从外部记录事件 AWS。

> **Note**
>
> 如果您缩短了事件数据存储的保留期，则 CloudTrail 会删除所有保留期`eventTime`早于新保留期的事件。例如，如果之前的保留期为 365 天，而您将其缩短为 100 天，则 CloudTrail 会移除`eventTime`超过 100 天的事件。

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

以下为响应示例。

```
{
```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

使用禁用终止保护 AWS CLI

默认情况下，事件数据存储已启用终止保护，以防止事件数据存储被意外删除。当终止保护启用时，您无法删除事件数据存储。如果要删除事件数据存储，您必须先禁用终止保护。

以下示例 AWS CLI update-event-data-store命令通过传递--no-termination-protection-enabled参数来禁用终止保护。

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

使用停止在事件数据存储上进行提取 AWS CLI

以下示例 AWS CLI stop-event-data-store-ingestion命令阻止事件数据存储接收事件。要停止摄取，事件数据存储 `Status` 必须是 `ENABLED`，并且 `eventCategory` 必须是 `Management`、`Data`

或 ConfigurationItem。事件数据存储由 --event-data-store 指定，它接受事件数据存储 ARN 或 ARN 的 ID 后缀。运行 stop-event-data-store-ingestion 后，事件数据存储的状态将更改为 STOPPED_INGESTION。

处于 STOPPED_INGESTION 状态时，事件数据存储计入您的账户最多十个事件数据存储的限额内。

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

如果成功执行操作，则没有响应。

使用开始在事件数据存储上进行提取 AWS CLI

以下示例 AWS CLI start-event-data-store-ingestion命令在事件数据存储上启动事件摄取。要开始摄取，事件数据存储 Status 必须是 STOPPED_INGESTION，并且 eventCategory 必须是 Management、Data 或 ConfigurationItem。事件数据存储由 --event-data-store 指定，它接受事件数据存储 ARN 或 ARN 的 ID 后缀。运行 start-event-data-store-ingestion 后，事件数据存储的状态将更改为 ENABLED。

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

如果成功执行操作，则没有响应。

在事件数据存储上启用联合身份验证

要启用联合身份验证，请运行 aws cloudtrail enable-federation 命令，以提供所需的 --event-data-store 和 --role 参数。对于 --event-data-store，请提供事件数据存储 ARN（或 ARN 的 ID 后缀）。对于 --role，请提供您的联合身份验证角色的 ARN。该角色必须存在于您的账户中，并提供所需的最低权限。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

此示例说明委托管理员如何通过在管理账户中指定事件数据存储的 ARN 和在委托管理员账户中指定联合身份验证角色的 ARN 来在组织事件数据存储上启用联合身份验证。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

在事件数据存储上禁用联合身份验证

要在事件数据存储上禁用联合身份验证，请运行 aws cloudtrail disable-federation 命令。事件数据存储由 `--event-data-store` 指定，它接受事件数据存储 ARN 或 ARN 的 ID 后缀。

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> 如果这是组织事件数据存储，则使用管理账户的账户 ID。

使用删除事件数据存储 AWS CLI

以下示例 AWS CLI delete-event-data-store 命令禁用 `--event-data-store` 指定的事件数据存储，它接受事件数据存储 ARN 或 ARN 的 ID 后缀。运行 delete-event-data-store 之后，事件数据存储的最终状态为 `PENDING_DELETION`，且事件数据存储将在 7 天等待期后自动删除。

在事件数据存储上运行 delete-event-data-store 之后，您无法在使用已禁用的数据存储的查询上运行 list-queries、describe-query 或 get-query-results。处于等待删除状态时，事件数据存储计入您的账户最多十个事件数据存储的限额内。

> **Note**
>
> 如果设置了 `--termination-protection-enabled` 或其 `FederationStatus` 为 `ENABLED`，则无法删除事件数据存储。

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

如果成功执行操作，则没有响应。

使用恢复事件数据存储 AWS CLI

以下示例 AWS CLI restore-event-data-store 命令恢复待删除的事件数据存储。事件数据存储由 `--event-data-store` 指定，它接受事件数据存储 ARN 或 ARN 的 ID 后缀。您只能在删除后的七天等待期内恢复被删除的事件数据存储。

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

响应包括有关事件数据存储的信息，包括其 ARN、高级事件选择器以及还原状态。

管理事件数据存储生命周期

以下是事件数据存储的生命周期阶段：

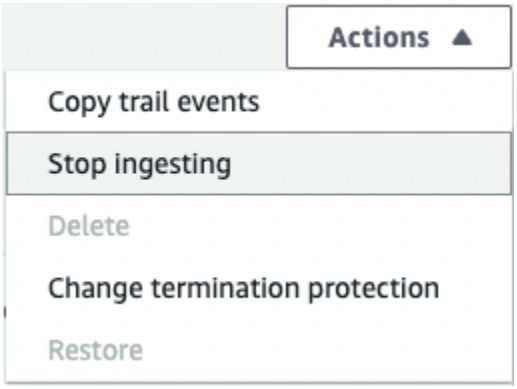
- CREATED – 短期状态，表示已创建事件数据存储。
- ENABLED – 事件数据存储处于活动状态，正在摄取事件。您可以运行查询并将跟踪事件复制到事件数据存储。
- STARTING_INGESTION – 短期状态，表示事件数据存储将开始摄取实时事件。
- STOPPING_INGESTION – 短期状态，表示事件数据存储将停止摄取实时事件。
- STOPPED_INGESTION – 事件数据存储未摄取实时事件。您仍然可以对事件数据存储中已存在的任何事件运行查询，并将跟踪事件复制到事件数据存储中。
- PENDING_DELETION – 事件数据存储处于 ENABLED 或 STOPPED_INGESTION 状态且已被删除，但尚处于永久删除之前的 7 天等待期内。您无法对事件数据存储运行查询，除了恢复之外，不能对事件数据存储执行任何操作。

您仅可以在联合身份验证和终止保护都被禁用时删除事件数据存储。终止保护可防止事件数据存储被意外删除。默认情况下，事件数据存储上已启用终止保护。通过联合身份验证，您可以在 Athena 中查询事件数据存储数据，该功能默认情况下处于禁用状态。

在您删除事件数据存储后，它将保留 PENDING_DELETION 状态 7 天，然后才被永久删除。在这 7 天的等待期内，您可以恢复事件数据存储。在 PENDING_DELETION 状态下，事件数据存储不可用于查询，除恢复操作之外，无法对事件数据存储执行其它操作。待删除的事件数据存储不会摄取事件，也不会产生成本。但是，待删除的事件数据存储会计入一个中可能存在的事件数据存储的配额 AWS 区域。

事件数据存储上可用的操作

要删除或恢复事件数据存储、复制跟踪事件、开始或停止摄取事件，或打开或关闭事件数据存储的终止保护，请使用事件数据存储详细信息页面的操作菜单上的命令。



复制跟踪事件的选项仅适用于包含 CloudTrail 管理和数据事件的事件数据存储。“开始摄取” 和 “停止摄取” 选项仅适用于包含事件（管理和数据 CloudTrail 事件）或配置项目的事件数据存储。 AWS Config

将跟踪事件复制到事件数据存储

您可以将跟踪事件复制到 CloudTrail Lake 事件数据存储中，以创建记录到跟踪的事件的 point-in-time 快照。复制跟踪的事件不会干扰跟踪记录事件的功能，也不会以任何方式修改跟踪。

您可以将跟踪事件复制到为事件配置的现有 CloudTrail 事件数据存储中，也可以创建新的 CloudTrail 事件数据存储并选择复制跟踪事件选项作为事件数据存储创建的一部分。有关将跟踪事件复制到现有事件数据存储的更多信息，请参阅 将跟踪事件复制到现有的事件数据存储。有关创建新的事件数据存储的更多信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储。

如果您要将跟踪事件复制到组织事件数据存储，则必须使用该组织的管理账户。您不能使用组织的委托管理员账户复制跟踪事件。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

将跟踪事件复制到 CloudTrail Lake 事件数据存储时，会根据事件数据存储提取的未压缩数据量产生费用。

将跟踪事件复制到 CloudTrail Lake 时， CloudTrail 解压缩以 gzip（压缩）格式存储的日志，然后将日志中包含的事件复制到您的事件数据存储中。未压缩数据的大小可能大于 S3 的实际存储大小。要对未压缩数据的大小进行总体估计，可以将 S3 存储桶中日志的大小乘以 10。

您可以通过为复制的事件指定更窄的时间范围来降低成本。如果您计划仅使用事件数据存储来查询复制的事件，则可以关闭事件摄取，以免对将来的事件产生费用。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

SCENARIOS（场景）

下表描述了复制跟踪事件的一些常见场景，以及如何使用控制台完成每个场景。

场景	如何在控制台中完成此操作？
无需摄取新事件即可分析和查询 CloudTrail Lake 中的历史轨迹事件	在创建事件数据存储时，创建新的事件数据存储并选择复制跟踪事件选项。创建事件数据存储时，请取消选择摄取事件（程序的步骤 15），以确保事件数据存储仅包含跟踪的历史事件，不包含未来事件。
用 CloudTrail Lake 事件数据存储替换现有跟踪	使用与您的跟踪相同的事件选择器创建事件数据存储，以确保事件数据存储与跟踪具有相同的覆盖范围。 为避免源跟踪和目标事件数据存储之间存在重复事件，请为复制的事件选择一个早于事件数据存储创建时间的时间范围。 创建事件存储后，您可以关闭跟踪的日志记录，避免产生额外费用。

主题

- 复制跟踪事件的注意事项
- 复制跟踪事件所需的权限
- 将跟踪事件复制到现有的事件数据存储
- 事件复制详细信息
- 示例：将跟踪事件复制到新的事件数据存储中

复制跟踪事件的注意事项

复制跟踪事件时，请将以下因素考虑在内。

- 复制跟踪事件时， CloudTrail 使用 S3 `GetObject`API 操作检索源 S3 存储桶中的跟踪事件。有些 S3 归档存储类，例如 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Outposts 和 S3

Intelligent-Tiering Deep Archive 层，无法使用 `GetObject` 来访问。要复制存储在这些归档存储类中的跟踪事件，必须先使用 S3 `RestoreObject` 操作还原副本。有关还原已归档的对象的信息，请参阅《Amazon S3 用户指南》中的恢复已归档的对象。

- 将跟踪事件复制到事件数据存储时， CloudTrail 无论目标事件数据存储的事件类型、高级事件选择器或 AWS 区域的配置如何，都会复制所有跟踪事件。
- 在将跟踪事件复制到现有的事件数据存储之前，请确保根据您的应用场景适当配置了事件数据存储的定价选项和保留期。
  - 定价选项：定价选项决定了摄取和存储事件的成本。有关定价选项的更多信息，请参阅 AWS CloudTrail 定价和 事件数据存储定价选项。
  - 保留期：保留期限决定事件数据在事件数据存储中保存多长时间。 CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`*）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。
- 如果您要将跟踪事件复制到事件数据存储中进行调查，并且不想摄取任何未来事件，则可以停止对事件数据存储的摄取。创建事件数据存储时，请取消选择摄取事件选项（程序的步骤 15），以确保事件数据存储仅包含跟踪的历史事件，不包含未来事件。
- 在复制跟踪事件之前，请禁用任何附加到源 S3 存储桶的访问控制列表（ACL），并更新目标事件数据存储的 S3 存储桶策略。有关更新 S3 存储桶策略的更多信息，请参阅 复制跟踪事件所用的 Amazon S3 存储桶策略。有关禁用 ACL 的更多信息，请参阅《Amazon S3 用户指南》中的为您的存储桶控制对象所有权和禁用 ACL。
- CloudTrail 仅复制源 S3 存储桶中的 Gzip 压缩日志文件中的跟踪事件。 CloudTrail 不会从未压缩的日志文件或使用 Gzip 以外的格式压缩的日志文件中复制跟踪事件。
- 为避免源跟踪和目标事件数据存储之间存在重复事件，请为复制的事件选择一个早于事件数据存储创建时间的时间范围。
- 默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的前缀，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，则必须在复制跟踪事件时选择前缀。
- 要将跟踪事件复制到组织事件数据存储，必须使用该组织的管理账户。委托管理员账户无法将跟踪事件复制到组织事件数据存储。

复制跟踪事件所需的权限

在复制跟踪事件之前，请确保您拥有 IAM 角色的所有必需权限。如果您选择现有 IAM 角色来复制跟踪事件，则只需要更新 IAM 角色权限。如果您选择创建新的 IAM 角色，请为该角色 CloudTrail 提供所有必要的权限。

如果源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密存储桶中的数据。如果源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。

主题

- 复制跟踪事件所需的 IAM 权限
- 复制跟踪事件所用的 Amazon S3 存储桶策略
- 用于解密源 S3 存储桶中数据的 KMS 密钥政策

复制跟踪事件所需的 IAM 权限

复制跟踪事件时，您可以选择创建新的 IAM 角色，也可以使用现有 IAM 角色。当您选择新的 IAM 角色时， CloudTrail 会创建一个具有所需权限的 IAM 角色，您无需采取任何进一步的操作。

如果您选择现有角色，请确保 IAM 角色的策略 CloudTrail 允许从源 S3 存储桶复制跟踪事件。此部分提供所需 IAM 角色权限和信任策略的示例。

以下示例提供了权限策略，该策略 CloudTrail 允许从源 S3 存储桶复制跟踪事件。将 *myBucketNamemyAccountID*、*##*、*##*和 *eventDataStoreID* 替换为适合您的配置的值。*myAccountID* 是用于 CloudTrail Lake 的 AWS 账户 ID，它可能与 S3 存储桶的 AWS 账户 ID 不同。

将 *key-region#keyAccountID* 和 *keyID* 替换为用于加密源 S3 存储桶的 KMS 密钥的值。如果源 S3 存储桶未使用 KMS 密钥进行加密，则可省略 `AWSCloudTrailImportKeyAccess` 语句。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
```

```
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

以下示例提供了 IAM 信任策略，该策略 CloudTrail 允许代入 IAM 角色从源 S3 存储桶复制跟踪事件。将 *myAccountID*、regi *on* 和 *eventDataStoreArn* 替换为适合您的配置的值。*myAccount AWS ## ID* 是用于 CloudTrail Lake 的 ID，它可能与 S3 存储桶的 AWS 账户 ID 不同。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

复制跟踪事件所用的 Amazon S3 存储桶策略

默认情况下，Simple Storage Service（Amazon S3）存储桶和对象都是私有的。仅资源所有者（创建存储桶的 AWS 账户）能够访问存储桶及其包含的对象。资源所有者可以通过编写访问策略来向其他资源和用户授予访问权。

在复制跟踪事件之前，必须更新 S3 存储桶策略 CloudTrail 以允许从源 S3 存储桶复制跟踪事件。

您可以在 S3 存储桶策略中添加以下语句以授予这些权限。将 *roLearn* 和，*myBucketName*替换为适合您的配置的值。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
```

```
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

用于解密源 S3 存储桶中数据的 KMS 密钥政策

如果源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 提供从启用了 SSE-KMS 加密的 S3 存储桶复制跟踪事件所需的`kms:Decrypt`和`kms:GenerateDataKey`权限。如果源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略。更新 KMS 密钥策略 CloudTrail 允许解密源 S3 存储桶中的数据，运行验证检查以确保事件符合 CloudTrail标准，并将事件复制到 CloudTrail Lake 事件数据存储中。

以下示例提供了 KMS 密钥策略，该策略 CloudTrail 允许解密源 S3 存储桶中的数据。将 *roLearn*、*myBucketName*、*myAccount eventDataStoreID#regi on # Id* 替换为适合您的配置的值。*myAccountID* 是用于 CloudTrail Lake 的 AWS 账户 ID，它可能与 S3 存储桶的 AWS 账户 ID 不同。

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

将跟踪事件复制到现有的事件数据存储

按照以下程序将跟踪事件复制到事件数据存储中。有关如何创建新的事件数据存储的信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储。

> **Note**
>
> 在将跟踪事件复制到现有的事件数据存储之前，请确保根据您的应用场景适当配置了事件数据存储的定价选项和保留期。
>
> - 定价选项：定价选项决定了摄取和存储事件的成本。有关定价选项的更多信息，请参阅 AWS CloudTrail 定价和 事件数据存储定价选项。
> - 保留期：保留期限决定事件数据在事件数据存储中保存多长时间。 CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`* ）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。

要将跟踪事件复制到事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Copy trail events（复制跟踪事件）。
4. 在 Copy trail events（复制跟踪事件）页面，在 Event source（事件源）下选择您想复制的跟踪。默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的前缀，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，请选择输入 S3 URI，然后选择浏览 S3 浏览到该前缀。如果跟踪的源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密数据。如果您的源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。有关更新 KMS 密钥政策的更多信息，请参阅 用于解密源 S3 存储桶中数据的 KMS 密钥政策。

   S3 存储桶策略必须授予从 S3 存储桶复制跟踪事件的 CloudTrail 访问权限。有关更新 S3 存储桶策略的更多信息，请参阅 复制跟踪事件所用的 Amazon S3 存储桶策略。

5. 在 “指定事件的时间范围” 中，选择复制事件的时间范围。 CloudTrail 在尝试复制跟踪事件之前，请检查前缀和日志文件名以验证该名称是否包含所选开始日期和结束日期之间的日期。您可以选择 Relative range（相对范围）或者 Absolute range（绝对范围）。为避免源跟踪和目标事件数据存储之间存在重复事件，请选择一个早于事件数据存储创建时间的时间范围。

   > **Note**
   >
   > CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。例如，如果事件数据存储的保留期为 90 天，则 CloudTrail 不会复制任何`eventTime`超过 90 天的跟踪事件。

   - 如果选择 “相对范围”，则可以选择复制过去 6 个月、1 年、2 年、7 年或自定义范围内记录的事件。 CloudTrail 复制选定时间段内记录的事件。
   - 如果选择 “绝对范围”，则可以选择特定的开始和结束日期。 CloudTrail 复制在所选开始日期和结束日期之间发生的事件。
6. 对于 Delivery location（送达位置），请从下拉列表中选择目标事件数据存储。
7. 对于 Permissions（权限），请从以下 IAM 角色选项中进行选择。如果您选择现有的 IAM 角色，请验证 IAM 角色策略是否提供了必要的权限。有关更新 IAM 角色权限的更多信息，请参阅 复制跟踪事件所需的 IAM 权限。

   - 选择 Create a new role (recommended)（创建新角色（推荐））以创建新的 IAM 角色。对于 Enter IAM role name（输入 IAM 角色名称），输入角色的名称。 CloudTrail 会自动为这个新角色创建必要的权限。
   - 选择使用自定义 IAM 角色 ARN 以使用未列出的自定义 IAM 角色。对于 Enter IAM role ARN（输入 IAM 角色 ARN），输入 IAM ARN。
   - 从下拉列表中选择现有的 IAM 角色。
8. 选择 Copy events（复制事件）。
9. 系统将提示您进行确认。如果您已准备好确认，请选择 Copy trail events to Lake（将跟踪事件复制到 Lake），然后选择 Copy events（复制事件）。
10. 在 Copy details（复制详情）页面中，您可以查看复制状态并检查是否复制失败。跟踪事件复制完成后，如果复制未出错，则 Copy status（复制状态）将设置为 Completed（已完成），否则如果出错了，则设置为 Failed（失败）。

> **Note**
>
> 事件复制详细信息页面上显示的详细信息不是实时的。Prefixes copied（已复制的前缀）等详细信息的实际值可能高于页面上显示的值。 CloudTrail 在事件副本的过程中逐步更新详细信息。

11. 如果 Copy status（复制状态）为 Failed（失败），则要先修复 Copy failures（复制失败）中显示的所有错误，然后选择 Retry copy（重试复制）。当您重试复制时，会在出现故障的位置 CloudTrail 恢复副本。

有关查看跟踪事件复制详细信息的更多信息，请参阅 事件复制详细信息。

事件复制详细信息

跟踪事件复制开始后，您可以查看事件复制详细信息，包括复制的状态以及有关任何复制失败的信息。

> **Note**
>
> 事件复制详细信息页面上显示的详细信息不是实时的。Prefixes copied（已复制的前缀）等详细信息的实际值可能高于页面上显示的值。CloudTrail 在事件副本的过程中以增量方式更新详细信息。

访问事件复制详细信息页面

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在左侧导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择事件数据存储。
4. 在 Event copy status（事件复制状态）部分中选择事件复制。

复制详细信息

在 Copy details（复制详细信息）中，您可以查看有关跟踪事件复制的以下详细信息。

- Event log S3 location（事件日志 S3 位置）– 包含跟踪事件日志文件的源 S3 存储桶的位置。

- Copy ID（复制 ID）– 复制的 ID。
- Prefixes copied（已复制的前缀）– 表示已复制的 S3 前缀的数量。在跟踪事件复制期间，将事件 CloudTrail 复制到存储在前缀中的跟踪日志文件中。
- Copy status（复制状态）– 复制的状态。
  - Initializing（正在初始化）– 跟踪事件复制开始时显示的初始状态。
  - In progress（正在进行中）– 表示跟踪事件复制正在进行中。

    > **Note**
    >
    > 当另一个跟踪事件复制 In progress（正在进行中）时，无法复制跟踪事件。要停止跟踪事件复制，请选择 Stop copy（停止复制）。

  - Stopped（已停止）– 表示发生了 Stop copy（停止复制）操作。要重试跟踪事件复制，请选择 Retry copy（重试复制）。
  - Failed（失败）– 复制已完成，但有些跟踪事件复制失败。查看 Copy failures（复制失败）中的错误消息。要重试跟踪事件复制，请选择 Retry copy（重试复制）。当您重试复制时，会在出现故障的位置 CloudTrail 恢复副本。
  - Completed（已完成）– 复制已完成，没有错误。您可以在事件数据存储中查询已复制的跟踪事件。
- Created time（创建时间）– 表示跟踪事件复制的开始时间。
- Finish time（完成时间）– 表示跟踪事件复制的完成或停止时间。

复制失败

在 Copy failures（复制失败）中，您可以查看每次复制失败的错误发生位置、错误消息和错误类型。常见的失败原因包括 S3 前缀是否包含未压缩的文件，或者是否包含由之外的CloudTrail服务交付的文件。另一个可能的失败原因与访问问题有关。例如，如果事件数据存储的 S3 存储桶未授予导入事件的 CloudTrail 访问权限，则会`AccessDenied`出现错误。

在每次复制失败时，查看以下错误信息。

- Error location（错误位置）– 表示 S3 存储桶中发生错误的位置。如果错误是由源 S3 存储桶包含未压缩的文件而导致的，则 Error location（错误位置）将包括您可以在其中找到该文件的前缀。
- Error message（错误消息）– 解释错误发生原因。
- Error type（错误类型）– 提供错误类型。例如，Error type（错误类型）`AccessDenied`显示错误原因为权限问题。有关复制跟踪事件所需权限的更多信息，请参阅 复制跟踪事件所需的权限。

解决所有失败问题后，选择 Retry copy（重试复制）。当您重试复制时，会在出现故障的位置 CloudTrail 恢复副本。

示例：将跟踪事件复制到新的事件数据存储中

本演练向您展示了如何将跟踪事件复制到新的 CloudTrail Lake 事件数据存储中以进行历史分析。有关复制跟踪事件的更多信息，请参阅 将跟踪事件复制到事件数据存储。

将跟踪事件复制到新的事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择 Create event data store（创建事件数据存储）。
4. 在 “配置事件数据存储” 页面的 “常规详细信息” 中，为您的事件数据存储命名，例如*my-management-events-eds*。作为最佳实践，请使用可快速识别事件数据存储用途的名称。有关 CloudTrail 命名要求的信息，请参见命名要求。
5. 选择您要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及您的事件数据存储的默认和最长保留期。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

   可用选项如下：

   - 一年可延期保留定价 - 如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），一般建议采用此选项。在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外收费。366 天后，可以按 pay-as-you-go 定价延长保留期。这是默认选项。
     - 默认保留期：366 天
     - 最长保留期：3653 天
   - 七年期保留定价 - 如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议采用此选项。保留包含在摄取定价中，没有额外费用。
     - 默认保留期：2557 天
     - 最长保留期：2557 天
6. 指定事件数据存储的保留期。一年可延期保留定价选项的保留期可以介于 7 天到 3653 天（大约 10 年）之间，七年期保留定价选项的保留期可以介于 7 天到 2557 天（约七年）之间。

   CloudTrail Lake 通过检查事件是否在`eventTime`指定的保留期内来确定是否保留该事件。例如，如果您将保留期指定为 90 天，`eventTime`则 CloudTrail 会删除超过 90 天的事件。

> **Note**
>
> CloudTrail 如果事件早于指定的保留期`eventTime`，则不会复制该事件。要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`*）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。

7. （可选）在加密中，选择是否要使用自己的 KMS 密钥加密事件数据存储。默认情况下，事件数据存储中的所有事件都 CloudTrail 使用为您 AWS 拥有和管理的 KMS 密钥进行加密。

   要使用自己的 KMS 密钥进行加密，请选择使用我自己的 AWS KMS key。选择 “新建” 为您 AWS KMS key 创建，或选择 “现有” 以使用现有 KMS 密钥。在输入 KMS 别名中，按格式指定别名`alias/`*`MyAliasName`*。使用自己的 KMS 密钥需要您编辑 KMS 密钥策略以允许对 CloudTrail 日志进行加密和解密。有关更多信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。

   > **Note**
   >
   > 要为组织事件数据存储启用 AWS Key Management Service 加密，必须使用管理账户的现有 KMS 密钥。

8. （可选）如果您想使用 Amazon Athena 对事件数据进行查询，请在 Lake 查询联合身份验证中选择启用。通过联合身份验证，您可以在 AWS Glue 数据目录中查看与事件数据存储相关的元数据，并在 Athena 中对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅 联合事件数据存储。

   要启用 Lake 查询联合身份验证，请选择启用，然后执行以下操作：

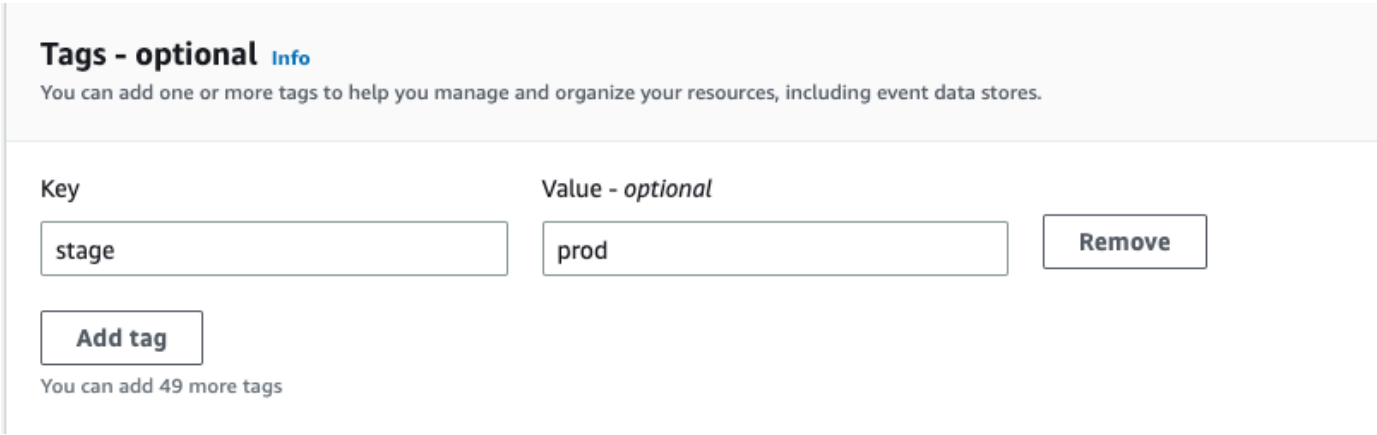
a. 选择是要创建新角色还是使用现有 IAM 角色。AWS Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时，CloudTrail 会自动创建一个具有所需权限的角色。如果您选择现有角色，请确保该角色的策略提供所需的最低权限。

b. 如果您在创建新角色，请输入名称来标识该角色。

c. 如果您使用现有角色，请选择要使用的角色。角色必须存在于您的账户中。

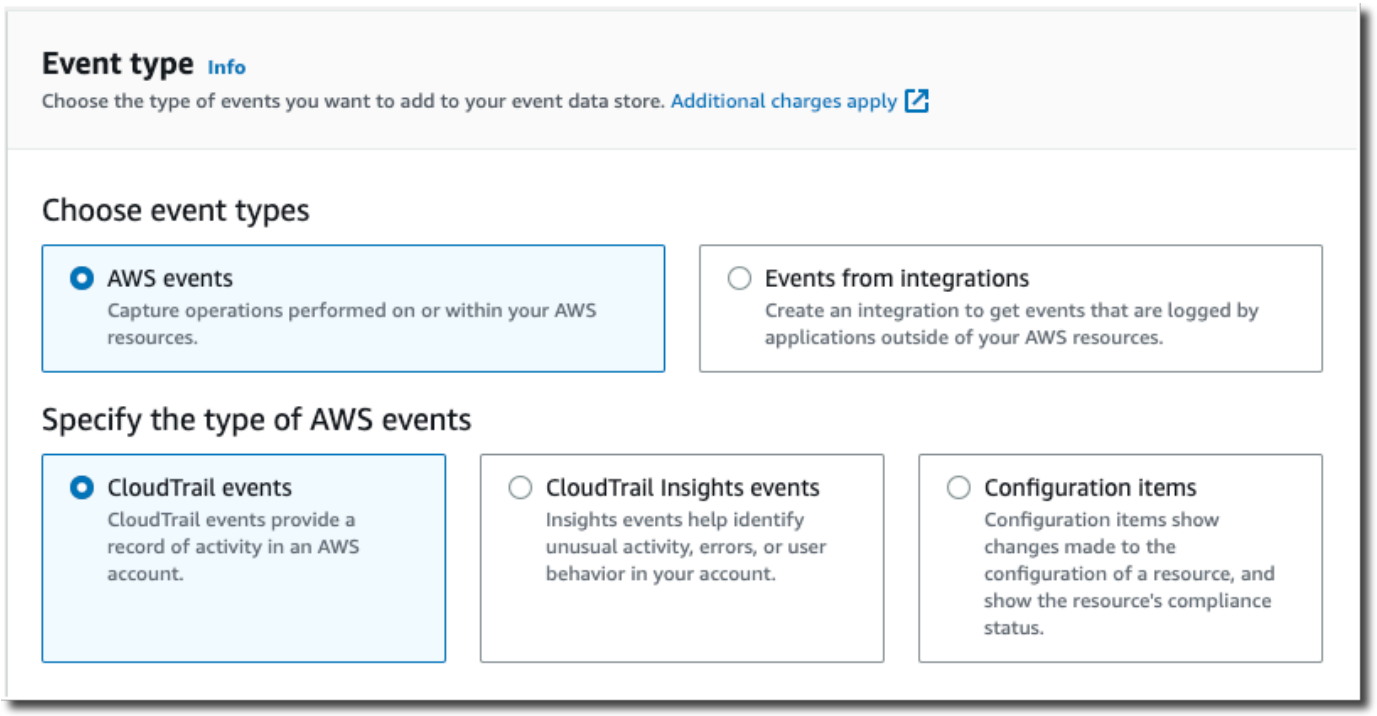
9. （可选）在标签中，将一个或多个自定义标签（键值对）添加到事件数据存储中。标签可以帮助您识别 CloudTrail 事件数据存储。例如，您可以附加名称为 **`stage`**、值为 **`prod`** 的标签。您可以使用标签来限制对事件数据存储的访问。您还可以使用标签来跟踪事件数据存储的查询和摄取成本。

   有关如何使用标签跟踪成本的信息，请参阅 为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签。有关如何使用 IAM 策略根据标签授权对事件数据存储的访问，请参阅 示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的信息 AWS，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。



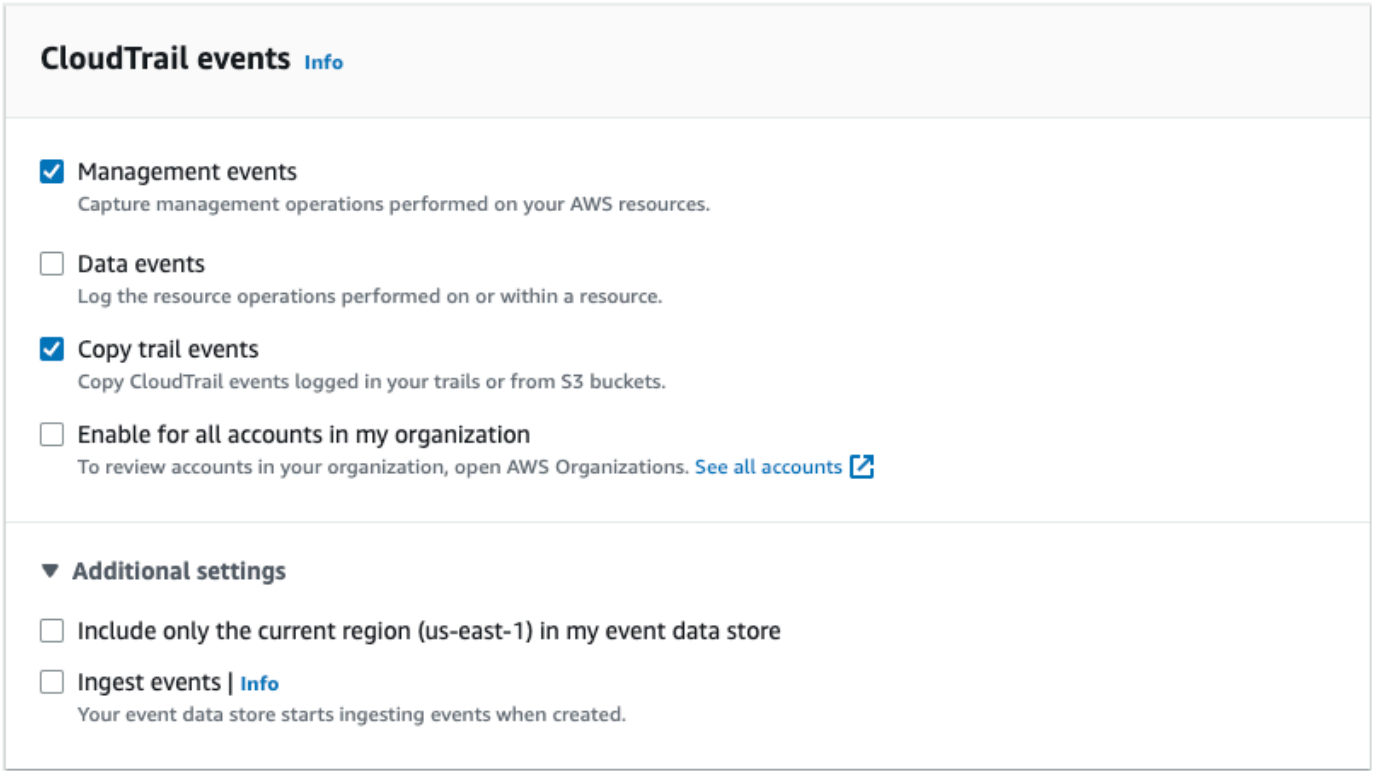
10. 选择 Next（下一步）以配置事件数据存储。

11. 在选择事件页面上，保留事件类型的默认选择。



12. 对于CloudTrail 事件，我们将选中 “管理” 事件，然后选择 “复制跟踪事件”。在此示例中，我们并不关心事件类型，因为我们仅使用事件数据存储来分析过去的事件，而不是摄取未来的事件。

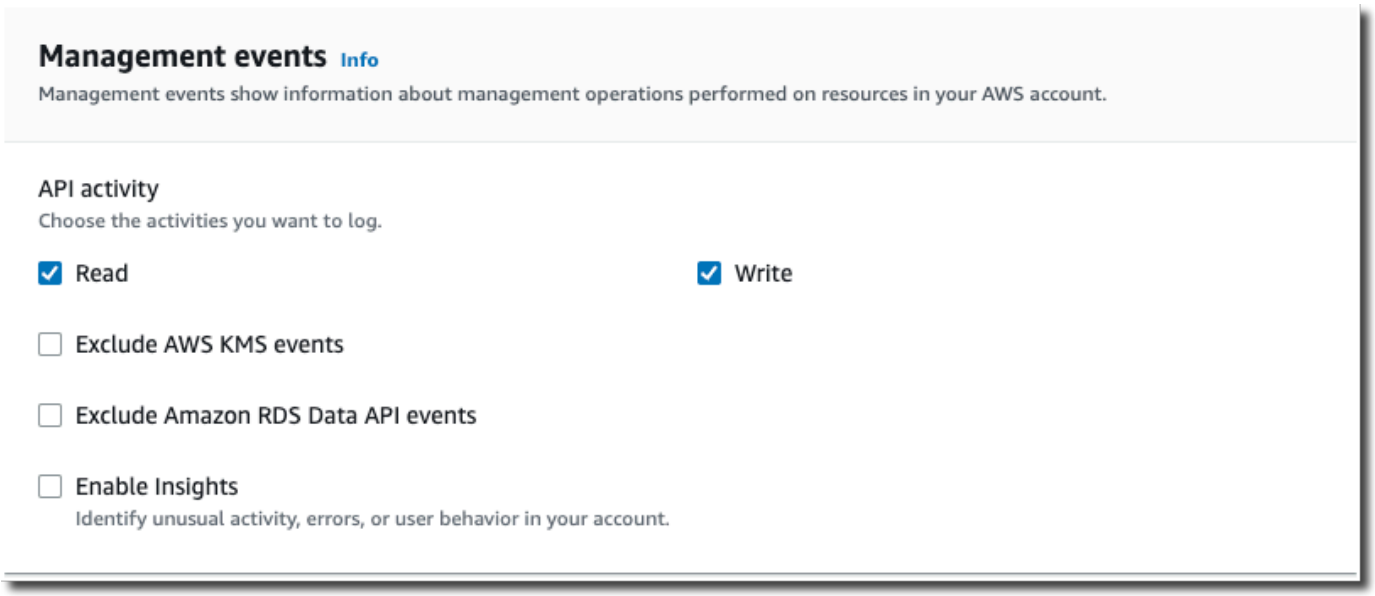
    如果您要创建事件数据存储来替换现有的跟踪，请选择与您的跟踪相同的事件选择器，以确保事件数据存储具有相同的事件覆盖范围。



13. 如果这是组织事件数据存储，请选择为我组织中的所有账户启用。除非您在 AWS Organizations中配置了账户，否则此选项将不能进行更改。

> **Note**
>
> 如果您要创建组织事件数据存储，则必须使用组织的管理账户登录，因为只有管理账户才能将跟踪事件复制到组织事件数据存储。

14. 对于其他设置，我们将取消选择摄取事件，因为在此示例中，我们不希望事件数据存储摄取任何未来事件，我们只对查询复制的事件感兴趣。默认情况下，事件数据存储会收集所有人的事件，AWS 区域 并在创建事件时开始摄取事件。
15. 对于管理事件，我们将保留默认设置。



16. 在复制跟踪事件区域中，完成以下步骤。

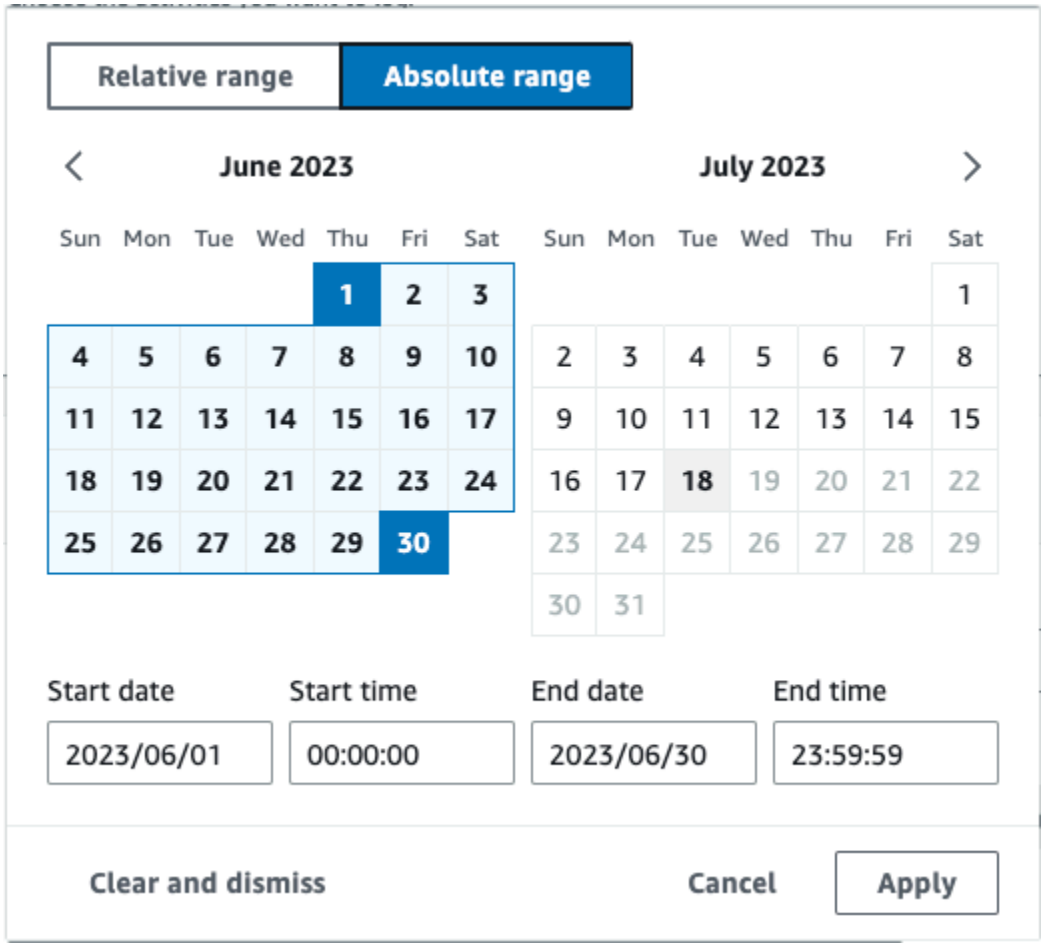
    a. 选择要复制的跟踪。在此示例中，我们将选择一个名为 *`management-events`* 的跟踪。

    默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的前缀，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，请选择输入 S3 URI，然后选择浏览 S3 浏览到该前缀。如果跟踪的源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密数据。如果您的源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。有关更新 KMS 密钥政策的更多信息，请参阅 用于解密源 S3 存储桶中数据的 KMS 密钥政策。

b. 选择复制事件的时间范围。 CloudTrail 在尝试复制跟踪事件之前，请检查前缀和日志文件名以验证该名称是否包含所选开始日期和结束日期之间的日期。您可以选择 Relative range（相对范围）或者 Absolute range（绝对范围）。为避免源跟踪和目标事件数据存储之间存在重复事件，请选择一个早于事件数据存储创建时间的时间范围。

- 如果选择 “相对范围”，则可以选择复制过去 6 个月、1 年、2 年、7 年或自定义范围内记录的事件。 CloudTrail 复制选定时间段内记录的事件。
- 如果选择 “绝对范围”，则可以选择特定的开始和结束日期。 CloudTrail 复制在所选开始日期和结束日期之间发生的事件。

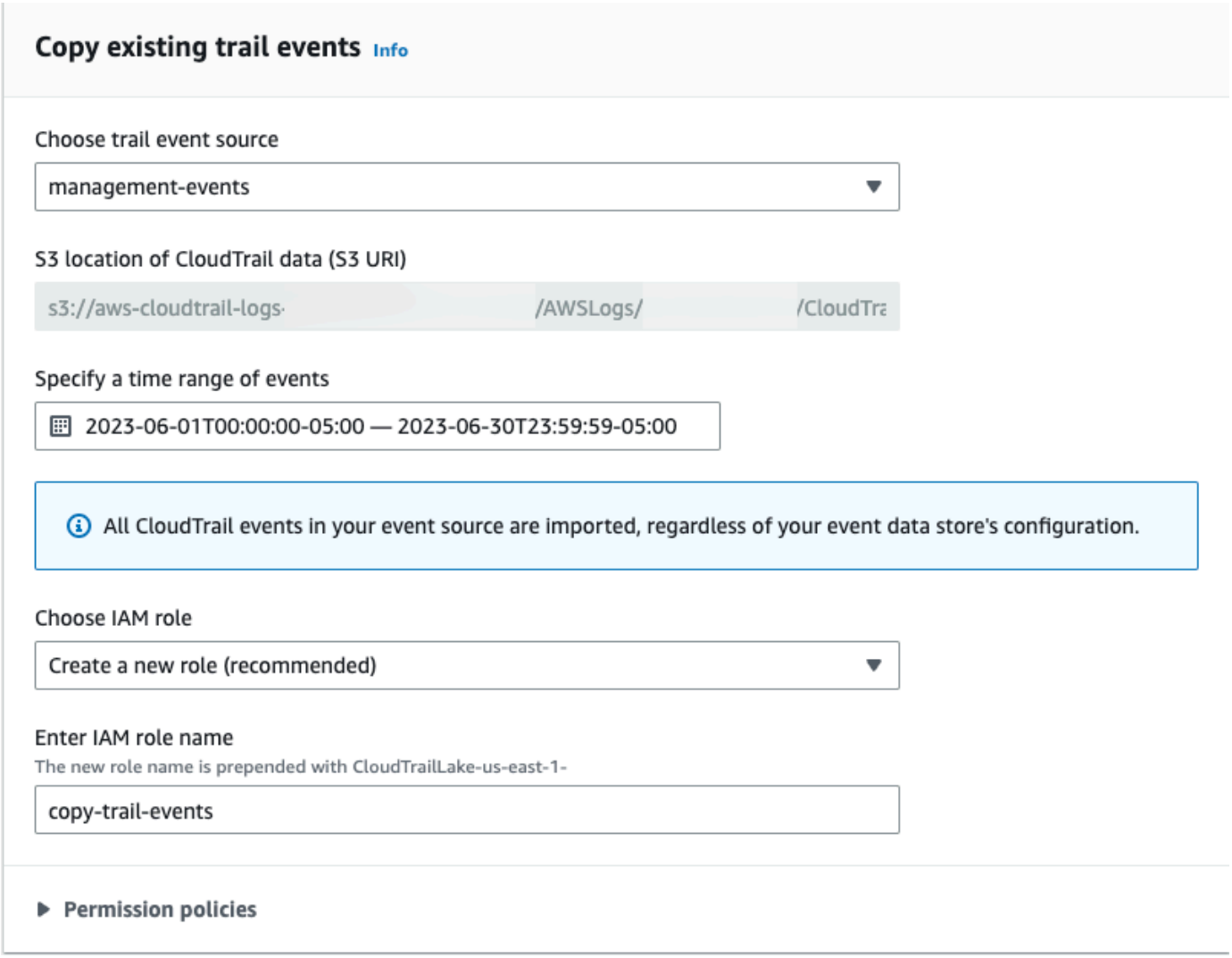
在此示例中，我们将选择绝对范围，然后选择整个 6 月份。



c. 对于 Permissions（权限），请从以下 IAM 角色选项中进行选择。如果您选择现有的 IAM 角色，请验证 IAM 角色策略是否提供了必要的权限。有关更新 IAM 角色权限的更多信息，请参阅 复制跟踪事件所需的 IAM 权限。

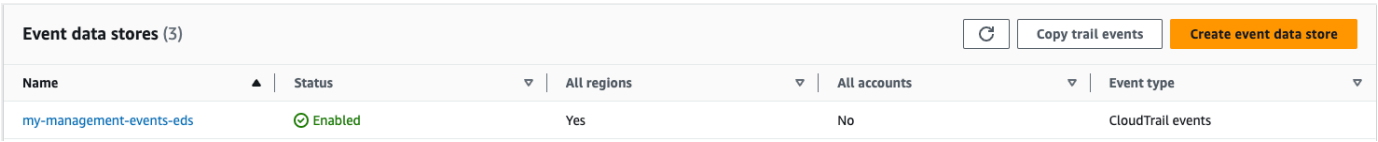
- 选择 Create a new role (recommended)（创建新角色（推荐））以创建新的 IAM 角色。在输入 IAM 角色名称中，输入角色的名称。 CloudTrail 会自动为这个新角色创建必要的权限。
- 选择使用自定义 IAM 角色 ARN 以使用未列出的自定义 IAM 角色。对于 Enter IAM role ARN（输入 IAM 角色 ARN），输入 IAM ARN。
- 从下拉列表中选择现有的 IAM 角色。

在此示例中，我们将选择新建角色（推荐）并提供名称 **`copy-trail-events`**。



17. 选择 Next（下一步）以查看您的选择。
18. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Edit（编辑）以对这节进行更改。当您准备好创建事件数据存储时，选择 Create event data store（创建事件数据存储）。

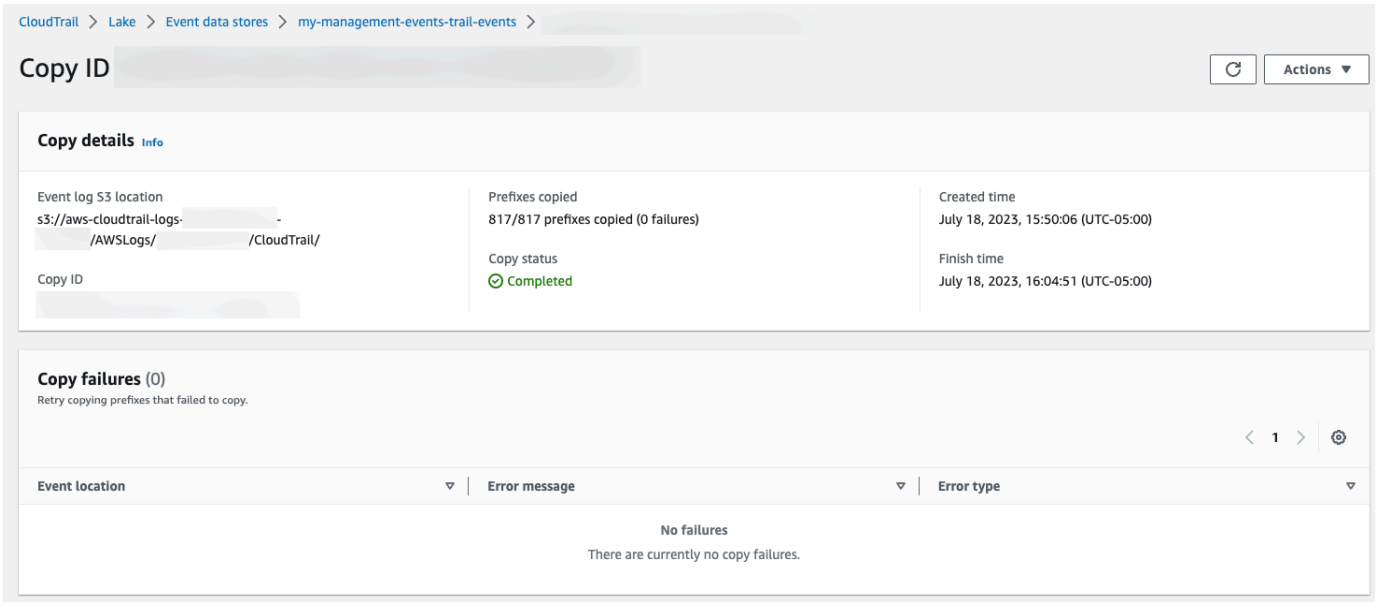
19. 在事件数据存储页面上的事件数据存储表中可以看到新的事件数据存储。



20. 选择事件数据存储名称以查看其详细信息页面。详细信息页面显示事件数据存储的详细信息以及复制状态。事件复制状态显示在事件复制状态区域中。

    跟踪事件复制完成后，如果复制未出错，则 Copy status（复制状态）将设置为 Completed（已完成），否则如果出错了，则设置为 Failed（失败）。

21. 要查看有关复制的更多详细信息，请在事件日志 S3 位置列中选择复制名称，或从操作菜单中选择查看详细信息选项。有关查看跟踪事件复制详细信息的更多信息，请参阅 事件复制详细信息。



22. 复制失败区域显示复制跟踪事件时发生的所有错误。如果 Copy status（复制状态）为 Failed（失败），则要先修复 Copy failures（复制失败）中显示的所有错误，然后选择 Retry copy（重试复制）。当您重试复制时，会在出现故障的位置 CloudTrail 恢复副本。

联合事件数据存储

联合事件数据存储允许您在数据目录中查看与事件数据存储相关的元数据，向注册 AWS Glue 数据目录 AWS Lake Formation，并允许您使用 Amazon Athena 对事件数据运行 SQL 查询。存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。

您可以使用 CloudTrail 控制台 AWS CLI、或 EnableFederationAPI 操作启用联合。启用 Lake 查询联合后， CloudTrail将在 AWS Glue 数据目录中创建一个名为`aws:cloudtrail`（如果该数据库尚不存在）的托管数据库和一个托管联合表。事件数据存储 ID 用于表名。 CloudTrail 在中注册联合角色 ARN 和事件数据存储 AWS Lake Formation，该服务负责允许对数据目录中的联合资源进行精细的访问控制。 AWS Glue

要启用 Lake 查询联合身份验证，您必须创建新的 IAM 角色或选择现有角色。Lake Formation 使用此角色管理联合事件数据存储的权限。使用 CloudTrail 控制台创建新角色时， CloudTrail 会自动为该角色创建所需的权限。如果您选择现有角色，请确保该角色提供最低权限。

您可以使用 CloudTrail 控制台 AWS CLI、或 DisableFederationAPI 操作禁用联合。当您禁用联合身份验证时，会禁 CloudTrail用与 AWS Glue AWS Lake Formation、和 Amazon Athena 的集成。禁用 Lake 查询联合身份验证后，您将无法再在 Athena 中查询事件数据。禁用联合后，不会删除任何 CloudTrail Lake 数据，并且您可以继续在 CloudTrail Lake 中运行查询。

联合 L CloudTrail ake 事件数据存储不 CloudTrail 收取任何费用。在 Amazon Athena 中运行查询将会产生费用。有关 Athena 定价的更多信息，请参阅 Amazon Athena 定价。

使用 La AWS CloudTrail ke 和 Amazon Athena 分析活动日志

主题

- 注意事项
- 联合身份验证所需的权限
- 启用 Lake 查询联合身份验证
- 禁用 Lake 查询联合身份验证
- 使用管理 CloudTrail 湖联盟资源 AWS Lake Formation

注意事项

联合事件数据存储时，请考虑以下因素：

- 联合 L CloudTrail ake 事件数据存储不 CloudTrail 收取任何费用。在 Amazon Athena 中运行查询将会产生费用。有关 Athena 定价的更多信息，请参阅 Amazon Athena 定价。

- Lake Formation 用于管理联合资源的权限。如果您删除了联合角色，或者从 Lake Formation 中撤消了对资源的权限 AWS Glue，或者，则无法从 Athena 运行查询。有关使用 Lake Formation 的更多信息，请参阅 使用管理 CloudTrail 湖联盟资源 AWS Lake Formation。
- 使用 Amazon Athena 查询向 Lake Formation 注册的数据的任何人都必须有一个 IAM 权限策略，此权限允许执行 `lakeformation:GetDataAccess` 操作。 AWS 托管策略：AmazonAthenaFullAccess允许此操作。如果您使用内联策略，请务必更新权限策略以允许此操作。有关更多信息，请参阅管理 Lake Formation 和 Athena 用户权限。
- 要在 Athena 中的联合表上创建视图，您需要一个除 `aws:cloudtrail` 之外的目标数据库。这是因为`aws:cloudtrail`数据库由管理 CloudTrail。
- 要在 Amazon 中创建数据集 QuickSight，您必须选择 “使用自定义 SQL” 选项。有关更多信息，请参阅使用 Amazon Athena 数据创建数据集。
- 如果启用了联合身份验证，则无法删除事件数据存储。要删除联合事件数据存储，必须先禁用联合身份验证和终止保护（如果已启用）。
- 以下注意事项适用于组织事件数据存储：
  - 只有一个委托管理员账户或管理账户才能在组织事件数据存储上启用联合身份验证。其他委托管理员账户仍可以使用 Lake Formation 数据共享功能查询和共享信息。
  - 任何委托管理员账户或组织的管理账户都可以禁用联合身份验证。

联合身份验证所需的权限

在联合事件数据存储之前，请确保您拥有联合身份验证角色以及启用和禁用联合身份验证所需的所有权限。如果您选择现有 IAM 角色来启用联合身份验证，则只需要更新联合身份验证角色权限。如果您选择使用 CloudTrail 控制台创建新的 IAM 角色，请为该角色 CloudTrail 提供所有必要的权限。

主题

- 联合事件数据存储的 IAM 权限
- 启用联合身份验证所需的权限
- 禁用联合身份验证所需的权限

联合事件数据存储的 IAM 权限

启用联合身份验证时，您可以选择创建新的 IAM 角色，也可以使用现有 IAM 角色。当您选择新的 IAM 角色时， CloudTrail 会创建一个具有所需权限的 IAM 角色，您无需采取任何进一步的操作。

如果您选择现有角色，请确保 IAM 角色的策略提供启用联合身份验证所需的权限。此部分提供所需 IAM 角色权限和信任策略的示例。

以下示例提供联合身份验证角色的权限策略。在第一个声明中，请提供 Resource 的事件数据存储的完整 ARN。

本策略的第二个声明允许 Lake Formation 解密使用 KMS 密钥加密的事件数据存储的数据。将 *key-region*、*account-id* 和 *key-id* 替换为您的 KMS 密钥的值。如果事件数据存储未使用 KMS 密钥进行加密，则可省略此声明。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

以下示例提供了 IAM 信任策略，该策略允许 AWS Lake Formation 代入 IAM 角色以管理联合事件数据存储的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

启用联合身份验证所需的权限

以下示例策略提供了在事件数据存储上启用联合身份验证所需的最低权限。此策略 CloudTrail 允许在事件数据存储上启用联合、 AWS Glue 在 AWS Glue 数据目录中创建联合资源以及 AWS Lake Formation 管理资源注册。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
```

```
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

禁用联合身份验证所需的权限

以下示例策略提供了在事件数据存储上禁用联合身份验证所需的最低资源。此策略 CloudTrail 允许在事件数据存储上禁用联合，AWS Glue 删除 AWS Glue 数据目录中的托管联合表，以及 Lake Formation 取消注册联合资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "Allow Lake Formation to deregister the resource",
```

```
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

启用 Lake 查询联合身份验证

您可以使用 CloudTrail 控制台、或 EnableFederationAPI 操作启用 Lak AWS CLI e 查询联合。启用 Lake 查询联合后， CloudTrail 将在 AWS Glue 数据目录中创建一个名为`aws:cloudtrail`（如果该数据库尚不存在）的托管数据库和一个托管联合表。事件数据存储 ID 用于表名。 CloudTrail 在中注册联合角色 ARN 和事件数据存储 AWS Lake Formation，该服务负责允许对数据目录中的联合资源进行精细的访问控制。 AWS Glue

本节介绍如何使用 CloudTrail 控制台和启用联合 AWS CLI。

CloudTrail console

以下过程演示了如何对现有事件数据存储启用 Lake 查询联合身份验证。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择要更新的事件数据存储。此操作会打开事件数据存储的详细信息页面。
4. 在 Lake 查询联合身份验证中，选择编辑，然后选择启用。
5. 选择是创建新的 IAM 角色还是使用现有角色。创建新角色时， CloudTrail 会自动创建一个具有所需权限的角色。如果您使用现有角色，请确保该角色的策略提供所需的最低权限。
6. 如果您在创建新的 IAM 角色，请为该角色输入名称。
7. 如果您选择现有的 IAM 角色，请选择要使用的角色。角色必须存在于您的账户中。
8. 选择保存更改。联合身份验证状态更改为 `Enabled`。

AWS CLI

要启用联合身份验证，请运行 aws cloudtrail enable-federation 命令，以提供所需的 --event-data-store 和 --role 参数。对于 --event-data-store，请提供事件数据存储 ARN（或 ARN 的 ID 后缀）。对于 --role，请提供您的联合身份验证角色的 ARN。该角色必须存在于您的账户中，并提供所需的最低权限。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

此示例说明委托管理员如何通过在管理账户中指定事件数据存储的 ARN 和在委托管理员账户中指定联合身份验证角色的 ARN 来在组织事件数据存储上启用联合身份验证。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

禁用 Lake 查询联合身份验证

您可以使用 CloudTrail 控制台 AWS CLI、或 DisableFederationAPI 操作禁用联合。当您禁用联合身份验证时，会禁 CloudTrail 用与 AWS Glue AWS Lake Formation、和 Amazon Athena 的集成。禁用 Lake 查询联合身份验证后，您将无法再在 Athena 中查询事件数据。禁用联合后，不会删除任何 CloudTrail Lake 数据，并且您可以继续在 CloudTrail Lake 中运行查询。

本节介绍如何使用 CloudTrail 控制台和禁用联合 AWS CLI。

CloudTrail console

以下过程演示了如何对现有事件数据存储禁用 Lake 查询联合身份验证。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择要更新的事件数据存储。此操作会打开事件数据存储的详细信息页面。
4. 在 Lake 查询联合身份验证中，选择编辑，然后选择禁用。
5. 选择保存更改。联合身份验证状态更改为 `Disabled`。

AWS CLI

要在事件数据存储上禁用联合身份验证，请运行 aws cloudtrail disable-federation 命令。事件数据存储由 `--event-data-store` 指定，它接受事件数据存储 ARN 或 ARN 的 ID 后缀。

```
aws cloudtrail disable-federation
```

```
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> 如果这是组织事件数据存储，则使用管理账户的账户 ID。

使用管理 CloudTrail 湖联盟资源 AWS Lake Formation

联合事件数据存储时，在其中 CloudTrail 注册联合角色 ARN 和事件数据存储，该服务负责允许对数据目录 AWS Lake Formation中的联合资源进行精细访问控制。 AWS Glue 本节介绍如何使用 Lake Formation 来管理 CloudTrail 湖联盟资源。

启用联合后， CloudTrail 将在 AWS Glue 数据目录中创建以下资源。

- 托管数据库-使用`aws:cloudtrail`每个账户的名称 CloudTrail 创建 1 个数据库。 CloudTrail 管理数据库。您无法在中删除或修改数据库 AWS Glue。
- 托管联合表-为每个联合事件数据存储 CloudTrail 创建 1 个表，并使用事件数据存储 ID 作为表名。 CloudTrail 管理表。您无法删除或修改中的表 AWS Glue。要删除表，您必须在事件数据存储上禁用联合身份验证。

控制对联合资源的访问权

您可以使用两种权限方法中的一种来控制对托管数据库和表的访问权。

- 仅限 IAM 访问控制 – 通过仅限 IAM 访问控制，账户中具有所需 IAM 权限的所有用户均可访问所有数据目录资源。有关如何 AWS Glue 使用 IAM 的信息，请参阅如何 AWS Glue 使用 IAM。

  在 Lake Formation 控制台上，此方法显示为仅使用 IAM 访问控制。

  > **Note**
  >
  > 如果要创建数据筛选条件并使用其他 Lake Formation 功能，必须使用 Lake Formation 访问控制。

- Lake Formation 访问控制 – 这种方法具有以下优势。
  - 您可以通过创建数据筛选条件来实现列级别、行级别和单元格级别安全性。

- 数据库和表仅可见于 Lake Formation 管理员以及数据库和资源的创建者。如果其他用户需要访问这些资源，则必须使用 Lake Formation 权限明确授予访问权。

有关访问控制的更多信息，请参阅精细访问控制的方法。

确定联合资源的权限方法

首次启用联合时，使用您的 Lake Formation 数据湖设置 CloudTrail 创建托管数据库和托管联合表。

CloudTrail 启用联合后，您可以通过检查托管数据库和托管联合表的权限来验证您对托管数据库和托管联合表使用的是哪种权限方法。如果资源存在 ALL（Super）到 IAM_ALLOWED_PRINCIPALS 设置，则该资源将由 IAM 权限独家管理。如果缺少该设置，则资源将由 Lake Formation 权限管理。有关 Lake Formation 权限的更多信息，请参阅 Lake Formation 权限参考。

托管数据库和托管联合表的权限方法可能有所不同。例如，如果您检查数据库和表的值，可能会看到以下内容：

- 对于数据库，将 ALL（Super）分配给 IAM_ALLOWED_PRINCIPALS 的值存在于权限中，表示您对数据库使用仅限 IAM 访问控制。
- 对于表，将 ALL（Super）分配给 IAM_ALLOWED_PRINCIPALS 的值不存在，表示通过 Lake Formation 权限进行访问控制。

您可以随时在访问方法之间切换，方法是在 Lake Formation 中的任何联合资源上添加或移除 ALL（Super）到 IAM_ALLOWED_PRINCIPALS 权限。

使用 Lake Formation 进行跨账户共享

本部分介绍如何使用 Lake Formation 在账户之间共享托管数据库和托管联合表。

通过执行以下步骤，您可以跨账户共享托管数据库：

1. 将跨账户数据共享版本更新为版本 4。
2. 从数据库中移除 Super 到 IAM_ALLOWED_PRINCIPALS 权限（如果有），以切换到 Lake Formation 访问控制。
3. 向数据库上的外部账户授予 Describe 权限。
4. 如果与您共享了数据目录资源， AWS 账户 并且您的账户与共享账户不在同一个 AWS 组织中，请接受 AWS Resource Access Manager (AWS RAM) 的资源共享邀请。有关更多信息，请参阅接受 AWS RAM 的资源共享邀请。

完成这些步骤后，数据库应对外部账户可见。默认情况下，共享数据库不允许访问数据库中的任何表。

您可以通过执行以下步骤与外部账户共享所有托管联合表或单个托管联合表：

1. 将跨账户数据共享版本更新为版本 4。
2. 从表中移除 Super 到 IAM_ALLOWED_PRINCIPALS 权限（如果有），以切换到 Lake Formation 访问控制。
3. （可选）指定任何数据筛选条件以限制列或行。
4. 向表上的外部账户授予 Select 权限。
5. 如果与您共享了数据目录资源， AWS 账户 并且您的账户与共享账户不在同一个 AWS 组织中，请接受 AWS Resource Access Manager (AWS RAM) 的资源共享邀请。对于组织，您可以使用 RAM 设置来自动接受。有关更多信息，请参阅接受 AWS RAM 的资源共享邀请。
6. 表格现在应可见。要在此表上启用 Amazon Athena 查询，请使用共享表在此账户中创建资源链接。

拥有者账户可以随时撤消共享，方法是从 Lake Formation 中删除外部账户的权限，或者在中禁用联合。 CloudTrail

组织事件数据存储

如果您在中创建了组织 AWS Organizations，则可以创建一个组织事件数据存储，用于记录该组织 AWS 账户 中所有人的所有事件。组织事件数据存储可以应用于所有区域 AWS 区域，也可以应用于当前区域。您不能使用组织事件数据存储从 AWS之外收集事件。

您可以使用管理账户或委派管理员账户创建组织事件数据存储。委托管理员创建组织事件数据存储时，组织事件数据存储存在于组织的管理账户中。之所以采用这种方法，是因为管理账户保留对所有组织资源的所有权。

组织的管理账户可以更新账户级事件数据存储以将其应用于组织。

在将组织事件数据存储指定为应用于某个组织时，它将自动应用于该组织中的所有成员账户。成员账户无法查看组织事件数据存储，也无法对其进行修改或删除。默认情况下，成员账户无权访问组织事件数据存储，也不能对组织事件数据存储进行查询。

下表显示了 AWS Organizations 组织内管理账户和委派管理员账户的权能。

功能	管理账户	委托管理员账户
注册或移除委托管理员账户。	是	不支持
为事件或 AWS Config 配置项目创建组织 AWS CloudTrail 事件数据存储。	支持	是
在组织事件数据存储上启用 Insights。	是	不支持
更新组织事件数据存储。	是	是[1]
在组织事件数据存储上启用 Lake 查询联合身份验证。[2]	支持	是
在组织事件数据存储上禁用 Lake 查询联合身份验证。	支持	是
删除组织事件数据存储。	支持	是
将跟踪事件复制到事件数据存储。	是	不支持
对组织事件数据存储运行查询。	支持	是
查看组织事件数据存储的 CloudTrail Lake 控制面板。	支持	是

[1] 只有管理账户才能将组织事件数据存储转换为账户级事件数据存储，或者将账户级事件数据存储转换为组织事件数据存储。因为组织事件数据存储仅存在于管理账户中，所以不允许委托管理员执行这些操作。将组织事件数据存储转换为账户级事件数据存储时，只有管理账户才能访问该事件数据存储。同样，只有管理账户中的账户级事件数据存储才能转换为组织事件数据存储。

[2]只有一个委托管理员账户或管理账户才能在组织事件数据存储上启用联合身份验证。其他委托管理员账户可以使用 Lake Formation 数据共享功能查询和共享信息。任何委托管理员账户以及组织的管理账户都可以禁用联合身份验证。

创建组织事件数据存储

组织的管理帐户或委托管理员帐户可以创建组织事件数据存储以收集 CloudTrail 事件（管理事件、数据事件）或 AWS Config 配置项目。

> **Note**
>
> 只有组织的管理账户才能将跟踪事件复制到事件数据存储中。

CloudTrail console

使用控制台创建组织事件数据存储

1. 按照为事件创建事件数据存储过程中的步骤，为 CloudTrail 管理 CloudTrail 事件或数据事件创建组织事件数据存储。

   或者

   按照为配置项目创建事件数据存储过程中的步骤为 AWS Config 配置项目创建组织事件数据存储。 AWS Config
2. 在选择活动页面上，为我的组织中的所有账户选择启用。

AWS CLI

要创建组织事件数据存储，请运行create-event-data-store命令并添加`--organization-enabled`选项。

以下示例 AWS CLI `create-event-data-store`命令创建了一个收集所有管理事件的组织事件数据存储。由于默认情况下会 CloudTrail 记录管理事件，因此如果您的事件数据存储正在记录所有管理事件并且未收集任何数据事件，则无需指定高级事件选择器。

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
```

```
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

下一个示例 AWS CLI create-event-data-store命令创建一个名为的组织事件数据存储config-items-org-eds，用于收集 AWS Config 配置项目。要收集配置项目，请在高级事件选择器ConfigurationItem中指定该eventCategory字段等于。

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

将账户级别的事件数据存储应用于组织

组织的管理账户可以转换账户级事件数据存储以将其应用于组织。

CloudTrail console

使用控制台更新账户级别的事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 选择要更新的事件数据存储。此操作会打开事件数据存储的详细信息页面。
4. 在 General details（一般详细信息）中，选择 Edit（编辑）。
5. 为我组织中的所有账户选择 “启用”。
6. 选择保存更改。

有关更新事件数据存储的其他信息，请参阅使用控制台更新事件数据存储。

AWS CLI

要更新账户级事件数据存储以将其应用于组织，请运行update-event-data-store命令并添加选项。`--organization-enabled`

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

另请参阅

- 组织的委托管理员
- 添加 CloudTrail 委派管理员
- 移除 CloudTrail 委派的管理员

与外部的事件源创建集成 AWS

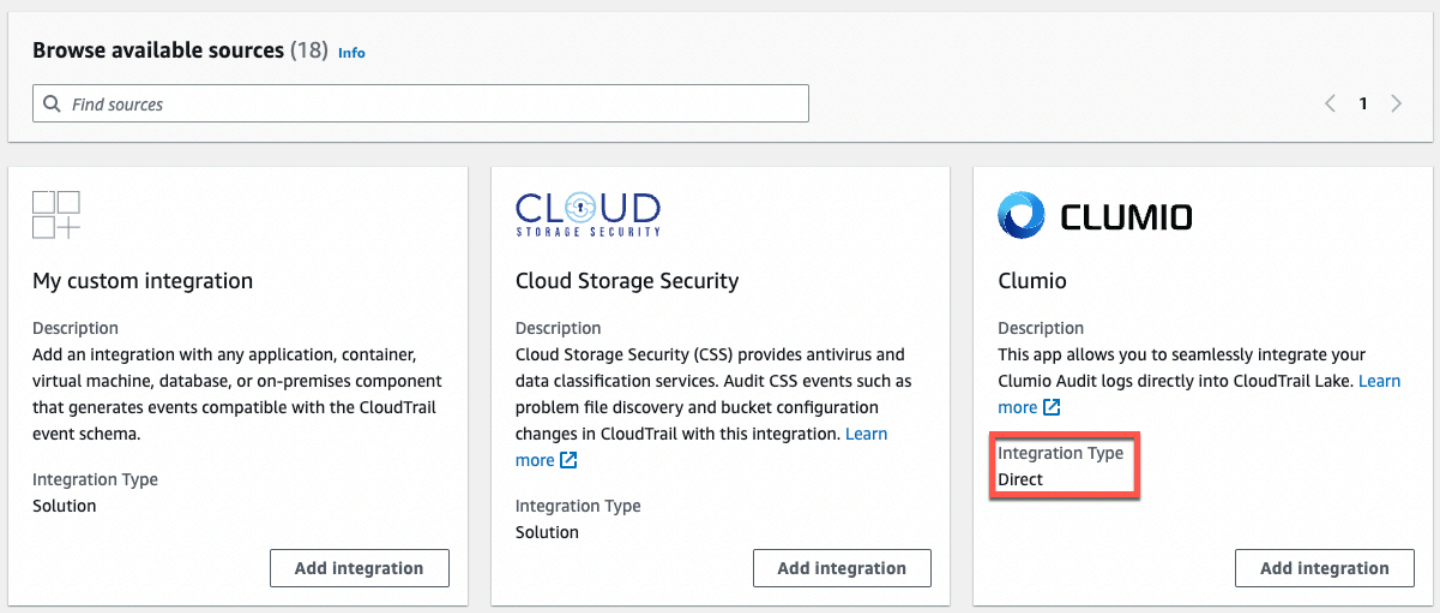
您可以使用 CloudTrail 来记录和存储混合环境中任何来源的用户活动数据，例如本地或云端托管的内部或 SaaS 应用程序、虚拟机或容器。您无需维护多个日志聚合器和报告工具，即可对这些数据进行存储、访问、分析、故障排除和操作。

来自非AWS 来源的活动通过使用渠道将与 CloudTrail您合作的外部合作伙伴或您自己的来源的活动带入 CloudTrail Lake。在创建通道时，您可以选择一个或多个事件数据存储，用于存储来自通道来源的事件。只要将目标事件数据存储设置为记录 `eventCategory="ActivityAuditLog"` 事件，即可根据需要更改通道的目标事件数据存储。当您为来自外部合作伙伴的活动创建通道时，您需要向合作伙伴或来源应用程序提供通道 ARN。附加到该通道的资源策略允许来源通过该通道传输事件。如果通道没有资源策略，则只有通道所有者可以针对该通道调用 `PutAuditEvents` API。

CloudTrail 已与许多事件源提供商合作，例如Okta和。 LaunchDarkly当你创建与外部事件源的集成时 AWS，你可以选择其中一个合作伙伴作为你的事件源，或者选择 “我的自定义集成”，将来自你自己来源的事件集成到 CloudTrail。每个来源最多允许一个通道。

有两种类型的集成：直接集成和解决方案集成。通过直接集成，合作伙伴可以调用 `PutAuditEvents` API 将事件传送到您 AWS 账户的事件数据存储。通过解决方案集成，应用程序将在您的 AWS 账户中运行，应用程序会调用 `PutAuditEvents` API 将事件传送到您 AWS 账户的事件数据存储。

在 Integrations（集成）页面上，您可以选择 Available sources（可用来源）选项卡，以查看合作伙伴的 Integration type（集成类型）。



首先，使用 CloudTrail 控制台创建一个集成，以记录来自合作伙伴或其他应用程序来源的事件。

主题

- 使用控制台创建与 CloudTrail 合作伙伴的集成
- 创建与控制台的自定义集成
- 使用 Lake 创建、更新和管理 CloudTrail Lake 集成 AWS CLI

- 有关集成合作伙伴的其他信息
- CloudTrail 湖泊集成事件架构

使用控制台创建与 CloudTrail 合作伙伴的集成

当您创建与外部事件源的集成时 AWS，可以选择其中一个合作伙伴作为您的事件源。当您创建 CloudTrail 与合作伙伴应用程序的集成时，合作伙伴需要您在此工作流程中创建的渠道的 Amazon 资源名称 (ARN) 才能向其发送事件。 CloudTrail在创建集成后，您可以按照合作伙伴的说明向合作伙伴提供所需的通道 ARN，以完成集成的配置。在合作伙伴调`PutAuditEvents`用整合频道 CloudTrail 后，集成开始将合作伙伴事件引入其中。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，打开 Lake 子菜单，然后选择集成。
3. 在 Add integration（添加集成）页面上，为您的通道输入名称。该名称可以包含 3-128 个字符。只允许使用字母、数字、句点、下划线和短划线。
4. 选择要从中获取事件的合作伙伴应用程序来源。如果您要与来自您自己的应用程序（在本地或云中托管）的事件集成，请选择 My custom integration（我的自定义集成）。
5. 在 Event delivery location（事件传送位置）中，选择将相同活动事件记录到现有事件数据存储中，或创建新的事件数据存储。

   如果您选择创建新的事件数据存储，请输入事件数据存储的名称，选择定价选项，并以天为单位指定保留期。事件数据存储将保留指定天数内的事件数据。

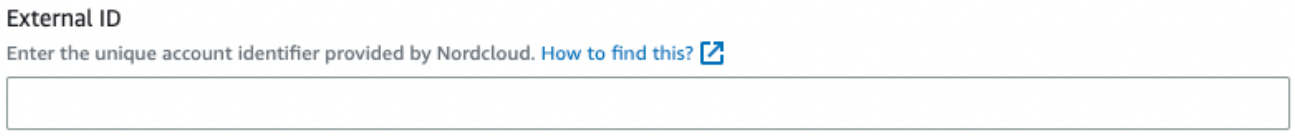
   如果您选择将活动事件记录到一个或多个现有事件数据存储中，请从列表中选择事件数据存储。事件数据存储只能包含活动事件。控制台中的事件类型必须是 Events from integrations（来自集成的事件）。在 API 中，`eventCategory` 值必须为 `ActivityAuditLog`。
6. 在 Resource policy（资源策略）中，为集成的通道配置资源策略。资源策略是 JSON 策略文档，它们指定了指定主体可在资源上执行的操作，以及在什么条件下执行操作。在资源策略中定义为主体的账户可以调用 `PutAuditEvents` API，以向您的通道传送事件。如果资源所有者的 IAM policy 允许 `cloudtrail-data:PutAuditEvents` 操作，则资源所有者将拥有对资源的隐式访问权限。

   该策略所需的信息由集成类型决定。对于方向集成， CloudTrail 会自动添加合作伙伴的 AWS 账户 ID，并要求您输入合作伙伴提供的唯一外部 ID。对于解决方案集成，您必须将至少一个 AWS 账户 ID 指定为委托人，并且可以选择输入外部 ID 以防止副手感到困惑。

> **Note**
>
> 如果您没有为通道创建资源策略，则只有通道所有者可以针对该通道调用 `PutAuditEvents` API。

a. 对于直接集成，请输入您的合作伙伴提供的外部 ID。集成合作伙伴将提供唯一的外部 ID（如账户 ID 或随机生成的字符串）用于集成，以防范混淆代理。合作伙伴负责创建和提供唯一的外部 ID。

   您可以选择 How to find this?（如何查找？），以查看描述如何查找外部 ID 的合作伙伴文档。



> **Note**
>
> 如果资源策略包括外部 ID，则针对 `PutAuditEvents` API 的所有调用都必须包括该外部 ID。但是，如果策略未定义外部 ID，合作伙伴仍然可以调用 `PutAuditEvents` API，并指定 `externalId` 参数。

b. 对于解决方案集成，请选择添加 AWS 账户以指定要作为委托人添加到策略中的 AWS 账户 ID。

7. （可选）在 Tags（标签）区域中，您最多可以添加 50 个标签键和值对，以帮助您对事件数据存储和通道的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅中的为AWS 资源添加标签。AWS 一般参考

8. 在准备好创建新的集成后，请选择 Add integration（添加集成）。没有评论页面。 CloudTrail 创建集成，但您必须向合作伙伴应用程序提供渠道 Amazon 资源名称 (ARN)。有关向合作伙伴应用程序提供通道 ARN 的说明，可在合作伙伴文档网站上找到。有关更多信息，请在 Integrations（集成）页面的 Available sources（可用来源）选项卡上，选择与合作伙伴相对应的 Learn more（了解更多）链接，以便在 AWS Marketplace中打开合作伙伴的页面。

要完成集成的设置，请向合作伙伴或来源应用程序提供通道 ARN。根据集成类型，您、合作伙伴或应用程序将运行 PutAuditEvents API，以将活动事件传送到您的 AWS 账户的事件数据存储。活动事件传送后，您可以使用 CloudTrail Lake 搜索、查询和分析应用程序中记录的数据。您的事件数据包括与 CloudTrail事件负载相匹配的字段eventVersion，例如eventSource、和userIdentity。

创建与控制台的自定义集成

您可以使用 CloudTrail 来记录和存储混合环境中任何来源的用户活动数据，例如本地或云端托管的内部或 SaaS 应用程序、虚拟机或容器。在 CloudTrail Lake 控制台中执行此过程的前半部分，然后调用 PutAuditEventsAPI 来采集事件，提供您的频道 ARN 和事件有效负载。在您使用 PutAuditEvents API 将应用程序活动导入后 CloudTrail，您可以使用 CloudTrail Lake 来搜索、查询和分析从您的应用程序中记录的数据。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，打开 Lake 子菜单，然后选择集成。
3. 在 Add integration（添加集成）页面上，为您的通道输入名称。该名称可以包含 3-128 个字符。只允许使用字母、数字、句点、下划线和短划线。
4. 选择 My custom integration（我的自定义集成）。
5. 在 Event delivery location（事件传送位置）中，选择将相同活动事件记录到现有事件数据存储中，或创建新的事件数据存储。

   如果您选择创建新的事件数据存储，请输入事件数据存储的名称，并以天为单位指定保留期。如果您选择一年可延期保留定价选项，则可以将事件数据在事件数据存储中最多保留 3653 天（大约 10 年）；如果您选择七年保留定价选项，则最多可以保留 2557 天（大约 7 年）。

   如果您选择将活动事件记录到一个或多个现有事件数据存储中，请从列表中选择事件数据存储。事件数据存储只能包含活动事件。控制台中的事件类型必须是 Events from integrations（来自集成的事件）。在 API 中，eventCategory 值必须为 ActivityAuditLog。
6. 在 Resource policy（资源策略）中，为集成的通道配置资源策略。资源策略是 JSON 策略文档，它们指定了指定主体可在资源上执行的操作，以及在什么条件下执行操作。在资源策略中定义为主体的账户可以调用 PutAuditEvents API，以向您的通道传送事件。

> **Note**
>
> 如果您没有为通道创建资源策略，则只有通道所有者可以针对该通道调用 PutAuditEvents API。

a. （可选）输入唯一的外部 ID，以提供额外一层保护。该外部 ID 是一个唯一的字符串，如账户 ID 或随机生成的字符串，以防范混淆代理。

> **Note**
>
> 如果资源策略包括外部 ID，则针对 `PutAuditEvents` API 的所有调用都必须包括该外部 ID。但是，如果策略未定义外部 ID，您仍然可以调用 `PutAuditEvents` API，并指定 `externalId` 参数。

b. 选择 Add AWS ac count（添加 AWS 账户），将每个账户 ID 指定为频道资源策略中的委托人。

7. （可选）在 Tags（标签）区域中，您最多可以添加 50 个标签键和值对，以帮助您对事件数据存储和通道的访问进行识别、排序和控制。要详细了解如何使用 IAM 策略以根据标签授权对事件数据存储的访问，请参阅示例：拒绝基于标签创建或删除事件数据存储的访问权限。有关如何在中使用标签的更多信息 AWS，请参阅中的为AWS 资源添加标签。AWS 一般参考

8. 在准备好创建新的集成后，请选择 Add integration（添加集成）。没有评论页面。 CloudTrail 创建集成，但要集成您的自定义事件，您必须在请求中指定渠道 ARN。`PutAuditEvents`

9. 调用 `PutAuditEvents` API 将你的活动事件摄取到其中 CloudTrail。每个 `PutAuditEvents` 请求最多可以添加 100 个活动事件（或最多 1MB）。您需要在前面的步骤中创建的频道 ARN、CloudTrail 要添加的事件的有效负载以及外部 ID（如果已为资源策略指定）。在将事件载荷摄入之前，请确保其中没有敏感或个人识别信息。 CloudTrail您收录的事件 CloudTrail 必须遵循. CloudTrail 湖泊集成事件架构

> **Tip**
>
> 用于AWS CloudShell确保您运行的是最新的 AWS API。

以下示例演示了如何使用 put-audit-events CLI 命令。--audit-events 和 --channel-arn 参数是必需的。您需要在前面的步骤中创建的通道的 ARN，可以从集成详细信息页面复制该 ARN。的值--audit-events是事件对象的 JSON 数组。 `--audit-events`包括来自事件的必需 ID、作为值的事件所需的有效负载`EventData`，以及一个可选的校验和，以帮助验证事件在摄取后是否完整性。CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
```

```
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

以下是包含两个事件示例的示例命令。

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

以下示例命令添加了 `--cli-input-json` 参数，以指定事件有效负载的 JSON 文件（`custom-events.json`）。

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

以下是示例 JSON 文件 `custom-events.json` 的示例内容。

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
```

```
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

（可选）计算校验和值

您在PutAuditEvents请求EventDataChecksum中指定为的值的校验和可帮助您验证 CloudTrail 收到的事件是否与校验和匹配；它有助于验证事件的完整性。校验和值采用一种 base64-SHA256 算法，您可以通过运行以下命令来计算该值。

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

该命令将返回校验和。示例如下：

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

校验和值将成为您的 PutAuditEvents 请求中 EventDataChecksum 的值。如果校验和与所提供事件的校验和不匹配，则 CloudTrail 会以错误拒绝该事件。InvalidChecksum

使用 Lake 创建、更新和管理 CloudTrail Lake 集成 AWS CLI

您可以使用 AWS CLI 来创建、更新和管理您的 CloudTrail Lake 集成。使用时 AWS CLI，请记住您的命令在 AWS 区域 配置文件中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

L CloudTrail ake 集成的可用命令

用于在 La CloudTrail ke 中创建、更新和管理集成的命令包括：

- create-event-data-store为之外的事件创建事件数据存储 AWS。
- delete-channel删除用于集成的频道。
- delete-resource-policy删除附加到 La CloudTrail ke 集成频道的资源策略。
- get-channel返回有关 CloudTrail 频道的信息。
- get-resource-policy检索附加到 CloudTrail 频道的基于资源的政策文档的 JSON 文本。
- list-channels列出当前账户中的频道及其来源名称。
- put-audit-events将您的应用程序事件摄取到 CloudTrail Lake 中。必填参数接受您要 CloudTrail 采集的事件的 JSON 记录（也称为有效负载）。auditEvents每个PutAuditEvents请求最多可以添加 100 个此类事件（或最多 1 MB）。
- put-resource-policy将基于资源的权限策略附加到用于与外部事件源集成的 CloudTrail 频道。AWS有关基于资源的策略的更多信息，请参阅AWS CloudTrail 基于资源的策略示例。
- update-channel更新由所需频道 ARN 或 UUID 指定的频道。

有关 La CloudTrail ke 事件数据存储的可用命令列表，请参阅事件数据存储的可用命令。

有关可用于 La CloudTrail ke 查询的命令列表，请参阅可用于 L CloudTrail ake 查询的命令。

创建用于从外部记录事件 AWS 的集成 AWS CLI

在中 AWS CLI，您可以创建一个集成，该集成通过四个命令记录来自外部 AWS 的事件（如果您已经有符合条件的事件数据存储，则使用三个命令）。用作集成目标的事件数据存储必须用于单个区域和单个账户；它们不能是多区域的，不能为组织记录事件 AWS Organizations，只能包括活动事件。控制台中的事件类型必须是 Events from integrations（来自集成的事件）。在 API 中，eventCategory 值必须为 ActivityAuditLog。有关集成的更多信息，请参阅 与外部的事件源创建集成 AWS。

1. 如果您还没有一个或多个可用于集成的事件数据存储，请运行 create-event-data-store 以创建事件数据存储。

   以下示例 AWS CLI 命令创建了用于记录外部事件的事件数据存储 AWS。对于活动事件，eventCategory 字段选择器值为 ActivityAuditLog。事件数据存储的保留期设置为 90 天。默认情况下，事件数据存储会收集来自所有区域的事件，但由于这是在收集非AWS 事件，因此请通过添加--no-multi-region-enabled选项将其设置为单个区域。默认情况下将启用终止保护，并且事件数据存储不会为组织中的账户收集事件。

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--no-multi-region-enabled \
--retention-period 90 \
--advanced-event-selectors '[
    {
      "Name": "Select all external events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

您需要事件数据存储 ID（ARN 的后缀，或前面的响应示例中的 EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE）才能继续进行下一步，并创建您的通道。

2. 运行create-channel命令创建一个通道，允许合作伙伴或源应用程序向中的事件数据存储发送事件CloudTrail。

   通道包含下列组件：

   源

   CloudTrail 使用此信息来确定代表您向 CloudTrail 哪些合作伙伴发送事件数据。来源是必填项，可以是所有有效非AWS 事件的 Custom，也可以是伙伴事件源的名称。每个来源最多允许一个通道。

   有关可用合作伙伴 Source 值的信息，请参阅 有关集成合作伙伴的其他信息。

   摄取状态

   该通道状态显示从通道来源接收到最后一次事件的时间。

   目标

   目的地是接收来自该频道的事件的 CloudTrail Lake 事件数据存储。您可以更改通道的目标事件数据存储。

   要停止接收来自某个来源的事件，请删除该通道。

   您需要至少一个目标事件数据存储的 ID 才能运行此命令。目标的有效类型为 EVENT_DATA_STORE。您可以将摄取的事件发送到多个事件数据存储。以下示例命令将创建一个通道，用于将事件发送到两个事件数据存储，这两个存储库在 --destinations 参数的 Location 属性中由其 ID 表示。--destinations、--name 和 --source 参数是必需的。要接收来自 CloudTrail 合作伙伴的事件，请将合作伙伴的名称指定为的值。--source要从您自己的应用程序外部提取事件 AWS，请指定Custom为的值。--source

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

在对您的 create-channel 命令的响应中，复制新通道的 ARN。在后续步骤中，您将需要该 ARN 来运行 `put-resource-policy` 和 `put-audit-events` 命令。

3. 运行put-resource-policy命令将资源策略附加到频道。资源策略是 JSON 策略文档，它们指定了指定主体可在资源上执行的操作，以及在什么条件下执行操作。在通道的资源策略中定义为主体的账户可以调用 `PutAuditEvents` API 来传送事件。

> **Note**
>
> 如果您没有为通道创建资源策略，则只有通道所有者可以针对该通道调用 `PutAuditEvents` API。

该策略所需的信息由集成类型决定。

- 对于方向集成， CloudTrail 要求策略包含合作伙伴的 AWS 账户 ID，并要求您输入合作伙伴提供的唯一外部 ID。 CloudTrail 使用 CloudTrail 控制台创建集成时，会自动将合作伙伴的 AWS 账户 ID 添加到资源策略中。请参阅合作伙伴的文档，了解如何获取保单所需的 AWS 账号。
- 对于解决方案集成，您必须将至少一个 AWS 账户 ID 指定为委托人，并且可以选择输入外部 ID 以防止副手感到困惑。

以下是对资源策略的要求：

- 该策略中定义的资源 ARN 必须与该策略附加到的通道 ARN 相匹配。
- 该策略只包含一个操作：cloudtrail-data：PutAuditEvents
- 该策略至少包含一个语句。该策略最多可以包含 20 个语句。
- 每个语句至少包含一个主体。一个语句最多可以包含 50 个主体。

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
```

```
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

有关资源策略的更多信息，请参阅AWS CloudTrail 基于资源的策略示例。

4. 运行 PutAuditEventsAPI 以将你的活动事件采集到其中 CloudTrail。您需要要 CloudTrail 添加的事件的有效负载。在将事件载荷摄入之前，请确保其中没有敏感或个人识别信息。 CloudTrail请注意，PutAuditEvents API 使用 cloudtrail-data CLI 端点，而不是 cloudtrail 端点。

   以下示例演示了如何使用 put-audit-events CLI 命令。--audit-events 和 --channel-arn 参数是必需的。如果在资源策略中定义了外部 ID，则需要 --external-id 参数。您需要在前面步骤中创建的通道的 ARN。的值--audit-events是事件对象的 JSON 数组。 --audit-events包括来自事件的必需 ID、作为值的事件所需的有效负载EventData，以及一个可选的校验和，以帮助验证事件在摄取后是否完整性。 CloudTrail

```
aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

以下是包含两个事件示例的示例命令。

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

以下示例命令添加了 `--cli-input-json` 参数，以指定事件有效负载的 JSON 文件（`custom-events.json`）。

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

以下是示例 JSON 文件 `custom-events.json` 的示例内容。

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
```

```
}
```

您可以通过运行命令来验证集成是否正常工作以及 CloudTrail 是否正确地从源接收事件。get-channel的输出get-channel显示了最近 CloudTrail收到事件的时间戳。

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

（可选）计算校验和值

您在PutAuditEvents请求EventDataChecksum中指定为的值的校验和可帮助您验证 CloudTrail 收到的事件与校验和匹配的事件；它有助于验证事件的完整性。校验和值采用一种 base64-SHA256 算法，您可以通过运行以下命令来计算该值。

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

该命令将返回校验和。示例如下：

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

校验和值将成为您的 PutAuditEvents 请求中 EventDataChecksum 的值。如果校验和与所提供事件的校验和不匹配，则 CloudTrail 会以错误拒绝该事件。InvalidChecksum

使用更新频道 AWS CLI

要更新通道的名称或目标事件数据存储，请运行 update-channel 命令。--channel 参数是必需的。您无法更新通道的来源。示例如下：

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

删除频道以删除与的集成 AWS CLI

要停止在外部推送合作伙伴或其他活动事件 AWS，请运行命令删除频道。delete-channel需要您要删除的通道的 ARN 或通道 ID（ARN 后缀）。示例如下：

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

有关集成合作伙伴的其他信息

本节中的表格提供了每个集成合作伙伴的来源名称，并标识了集成类型（直接集成或解决方案集成）。

在调用 `CreateChannel` API 时，需要提供 Source name（源名称）列中的信息。您可以将源名称指定为 `Source` 参数的值。

合作伙伴名称（控制台）	源名称（API）	集成类型
我的自定义集成	`Custom`	solution
Cloud Storage Security	`CloudStorageSecurityConsole`	solution
Clumio	`Clumio`	直接
CrowdStrike	`CrowdStrike`	solution
CyberArk	`CyberArk`	solution
GitHub	`GitHub`	solution
Kong Inc	`KongGatewayEnterprise`	solution

合作伙伴名称（控制台）	源名称（API）	集成类型
LaunchDarkly	`LaunchDarkly`	直接
Netskope	`NetskopeCloudExchange`	solution
Nordcloud，IBM 旗下的一家公司	`IBMMulticloud`	直接
MontyCloud	`MontyCloud`	直接
Okta	`OktaSystemLogEvents`	solution
One Identity	`OneLogin`	solution
Shoreline.io	`Shoreline`	solution
Snyk.io	`Snyk`	直接
Wiz	`WizAuditLogs`	solution

查看合作伙伴文档

您可以通过查看合作伙伴的文档，详细了解合作伙伴与 CloudTrail Lake 的集成。

查看合作伙伴文档

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，打开 Lake 子菜单，然后选择集成。
3. 在 Integrations（集成）页面上，选择 Available sources（可用资源），然后选择与您要查看其文档的合作伙伴相对应的 Learn more（了解更多）。

CloudTrail 湖泊集成事件架构

下表描述了与 CloudTrail 事件记录中的架构元素相匹配的必需和可选架构元素。的`eventData`内容由您的事件提供；其他字段由摄取 CloudTrail 后提供。

CloudTrail 中对事件记录内容进行了更详细的描述CloudTrail 录制内容。

- 摄取 CloudTrail 后提供的字段
- 由您的事件提供的字段

摄取 CloudTrail 后提供的字段

字段名称	输入类型	要求	描述
eventVersion	字符串	必需	事件版本。
eventCategory	字符串	必需	事件类别。对于非AWS 事件，该值为ActivityAuditLog 。
eventType	字符串	必需	事件类型。对于非 AWS 事件，有效值为ActivityLog 。
eventID	字符串	必需	事件的唯一 ID。
eventTime	字符串	必需	采用通用协调时间（UTC）的事件时间戳，格式为 yyyy-MM-DDTHH:mm:ss 。
awsRegion	字符串	必需	PutAuditEvents 拨打电话 AWS 区域 的地点。
recipientAccountId	字符串	必需	表示收到此事件的账户 ID。 CloudTrail 通过根据事件负载计算来填充此字段。

字段名称	输入类型	要求	描述
附录	-	可选	显示有关事件处理延迟原因的信息。如果现有事件中缺少信息，则附录块将包含缺失的信息，以及缺失信息的原因。
• reason	字符串	可选	事件或其部分内容丢失的原因。
• updatedFields	字符串	可选	由附录更新的事件记录字段。只有在原因为 UPDATED_DATA 时才提供此信息。
• originalUID	字符串	可选	来自源的原始事件 UID。只有在原因为 UPDATED_DATA 时才提供此信息。
• originalEventID	字符串	可选	原始事件 ID。只有在原因为 UPDATED_DATA 时才提供此信息。
metadata	-	必需	有关活动使用的通道的信息。
• ingestionTime	字符串	必需	处理事件时的时间戳，格式为 yyyy-MM-DDTHH:mm:ss ，采用通用协调时间（UTC）。
• channelARN	字符串	必需	活动使用的通道的 ARN。

由客户事件提供的字段

字段名称	输入类型	要求	描述
eventData	-	必需	在PutAuditEvents 通话 CloudTrail 中发送到的审计数据。
• 版本	字符串	必需	来自事件源的事件版本。 长度限制：最大长度为 256。
• userIdentity	-	必需	有关发出请求的用户的信息。
• • type	字符串	必需	用户身份的类型。 长度限制：最大长度为 128。
• • principalId	字符串	必需	事件的角色的唯一标识符。 长度限制：最大长度为 1024。
• • details	JSON 对象	可选	有关身份的其他信息。
• userAgent	字符串	可选	通过其发出请求的代理。 长度限制：最大长度为 1024。
• eventSource	字符串	必需	这是合作伙伴事件源，或有关记录哪些事

字段名称	输入类型	要求	描述
			件的自定义应用程序。 长度限制：最大长度为 1024。
• eventName	字符串	必需	请求的操作，是源服务或应用程序的 API 中的操作之一。 长度限制：最大长度为 1024。
• eventTime	字符串	必需	采用通用协调时间（UTC）的事件时间戳，格式为 `yyyy-MM-DDTHH:mm:ss` 。
• UID	字符串	必需	用于标识请求的 UID 值。被调用的服务或应用程序将生成此值。 长度限制：最大长度为 1024。
• requestParameters	JSON 对象	可选	与请求一起发送的参数（如果有）。此字段的最大大小为 100kB，超过该限制的内容将被拒绝。

字段名称	输入类型	要求	描述
• responseElements	JSON 对象	可选	可做出更改的操作（创建、更新或删除操作）的响应元素。此字段的最大大小为 100kB，超过该限制的内容将被拒绝。
• errorCode	字符串	可选	表示事件错误的字符串。 长度限制：最大长度为 256。
• errorMessage	字符串	可选	错误的描述。 长度限制：最大长度为 256。
• sourceIPAddress	字符串	可选	已从中发出请求的 IP 地址。IPv4 和 IPv6 地址均可接受。
• recipientAccountId	字符串	必需	表示已收到此事件的账户 ID。账户 ID 必须与拥有该频道的 AWS 账户 ID 相同。
• additionalEventData	JSON 对象	可选	不是请求或响应一部分的关于事件的其他数据。此字段的最大大小为 28kB，超过该限制的内容将被拒绝。

以下示例显示了与 CloudTrail 事件记录中的架构元素相匹配的架构元素的层次结构。

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
       "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
             JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
```

```
            JSON
        }
    }
}
```

查看 CloudTrail 湖泊仪表板

您可以使用 CloudTrail Lake 仪表板对事件数据存储中的事件进行可视化。您可以从几种不同的控制面板类型中选择。可用于事件数据存储的控制面板类型取决于事件数据存储的高级事件选择器配置。例如，如果仪表板类型显示有关 CloudTrail 管理事件的信息，则只有当当前选定的事件数据存储收集 CloudTrail 管理事件时，您才能选择该仪表板。

每种控制面板类型都由多个小组件组成，每个小组件代表一个 SQL 查询。要查看小组件的查询，请选择在查询编辑器中查看和分析，以打开查询编辑器。您无法修改系统生成的用于填充小组件的查询，但可以编辑查询并在查询编辑器中运行查询以进行进一步分析。

要填充和更新控制面板，请选择运行查询。选择 “运行查询” 后，将代表您 CloudTrail 运行系统生成的查询。由于运行查询会产生费用，因此 CloudTrail 要求您确认与运行查询相关的成本。您只需确认此操作一次。有关 CloudTrail 定价的更多信息，请参阅CloudTrail 定价。

主题

- 限制
- 先决条件
- 选择控制面板
- 根据日期或时间范围筛选控制面板
- 查看控制面板小组件的查询

限制

以下限制适用于当前版本。

- 当前版本不支持自定义控制面板、小组件或查询。
- 当前版本仅为收集事件（数据事件、管理 CloudTrail 事件）和 Insights 事件的事件数据存储提供仪表板。
- 当前版本不支持编辑用于填充控制面板的系统生成的查询。您可以在查询编辑器选项卡上查看和编辑任何小组件的基础查询，但是，您对查询所做的任何更改都将用于控制面板之外的补充分析。

先决条件

以下先决条件适用于 Lake 控制面板。

- 要查看和使用 Lake 仪表板，必须至少创建一个 CloudTrail Lake 事件数据存储。您可以使用控制台、 AWS CLI或 SDK 创建事件数据存储。有关使用控制台创建数据存储的信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储。有关使用创建事件数据存储的信息 AWS CLI，请参阅使用创建、更新和管理事件数据存储 AWS CLI。
- 要填充控制面板，请代表您 CloudTrail 运行查询。首次查看 “控制面板” 页面时， CloudTrail 会要求您确认与运行查询相关的费用。选择我同意以确认运行查询的费用。

选择控制面板

按照以下步骤选择要查看的事件数据存储和控制面板类型。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在左侧导航窗格中，在 Lake 下，选择控制面板。
3. 选择要直观显示数据的事件数据存储。
4. 选择要查看的控制面板类型。控制面板列表是根据所选事件数据存储的高级事件选择器配置填充的。

   以下是可能的控制面板类型。

   - 概览仪表板- AWS 服务 按事件计数显示最活跃的用户。 AWS 区域您还可以查看有关 `read` 和 `write` 管理事件活动、最受限制的事件以及最常出现的错误的信息。此控制面板可用于收集管理事件的事件数据存储。
   - 管理事件控制面板 – 按用户显示控制台登录事件、访问被拒事件、破坏性操作和最常出现的错误。您还可以按用户查看有关 TLS 版本和过时的 TLS 调用的信息。此控制面板可用于收集管理事件的事件数据存储。
   - S3 数据事件控制面板 – 显示 S3 账户活动、访问次数最多的 S3 对象、排名靠前的 S3 用户和排名靠前的 S3 操作。此控制面板可用于收集 Amazon S3 数据事件的事件数据存储。
   - Insights 事件控制面板 - 按 Insights 类型显示 Insights 事件的总体比例、按 Insights 类型显示主要用户的服务的 Insights 事件比例以及每天的 Insights 事件数量。控制面板还包括一个小部件，可最多列出 30 天的 Insights 事件。此控制面板仅可用于收集 Insights 事件的事件数据存储。

> **Note**
>
> - 首次在源事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。有关更多信息，请参阅 了解 Insights 事件传输情况。
> - Insights 事件控制面板仅显示有关选定事件数据存储收集的 Insights 事件的信息，这些信息由源事件数据存储的配置决定。例如，如果您将源事件数据存储配置为在 `ApiCallRateInsight` 上启用 Insights 事件，而不是 `ApiErrorRateInsight`，则您将不会看到有关 `ApiErrorRateInsight` 上的 Insights 事件的信息。

5. 选择按绝对范围或相对范围筛选控制面板数据。选择绝对范围，以选择特定的日期和时间范围。选择相对范围，以选择预定义的时间范围或自定义范围。默认情况下，控制面板显示过去 24 小时的事件数据。

> **Note**
>
> CloudTrail Lake 查询会根据扫描的数据量产生费用。为了帮助控制成本，您可以在较小的时间范围内进行筛选。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

6. 选择运行查询以运行控制面板小组件的查询。

根据日期或时间范围筛选控制面板

默认情况下，控制面板显示过去 24 小时的数据。您可以按绝对范围或相对范围筛选控制面板。

选择绝对范围，以选择特定的日期和时间范围。

选择相对范围，以选择预定义的时间范围或自定义范围。

选择时间范围后，选择运行查询以刷新控制面板。

> **Note**
>
> CloudTrail Lake 查询会根据扫描的数据量产生费用。为了帮助控制成本，您可以在较小的时间范围内进行筛选。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

查看控制面板小组件的查询

每个小组件代表一个 SQL 查询。要查看小组件的查询，请选择在查询编辑器中查看和分析，以打开查询编辑器。使用查询编辑器，您可以在控制面板之外进一步优化查询，然后运行查询以查看更新后的查询的结果。有关使用查询的更多信息，请参阅 创建或编辑查询。

> **Note**
>
> 您无法修改系统为控制面板小组件生成的查询。在查询编辑器选项卡上对查询所做的任何更改，仅用于控制面板之外的进一步分析。

CloudTrail 湖泊查询

La CloudTrail ke 中的查询是用 SQL 编写的。您可以在 L CloudTrail ake E ditor 选项卡上生成查询，方法是从头开始用 SQL 编写查询，或者打开已保存的查询或示例查询并对其进行编辑。您无法用更改覆盖已包含的示例查询，但可以将其另存为新查询。有关允许的 SQL 查询语言的详细信息，请参阅 CloudTrail 湖泊 SQL 限制。

无界查询（例如 `SELECT * FROM edsID`）会扫描事件数据存储中的所有数据。为了帮助控制成本，我们建议您通过为查询添加开始和结束 `eventTime` 时间戳，来限制查询。以下示例搜索指定事件数据存储中的所有事件，其中事件时间介于（>）2023 年 1 月 5 日下午 1:51 和（<）2023 年 1 月 19 日下午 1:51 之间。由于事件数据存储的保留期至少为七天，因此开始和结束 `eventTime` 值之间的最短时间跨度值也是七天。

```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

主题

- 查询编辑器工具
- 在 CloudTrail 控制台中查看示例查询
- 创建或编辑查询
- 运行查询并保存查询结果
- 查看查询结果

- 下载已保存的查询结果
- 验证已保存的查询结果
- 使用运行和管理 CloudTrail Lake 查询 AWS CLI

查询编辑器工具

查询编辑器右上角的工具栏提供多个命令，以帮助编写 SQL 查询和对其进行格式化。

下表介绍了工具栏上的命令。

- Undo（撤消）– 恢复在查询编辑器中所做的上次内容更改。
- Redo（重做）– 重复在查询编辑器中所做的上次内容更改。
- Format selected（已选格式）- 根据 SQL 格式和间距惯例，排列查询编辑器内容。
- 已选择注释/取消注释 – 如果尚未注释查询的选定部分，则对其进行注释。如果选定部分已进行注释，则选择此选项会删除注释。

在 CloudTrail 控制台中查看示例查询

CloudTrail 控制台提供了许多示例查询，可以帮助您开始编写自己的查询。

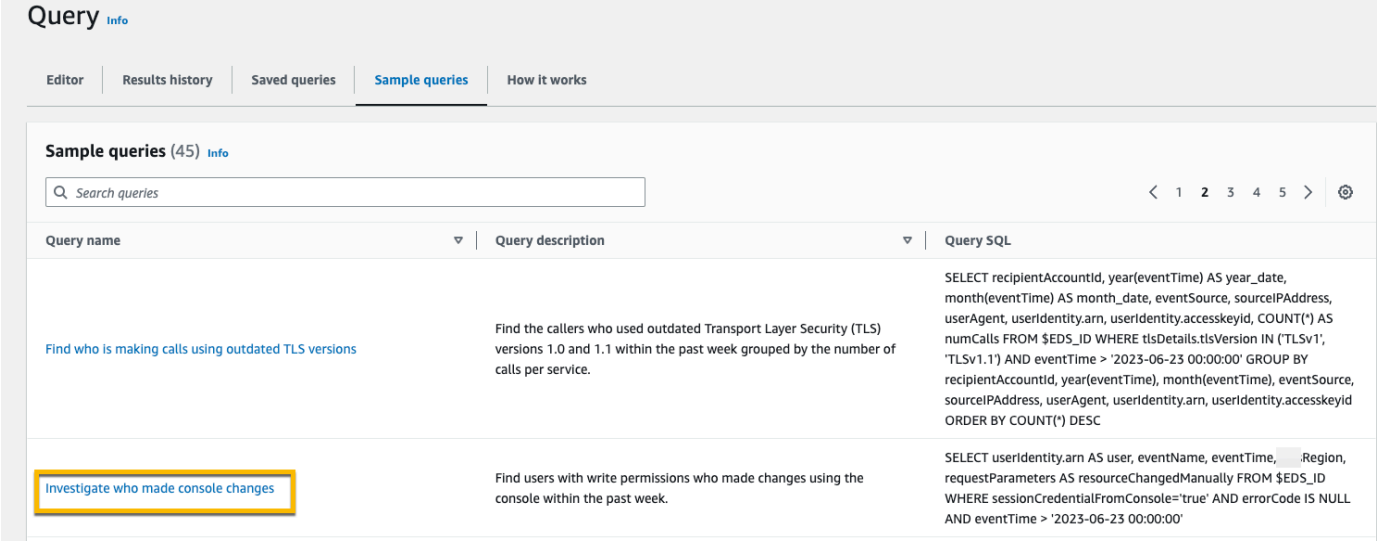
CloudTrail 查询会根据扫描的数据量收取费用。为了帮助控制成本，我们建议您通过为查询添加开始和结束 `eventTime` 时间戳，来限制查询。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

> **Note**
>
> 您还可以查看 GitHub 社区创建的查询。要了解更多信息并查看这些示例查询，请参阅 GitHub 网站上的 CloudTrailLake 示例查询。 AWS CloudTrail 尚未评估中的查询 GitHub。

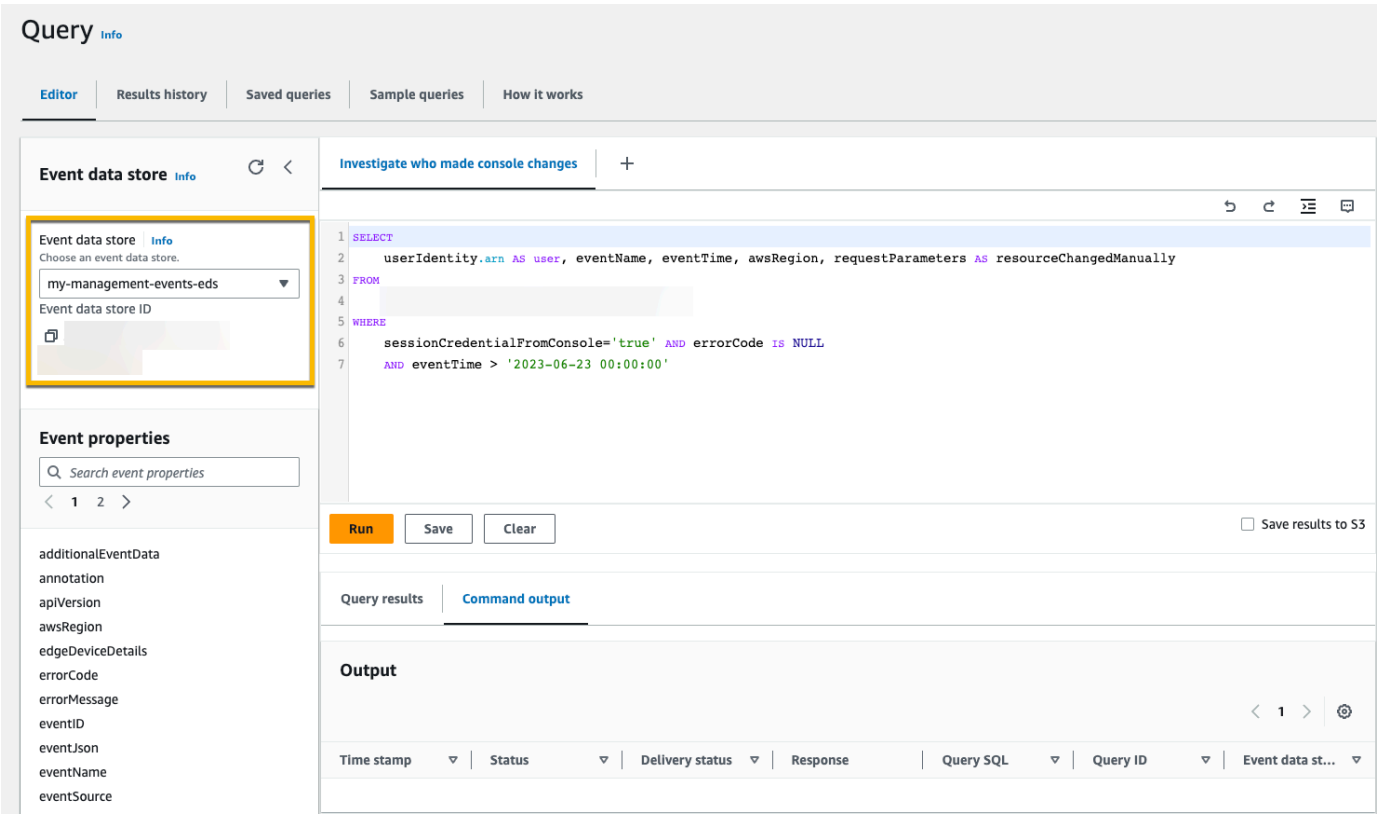
查看和运行示例查询

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。

2. 在导航窗格中，在 Lake 下，选择查询。
3. 在 Query（查询）页面上，选择 Sample queries（示例查询）选项卡。
4. 从列表中选择示例查询或搜索查询以筛选列表。在此示例中，我们将通过选择查询名称来打开调查谁对控制台进行了更改查询。这将在 Editor（编辑器）选项卡中打开此查询。

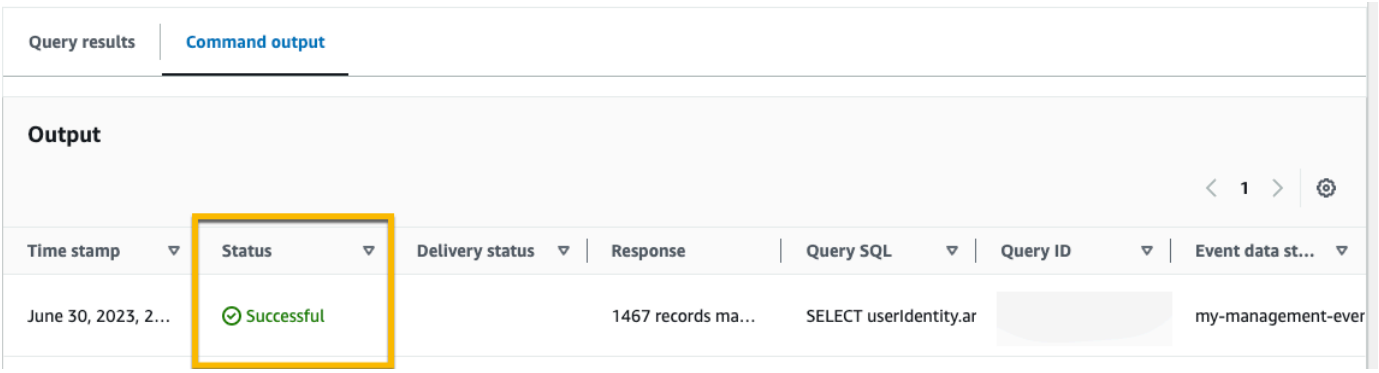


5. 在编辑器选项卡上，选择要为其运行查询的事件数据存储。当您从列表中选择事件数据存储时，CloudTrail 会在查询编辑器的FROM行中自动填充事件数据存储 ID。

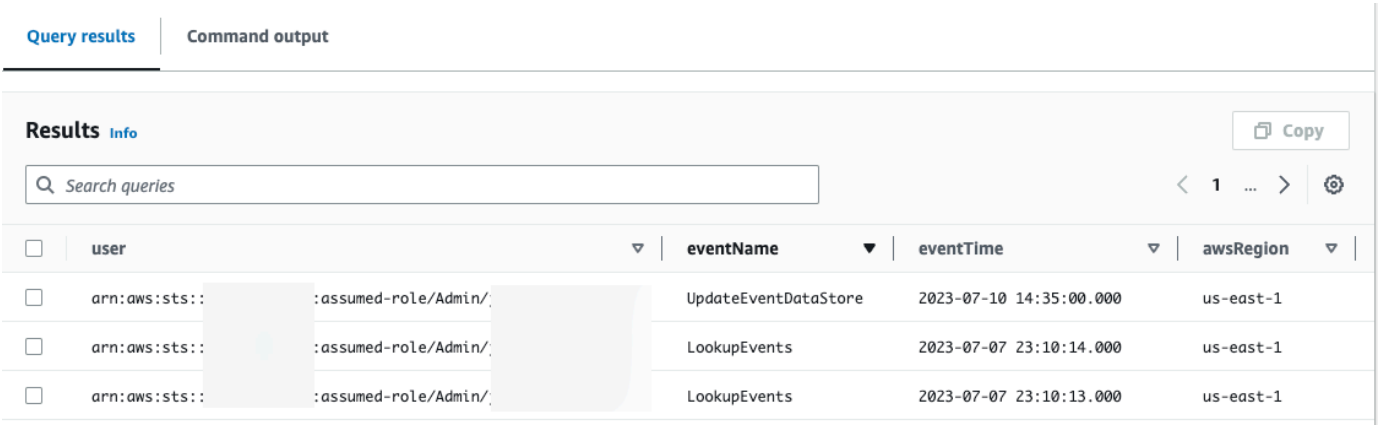


6. 选择运行以运行查询。

命令输出选项卡显示有关查询的元数据，例如查询是否成功、匹配的记录数量以及查询的运行时间。



查询结果选项卡显示选定事件数据存储中与查询匹配的事件数据。



有关编辑查询的更多信息，请参阅 创建或编辑查询。有关运行查询和保存查询结果的更多信息，请参阅 运行查询并保存查询结果。

创建或编辑查询

在本演练中，我们打开其中一个示例查询，对其进行编辑，以查找名为 `Alice` 的特定用户执行的操作，然后将其另存为新查询。如果您已保存查询，您也可以在 Saved queries（保存的查询）选项卡上编辑已保存的查询。为了帮助控制成本，我们建议您通过为查询添加开始和结束 `eventTime` 时间戳，来限制查询。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择查询。
3. 在 Query（查询）页面上，选择 Sample queries（示例查询）选项卡。

4. 通过选择查询名称打开示例查询。这将在 Editor（编辑器）选项卡中打开此查询。在此示例中，我们将选择名为调查用户操作的查询，然后编辑查询，以查找名为 `Alice` 的特定用户的操作。

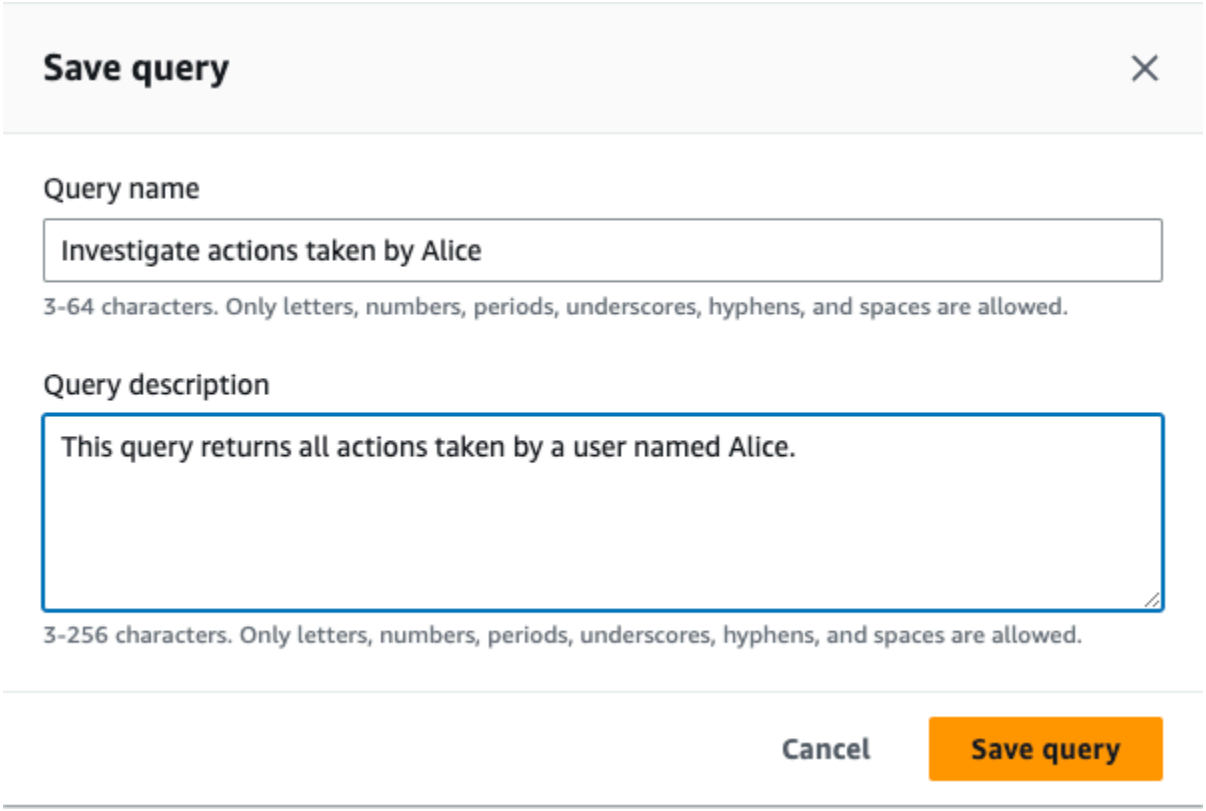
5. 在编辑器选项卡中，编辑 `WHERE` 行以指定要调查的用户，并根据需要更新 `eventTime` 值。的值`FROM`是事件数据存储 ARN 的 ID 部分，在您选择事件数据存储 CloudTrail 时会自动填充。

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. 您可以运行查询，然后再保存，以验证查询是否有效。要运行查询，请从 Event data store（事件数据存储）下拉列表中选择事件数据存储，然后选择 Run（运行）。查看 Command output（命令输出）选项卡的 Status（状态）列中的活跃查询，以验证查询是否成功运行。

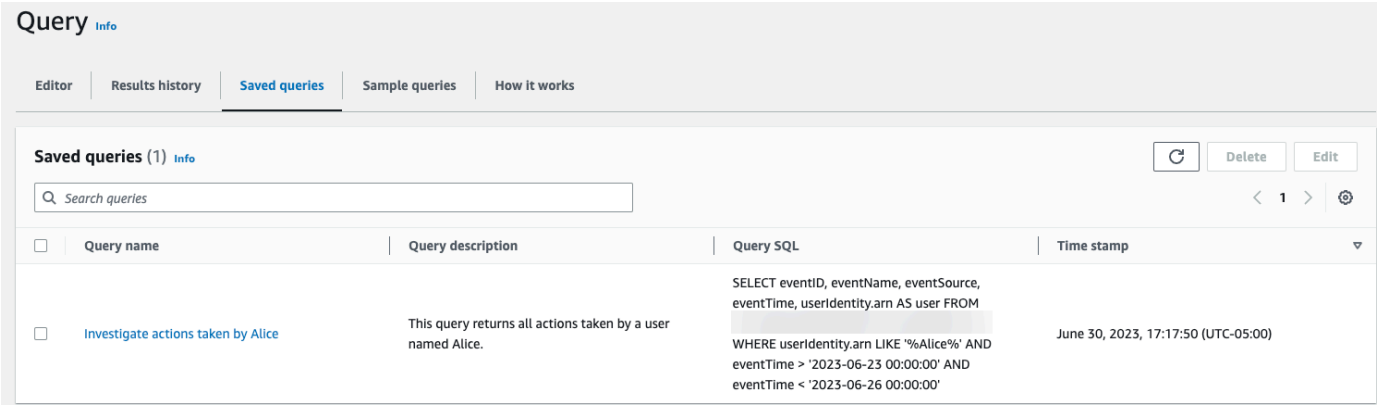
7. 在您更新示例查询后，请选择保存。

8. 在 Save query（保存查询）中，输入查询的名称和描述。选择 Save query（保存查询），将您的更改保存为新查询。要放弃对查询的更改，请选择 Cancel（取消），或者关闭 Save query（保存查询）窗口。



> **Note**
>
> 保存的查询与您的浏览器绑定；如果您使用不同的浏览器或不同的设备访问 CloudTrail 控制台，则保存的查询不可用。

9. 打开 Saved queries（已保存查询）选项卡，以查看表中的新查询。



运行查询并保存查询结果

选择或保存查询后，您可以在事件数据存储中运行查询。

运行查询时，您可以选择将查询结果保存到 Amazon S3 存储桶。在 CloudTrail Lake 中运行查询时，会根据查询扫描的数据量产生费用。将查询结果保存到 S3 存储桶不会产生额外的 CloudTrail Lake 费用，但会收取 S3 存储费用。有关 S3 定价的更多信息，请参阅 Amazon S3 定价。

保存查询结果时，查询结果可能会先显示在 CloudTrail 控制台中，然后才能在 S3 存储桶中查看，因为查询扫描完成后才会 CloudTrail 提供查询结果。虽然大多数查询会在几分钟内完成，但根据事件数据存储的大小，将查询结果传送 CloudTrail 到 S3 存储桶可能需要更长的时间。 CloudTrail 以压缩的 gzip 格式将查询结果传送到 S3 存储桶。平均而言，查询扫描完成后，传送到 S3 存储桶的每 GB 数据预计将出现 60 至 90 秒的延迟。

使用 La CloudTrail ke 运行查询

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择查询。
3. 在已保存查询或示例查询选项卡中，通过选择查询名称来选择要运行的查询。

4. 在 Editor（编辑器）选项卡的 Event data store（事件数据存储）中，从下拉列表中选择事件数据存储。
5. （可选）在 Editor（编辑器）选项卡上，选择 Save results to S3（将结果保存到 S3）以将查询结果保存到 S3 存储桶。当您选择默认 S3 存储桶时， CloudTrail 会创建并应用所需的存储桶策略。如果您选择默认 S3 存储桶，则您的 IAM 策略需要包含`s3:PutEncryptionConfiguration`操作权限，因为默认情况下，该存储桶已启用服务器端加密。有关保存查询结果的更多信息，请参阅有关已保存查询结果的其他信息。

   > **Note**
   >
   > 要使用其他存储桶，请指定存储桶名称，或选择 Browse S3（浏览 S3）以选择存储桶。存储桶策略必须授予向存储桶传送查询结果的 CloudTrail 权限。有关手动编辑存储桶策略的信息，请参阅适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略。

6. 在 Editor（编辑器）选项卡上，选择 Run（运行）。

   根据事件数据存储的大小及其包含的数据天数，运行查询可能需要几分钟时间。Command output（命令输出）选项卡用于显示查询的状态以及查询是否已完成运行。在完成运行查询后，打开 Query results（查询结果）选项卡，以查看活跃查询（编辑器中当前显示的查询）的结果表。

> **Note**
>
> 运行时间超过一小时的查询可能会超时。您仍然可以获得在查询超时之前处理的部分结果。CloudTrail 不会将部分查询结果传送到 S3 存储桶。要避免超时，您可以通过指定较短的时间范围来优化查询，从而限制扫描的数据量。

有关已保存查询结果的其他信息

保存查询结果后，可从 S3 存储桶下载已保存的查询结果。有关寻找和下载已保存查询结果的更多信息，请参阅 下载已保存的查询结果。

您还可以验证已保存的查询结果，以确定查询结果在 CloudTrail 传送查询结果后是已修改、删除还是未更改。有关验证已保存查询结果的更多信息，请参阅 验证已保存的查询结果。

示例：将查询结果保存到 Amazon S3 存储桶

本演练展示了如何将查询结果保存到 S3 存储桶中，然后下载这些查询结果。

将查询结果保存到 Amazon S3 存储桶中

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择查询。
3. 在示例查询或已保存的查询选项卡上，通过选择查询名称来选择要运行的查询。在此示例中，我们将选择名为调查用户操作的示例查询。
4. 在 Editor（编辑器）选项卡的 Event data store（事件数据存储）中，从下拉列表中选择事件数据存储。从列表中选择事件数据存储时， CloudTrail 会自动填充`From`行中的事件数据存储 ID。
5. 在此示例查询中，我们将编辑 `userIdentity.ARN` 值以指定名为 `Admin` 的用户，并保留 `eventTime` 的默认值。运行查询时，您需要按扫描的数据量付费。为了帮助控制成本，我们建议您通过为查询添加开始和结束 `eventTime` 时间戳，来限制查询。

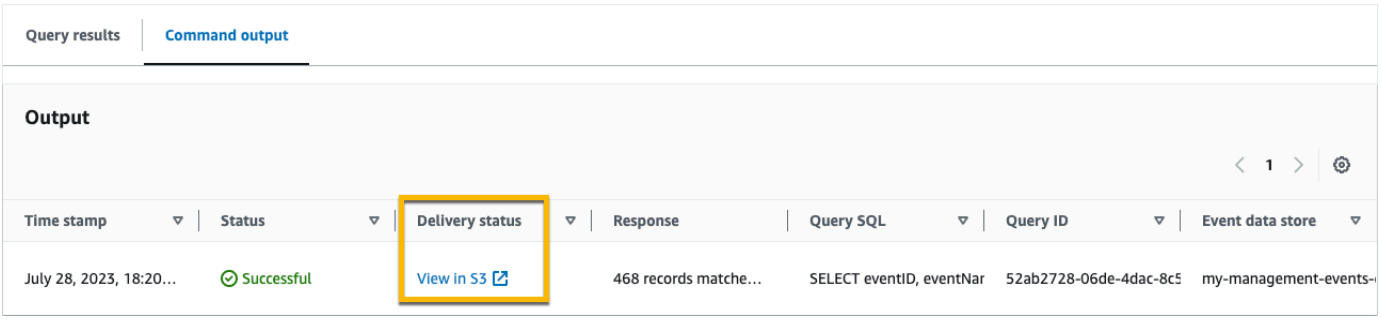
6. 选择将结果保存到 S3 中以将查询结果保存到 S3 存储桶中。当您选择默认 S3 存储桶时， CloudTrail 会创建并应用所需的存储桶策略。如果您选择默认 S3 存储桶，则您的 IAM 策略需要包含`s3:PutEncryptionConfiguration`操作权限，因为默认情况下，该存储桶已启用服务器端加密。在此示例中，我们将使用默认的 S3 存储桶。

> **Note**
>
> 要使用其他存储桶，请指定存储桶名称，或选择 Browse S3（浏览 S3）以选择存储桶。存储桶策略必须授予向存储桶传送查询结果的 CloudTrail 权限。有关手动编辑存储桶策略的信息，请参阅适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略。

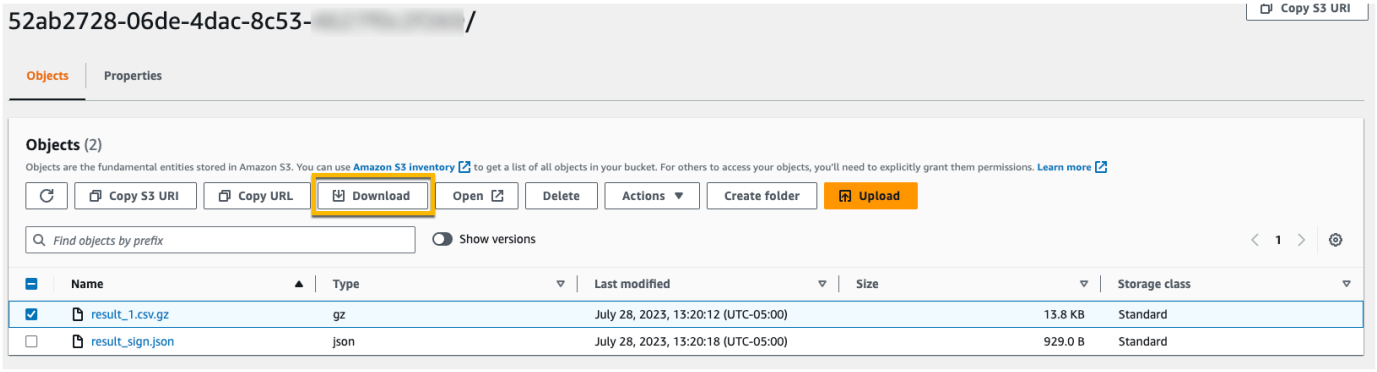
7. 选择运行。根据事件数据存储的大小及其包含的数据天数，运行查询可能需要几分钟时间。Command output（命令输出）选项卡用于显示查询的状态以及查询是否已完成运行。在完成运行查询后，打开 Query results（查询结果）选项卡，以查看活跃查询（编辑器中当前显示的查询）的结果表。

8. 将保存的查询结果传送到您的 S3 存储桶 CloudTrail 后，“交付状态” 列将提供指向 S3 存储桶的链接，其中包含您保存的查询结果文件以及可用于验证保存的查询结果的签名文件。选择在 S3 中查看以查看 S3 存储桶中的查询结果文件和签名文件。

> **Note**
>
> 保存查询结果时，查询结果可能会先显示在 CloudTrail 控制台中，然后才能在 S3 存储桶中查看，因为查询扫描完成后才会 CloudTrail 提供查询结果。虽然大多数查询会在几分钟内完成，但根据事件数据存储的大小，将查询结果传送 CloudTrail 到 S3 存储桶可能需要更长的时间。 CloudTrail 以压缩的 gzip 格式将查询结果传送到 S3 存储桶。平均而言，查询扫描完成后，传送到 S3 存储桶的每 GB 数据预计将出现 60 至 90 秒的延迟。



9. 要下载查询结果，请选择查询结果文件（在此示例中为 `result_1.csv.gz`），然后选择下载。



有关验证保存的查询结果的信息，请参阅 [验证已保存的查询结果](#)。

查看查询结果

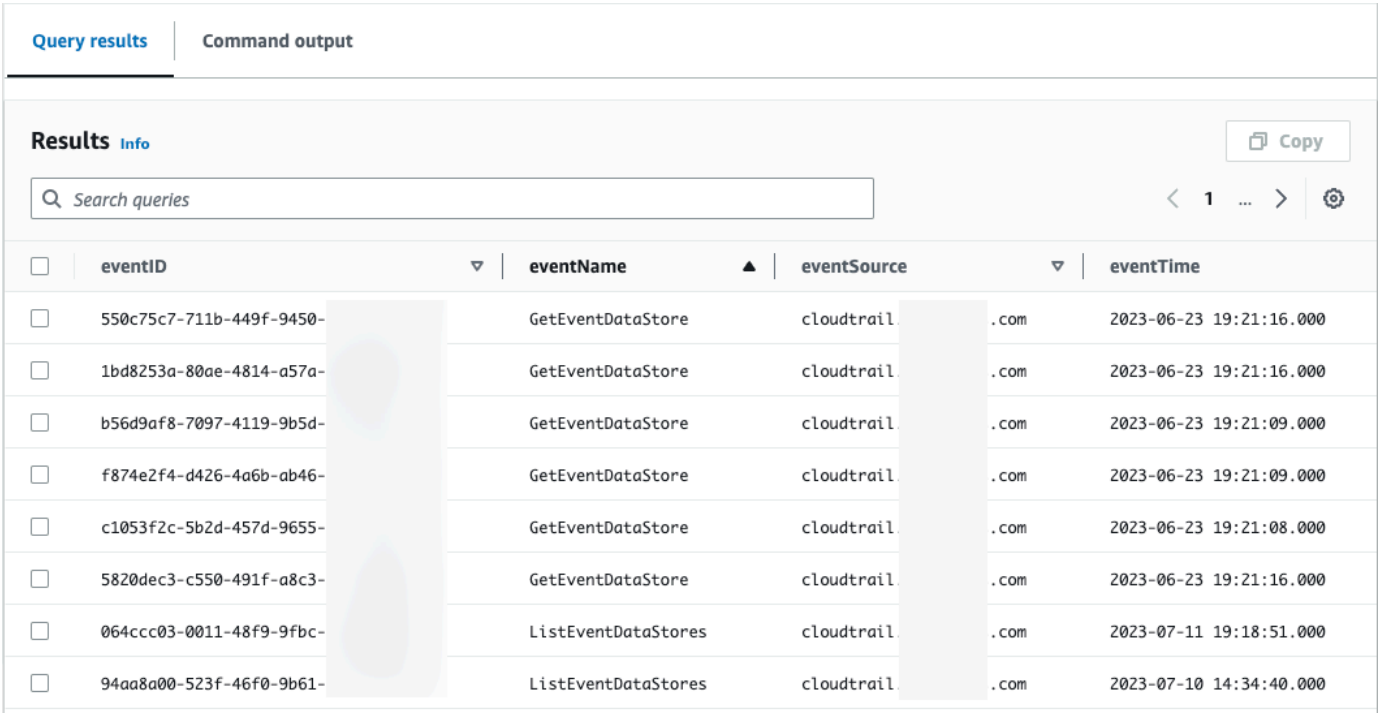
查询完成后，您可以查看其结果。查询结果在查询完成后的七天内可用。您可以在 Query results（查询结果）选项卡上查看活跃查询的结果，也可以在 Lake 主页的 Results history（结果历史记录）选项卡上访问所有最近查询的结果。

查询结果可以从较早的查询运行更改为较新的查询，因为可以在查询之间记录查询期间较新的事件。

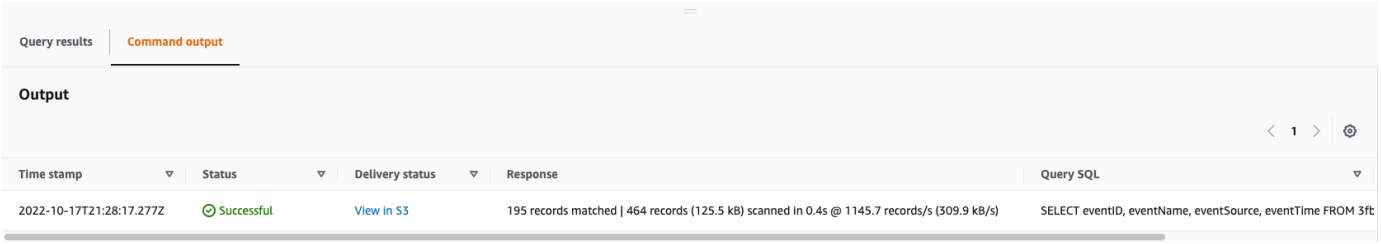
保存查询结果时，查询结果可能会先显示在 CloudTrail 控制台中，然后才能在 S3 存储桶中查看，因为查询扫描完成后才会 CloudTrail 提供查询结果。虽然大多数查询会在几分钟内完成，但根据事件数据存储的大小，将查询结果传送 CloudTrail 到 S3 存储桶可能需要更长的时间。 CloudTrail 以压缩的 gzip 格式将查询结果传送到 S3 存储桶。 平均而言，查询扫描完成后，您预计每 GB 数据传输到 S3 存储桶就会有 60 到 90 秒的延迟。有关寻找和下载已保存查询结果的更多信息，请参阅 [下载已保存的查询结果](#)。

> **Note**
>
> 运行时间超过一小时的查询可能会超时。您仍然可以获得在查询超时之前处理的部分结果。CloudTrail 不会将部分查询结果传送到 S3 存储桶。要避免超时，您可以通过指定较短的时间范围来优化查询，从而限制扫描的数据量。

1. 在活跃查询的 Query results（查询结果）选项卡中，每行表示与查询匹配的事件结果。通过在搜索栏中输入全部或部分事件字段值来筛选结果。要复制事件，请选择要复制的事件，然后选择复制。



2. 在 Command output（命令输出）选项卡中，查看有关已运行查询的元数据，例如事件数据存储 ID、运行时间、扫描的结果数以及查询是否成功。如果您将查询结果保存到 Amazon S3 存储桶，则元数据还将包括指向包含已保存查询结果的 S3 存储桶的链接。



下载已保存的查询结果

保存查询结果后，您需要能够找到包含查询结果的文件。 CloudTrail 将您的查询结果传送到您在保存查询结果时指定的 Amazon S3 存储桶。

> **Note**
>
> 保存查询结果时，查询结果可能会先显示在控制台中，然后才能在 S3 存储桶中查看，因为查询扫描完成后才会 CloudTrail 提供查询结果。虽然大多数查询会在几分钟内完成，但根据事件数据存储的大小，将查询结果传送 CloudTrail 到 S3 存储桶可能需要更长的时间。 CloudTrail 以压缩的 gzip 格式将查询结果传送到 S3 存储桶。平均而言，查询扫描完成后，传送到 S3 存储桶的每 GB 数据预计将出现 60 至 90 秒的延迟。

主题

- 查找您的 CloudTrail Lake 已保存查询结果
- 下载您的 CloudTrail Lake 已保存的查询结果

查找您的 CloudTrail Lake 已保存查询结果

CloudTrail 将查询结果发布到您的 S3 存储桶并签署文件。查询结果文件包含已保存查询的输出，并且签名文件会提供查询结果的签名和哈希值。您可以使用签名文件验证查询结果。有关验证查询结果的更多信息，请参阅 验证已保存的查询结果。

要检索查询结果或签名文件，您可以使用 Amazon S3 控制台、Amazon S3 命令行界面（CLI）或 API。

使用 Amazon S3 控制台查找查询结果和签名文件

1. 打开 Simple Storage Service（Amazon S3）控制台。
2. 选择您指定的存储桶。
3. 在对象层次结构中导航，直至找到查询结果和签名文件。查询结果文件的扩展名为 .csv.gz，签名文件的扩展名为 .json。

您将看到一个与下面示例类似的对象层次结构，但具体存储桶名称、账户 ID、日期和查询 ID 有所不同。

```
All Buckets
    Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

下载您的 CloudTrail Lake 已保存的查询结果

保存查询结果时，会将两种类型的文件 CloudTrail 传送到您的 Amazon S3 存储桶。

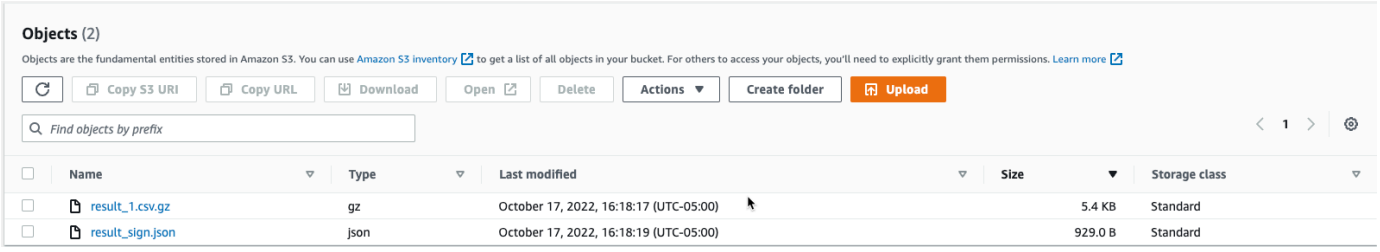
- JSON 格式的签名文件，可用于验证查询结果文件。该签名文件名为 result_sign.json。有关签名文件的更多信息，请参阅 CloudTrail 签名文件结构。
- 一个或多个 CSV 格式的查询结果文件，其中包含查询结果。传送的查询结果文件数量取决于查询结果的总大小。查询结果文件的最大文件大小为 1 TB。每个查询结果文件均以 result_*number*.csv.gz 命名。例如，如果查询结果的总大小为 2 TB，则您将有两个查询结果文件，result_1.csv.gz 和 result_2.csv.gz。

CloudTrail 查询结果和签名文件是 Amazon S3 对象。您可以使用 S3 控制台、 AWS Command Line Interface (CLI) 或 S3 API 来检索查询结果并签署文件。

以下过程介绍了如何使用 Amazon S3 控制台下载查询结果和签名文件。

使用 Amazon S3 控制台下载查询结果或签名文件

1. 打开 Amazon S3 控制台。
2. 选择存储桶并选择要下载的文件。



3. 选择 Download（下载），然后按照提示保存文件。

> **Note**
>
> 某些浏览器（例如 Chrome）会自动为您提取查询结果文件。如果您的浏览器有这种功能，请跳到步骤 5。

4. 使用 7-Zip 等产品提取查询结果文件。
5. 打开查询结果或签名文件。

验证已保存的查询结果

要确定查询结果在 CloudTrail 传送查询结果后是修改、删除还是未更改，您可以使用 CloudTrail 查询结果完整性验证。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在不被发现的情况下修改、删除或伪造 CloudTrail 查询结果文件在计算上是不可行的。您可以使用命令行验证查询结果文件。

为什么使用它？

在安全和事故调查中，经验证的查询结果文件非常重要。例如，经验证的查询结果文件可帮助您明确地断言查询结果文件未经更改。 CloudTrail 查询结果文件完整性验证过程还会让您知道查询结果文件是否已被删除或更改。

主题

- 使用验证保存的查询结果 AWS CLI
- CloudTrail 签名文件结构
- CloudTrail 查询结果文件完整性验证的自定义实现

使用验证保存的查询结果 AWS CLI

您可以使用 aws cloudtrail verify-query-results 命令验证查询结果和签名文件的完整性。

先决条件

要使用命令行验证查询结果的完整性，必须满足以下条件：

- 您必须联机连接到 AWS。
- 您必须使用 AWS CLI 版本 2。

- 要在本地验证查询结果文件和签名文件，应满足以下条件：
  - 必须将查询结果文件和签名文件放入指定的文件路径。将文件路径指定为 --local-export-path 参数的值。
  - 不得重命名查询结果文件和签名文件。
- 要在 S3 存储桶中验证查询结果文件和签名文件，应满足以下条件：
  - 不得重命名查询结果文件和签名文件。
  - 必须拥有包含查询结果文件和签名文件的 Amazon S3 存储桶的读取访问权限。
  - 指定的 S3 前缀必须包含查询结果文件和签名文件。将 S3 前缀指定为 --s3-prefix 参数的值。

verify-query-results

verify-query-results 命令将每个查询结果文件的哈希值与签名文件中的 `fileHashValue` 进行比对，再验证签名文件中的 `hashSignature`，从而验证前述哈希值。

验证查询结果时，您可以使用 --s3-bucket 和 --s3-prefix 命令行选项来验证存储在 S3 存储桶中的查询结果文件和签名文件，也可以使用 --local-export-path 命令行选项对下载的查询结果文件和签名文件执行本地验证。

> **Note**
>
> verify-query-results 命令与特定区域相关。必须指定--region全局选项才能验证特定项的查询结果 AWS 区域。

verify-query-results 命令的选项如下：

--s3-bucket *<string>*

指定存储查询结果文件和签名文件的 S3 存储桶名称。此参数不能与 --local-export-path 一起使用。

--s3-prefix *<string>*

指定包含查询结果文件和签名文件的 S3 文件夹的 S3 路径（例如 `s3/path/`）。此参数不能与 --local-export-path 一起使用。如果文件位于 S3 存储桶的根目录中，则无需提供此参数。

--local-export-path *<string>*

指定包含查询结果文件和签名文件的本地目录（例如 /local/path/to/export/file/）。此参数不能与 --s3-bucket 或 --s3-prefix 一起使用。

示例

以下示例使用 --s3-bucket 和 --s3-prefix 命令行选项来指定包含查询结果文件和签名文件的 S3 存储桶名称和前缀，从而验证查询结果。

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

以下示例使用 --local-export-path 命令行选项来指定查询结果文件和签名文件的本地路径，从而验证下载的查询结果。有关下载查询结果文件的更多信息，请参阅 下载您的 CloudTrail Lake 已保存的查询结果。

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

验证结果

下表描述了查询结果文件和签名文件可能会出现的验证消息。

文件类型	验证消息	描述
Sign file	Successfully validated sign and query result files	签名文件的签名有效。其引用的查询结果文件可供检查。
Query result file	ValidationError: "File *file_name* has inconsistent hash value with hash value recorded in sign file, hash value in sign file is *expected_hash* , but get *computed_hash*	验证失败，因为查询结果文件的哈希值与签名文件中的 fileHashValue 不相符。

文件类型	验证消息	描述
Sign file	ValidationError: Invalid signature in sign file	签名文件验证失败，因为签名无效。

CloudTrail 签名文件结构

签名文件包含保存查询结果时传送到 Amazon S3 存储桶的每个查询结果文件的名称、每个查询结果文件的哈希值以及文件的数字签名。数字签名和哈希值用于验证查询结果文件和签名文件本身的完整性。

签名文件位置

签名文件将传送到遵循以下语法的 Amazon S3 存储桶位置。

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

示例签名文件内容

以下示例签名文件包含 La CloudTrail ke 查询结果的信息。

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

签名文件字段描述

以下是对签名文件中每个字段的描述：

`version`

签名文件的版本。

`region`

用于保存查询结果的 AWS 账户的区域。

`files.fileHashValue`

已压缩的查询结果文件内容的十六进制编码哈希值。

`files.fileName`

查询结果文件的名称。

`hashAlgorithm`

用于对查询结果文件进行哈希处理的哈希算法。

`signatureAlgorithm`

用于对文件进行签名的算法。

`queryCompleteTime`

表示何时将查询结果 CloudTrail 传送到 S3 存储桶。您可以使用此值来查找公钥。

`hashSignature`

文件的哈希签名。

`publicKeyFingerprint`

用于对文件进行签名的公钥的十六进制编码指纹。

CloudTrail 查询结果文件完整性验证的自定义实现

由于 CloudTrail 使用行业标准、公开可用的加密算法和哈希函数，因此您可以创建自己的工具来验证 CloudTrail 查询结果文件的完整性。当您将查询结果保存到 Amazon S3 存储桶时，会 CloudTrail 将签名文件发送到您的 S3 存储桶。您可以实施自己的验证解决方案以验证签名和查询结果文件。有关签名文件的更多信息，请参阅 CloudTrail 签名文件结构。

本主题介绍了签名文件的签名方式，并详述了实施验证签名文件及签名文件所引用查询结果文件的解决方案所需采取的步骤。

了解 CloudTrail 签名文件的签名方式

CloudTrail 签名文件使用 RSA 数字签名进行签名。对于每个签名文件，执行以下 CloudTrail操作：

1. 创建一个哈希列表，其中包含每个查询结果文件的哈希值。
2. 获取区域唯一的私钥。
3. 将此字符串的 SHA-256 哈希值和私钥传递给 RSA 签名算法（生成数字签名）。
4. 将签名的字节代码编码成十六进制格式。
5. 将数字签名放入签名文件中。

数据签名字符串的内容

数据签名字符串包含以空格分隔的每个查询结果文件的哈希值。签名文件列出了每个查询结果文件的 `fileHashValue`。

自定义验证实现步骤

实施自定义验证解决方案时，需要验证签名文件及其引用的查询结果文件。

验证签名文件

要验证签名文件，您需要其签名、与用于对其进行签名的私钥对应的公钥以及您计算的数据签名字符串。

1. 获取签名文件。
2. 验证是否已从签名文件的原始位置检索到签名文件。
3. 获取签名文件的十六进制编码签名。
4. 获取与用于对签名文件进行签名的私钥对应的公钥的十六进制编码指纹。

5. 检索与签名文件中的 queryCompleteTime 对应的时间范围的公钥。对于时间范围，请选择早于 queryCompleteTime 的 StartTime 和晚于 queryCompleteTime 的 EndTime。
6. 从检索到的公钥中，选择指纹与签名文件中的 publicKeyFingerprint 值匹配的公钥。
7. 使用包含以空格分隔的每个查询结果文件哈希值的哈希列表，重新创建用于验证签名文件签名的数据签名字符串。签名文件列出了每个查询结果文件的 fileHashValue。

   例如，如果签名文件的 files 数组包含以下三个查询结果文件，则哈希列表为“aaa bbb ccc”。

```
“files": [

   {

        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"

   },
   {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

   },
   {

        "fileHashValue" : “ccc”,

        "fileName" : "result_3.csv.gz"

   }
],
```

8. 将此字符串的 SHA-256 哈希值、公钥及签名作为参数传递给 RSA 签名验证算法，以验证签名。如果结果为 true，则签名文件有效。

验证查询结果文件

如果签名文件有效，请验证签名文件引用的查询结果文件。要验证查询结果文件的完整性，请计算其压缩内容的 SHA-256 哈希值，并将结果与签名文件中记录的查询结果文件中的 fileHashValue 进行比较。如果哈希值匹配，则查询结果文件有效。

以下部分详细介绍了验证过程。

A. 获取签名文件

第一步是获取签名文件并获取公钥的指纹。

1. 从 Amazon S3 存储桶中获取要验证的查询结果的签名文件。
2. 接下来，从签名文件中获取 `hashSignature` 值。
3. 在签名文件中，从 `publicKeyFingerprint` 字段中获取与用于对文件进行签名的私钥对应的公钥的指纹。

B. 检索用于验证签名文件的公钥

要获取用于验证签名文件的公钥，您可以使用 AWS CLI 或 CloudTrail API。在这两种情况下，您都需要指定要验证的签名文件的时间范围（即起始时间和结束时间）。使用与签名文件中的 `queryCompleteTime` 对应的时间范围。对于您指定的时间范围，可能会返回一个或多个公钥。返回的密钥的有效时间范围可能会发生重叠。

> **Note**
>
> 由于每个区域 CloudTrail 使用不同的私钥/公钥对，因此每个签名文件都使用其区域独有的私钥进行签名。因此，当您验证来自特定区域的签名文件时，必须从同一区域检索其公钥。

使用检 AWS CLI 索公钥

要使用检索签名文件的公钥 AWS CLI，请使用`cloudtrail list-public-keys`命令。此命令采用以下格式：

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

start-time 和 end-time 参数为 UTC 时间戳且是可选的。如果未指定，则使用当前时间，且返回当前有效的一个或多个公钥。

示例响应

响应是代表所返回的一个或多个密钥的 JSON 对象的列表：

使用 CloudTrail API 检索公钥

要使用 CloudTrail API 检索签名文件的公钥，请将开始时间和结束时间值传递给 `ListPublicKeys` API。`ListPublicKeys` API 会返回与用于在指定时间范围对文件进行签名的私钥对应的公钥。对于每个公钥，此 API 还返回相应的指纹。

`ListPublicKeys`

本部分介绍 `ListPublicKeys` API 的请求参数和响应元素。

> **Note**
>
> `ListPublicKeys` 的二进制字段的编码可能随时发生变化。

请求参数

名称	描述
`StartTime`	（可选）以 UTC 为单位指定查找 CloudTrail 签名文件公钥的时间范围的起始时间。如果 StartTime 未指定，则使用当前时间，并返回当前的公钥。 类型: DateTime
`EndTime`	（可选）以 UTC 为单位指定查找 CloudTrail 签名文件公钥的时间范围的结束时间。如果 EndTime 未指定，则使用当前时间。 类型: DateTime

响应元素

`PublicKeyList` - `PublicKey` 对象数组，包含：

名称	描述
`Value`	DER 编码的公钥值（采用 PKCS #1 格式）。 类型：Blob

ValidityStartTime	公钥有效的起始时间。 类型: DateTime
ValidityEndTime	公钥有效的结束时间。 类型: DateTime
Fingerprint	公钥的指纹。指纹可用于识别验证签名文件所必需的公钥。 类型：字符串

C. 选择要用于验证的公钥

从 list-public-keys 或 ListPublicKeys 检索到的公钥中，选择指纹与签名文件的 publicKeyFingerprint 字段中记录的指纹匹配的公钥。此即为用于验证签名文件的公钥。

D. 重新创建数据签名字符串

现在，您已拥有签名文件的签名及关联公钥，接下来，您需要计算数据签名字符串。算出数据签名字符串后，您就有了验证签名所需的输入。

数据签名字符串包含以空格分隔的每个查询结果文件的哈希值。重新创建此字符串后，您可以验证签名文件。

E. 验证签名文件

将重新创建的数据签名字符串、数字签名和公钥传递给 RSA 签名验证算法。如果输出为 true，则已验证签名文件的签名，且签名文件有效。

F. 验证查询结果文件

验证签名文件后，您可以验证其引用的查询结果文件。签名文件包含查询结果文件的 SHA-256 哈希值。如果其中一个查询结果文件在 CloudTrail 交付后被修改，则 SHA-256 哈希值将发生变化，并且签名文件的签名将不匹配。

使用以下步骤验证签名文件的 files 数组中列出的查询结果文件。

1. 从签名文件中的 files.fileHashValue 字段检索文件的原始哈希值。
2. 使用 hashAlgorithm 中指定的哈希算法计算压缩的查询结果文件内容的哈希值。

3. 将您为每个查询结果文件生成的哈希值与签名文件中的 `files.fileHashValue` 进行比较。如果哈希值匹配，则查询结果文件有效。

离线验证签名和查询结果文件

离线验证签名和查询结果文件时，您通常可以按照前述部分中介绍的流程进行。但是，您必须考虑以下有关公钥的信息。

公钥

要进行离线验证，首先必须在线获取验证给定时间范围内的查询结果文件所需的公钥（例如，通过调用 `ListPublicKeys` 实现），然后将其离线存储。每当您需要验证超出指定的初始时间范围的其他文件时，都必须重复执行这一步。

示例验证代码段

以下示例片段提供了用于验证 CloudTrail 签名和查询结果文件的基本代码。此框架代码未指定在线/离线条件；也就是说，由您决定是否实现在线连接到 AWS的代码。建议在实现中使用 Java Cryptography Extension (JCE) 和 Bouncy Castle 作为安全提供程序。

示例代码段：

- 如何创建用于验证签名文件签名的数据签名字符串。
- 如何验证签名文件的签名。
- 如何计算查询结果文件的哈希值，并将其与签名文件中列出的 `fileHashValue` 进行比较，以验证查询结果文件的真实性。

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
```

```
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
 file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
 copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
 fileS3ObjectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
 match.\tExpected: %s Actual: %s",
```

```
                        s3Bucket, fileS3ObjectKey,
                        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                        s3Bucket, fileS3ObjectKey));
            }

            hashList.add(file.getString("fileHashValue"));
        }
        String hashListString = hashList.stream().collect(Collectors.joining(" "));

        /*
            NOTE:
            To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
            of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
            returned from ListPublicKey API are DER encoded in PKCS#1 format:

            PublicKeyInfo ::= SEQUENCE {
                algorithm       AlgorithmIdentifier,
                PublicKey       BIT STRING
            }

            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
rsaPublicKey);

        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
```

```
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

使用运行和管理 CloudTrail Lake 查询 AWS CLI

您可以使用 AWS CLI 来运行和管理您的 CloudTrail Lake 查询。使用时 AWS CLI，请记住您的命令在 AWS 区域 配置文件中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

可用于 L CloudTrail ake 查询的命令

用于在 L CloudTrail ake 中运行和管理查询的命令包括：

- `start-query`来运行查询。
- `describe-query`返回有关查询的元数据。
- `get-query-results`返回指定查询 ID 的查询结果。
- `list-queries`以获取指定事件数据存储的查询列表。
- `cancel-query`取消正在运行的查询。

有关 La CloudTrail ke 事件数据存储的可用命令列表，请参阅事件数据存储的可用命令。

有关 La CloudTrail ke 集成的可用命令列表，请参阅L CloudTrail ake 集成的可用命令。

使用开始查询 AWS CLI

以下示例 AWS CLI start-query命令对在查询语句中指定为 ID 的事件数据存储运行查询，并将查询结果传送到指定的 S3 存储桶。`--query-statement` 参数提供 SQL 查询，用单引号括起来。可选参数包括 `--delivery-s3uri`，用于将查询结果传送到指定的 S3 存储桶。有关您可以在 La CloudTrail ke 中使用的查询语言的更多信息，请参阅CloudTrail 湖泊 SQL 限制。

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

响应是 `QueryId` 字符串。要获取查询的状态，请使用 start-query 返回的值 `QueryId` 运行 describe-query。如果查询成功，您可以运行 get-query-results 以获取结果。

输出

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> 运行时间超过一小时的查询可能会超时。您仍可获得在查询超时之前处理的部分结果。
> 如果您使用可选`--delivery-s3uri`参数将查询结果传送到 S3 存储桶，则存储桶策略必须授予将查询结果传送到该存储桶的 CloudTrail权限。有关手动编辑存储桶策略的信息，请参阅适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略。

使用获取有关查询的元数据 AWS CLI

以下示例 AWS CLI describe-query命令获取有关查询的元数据，包括以毫秒为单位的查询运行时间、扫描和匹配的事件数、扫描的总字节数以及查询状态。`BytesScanned` 值与账户支付查询费用的总字节数匹配，除非查询仍在运行。如果查询结果已传送到 S3 存储桶，则响应还会提供 S3 URI 和交付状态。

您可以指定 `--query-id` 或 `--query-alias` 参数的值。指定 `--query-alias` 参数会返回有关该别名的上次查询运行的信息。

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

以下为响应示例。

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

使用获取查询结果 AWS CLI

以下示例 AWS CLI get-query-results 命令获取查询的事件数据结果。您必须指定 `--query-id` 返回的 start-query 命令。`BytesScanned` 值与账户支付查询费用的总字节数匹配，除非查询仍在运行。可选参数包括 `--max-query-results`，以指定希望在单个页面上通过命令返回的最大结果数。如果结果数超过指定的 `--max-query-results` 值，请再次运行命令，添加返回 `NextToken` 值来获取下一页的结果。

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

输出

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
```

```
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

使用列出事件数据存储上的所有查询 AWS CLI

以下示例 AWS CLI list-queries 命令返回过去七天内指定事件数据存储中的查询和查询状态的列表。您必须指定 ARN 或 `--event-data-store` ARN 值的 ID 后缀。或者，要缩短结果列表，您可以通过添加 `--start-time` 和 `--end-time` 参数和 `--query-status` 值来指定时间范围、格式化为时间戳。`QueryStatus` 的有效值包括 QUEUED、RUNNING、FINISHED、FAILED 或 CANCELLED。

list-queries 还有可选的分页参数。使用 `--max-results` 以指定希望在单个页面上通过命令返回的最大结果数。如果结果数超过指定的 `--max-results` 值，请再次运行命令，添加返回 `NextToken` 值来获取下一页的结果。

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

输出

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
```

```
    "NextToken": "20add42078135EXAMPLE"
}
```

使用取消正在运行的查询 AWS CLI

以下示例 AWS CLI cancel-query命令取消状态为的查询。RUNNING您必须为 `--query-id` 指定一个值。当您运行 cancel-query 时，即使尚未完成 cancel-query 操作，查询状态也可能会显示为 CANCELLED。

> **Note**
>
> 取消的查询可能会产生费用。您的账户仍需为取消查询之前扫描的数据量支付费用。

以下是 CLI 示例。

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

输出

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail 湖泊 SQL 限制

CloudTrail 湖泊查询是 SQL 字符串。本节提供有关支持的函数、运算符和架构相关信息。

仅允许使用 SELECT 语句。没有查询字符串可以更改或变更数据。

CloudTrail Lake 支持所有有效的 Presto SQL SELECT 语句、函数和运算符。如需详细了解支持的 SQL 函数和运算符，请参阅 Presto 文档网站中的函数和运算符。

CloudTrail 控制台提供了许多示例查询，可以帮助您开始编写自己的查询。有关更多信息，请参阅 在 CloudTrail 控制台中查看示例查询。

主题

- 支持的函数、条件和联接运算符
- 高级多表查询支持

支持的函数、条件和联接运算符

支持的函数

CloudTrail Lake 支持 Presto 的所有功能。如需详细了解支持的函数，请参阅 Presto 文档网站中的函数和运算符。

CloudTrail Lake 不支持该INTERVAL关键字。

支持的条件运算符

以下是支持的条件运算符。

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

支持的联接运算符

以下是支持的 JOIN 运算符。有关运行多表查询的更多信息，请参阅 高级多表查询支持。

```
UNION
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

高级多表查询支持

CloudTrail Lake 支持跨多个事件数据存储的高级查询语言。

- UNION|UNION ALL|EXCEPT|INTERSECT
- LEFT|RIGHT|INNER JOIN

要运行查询，请在 AWS CLI中使用 start-query 命令。以下是一个示例，它使用本节中的一个示例查询。

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

响应是 QueryId 字符串。要获取查询的状态，请使用 start-query 返回的值 QueryId 运行 describe-query。如果查询成功，您可以运行 get-query-results 以获取结果。

UNION|UNION ALL|EXCEPT|INTERSECT

以下是一个示例查询，它使用 UNION 和 UNION ALL 在三个事件数据存储（EDS1、EDS2 和 EDS3）中按它们的事件 ID 和事件名称查找事件。首先从每个事件数据存储中选择结果，然后将结果串联起来，按事件 ID 排序，并限制为十个事件。

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

LEFT|RIGHT|INNER JOIN

以下是一个示例查询，它使用 LEFT JOIN 查找名为 eds2、映射到 edsB 的事件数据存储中的所有事件，这些事件与主（左侧）事件数据存储 edsA 中的事件匹配。返回的事件发生在 2020 年 1 月 1 日或之前，并且仅返回事件名称。

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
```

```
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

支持的事件数据存储的 SQL 架构

以下各节提供了每种事件数据存储类型支持的 SQL 架构。

主题

- CloudTrail 事件记录字段支持的架构
- Ins CloudTrail ights 事件记录字段支持的架构
- AWS Config 配置项目记录字段支持的架构
- AWS Audit Manager 证据记录字段支持的架构
- 非AWS 事件字段支持的架构

CloudTrail 事件记录字段支持的架构

以下是 CloudTrail 管理和数据事件记录字段的有效 SQL 架构。有关 CloudTrail 事件记录字段的更多信息，请参阅CloudTrail 录制内容。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
 "struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

 username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

 mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

 accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

 attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
                ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
```

```
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
    {
        "Name": "eventname",
        "Type": "string"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
        "Type": "string"
    },
    {
        "Name": "errorcode",
        "Type": "string"
    },
    {
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
```

```
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
 "array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
```

```
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsoncheckсum",
        "Type": "string"
    }
]
```

Ins CloudTrail ights 事件记录字段支持的架构

以下是 Insights 事件记录字段的有效 SQL 架构。对于 Insights 事件，`eventcategory` 的值为 `Insight`，`eventtype` 的值为 `AwsCloudTrailInsight`。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
```

```
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type":
 "struct<baselineaverage:double,insightaverage:double,baselineduration:integer,

 insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
                insightaverage:double,baselinevalue:string,baselineaverage:double>>"
    }
]
```

AWS Config 配置项目记录字段支持的架构

以下是配置项目记录字段的有效 SQL 架构。对于配置项目，eventcategory 的值为 ConfigurationItem，eventtype 的值为 AwsConfigurationItem。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
```

```
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

AWS Audit Manager 证据记录字段支持的架构

以下是 Audit Manager 证据记录字段的有效 SQL 架构。对于 Audit Manager 证据记录字段，`eventcategory` 的值为 `Evidence`，`eventtype` 的值为 `AwsAuditManagerEvidence`。有关使用 Audit Manager 在 CloudTrail Lake 中汇总证据的更多信息，请参阅《AWS Audit Manager 用户指南》中的证据查找器。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,
```

```
 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

非AWS 事件字段支持的架构

以下是非AWS 事件的有效 SQL 架构。对于非AWS 事件，的值`eventcategory`为`ActivityAuditLog`，的值`eventtype`为`ActivityLog`。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
```

```
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

控制 L CloudTrail ake 的用户权限

AWS CloudTrail 与 AWS Identity and Access Management (IAM) 集成，可帮助您控制对 CloudTrail Lake 和其他 AWS 所需资源的访问权限。 CloudTrail 您可以使用 IAM 来控制哪些 AWS 用户可以创建、配置或删除 CloudTrail 事件数据存储或频道、启动和停止事件摄取以及复制跟踪事件。要了解更多信息，请参阅适用于 Identity and Access 管理 AWS CloudTrail。

以下主题可帮助您了解权限、策略和 CloudTrail 安全性：

- 授予CloudTrail 管理权限
- 适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略
- 复制跟踪事件所需的权限
- 联合身份验证所需的权限

- 根据标签限制对事件数据存储访问的示例策略：示例：拒绝基于标签创建或删除事件数据存储的访问权限
- AWS CloudTrail 基于资源的策略示例
- 指定委托管理员所需的权限
- CloudTrail Lake 事件数据存储的默认 KMS 密钥策略

管理 CloudTrail 湖泊成本

AWS CloudTrail 湖泊事件数据存储和查询会产生费用。作为最佳实践，我们建议使用 AWS 服务 可以帮助您管理 CloudTrail 成本的工具。您还可以采用捕获所需数据的方式配置事件数据存储，同时保持经济高效。有关 CloudTrail 定价的信息，请参阅 AWS CloudTrail 定价。

主题

- 事件数据存储定价选项
- 了解 CloudTrail Lake 费用
- 关于如何降低成本的建议
- 可帮助管理成本的工具
- 另请参阅

事件数据存储定价选项

创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。

下表介绍了可用的定价选项。下表显示了控制台中的定价选项和 API 的相应 `BillingMode` 值，并列出了每个选项的默认保留期和最长保留期。

定价选项（控制台）	BillingMode (API)	描述
一年的可延期保留定价	`EXTENDABLE_RETENTION_PRICING`	如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），则建议这样做。如果事件数据存储从 AWS外部收集 AWS Config 配置项目、Audit Manager 证据和事件，也建议使用此选项。

定价选项（控制台）	BillingMode (API)	描述
		在前 366 天（默认保留期）内，存储包含在摄取定价中，没有额外费用。366 天后，可以按 pay-as-you-go定价延长保留期。 这是默认选项。 默认保留期：366 天 最长保留期：3653 天
七年期保留定价	`FIXED_RETENTION_PRICING`	如果您希望每月摄取的事件数据大于 25TB，并且需要最长 7 年的保留期，则建议这样做。 保留包含在摄取定价中，没有额外费用。 默认保留期：2557 天 最长保留期：2557 天

了解 CloudTrail Lake 费用

下表提供了有关 L CloudTrail ake 事件数据存储和查询如何产生费用的信息。有关 CloudTrail 定价的信息，请参阅 AWS CloudTrail 定价。

费用类型	您的费用是如何产生的
数据摄取（未压缩的数据）	对于 CloudTrail Lake，您需要根据提取的未压缩数据付费。事件数据存储的定价选项决定了摄取事件的成本： • 一年可延期保留定价：根据事件类型提供摄取定价。 • 七年期保留定价：根据摄取的数据量提供摄取定价。当每月摄取的数据量超过 25TB 时，可以实现最大的节省。 复制跟踪事件

费用类型	您的费用是如何产生的
	将跟踪事件复制到 CloudTrail Lake 时，CloudTrail 解压缩以 gzip（压缩）格式存储的日志。然后 CloudTrail 将日志中包含的事件复制到您的事件数据存储中。未压缩数据的大小可能大于 Amazon S3 的实际存储大小。要对未压缩数据的大小进行总体估计，将 S3 存储桶中日志的大小乘以 10。 **Note** CloudTrail 如果事件的时间早于指定的保留期，则不会复制该事件。要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要将事件在事件数据存储中保留的天数之和，如以下公式所示： 保留期 = *oldest-event-in-days* + *number-days-to-retain* 例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。
数据留存（经过优化和压缩的数据）	CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索压缩数据进行优化的列式存储格式。 事件数据存储的保留期决定了事件数据在事件数据存储中保存多长时间。 CloudTrail Lake 通过检查事件的事件时间是否在指定的保留期内来决定是否保留事件。例如，如果您将保留期指定为 90 天，则 CloudTrail 会在事件时间超过 90 天时将其删除。 对于使用七年期保留定价选项的事件数据存储，存储包含在摄取定价中，没有额外费用。 对于使用一年可延期保留定价选项的事件数据存储，存储包含在前 366 天（默认保留期）的摄取定价中，无需付费。366 天后，将提供存储空间， pay-as-you-pricing 并根据事件数据存储中经过优化和压缩的数据收费。

费用类型	您的费用是如何产生的
在 CloudTrail Lake 中运行查询（经过优化和压缩的数据）	在 CloudTrail Lake 中运行查询时，您需要根据扫描的优化和压缩数据量付费。

关于如何降低成本的建议

本节提供了有关在使用 La CloudTrail ke 时如何降低成本的建议。

根据您的事件数据存储将收集的事件类型以及预计的每月摄入量来选择定价选项

创建事件数据存储时，根据您的事件数据存储将收集的事件类型以及预计的每月摄入量来选择定价选项。

如果您希望每月摄取的事件数据少于 25TB，并且想要灵活的保留期（最长 10 年），请选择一年可延期保留定价选项。对于从外部收集 AWS Config 配置项目、Audit Manager 证据和事件的事件数据存储，我们通常也建议使用此选项 AWS。

如果您希望每月摄取的事件数据多于 25TB，并且需要 7 年保留期，请选择i七年保留定价选项。

评估事件数据存储在一段时间内的月摄取量

评估事件数据存储的历史月度摄取量，了解是否有更适合您需求的定价选项。

如果您的现有事件数据存储使用七年保留定价选项，并且每月摄取的数据少于 25TB，请考虑更新事件数据存储以使用一年可延期保留定价。对于使用七年保留定价选项的事件数据存储，您可以使用CloudTrail 控制台或 UpdateEventDataStoreAPI 操作更改定价选项。AWS CLI

如果您的现有事件数据存储使用一年可延期保留定价选项，并且每月摄取的数据多于 25TB，请考虑七年保留定价是否更适合您的需求。要使用新的定价选项，请停止对您的事件数据存储进行摄取，并使用七年保留定价选项创建一个新的事件数据存储。

请使用高级事件选择器筛选出不感兴趣的事件

为 CloudTrail 管理事件或数据事件配置事件数据存储时，请使用高级事件选择器筛选出不感兴趣的事件。

如果您要创建事件数据存储来收集管理事件，则可以筛选出 AWS Key Management Service (AWS KMS) 或亚马逊关系数据库服务 (Amazon RDS) 数据 API 事件。通常，诸如`Encrypt`、`Decrypt`、和之类的 AWS KMS 操作`GenerateDataKey`会生成超过 99% 的事件。

如果您正在创建事件数据存储来收集数据事件，则可以使用高级事件选择器对 `eventName`、`resources.type`、`resources.ARN` 和 `readOnly` 字段进行筛选。有关示例，请参阅示例：为 S3 数据事件创建事件数据存储。

复制跟踪事件时，请选择较窄的时间范围

将跟踪事件复制到 CloudTrail Lake 时，请指定较窄的开始事件时间和结束事件时间，以减少摄取的数据量。

如果您要将跟踪事件复制到 CloudTrail Lake 进行历史分析，并且不想采集 future 事件，请取消选择采集事件的选项，这样您就不会因为摄取任何其他事件而产生费用。

设置查询格式，以使用开头和结尾 **`eventTime`**

在 Lake 中运行查询时，您需要按扫描的数据量付费。您可以通过指定查询的开头和结尾 `eventTime` 来限制成本。

可帮助管理成本的工具

AWS 预算是一项功能 AWS Billing and Cost Management，它允许您设置自定义预算，当您的成本或使用量超过（或预计将超过）预算金额时提醒您。

在创建事件数据存储时，建议使用 AWS 预算 CloudTrail 来创建预算，这可以帮助您跟踪 CloudTrail 支出。基于成本的预算有助于提高人们对可能要支付多少使用费用的认识。 CloudTrail 当您的账单达到您定义的阈值时，预算提醒会通知您。在收到预算提醒时，可以在账单周期结束之前进行更改以管理成本。

创建预算后，您可以使用 AWS Cost Explorer 来查看您的 CloudTrail 成本如何影响您的总 AWS 账单。在 AWS Cost Explorer 中， CloudTrail 添加到服务筛选器后，您可以按地区和账户将历史 CloudTrail支出与当前 month-to-date (MTD) 支出进行比较。此功能可帮助您监控和检测每月 CloudTrail支出中的意外成本。Cost Explorer 中的其他功能使您可以将 CloudTrail 支出与特定资源级别的每月支出进行比较，从而提供有关可能导致账单成本增加或减少的原因的信息。

要开始使用 AWS 预算，请打开 AWS Billing and Cost Management，然后在左侧导航栏中选择预算。我们建议您在创建预算时配置预算提醒以跟踪 CloudTrail 支出。有关如何使用 AWS 预算的更多信息，请参阅使用预算管理成本 AWS Budgets和AWS 预算最佳实践。

为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签

您可以创建用户定义的成本分配标签来跟踪 La CloudTrail ke 事件数据存储的查询和摄取成本。用户定义的成本分配标签是您可以与事件数据存储关联的键值对。激活成本分配标签后，AWS 使用标签在成本分配报告中整理资源成本。

- 要在控制台中创建标签，请参阅 为 CloudTrail 管理事件或数据事件创建事件数据存储 过程的步骤 9。
- 要使用 CloudTrail API 创建标签，请参阅 AWS CloudTrail API 参考AddTags中的CreateEventDataStore和。
- 要使用AWS CLI 命令参考中的创建标签 AWS CLI，请参阅create-event-data-store和添加标签。

有关激活标签的更多信息，请参阅激活用户定义的成本分配标签。

另请参阅

- AWS CloudTrail 定价
- 支持的 CloudWatch 指标
- 通过以下方式管理成本 AWS Budgets
- 开始使用 Cost Explorer 成本管理服务

支持的 CloudWatch 指标

CloudTrail Lake 支持亚马逊 CloudWatch 指标。 CloudWatch 是一项 AWS 资源监控服务。您可以使用 CloudWatch 来收集和跟踪指标、设置警报以及自动对 AWS 资源变化做出反应。

`AWS/CloudTrail`命名空间包括 CloudTrail Lake 的以下指标。

指标	描述	单位
`HourlyDataIngested`	过去一小时内摄取入事件数据存储的数据量。此指标每小时更新一次。 此指标可用于所有事件数据存储类型。	字节

指标	描述	单位
TotalDataRetained	事件数据存储在整个保留期内保留的数据量。此指标每晚更新一次。 此指标可用于所有事件数据存储类型。	字节
TotalStorageBytes	事件数据存储截至当天的压缩字节总数。 此指标可用于所有事件数据存储类型。	字节
TotalPaidStorageBytes	对于使用一年可延期保留定价选项的事件数据存储，这是 366 天到为事件数据存储配置的最大保留期后的总压缩字节数。 对于使用一年可延期保留定价选项的事件数据存储，存储包含在前 366 天的摄取定价中，无需额外费用，这是事件数据存储的默认保留期限。366 天后，存储时间为。 pay-as-you-go有关定价的信息，请参阅 AWS CloudTrail 定价。 此指标仅可用于使用一年可延期保留定价选项的事件数据存储。	字节

指标	描述	单位
HourlyEventsAnalyzed	CloudTrail Insights 在事件数据存储中分析的事件总数。此指标每小时更新一次。 该指标适用于启用 CloudTrail Insights CloudTrail 的事件数据存储。	计数

有关 CloudWatch 指标的更多信息，请参阅以下主题。

- 使用亚马逊 CloudWatch 指标
- 使用 Amazon CloudWatch 警报

处理 CloudTrail 轨迹

T@@ rail s 会捕获 AWS 活动记录，将这些事件传送并存储在 Amazon S3 存储桶中，也可以选择传送到 CloudWatch Logs 和 Amazon EventBridge。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到 S3 存储桶，但是 Amazon S3 会收取存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

您可以为创建两种类型的跟踪 AWS 账户：多区域跟踪和单区域跟踪。

多区域跟踪

创建多区域跟踪时，会在您工作的AWS 分区 AWS 区域中 CloudTrail 记录所有事件，并将 CloudTrail 事件日志文件传送到您指定的 S3 存储桶。如果在创建多区域跟踪后添加了，则会自动包含该新区域，并记录该区域中的事件。 AWS 区域 推荐的最佳实践是创建多区域跟踪，因为您可记录您账户中的所有区域的活动。您使用 CloudTrail 控制台创建的所有跟踪都是多区域的。您可以使用将单区域跟踪转换为多区域跟踪。 AWS CLI有关更多信息，请参阅 在控制台中创建跟踪 和 将应用到一个区域的跟踪转换为应用到所有区域。

单区域跟踪

创建单区域跟踪时，仅 CloudTrail 记录该区域的事件。然后，它 CloudTrail 会将事件日志文件传送到您指定的 Amazon S3 存储桶。您只能使用 AWS CLI创建单区域跟踪。如果您创建其他单个跟踪，则可以让这些跟踪将 CloudTrail 事件日志文件传送到同一 S3 存储桶或单独的存储桶。这是您使用 AWS CLI 或 CloudTrail API 创建跟踪时的默认选项。有关更多信息，请参阅 使用创建、更新和管理跟踪 AWS CLI。

> **Note**
>
> 对于这两种类型的跟踪，您可以在任何区域中指定 Amazon S3 存储桶。

如果您在中创建了组织 AWS Organizations，则可以创建组织跟踪，记录该组织中所有 AWS 账户的所有事件。组织跟踪可以应用于所有 AWS 地区或当前区域。组织跟踪必须使用管理账户或委托管理员账户创建，并且在指定为应用于某个组织时，组织跟踪将自动应用于该组织中的所有成员账户。成员账户可以看到组织记录，但不能对其进行修改或删除。默认情况下，成员账户无权访问 Amazon S3 存储桶中组织跟踪的日志文件。有关更多信息，请参阅 为组织创建跟踪。

主题

- 为您创建路线 AWS 账户
- 为组织创建跟踪
- 查看路径的 CloudTrail Insights 事件
- 将追踪事件复制到 CloudTrail湖中
- 获取和查看您的 CloudTrail 日志文件
- 配置 Amazon SNS 通知 CloudTrail
- 关于管理跟踪记录的提示
- 控制用户对 CloudTrail 跟踪的权限
- AWS CloudTrail 与接口 VPC 终端节点一起使用
- AWS 账户 封闭和步道

为您创建路线 AWS 账户

创建跟踪时，可以将事件作为日志文件持续传送到指定的 Simple Storage Service（Amazon S3）存储桶。创建跟踪可提供许多好处，其中包括：

- 超过 90 天的事件记录。
- 通过向 Amazon Log CloudWatch s 发送日志事件来自动监控指定事件并发出警报的选项。
- 使用 Amazon Athena 查询日志和分析 AWS 服务活动的选项。

从 2019 年 4 月 12 日起，您只能在记录事件的 AWS 区域中查看跟踪。如果您创建的跟踪记录了所有 AWS 区域的事件，则该跟踪将显示在控制台中您正在工作的 AWS 分区中所有区域中。如果您创建仅记录单个 区域中事件的日志，则可以在该 区域中查看和管理它。如果您使用 AWS CloudTrail 控制台创建跟踪，则创建多区域跟踪是默认选项，也是推荐的最佳做法。要创建单区域跟踪，您必须使用 AWS CLI。

如果您使用 AWS Organizations，则可以创建一个跟踪来记录组织中所有 AWS 账户的事件。将在每个成员账户中创建同名的跟踪，并且来自每个跟踪的事件将传递到您指定的 Simple Storage Service（Amazon S3）存储桶。

> **Note**
>
> 只有组织的管理账户或委托管理员账户才能为组织创建跟踪。为组织创建跟踪会自动启用和 Organization CloudTrail s 之间的集成。有关更多信息，请参阅 为组织创建跟踪。

主题

- 使用控制台创建和更新跟踪
- 使用创建、更新和管理跟踪 AWS CLI

使用控制台创建和更新跟踪

您可以使用 CloudTrail 控制台创建、更新或删除您的跟踪。使用控制台创建的跟踪具有多区域属性。要创建仅在一个中记录事件的跟踪 AWS 区域，请使用 AWS CLI。

您最多可以为每个区域创建 5 个跟踪。创建跟踪后， CloudTrail会自动开始将您账户中的 API 调用和相关事件记录到您指定的 Amazon S3 存储桶中。要停止记录，您可以对跟踪禁用日志记录或将其删除。

使用 CloudTrail 控制台创建或更新跟踪具有以下优点。

- 如果这是您第一次创建跟踪，则使用 CloudTrail 控制台可以查看可用的功能和选项。
- 如果您正在配置记录数据事件的跟踪，则使用 CloudTrail 控制台可以查看可用的数据类型。有关记录事件数据的更多信息，请参阅 记录数据事件。

有关在中为组织创建跟踪的特定信息 AWS Organizations，请参阅为组织创建跟踪。

主题

- 创建跟踪
- 更新跟踪
- 删除跟踪
- 关闭跟踪的日志记录

创建跟踪

作为最佳实践，请创建应用于所有 AWS 区域的跟踪。这是您在 CloudTrail控制台中创建跟踪时的默认设置。当跟踪应用于所有区域时，会将您所在AWS 分区中所有区域的日志文件 CloudTrail 传送到您指定的 S3 存储桶。创建跟踪后， AWS CloudTrail 会自动开始记录您指定的事件。

> **Note**
>
> 创建跟踪后，您可以配置其他跟踪 AWS 服务 以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅 AWS 与日志的服务集成 CloudTrail 。

主题

- 在控制台中创建跟踪
- 后续步骤

在控制台中创建跟踪

使用以下过程创建一个跟踪，该跟踪记录您正在工作的 AWS 分区 AWS 区域 中的所有事件。这是推荐的最佳实践。要记录单区域中的事件（不推荐），请使用 AWS CLI。

要使用创建 CloudTrail 跟踪 AWS Management Console

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 服务主页、“跟踪” 页面或 “控制面板” 页面的 “跟踪” 部分，选择 “创建跟踪”。
3. 在 Create Trail 页面上，对于 Trail name，键入一个跟踪名。有关更多信息，请参阅 命名要求。
4. 如果这是 AWS Organizations 组织跟踪，则可以为组织中的所有账户启用跟踪。要查看此选项，您必须使用管理账户或委托管理员账户中的用户或角色登录到控制台。要成功创建组织跟踪，请确保相应用户或角色具有足够的权限。有关更多信息，请参阅 为组织创建跟踪。
5. 对于 Storage location（存储位置，选择 Create new S3 bucket（创建 S3 存储桶）以创建存储桶。创建存储桶时， CloudTrail会创建并应用所需的存储桶策略。如果您选择创建新的 S3 存储桶，则您的 IAM 策略需要包含`s3:PutEncryptionConfiguration`操作权限，因为默认情况下，该存储桶已启用服务器端加密。

> **Note**
>
> 如果选择了使用现有 S3 存储桶，则在跟踪日志存储桶名称中指定一个存储桶，或选择浏览以选择自己账户中的存储桶。如果您想使用其他账户中的存储桶，则需要指定存储桶名称。存储桶策略必须授予对其进行写入的 CloudTrail 权限。有关手动编辑存储桶策略的信息，请参阅适用于 Amazon S3 存储桶的政策 CloudTrail。

为了便于查找日志，请在现有存储桶中创建一个新文件夹（也称为前缀）来存储 CloudTrail 日志。在 Prefix（前缀）字段中输入前缀。

6. 对于 Log file SSE-KMS encryption（日志文件 SSE-KMS 加密），如果您希望使用 SSE-KMS 加密而非 SSE-S3 加密对您的日志文件进行加密，请选择 Enabled（已启用）。默认值为 Enabled（已启用）。如果您未启用 SSE-KMS 加密，则将使用 SSE-S3 加密对您的日志进行加密。有关 SSE-KMS 加密的更多信息，请参阅将服务器端加密与 AWS Key Management Service (SSE-KMS) 一起使用。有关 SSE-S3 加密的更多信息，请参阅配合使用服务器端加密与 Amazon S3 托管加密密钥（SSE-S3）。

   如果您启用 SSE-KMS 加密，请选择 “新建” 或 “现有”。 AWS KMS key在AWS KMS 别名中，按以下格式指定别名`alias/`*`MyAliasName`*。有关更多信息，请参阅 更新资源以使用 KMS 密钥。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

   > **Note**
   >
   > 您也可以键入其他账户的密钥 ARN。有关更多信息，请参阅 更新资源以使用 KMS 密钥。密钥策略必须 CloudTrail 允许使用密钥加密您的日志文件，并允许您指定的用户读取未加密形式的日志文件。有关手动编辑密钥政策的信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

7. 在 Additional configuration（其他配置）中，请配置以下内容。

   a. 对于 Log file validation（日志文件验证），选择 Enabled（已启用）以将日志摘要传输到您的 S3 存储桶。您可以使用摘要文件来验证您的日志文件在 CloudTrail 交付后是否没有更改。有关更多信息，请参阅 验证 CloudTrail 日志文件完整性。

   b. 要传送 SNS 通知，请选择 “启用”，以便每次向您的存储桶传送日志时都会收到通知。CloudTrail 在日志文件中存储多个事件。SNS 通知针对每个日志文件而不是每个事件发送。有关更多信息，请参阅 配置 Amazon SNS 通知 CloudTrail。

如果您启用了 SNS 通知，则对于 Create a new SNS topic（创建新 SNS 主题），选择 New（新建）创建主题，或选择 Existing（现有）使用现有的主题。如果您创建的是应用到所有区域的跟踪，则针对来自所有区域的日志文件传输的 SNS 通知将发送到您创建的单个 SNS 主题中。

如果选择 “新建”，则会为您 CloudTrail 指定新主题的名称，也可以键入名称。如果选择 Existing（现有），则从下拉列表中选择一个 SNS 主题。您还可以输入来自另一个区域或来自一个具有适当权限的账户的主题的 ARN。有关更多信息，请参阅 Amazon SNS 主题政策 CloudTrail。

如果您创建一个主题，则必须订阅该主题以便获取日志文件传送的通知。您可通过 Amazon SNS 控制台进行订阅。由于通知的频率，建议您将该订阅配置为使用 Amazon SQS 队列来以编程方式处理通知。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。

8. 或者，通过选择在日志中启用，配置 CloudTrail 为将 CloudWatch 日志文件发送到CloudWatch 日志。有关更多信息，请参阅 将事件发送到 CloudWatch 日志。

   a. 如果您启用了与 CloudWatch 日志的集成，请选择 “新建” 来创建新的日志组，或者选择 “现有” 以使用现有的日志组。如果选择 “新建”，则会为您 CloudTrail 指定新日志组的名称，也可以键入名称。

   b. 如果选择 Existing（现有），则从下拉列表中选择一个日志组。

   c. 选择 “新建” 创建新的 IAM 角色，以获得向日志发送 CloudWatch 日志的权限。选择 Existing（现有）以从下拉列表中选择一个现有 IAM 角色。展开 Policy document（策略文档）时，将显示新角色或现有角色的策略语句。有关该角色的更多信息，请参阅 使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档。

   > **Note**
   >
   > - 在您配置跟踪时，可以选择属于另一个账户的 S3 存储桶和 SNS 主题。但是，如果 CloudTrail 要将事件传送到 CloudWatch 日志日志组，则必须选择当前账户中存在的日志组。
   > - 只有管理账户才能使用控制台为组织跟踪配置 CloudWatch 日志组。授权的管理员可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 操作配置 CloudWatch 日志组。

9. 对于 Tags（标签），将一个或多个自定义标签（键值对）添加到跟踪中。标签可以帮助您识别您的 CloudTrail 跟踪和包含 CloudTrail 日志文件的 Amazon S3 存储桶。然后，您可以将资源组用于您的 CloudTrail 资源。有关更多信息，请参阅 AWS Resource Groups 和 标签。
10. 在 Choose log events（选择日志事件）页面中，选择要记录的事件类型。对于 Management events (管理事件)，请执行以下操作。

    a. 对于 API activity（API 活动），选择您希望跟踪记录 Read（读取）事件、Write（写入）事件，还是记录两者。有关更多信息，请参阅 管理事件。

    b. 选择 “排除 AWS KMS 事件”，从您的跟踪中筛选 AWS Key Management Service (AWS KMS) 事件。默认设置是包括所有 AWS KMS 事件。

    仅当您在跟踪中记录管理 AWS KMS 事件时，才可使用记录或排除事件的选项。如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件日志记录设置。

    AWS KMS 诸如`Encrypt`、`Decrypt`和之类的操作`GenerateDataKey`通常会生成大量事件（超过 99%）。这些操作现在记录为读取事件。诸如`DisableDelete`、`ScheduleKey`和（通常占事件量不到 0.5%）之类的低容量相关 AWS KMS 操作被记录为写入 AWS KMS 事件。

    要排除高容量事件（如`Encrypt`、`Decrypt`、`GenerateDataKey`和），但仍记录相关事件（例如`DisableScheduleKey`、`Delete`和），请选择记录写入管理事件，然后清除 “排除” AWS KMS 事件复选框。

    c. 选择 Exclude Amazon RDS Data API events（排除 Amazon RDS 数据 API 事件以从跟踪中筛选出 Amazon Relational Database Service 数据 API 事件。默认设置是包含所有 Amazon RDS 数据 API 事件。有关 Amazon RDS 数据 API 事件的更多信息，请参阅 Amazon RDS Aurora 用户指南中的使用 AWS CloudTrail记录数据 API 调用。
11. 要记录数据事件，请选择 Data events（数据事件）。记录数据事件将收取额外费用。有关更多信息，请参阅AWS CloudTrail 定价。
12. **Important**

    默认情况下，步骤 12-16 用于使用高级事件选择器配置数据事件。高级事件选择器让您可以配置更多数据事件类型，并对跟踪捕获的数据事件进行精细控制。如果您选择使用基本事件选择器，请完成 使用基本事件选择器配置数据事件设置 中的步骤，然后返回到此程序的步骤 17。

对于 Data event type（数据事件类型），选择要在其上记录数据事件的资源类型。有关可用数据事件类型的更多信息，请参阅 数据事件。

> **Note**
>
> 要记录由 Lake Formati AWS Glue on 创建的表的数据事件，请选择 La ke Formation。

13. 选择日志选择器模板。 CloudTrail 包括用于记录该资源类型的所有数据事件的预定义模板。要构建自定义日志选择器模板，请选择 Custom（自定义）。

> **Note**
>
> 为 S3 存储桶选择预定义的模板可以记录当前您 AWS 账户中的所有存储分段以及您在创建完跟踪后创建的任何存储分段的数据事件。它还允许记录您 AWS 账户中任何 IAM 身份执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的存储桶上执行的。
> 如果跟踪仅应用于一个区域，则选择记录所有 S3 存储桶的预定义模板可为跟踪所在的区域中的所有存储桶和您后来在该区域中创建的任何存储桶启用数据事件日志记录。它不会在您的 AWS 账户中记录其他区域的 Amazon S3 存储桶的数据事件。
> 如果您要为所有区域创建跟踪，则选择 Lambda 函数的预定义模板可以记录当前 AWS 账户中的所有函数以及完成跟踪后可能在任何区域创建的任何 Lambda 函数的数据事件。如果您要为单个区域创建跟踪（使用完成 AWS CLI），则此选择将启用您 AWS 账户中该区域中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
> 记录所有函数的数据事件还可以记录 AWS 账户中任何 IAM 身份执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

14. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。
15. 在 Advanced event selectors（高级事件选择器）中，为您要记录其数据事件的特定资源构建表达式。如果您使用的是预定义日志模板，则可跳过此步骤。

    a. 从下面的字段中选择。

    - **readOnly**-readOnly 可以设置为等于`true`或`false`的值。只读数据事件是不会更改资源状态的事件，例如 `Get*` 或 `Describe*` 事件。写入事件可添加、更改或删除资源、属性或

构件，例如 Put*、Delete* 或 Write* 事件。要记录 read 和 write 两种事件，请不要添加 readOnly 选择器。

- **eventName** - eventName 可以使用任何运算符。您可以使用它来包含或排除记录到的任何数据事件 CloudTrail，例如PutBucketPutItem、或GetSnapshotBlock。
- **resources.ARN**-您可以将任何运算符与一起使用resources.ARN，但是如果您使用等于或不等于，则该值必须与您在模板中指定为的值的有效资源的 ARN 完全匹配。resources.type

  下表显示每个 resources.type 的有效 ARN 格式。

  > **Note**
  >
  > 您不能使用该resources.ARN字段筛选没有 ARN 的资源类型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	resources.ARN
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	ARN 必须采用以下格式之一： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必须采用以下格式之一： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] 对于启用了流的表，数据事件中的 resources 字段同时包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您为 resources.type 指定 AWS::DynamoDB::Table，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName在该字段上添加过滤器。

[2] 要记录特定 S3 存储桶中所有对象的所有数据事件，请使用 StartsWith 运算符，并且仅包含存储桶 ARN 作为匹配值。刻意使用尾部斜杠；切勿排除它。

[3] 要记录 S3 接入点中的所有对象的事件，建议您仅使用接入点 ARN，而不要包含对象路径，并且使用 StartsWith 或 NotStartsWith 运算符。

有关数据事件资源的 ARN 格式的更多信息，请参阅 AWS Identity and Access Management 用户指南中的操作、资源和条件键。

b. 对于每个字段，请选择 + 条件以根据需要添加任意数量的条件，所有条件总共可有最多 500 个指定值。例如，要从跟踪中记录的数据事件中排除两个 S3 存储桶的数据事件，您可以将该字段设置为 Resou rces.arn，将运算符设置为 “不以开头”，然后粘贴到 S3 存储桶 ARN 中，或者浏览您不想为其记录事件的 S3 存储桶。

要添加第二个 S3 存储桶，请选择 + 条件，然后重复上述说明，在 ARN 中粘贴或浏览到不同的存储桶。

> **Note**
>
> 对于跟踪上的所有选择器，最多可以有 500 个值。这包括选择器的多个值的数组，例如 `eventName`。如果所有选择器均为单个值，则最多可以向选择器添加 500 个条件。
>
> 如果您的账户中有超过 15,000 个 Lambda 函数，则在创建跟踪时无法在 CloudTrail 控制台中查看或选择所有函数。您仍可使用预定义选择器模板记录所有函数，即使这些函数未显示出来也是如此。如果您要记录特定函数的数据事件，则可手动添加一个函数 (如果您知道其 ARN)。您也可以在控制台中完成跟踪的创建，然后使用 AWS CLI 和put-event-selectors命令为特定 Lambda 函数配置数据事件记录。有关更多信息，请参阅 使用管理跟踪 AWS CLI。

c. 根据需要，选择 + Field（+ 字段）以添加其他字段。为了避免错误，请不要为字段设置冲突或重复的值。例如，不要在一个选择器中将 ARN 指定为等于某个值，然后在另一个选择器中指定 ARN 不等于相同的值。

16. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。重复步骤 12 至此步骤，为数据事件类型配置高级事件选择器。
17. 如果您希望跟踪记录见解事件，请选择 CloudTrail Insights 事件。

    在 Event type（事件类型）中，选择 Insights events（Insights 事件）。您必须记录写入管理事件，以针对 API 调用率记录 Insights 事件。您必须记录读取或写入管理事件，以针对 API 错误率记录 Insights 事件。

    CloudTrail Insights 会分析管理事件中是否存在异常活动，并在检测到异常时记录事件。默认情况下，跟踪记录不记录 Insights 事件。有关 Insights 事件的更多信息，请参阅记录 Insights 事件。记录 Insights 事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

    Insights 事件将传送到另一个文件夹，该文件夹以同一 S3 存储桶命名`/CloudTrail-Insight`，该存储桶在跟踪详细信息页面的存储位置区域中指定。 CloudTrail为您创建新的前缀。例如，如果当前目标 S3 存储桶命名为 `S3bucketName/AWSLogs/CloudTrail/`，则带有新前缀的 S3 存储桶名称会命名为 `S3bucketName/AWSLogs/CloudTrail-Insight/`。
18. 完成选择要记录的事件类型的操作后，选择 Next（下一步）。
19. 在 Review and create（审核和重建）页面上，审核您的选择。在相关部分中选择 Edit（编辑）以更改该部分中显示的跟踪设置。在准备好创建跟踪时，选择 Create trail（创建跟踪）。
20. 新跟踪记录出现在 Trails（跟踪记录）页面上。大约 5 分钟后，将 CloudTrail 发布日志文件，显示在您的账户中进行的 AWS API 调用。您可以在指定的 S3 存储桶中查看日志文件。如果您启用

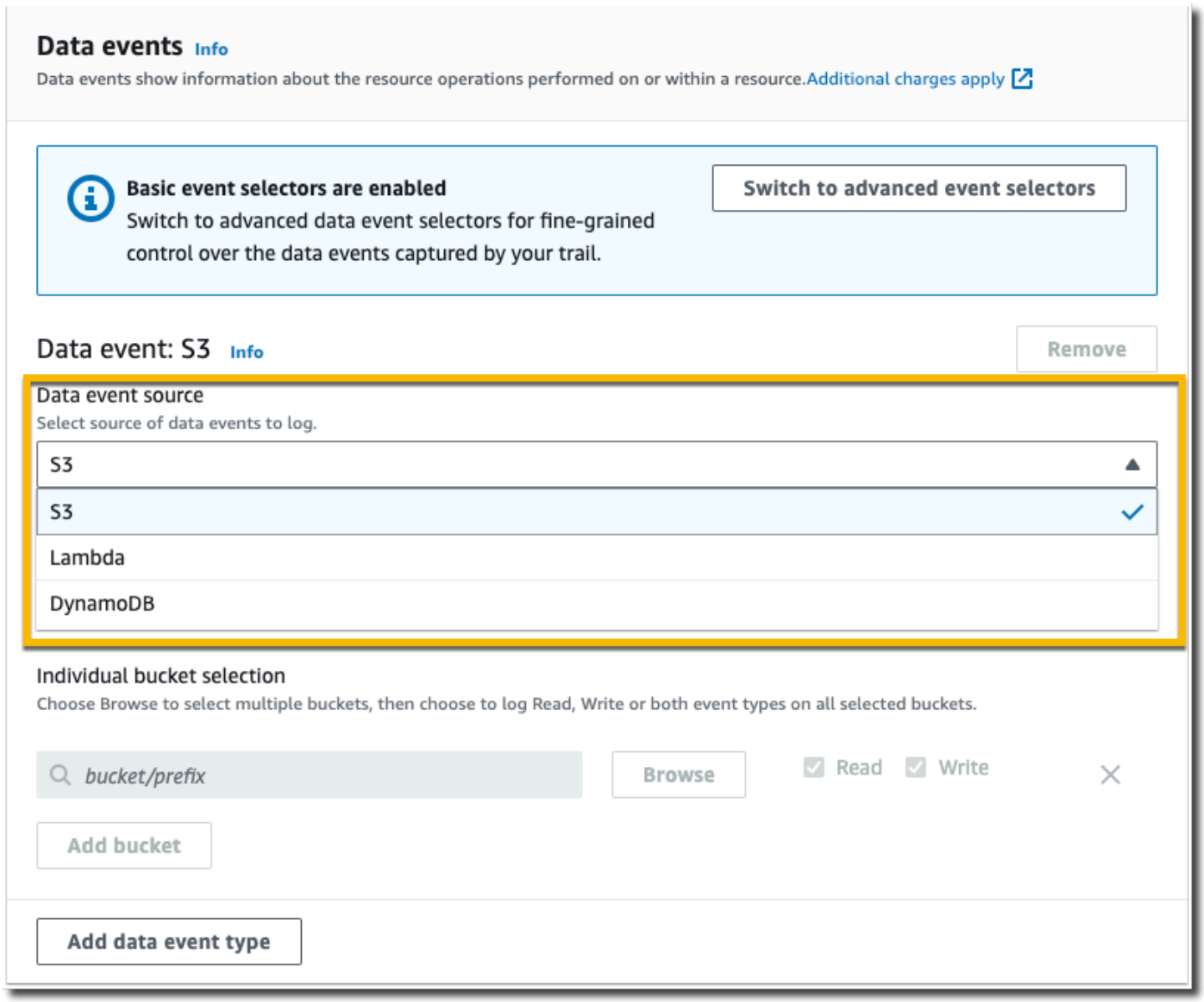
了 Insights 事件记录，并且检测 CloudTrail 到异常活动，则最长可能需要 36 小时才能交付第一个 Insights 事件。

> **Note**
>
> CloudTrail 通常在 API 调用后的平均大约 5 分钟内传送日志。此时间并不能得到保证。有关更多信息，请参阅 AWS CloudTrail 服务等级协议。
> 如果您错误配置了跟踪（例如，无法访问 S3 存储桶），则 CloudTrail 会尝试将日志文件重新传送到您的 S3 存储桶，持续 30 天，这些 attempted-to-deliver 事件将按标准费用收费。 CloudTrail 为避免配置错误的跟踪产生费用，您需要删除跟踪。

使用基本事件选择器配置数据事件设置

您可以使用高级事件选择器来配置所有数据事件类型。高级事件选择器允许您创建细粒度的选择器，以仅记录那些感兴趣的事件。

如果您使用基本事件选择器来记录数据事件，则只能记录 Amazon S3 存储桶、 AWS Lambda 函数和 Amazon DynamoDB 表的数据事件。您无法使用基本的事件选择器对`eventName`字段进行筛选。



按照以下程序使用基本事件选择器配置数据事件设置。

使用基本事件选择器配置数据事件设置

1. 在事件中，选择数据事件以记录数据事件。记录数据事件将收取额外费用。有关更多信息，请参阅AWS CloudTrail 定价。
2. 对于 Simple Storage Service（Amazon S3）存储桶：
   a. 对于 Data event source（数据事件源），选择 S3。
   b. 您可以选择记录 All current and future S3 buckets（所有当前和未来 S3 存储桶），也可以指定单个存储桶或函数。默认情况下，记录所有当前和未来 S3 存储桶的数据事件。

> **Note**
>
> 保留默认 “All current and future S3 存储桶” 选项将允许您 AWS 账户中当前的所有存储分段以及您在完成跟踪创建后创建的任何存储分段的数据事件记录。它还允许记录您 AWS 账户中任何 IAM 身份执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的存储桶上执行的。
> 如果您要为单个区域创建跟踪（使用完成 AWS CLI），则选择 All current 和 future S3 存储桶可为与您的跟踪位于同一区域的所有存储桶以及您稍后在该区域创建的任何存储桶启用数据事件记录。它不会在您的 AWS 账户中记录其他区域的 Amazon S3 存储桶的数据事件。

c. 如果保留默认值 All current and future S3 buckets（所有当前和未来 S3 存储桶），则选择记录 Read（读取）事件、Write（写入）事件，还是记录两者。

d. 要选择单个存储桶，请清空 All current and future S3 buckets（所有当前和未来 S3 存储桶）的 Read（读取）和Write（写入）复选框。在 Individual bucket selection（单个存储桶选择）中，浏览要在其上记录数据事件的存储桶。通过键入所需存储桶的存储桶前缀来查找特定存储桶。您可以在此窗口中选择多个存储桶。选择添加存储桶，记录更多存储桶的数据事件。选择记录 Read（读取）事件（如 `GetObject`）、Write（写入）事件（如 `PutObject`）或同时记录两种事件。

   此设置优先于为各个存储桶配置的个别设置。例如，如果指定记录所有 S3 存储桶的 Read 事件，然后选择为数据事件日志记录添加一个特定存储桶，则所添加存储桶的 Read 已经是选中状态。您无法清除此选择。只能配置 Write 选项。

   要从日志记录中删除存储桶，请选择 X。

3. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。
4. 对于 Lambda 函数：

   a. 对于 Data event source（数据事件源），选择 Lambda。

   b. 在 Lambda function（Lambda 函数）中，选择 All regions（所有区域）记录所有 Lambda 函数，或选择 Input function as ARN（输入函数作为 ARN）以记录特定函数上的数据事件。

      要记录您 AWS 账户中所有 Lambda 函数的数据事件，请选择记录所有当前和将来的函数。此设置优先于为各个函数配置的个别设置。将记录所有函数，即便这些函数未显示。

> **Note**
>
> 如果为所有区域创建了一个跟踪，则此选择将为您的 AWS 账户中当前包含的所有函数以及您在创建跟踪后可能在任何区域中创建的任何 Lambda 函数启用数据事件日志记录。如果您要为单个区域创建跟踪（使用完成 AWS CLI），则此选择将启用您 AWS 账户中该区域中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
> 记录所有函数的数据事件还可以记录 AWS 账户中任何 IAM 身份执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

c. 如果选择 Input function as ARN（输入函数作为 ARN），则输入 Lambda 函数的 ARN。

> **Note**
>
> 如果您的账户中有超过 15,000 个 Lambda 函数，则在创建跟踪时无法在 CloudTrail 控制台中查看或选择所有函数。您仍可以选择该选项来记录所有函数，即使未显示这些函数也是如此。如果您要记录特定函数的数据事件，则可手动添加一个函数 (如果您知道其 ARN)。您也可以在控制台中完成跟踪的创建，然后使用 AWS CLI 和put-event-selectors命令为特定 Lambda 函数配置数据事件记录。有关更多信息，请参阅使用管理跟踪 AWS CLI。

5. 对于 DynamoDB 表：

   a. 对于 Data event source（数据事件源），选择 DynamoDB。

   b. 在 DynamoDB table selection（DynamoDB 表选择）中，选择 Browse（浏览）以选择一个表，或粘贴到您有权访问的 DynamoDB 表的 ARN 中。DynamoDB 表 ARN 使用以下格式：

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   要添加另一个表，请选择 Add row（添加行），然后浏览到某个表或粘贴到您有权访问的表的 ARN 中。

6. 要为跟踪配置 Insights 事件和其他设置，请返回本主题中前面的程序 ???。

后续步骤

创建您的跟踪后，您可以返回到该跟踪以进行更改：

- 如果还没有，则可以配置为将日志文件发送 CloudTrail 到 Lo CloudWatch gs。有关更多信息，请参阅 将事件发送到 CloudWatch 日志。
- 创建表并将其用于在 Amazon Athena 中运行查询，以便分析 AWS 服务活动。有关更多信息，请参阅 Amazon Athen a 用户 CloudTrail 指南中的在控制台中创建 CloudTrail 日志表。
- 向跟踪添加自定义标签（键-值对）。
- 要创建另一个跟踪，打开跟踪页面并选择创建跟踪。

更新跟踪

本节旨在介绍如何更改跟踪设置。

要更新单区域跟踪以记录您正在工作的AWS 分区 AWS 区域中的所有事件，或者更新多区域跟踪以仅记录单个区域中的事件，则必须使用。 AWS CLI有关如何更新单区域跟踪以记录所有区域中事件的详细信息，请参阅 将应用到一个区域的跟踪转换为应用到所有区域。有关如何更新多区域跟踪以记录单区域中事件的详细信息，请参阅 将多区域跟踪转换为单区域跟踪。

如果您已在 Amazon Security Lake 中启用 CloudTrail 管理事件，则需要至少维护一条多区域组织跟踪，并记录两者`read`以及`write`管理事件。您不能以不符合 Security Lake 要求的方式更新符合条件的跟踪。例如，通过将跟踪更改为单区域，或者关闭 `read` 或 `write` 管理事件的日志记录。

> **Note**
>
> CloudTrail 即使资源验证失败，也会更新成员账户中的组织跟踪。验证失败的示例包括：
>
> - Amazon S3 存储桶策略不正确
> - 不正确的 Amazon SNS 主题政策
> - 无法传送到 CloudWatch 日志组
> - 权限不足，无法使用 KMS 密钥进行加密
>
> 拥有 CloudTrail 权限的成员账户可以通过在 CloudTrail 控制台上查看跟踪的详细信息页面或运行 AWS CLI get-trail-status命令来查看组织跟踪的任何验证失败。

要使用更新跟踪 AWS Management Console

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择跟踪，然后选择跟踪名称。
3. 在 General details（一般详细信息）中，选择 Edit（编辑）以更改以下设置。您无法更改跟踪的名称。

   - 将跟踪应用到我的组织-更改此跟踪是否为 AWS Organizations 组织跟踪。

     > **Note**
     >
     > 只有组织的管理账户才能将组织跟踪转换为非组织跟踪，或者将非组织跟踪转换为组织跟踪。

   - Trail log location（跟踪日志位置）- 更改您要在其中存储此跟踪的日志的 S3 存储桶或前缀的名称。
   - Log file SSE-KMS encryption（日志文件 SSE-KMS 加密）- 选择此选项可启用或禁用通过 SSE-KMS 而非 SSE-S3 加密日志文件的功能。
   - Log file validation（日志文件验证）- 选择此选项可启用或禁用日志文件完整性验证。
   - SNS notification delivery(SNS 通知传输）- 选择此选项可启用或禁用关于日志文件已传输到为跟踪指定的存储桶的 Amazon Simple Notification Service (Amazon SNS) 通知。

   a. 要将跟踪更改为 AWS Organizations 组织跟踪，您可以选择为组织中的所有账户启用跟踪。有关更多信息，请参阅 为组织创建跟踪。

   b. 要更改 Storage location（存储位置）中的指定存储桶，请选择Create new S3 bucket（创建新 S3 存储桶）以创建存储桶。创建存储桶时， CloudTrail 会创建并应用所需的存储桶策略。如果您选择创建新的 S3 存储桶，则您的 IAM 策略需要包含`s3:PutEncryptionConfiguration`操作权限，因为默认情况下，该存储桶已启用服务器端加密。

      > **Note**
      >
      > 如果选择 Use existing S3 bucket（使用现有 S3 存储桶），则在 Trail log bucket name（跟踪日志存储桶名称）中指定一个存储桶，或选择 Browse（浏览）以选择存

储桶。存储桶策略必须授予对其进行写入的 CloudTrail 权限。有关手动编辑存储桶策略的信息，请参阅适用于 Amazon S3 存储桶的政策 CloudTrail。

为了便于查找日志，请在现有存储桶中创建一个新文件夹（也称为前缀）来存储 CloudTrail 日志。在 Prefix（前缀）字段中输入前缀。

c. 对于 Log file SSE-KMS encryption（日志文件 SSE-KMS 加密），如果您希望使用 SSE-KMS 加密而非 SSE-S3 加密对您的日志文件进行加密，请选择 Enabled（已启用）。默认值为 Enabled（已启用）。如果您未启用 SSE-KMS 加密，则将使用 SSE-S3 加密对您的日志进行加密。有关 SSE-KMS 加密的更多信息，请参阅将服务器端加密与 AWS Key Management Service (SSE-KMS) 一起使用。有关 SSE-S3 加密的更多信息，请参阅配合使用服务器端加密与 Amazon S3 托管加密密钥（SSE-S3）。

如果您启用 SSE-KMS 加密，请选择 “新建” 或 “现有”。 AWS KMS key在AWS KMS 别名中，按以下格式指定别名`alias/MyAliasName`。有关更多信息，请参阅 更新资源以使用 KMS 密钥。 CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

> **Note**
>
> 您也可以键入其他账户的密钥 ARN。有关更多信息，请参阅 更新资源以使用 KMS 密钥。密钥策略必须 CloudTrail 允许使用密钥加密您的日志文件，并允许您指定的用户读取未加密形式的日志文件。有关手动编辑密钥政策的信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

d. 对于 Log file validation（日志文件验证），选择 Enabled（已启用）以将日志摘要传输到您的 S3 存储桶。您可以使用摘要文件来验证您的日志文件在 CloudTrail 交付后是否没有更改。有关更多信息，请参阅 验证 CloudTrail 日志文件完整性。

e. 要传送 SNS 通知，请选择 “启用”，以便每次向您的存储桶传送日志时都会收到通知。CloudTrail 在日志文件中存储多个事件。SNS 通知针对每个日志文件而不是每个事件发送。有关更多信息，请参阅 配置 Amazon SNS 通知 CloudTrail。

如果您启用了 SNS 通知，则对于 Create a new SNS topic（创建新 SNS 主题），选择 New（新建）创建主题，或选择 Existing（现有）使用现有的主题。如果您创建的是应用到所有区域的跟踪，则针对来自所有区域的日志文件传输的 SNS 通知将发送到您创建的单个 SNS 主题中。

如果选择 “新建”，则会为您 CloudTrail 指定新主题的名称，也可以键入名称。如果选择 Existing（现有），则从下拉列表中选择一个 SNS 主题。您还可以输入来自另一个区域或来自一个具有适当权限的账户的主题的 ARN。有关更多信息，请参阅 Amazon SNS 主题政策 CloudTrail。

如果您创建一个主题，则必须订阅该主题以便获取日志文件传送的通知。您可通过 Amazon SNS 控制台进行订阅。由于通知的频率，建议您将该订阅配置为使用 Amazon SQS 队列来以编程方式处理通知。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。

4. 在CloudWatch 日志中，选择编辑以更改将 CloudTrail 日志文件发送到 CloudWatch 日志的设置。选择 “在CloudWatch 日志中启用” 以启用发送日志文件。有关更多信息，请参阅 将事件发送到 CloudWatch 日志。

   a. 如果您启用了与 CloudWatch 日志的集成，请选择 “新建” 来创建新的日志组，或者选择 “现有” 以使用现有的日志组。如果选择 “新建”，则会为您 CloudTrail 指定新日志组的名称，也可以键入名称。

   b. 如果选择 Existing（现有），则从下拉列表中选择一个日志组。

   c. 选择 “新建” 创建新的 IAM 角色，以获得向日志发送 CloudWatch 日志的权限。选择 Existing（现有）以从下拉列表中选择一个现有 IAM 角色。展开 Policy document（策略文档）时，将显示新角色或现有角色的策略语句。有关该角色的更多信息，请参阅 使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档。

   > **Note**
   >
   > - 在您配置跟踪时，可以选择属于另一个账户的 S3 存储桶和 SNS 主题。但是，如果 CloudTrail 要将事件传送到 CloudWatch 日志日志组，则必须选择当前账户中存在的日志组。
   > - 只有管理账户才能使用控制台为组织跟踪配置 CloudWatch 日志组。授权的管理员可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 操作配置 CloudWatch 日志组。

5. 在 Tags（标记）中，选择 Edit（编辑）以更改、添加或删除跟踪上的标签。将一个或多个自定义标签（键值对）添加到跟踪中。标签可以帮助您识别您的 CloudTrail 跟踪和包含 CloudTrail 日志文件的 Amazon S3 存储桶。然后，您可以将资源组用于您的 CloudTrail 资源。有关更多信息，请参阅 AWS Resource Groups 和 标签。

6. 在 Management events（管理事件）中，选择 Edit（编辑）以更改管理事件日志记录设置。

   a. 对于 API activity（API 活动），选择您希望跟踪记录 Read（读取）事件、Write（写入）事件，还是记录两者。有关更多信息，请参阅 管理事件。

   b. 选择 “排除 AWS KMS 事件”，从您的跟踪中筛选 AWS Key Management Service (AWS KMS) 事件。默认设置是包含所有 AWS KMS 事件。

      只有在跟踪中记录管理 AWS KMS 事件时，才可使用记录或排除事件的选项。如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件日志记录设置。

      AWS KMS 诸如`Encrypt`、`Decrypt`和之类的操作`GenerateDataKey`通常会生成大量事件（超过 99%）。这些操作现在记录为读取事件。诸如`DisableDelete`、和`ScheduleKey`（通常占事件量不到 0.5%）之类的低容量相关 AWS KMS 操作被记录为写入 AWS KMS 事件。

      如果要排除大批量事件（例如 `Encrypt`、`Decrypt` 和 `GenerateDataKey`），但仍然记录相关事件（例如 `Disable`、`Delete` 和 `ScheduleKey`），选择记录 Write（写入）管理事件，然后清除 Exclude AWS KMS events（排除 Amazon KMS 事件）复选框。

   c. 选择 Exclude Amazon RDS Data API events（排除 Amazon RDS 数据 API 事件以从跟踪中筛选出 Amazon Relational Database Service 数据 API 事件。默认设置是包含所有 Amazon RDS 数据 API 事件。有关 Amazon RDS 数据 API 事件的更多信息，请参阅 Amazon RDS Aurora 用户指南中的使用 AWS CloudTrail记录数据 API 调用。

7.

   Important

   使用高级事件选择器配置数据事件会用到步骤 7-11。高级事件选择器让您可以配置更多数据事件类型，并对跟踪捕获的数据事件进行精细控制。如果您使用的是基本事件选择器，请参阅 使用基本事件选择器更新数据事件设置，然后返回此过程的步骤 12。

   在 Data events（数据事件）中，选择 Edit（编辑）以更改数据事件日志记录设置。默认情况下，跟踪记录不记录数据事件。记录数据事件将收取额外费用。有关 CloudTrail 定价，请参阅 AWS CloudTrail 定价。

   对于 Data event type（数据事件类型），选择要在其上记录数据事件的资源类型。有关可用数据事件类型的更多信息，请参阅 数据事件。

> **Note**
>
> 要记录由 Lake Formati AWS Glue on 创建的表的数据事件，请选择 La ke Formation。

8. 选择日志选择器模板。 CloudTrail 包括用于记录该资源类型的所有数据事件的预定义模板。要构建自定义日志选择器模板，请选择 Custom（自定义）。

> **Note**
>
> 为 S3 存储桶选择预定义的模板可以记录当前您 AWS 账户中的所有存储分段以及您在创建完跟踪后创建的任何存储分段的数据事件。它还允许记录您 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于其他 AWS 账户的存储桶上执行的。
> 如果跟踪仅应用于一个区域，则选择记录所有 S3 存储桶的预定义模板可为跟踪所在的区域中的所有存储桶和您后来在该区域中创建的任何存储桶启用数据事件日志记录。不会为您的 AWS 账户的其他区域中的 Simple Storage Service（Amazon S3）存储桶记录数据事件。
> 如果您要为所有区域创建跟踪，则选择 Lambda 函数的预定义模板可以记录当前 AWS 账户中的所有函数以及您在完成跟踪创建后可能在任何区域创建的任何 Lambda 函数的数据事件。如果您要为单个区域创建跟踪（使用完成 AWS CLI），则此选择将启用您 AWS 账户中该区域中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
> 记录所有功能的数据事件还允许记录 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

9. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。

10. 在 Advanced event selectors（高级事件选择器）中，为您要收集其数据事件的特定资源构建表达式。如果您使用的是预定义日志模板，则可跳过此步骤。

    a. 从下面的字段中选择。

    - **readOnly**-readOnly 可以设置为等于true或false的值。要记录 read 和 write 两种事件，请不要添加 readOnly 选择器。
    - **eventName** - eventName 可以使用任何运算符。您可以使用它来包含或排除记录到的任何数据事件 CloudTrail，例如PutBucket或GetSnapshotBlock。

- **resources.ARN**-您可以将任何运算符与一起使用resources.ARN，但是如果您使用等于或不等于，则该值必须与您在模板中指定为的值的有效资源的 ARN 完全匹配。resources.type

  下表显示每个 resources.type 的有效 ARN 格式。

  > **Note**
  >
  > 您不能使用该resources.ARN字段筛选没有 ARN 的资源类型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*

resources.type	resources.ARN
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*

resources.type	resources.ARN
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*

resources.type	resources.ARN
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*

resources.type	resources.ARN
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*

resources.type	resources.ARN
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*

resources.type	resources.ARN
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必须采用以下格式之一： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*

resources.type	resources.ARN
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必须采用以下格式之一： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	resources.ARN
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 对于启用了流的表，数据事件中的 resources 字段同时包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您为 resources.type 指定 AWS::DynamoDB::Table，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName在该字段上添加过滤器。

[2] 要记录特定 S3 存储桶中所有对象的所有数据事件，请使用 StartsWith 运算符，并且仅包含存储桶 ARN 作为匹配值。刻意使用尾部斜杠；切勿排除它。

[3] 要记录 S3 接入点中的所有对象的事件，建议您仅使用接入点 ARN，而不要包含对象路径，并且使用 StartsWith 或 NotStartsWith 运算符。

有关数据事件资源的 ARN 格式的更多信息，请参阅 AWS Identity and Access Management 用户指南中的操作、资源和条件键。

b. 对于每个字段，请选择 + 条件以根据需要添加任意数量的条件，所有条件总共可有最多 500 个指定值。例如，要从跟踪中记录的数据事件中排除两个 S3 存储桶的数据事件，您可以将该字段设置为 Resou rces.arn，将运算符设置为 “不以开头”，然后粘贴到 S3 存储桶 ARN 中，或者浏览您不想为其记录事件的 S3 存储桶。

要添加第二个 S3 存储桶，请选择 + 条件，然后重复上述说明，在 ARN 中粘贴或浏览到不同的存储桶。

> **Note**
>
> 对于跟踪上的所有选择器，最多可以有 500 个值。这包括选择器的多个值的数组，例如 eventName。如果所有选择器均为单个值，则最多可以向选择器添加 500 个条件。
> 如果您的账户中有超过 15,000 个 Lambda 函数，则在创建跟踪时无法在 CloudTrail 控制台中查看或选择所有函数。您仍可使用预定义选择器模板记录所有函数，即使这些函数未显示出来也是如此。如果您要记录特定函数的数据事件，则可手动添加一个函数 (如果您知道其 ARN)。您也可以在控制台中完成跟踪的创建，然后使用 AWS

CLI 和put-event-selectors命令为特定 Lambda 函数配置数据事件记录。有关更多信息，请参阅 使用管理跟踪 AWS CLI。

c. 根据需要，选择 + Field（+ 字段）以添加其他字段。为了避免错误，请不要为字段设置冲突或重复的值。例如，不要在一个选择器中将 ARN 指定为等于某个值，然后在另一个选择器中指定 ARN 不等于相同的值。

11. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。重复步骤 3 至此步骤，为数据事件类型配置高级事件选择器。
12. 如果您希望跟踪记录见解事件，请在 CloudTrail Insights 事件中选择编辑。

    在 Event type（事件类型）中，选择 Insights events（Insights 事件）。

    在 Insights events（Insights 事件）中，选择 API call rate（API 调用率）和/或 API error rate（API 错误率）。您必须记录写入管理事件，以针对 API 调用率记录 Insights 事件。您必须记录读取或写入管理事件，以针对 API 错误率记录 Insights 事件。

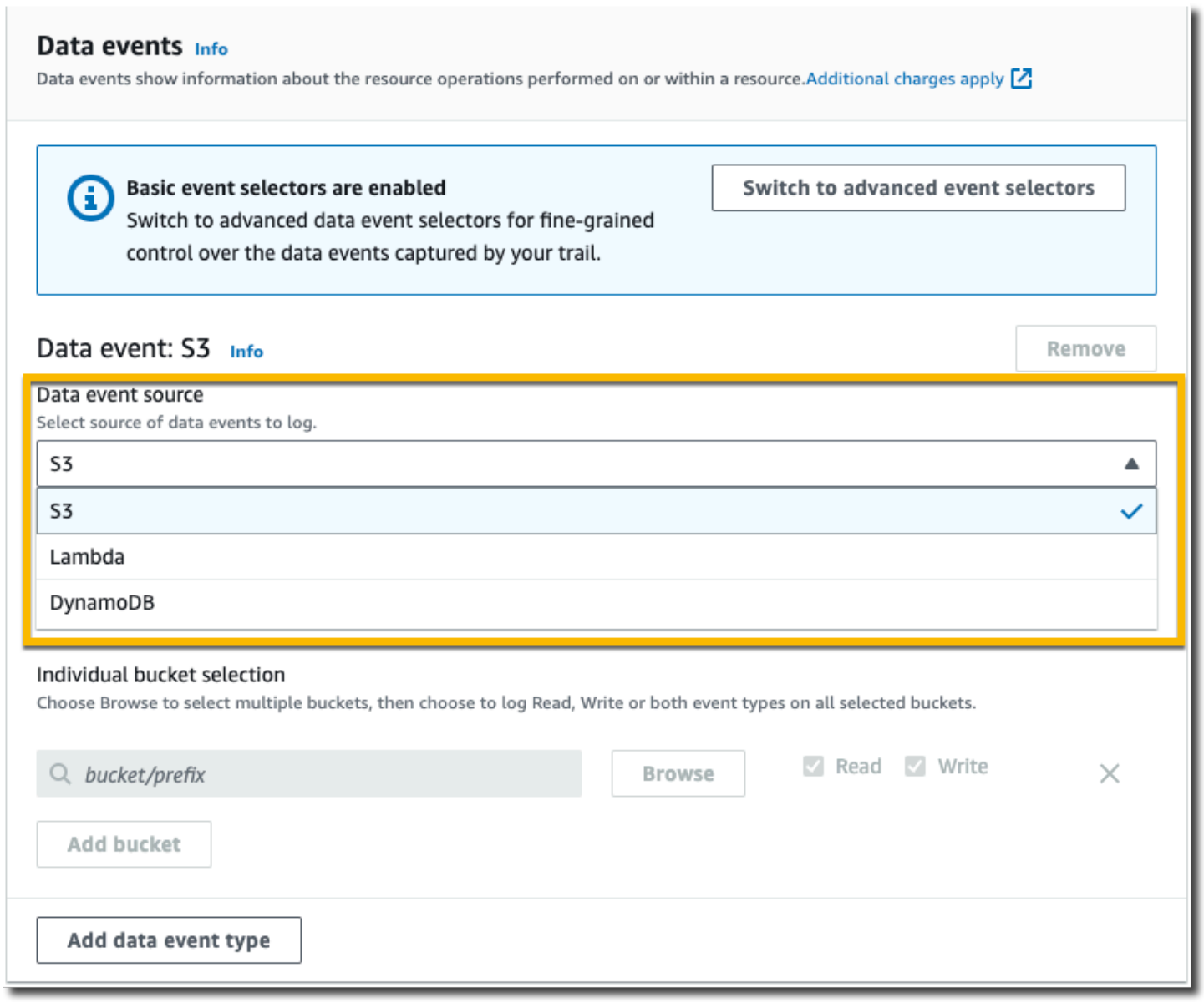
    CloudTrail Insights 会分析管理事件中是否存在异常活动，并在检测到异常时记录事件。默认情况下，跟踪记录不记录 Insights 事件。有关 Insights 事件的更多信息，请参阅记录 Insights 事件。记录 Insights 事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

    Insights 事件将传送到另一个文件夹，该文件夹以同一 S3 存储桶命名/CloudTrail-Insight，该存储桶在跟踪详细信息页面的存储位置区域中指定。 CloudTrail为您创建新的前缀。例如，如果当前目标 S3 存储桶命名为 S3bucketName/AWSLogs/CloudTrail/，则带有新前缀的 S3 存储桶名称会命名为 S3bucketName/AWSLogs/CloudTrail-Insight/。
13. 当您更改完跟踪上的设置后，选择 Update trail（更新跟踪）。

使用基本事件选择器更新数据事件设置

您可以使用高级事件选择器来配置所有数据事件类型。高级事件选择器允许您创建细粒度的选择器，以仅记录那些感兴趣的事件。

如果您使用基本事件选择器来记录数据事件，则只能记录 Amazon S3 存储桶、 AWS Lambda 函数和 Amazon DynamoDB 表的数据事件。您无法使用基本的事件选择器对eventName字段进行筛选。



按照以下程序使用基本事件选择器配置数据事件设置。

1. 在 Data events（数据事件）中，选择 Edit（编辑）以更改数据事件日志记录设置。使用基本事件选择器，您可以为 Amazon S3 存储桶、 AWS Lambda 函数、DynamoDbtables 或这些资源的组合指定日志数据事件。其他数据事件类型可通过高级事件选择器获得支持。默认情况下，跟踪记录不记录数据事件。记录数据事件将收取额外费用。有关更多信息，请参阅 数据事件。有关 CloudTrail 定价，请参阅 AWS CloudTrail 定价。

   对于 Simple Storage Service（Amazon S3）存储桶：

   a. 对于 Data event source（数据事件源），选择 S3。

b. 您可以选择记录 All current and future S3 buckets（所有当前和未来 S3 存储桶），也可以指定单个存储桶或函数。默认情况下，记录所有当前和未来 S3 存储桶的数据事件。

> **Note**
>
> 保留默认 “All current and future S3 存储桶” 选项将允许您 AWS 账户中当前的所有存储分段以及您在完成跟踪创建后创建的任何存储分段的数据事件记录。它还允许记录您 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于其他 AWS 账户的存储桶上执行的。
> 如果跟踪仅应用于一个区域，则选择 All current and future S3 buckets（所有当前和未来 S3 存储桶）可为跟踪所在的区域中的所有存储桶和您后来在该区域中创建的任何存储桶启用数据事件日志记录。它不会在您的 AWS 账户中记录其他区域的 Amazon S3 存储桶的数据事件。

c. 如果保留默认值 All current and future S3 buckets（所有当前和未来 S3 存储桶），则选择记录 Read（读取）事件、Write（写入）事件，还是记录两者。

d. 要选择单个存储桶，请清空 All current and future S3 buckets（所有当前和未来 S3 存储桶）的 Read（读取）和Write（写入）复选框。在 Individual bucket selection（单个存储桶选择）中，浏览要在其上记录数据事件的存储桶。要查找特定存储桶，键入所需存储桶的存储桶前缀。您可以在此窗口中选择多个存储桶。选择添加存储桶，记录更多存储桶的数据事件。选择记录 Read（读取）事件（如 `GetObject`）、Write（写入）事件（如 `PutObject`）或同时记录两种事件。

   此设置优先于为各个存储桶配置的个别设置。例如，如果指定记录所有 S3 存储桶的 Read 事件，然后选择为数据事件日志记录添加一个特定存储桶，则所添加存储桶的 Read 已经是选中状态。您无法清除此选择。只能配置 Write 选项。

   要从日志记录中删除存储桶，请选择 X。

2. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。

3. 对于 Lambda 函数：

   a. 对于 Data event source（数据事件源），选择 Lambda。

   b. 在 Lambda function（Lambda 函数）中，选择 All regions（所有区域）记录所有 Lambda 函数，或选择 Input function as ARN（输入函数作为 ARN）以记录特定函数上的数据事件。

      要记录您 AWS 账户中所有 Lambda 函数的数据事件，请选择记录所有当前和将来的函数。此设置优先于为各个函数配置的个别设置。将记录所有函数，即便这些函数未显示。

> **Note**
>
> 如果您要为所有区域创建跟踪，则此选择将启用您 AWS 账户中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在任何区域创建的任何 Lambda 函数的数据事件记录。如果您要为单个区域创建跟踪（使用完成 AWS CLI），则此选择将启用您 AWS 账户中该区域中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
> 记录所有功能的数据事件还允许记录 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

c. 如果选择 Input function as ARN（输入函数作为 ARN），则输入 Lambda 函数的 ARN。

> **Note**
>
> 如果您的账户中有超过 15,000 个 Lambda 函数，则在创建跟踪时无法在 CloudTrail 控制台中查看或选择所有函数。您仍可以选择该选项来记录所有函数，即使未显示这些函数也是如此。如果您要记录特定函数的数据事件，则可手动添加一个函数 (如果您知道其 ARN)。您也可以在控制台中完成跟踪的创建操作，然后使用 AWS CLI 和 put-event-selectors 命令为特定 Lambda 函数配置数据事件日志记录。有关更多信息，请参阅 使用管理跟踪 AWS CLI。

4. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。
5. 对于 DynamoDB 表：
   a. 对于 Data event source（数据事件源），选择 DynamoDB。
   b. 在 DynamoDB table selection（DynamoDB 表选择）中，选择 Browse（浏览）以选择一个表，或粘贴到您有权访问的 DynamoDB 表的 ARN 中。DynamoDB 表 ARN 采用以下格式：

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   要添加另一个表，请选择 Add row（添加行），然后浏览到某个表或粘贴到您有权访问的表的 ARN 中。
6. 要为跟踪配置 Insights 事件和其他设置，请返回本主题中前面的程序 更新跟踪。

删除跟踪

您可以使用 CloudTrail 控制台删除跟踪。如果组织的管理账户或委托管理员账户删除了组织跟踪，则该跟踪将从该组织的所有成员账户中移除。

如果您已在 Amazon Security Lake 中启用 CloudTrail 管理事件，则需要至少维护一条多区域组织跟踪，并记录两者`read`以及`write`管理事件。如果跟踪是您拥有的唯一符合此要求的跟踪，则无法将其删除，除非您在 Security Lake 中关闭 CloudTrail 管理事件。

使用 CloudTrail 控制台删除跟踪

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 打开 CloudTrail 控制台的 T rail s 页面。
3. 选择跟踪名称。
4. 在跟踪详细信息页面顶部，选择 Delete（删除）。
5. 在提示您确认时，选择 Delete（删除）以永久删除该跟踪。从跟踪记录列表中删除该跟踪记录。已经传递至 Simple Storage Service（Amazon S3）存储桶的日志文件不会被删除。

> **Note**
>
> 发送到 Simple Storage Service（Amazon S3）存储桶的内容可能包含客户内容。有关删除敏感数据的更多信息，请参阅 Amazon S3 用户指南中的清空存储桶和删除存储桶。

关闭跟踪的日志记录

创建跟踪时，系统会自动启用日志记录。您可以关闭跟踪的日志记录。

关闭日志记录功能后，现有日志仍存储在跟踪的 Amazon S3 存储桶中，并会继续产生 S3 费用。

使用 CloudTrail 控制台关闭跟踪日志记录

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择 Trails（跟踪记录），然后选择跟踪记录的名称。
3. 在跟踪详细信息页面顶部，选择 Stop logging（停止日志记录）以关闭该跟踪的日志记录。
4. 当系统提示您确认时，选择停止记录。 CloudTrail停止记录该跟踪的活动。

5. 要恢复该跟踪的日志记录，在跟踪配置页面上选择 Start logging（开始日志记录）。

使用创建、更新和管理跟踪 AWS CLI

您可以使用 AWS CLI 来创建、更新和管理您的跟踪。使用时 AWS CLI，请记住您的命令在为您的个人资料配置的 AWS 区域中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

> **Note**
>
> 您需要 AWS 命令行工具才能运行本主题中的 AWS Command Line Interface (AWS CLI) 命令。确保您 AWS CLI 安装的是最新版本的。有关更多信息，请参阅《AWS Command Line Interface 用户指南》。要获取命令行 CloudTrail AWS CLI 命令的帮助，请键入`aws cloudtrail help`。

常用的跟踪创建、管理和状态命令

中用于创建和更新跟踪的一些比较常用的命令 CloudTrail 包括：

- create-trail：创建跟踪。
- update-trail：更改现有跟踪的配置。
- add-tags：向现有跟踪添加一个或多个标签（键值对）。
- remove-tags：从跟踪中删除一个或多个标签。
- list-tags：返回与跟踪关联的标签的列表。
- put-event-selectors：添加或修改跟踪的时间选择器。
- put-insight-selectors：为现有跟踪添加或修改见解事件选择器，并启用或禁用 Insights 事件。
- start-logging：开始使用跟踪记录事件。
- stop-logging：停止使用跟踪记录事件。
- delete-trail：删除跟踪。该命令不会删除含有该跟踪的日志文件的 Simple Storage Service（Amazon S3）存储桶（如果有）。
- describe-trails返回有关某个 AWS 区域中路径的信息。
- get-trail：返回跟踪的设置信息。
- get-trail-status：返回有关跟踪的当前状态的信息。

- get-event-selectors：返回有关为跟踪配置的事件选择器的信息。
- get-insight-selectors：返回有关为跟踪配置的 Insights 事件选择器的信息。

支持的创建和更新跟踪记录的命令：create-trail 和 update-trail

`create-trail` 和 `update-trail` 命令提供用于创建和管理跟踪记录的各种功能，包括：

- 创建跨区域接收日志的跟踪，或使用 `--is-multi-region-trail` 选项更新跟踪。在大多数情况下，您应该创建记录所有 AWS 区域事件的跟踪。
- 使用--is-organization-trail选项创建用于接收组织中所有 AWS 账户日志的跟踪。
- 使用 `--no-is-multi-region-trail` 选项将多区域跟踪转换为单区域跟踪。
- 使用 `--kms-key-id` 选项启用或禁用日志文件加密。该选项指定了您已经创建的 AWS KMS 密钥，并且您已将允许加密日志的策略附加 CloudTrail 到该密钥。有关更多信息，请参阅 使用启用和禁用 CloudTrail 日志文件加密 AWS CLI。
- 使用 `--enable-log-file-validation` 和 `--no-enable-log-file-validation` 选项启用或禁用日志文件验证。有关更多信息，请参阅 验证 CloudTrail 日志文件完整性。
- 指定 CloudWatch 日志组和角色，以便 CloudTrail 可以将事件传送到 CloudWatch 日志日志组。有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

已弃用的命令：create-subscription 和 update-subscription

> **Important**
>
> `create-subscription` 和 `update-subscription` 命令曾用来创建和更新跟踪记录，但已弃用。请勿使用这些命令。它们不提供用于创建和管理跟踪记录的完整功能。
> 如果您配置了使用其中一个命令或同时使用这两个命令的自动执行，我们建议您更新您的代码或脚本以使用支持的命令，例如 create-trail。

使用 create-trail

您可以运行 `create-trail` 命令来创建专门配置为满足您的商业需求的跟踪记录。使用时 AWS CLI，请记住您的命令在为您的个人资料配置的 AWS 区域中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

创建应用到所有区域的跟踪

要创建应用到所有区域的跟踪，请使用 `--is-multi-region-trail` 选项。默认情况下，`create-trail` 命令创建的跟踪仅记录在其中创建该跟踪的 AWS 区域中的事件。为确保记录全球服务事件并捕获 AWS 账户中的所有管理事件活动，您应创建记录所有 AWS 区域事件的跟踪。

> **Note**
>
> 创建跟踪时，如果您指定的 Amazon S3 存储桶不是用创建的 CloudTrail，则需要附加相应的策略。请参阅 适用于 Amazon S3 存储桶的政策 CloudTrail。

以下示例创建一个名为 *my-trail* 的跟踪和一个名为 *Group* 且值为 *Marketing* 的标签，此标签将来自所有区域的日志传送到名为 *my-bucket* 的现有存储桶。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --tags-list [key=Group,value=Marketing]
```

要确认您的跟踪存在于所有区域中，请验证输出中的 `IsMultiRegionTrail` 元素是否为 `true`。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 使用 `start-logging` 命令可以为您的跟踪启动日志记录操作。

为跟踪启动日志记录操作

在 `create-trail` 命令完成后，运行 `start-logging` 命令可以为跟踪启动日志记录。

> **Note**
>
> 使用 CloudTrail 控制台创建跟踪时，日志记录会自动开启。

以下示例为跟踪启动日志记录。

```
aws cloudtrail start-logging --name my-trail
```

虽然此命令不返回输出，但您可以使用 `get-trail-status` 命令验证日志记录是否已启动。

```
aws cloudtrail get-trail-status --name my-trail
```

为了确认正在记录跟踪，输出中的 `IsLogging` 元素将显示 `true`。

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

创建单区域跟踪

以下命令创建单区域跟踪。指定的 Amazon S3 存储桶必须已经存在并且已应用相应的 CloudTrail 权限。有关更多信息，请参阅 适用于 Amazon S3 存储桶的政策 CloudTrail。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

有关更多信息，请参阅 命名要求。

下面是示例输出。

```
{
    "IncludeGlobalServiceEvents": true,
```

```
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

创建应用到所有区域且启用了日志文件验证功能的跟踪

要在使用 `create-trail` 时启用日志文件验证功能，请使用 `--enable-log-file-validation` 选项。

有关日志文件验证的信息，请参阅[验证 CloudTrail 日志文件完整性]。

以下示例创建将所有区域的日志传送到指定存储桶的跟踪。此命令使用 `--enable-log-file-validation` 选项。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --enable-log-file-validation
```

要确认系统已启用日志文件验证功能，请验证输出中的 `LogFileValidationEnabled` 元素是否为 `true`。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

使用 update-trail

> **Important**
>
> 自 2021 年 11 月 22 日起， AWS CloudTrail 更改了跟踪捕获全球服务事件的方式。现在，事件由 Amazon 创建 CloudFront AWS Identity and Access Management，并 AWS STS 记录在创建这些事件的区域，即美国东部（弗吉尼亚北部）区域 us-east-1。这使得如何 CloudTrail

对待这些服务与其他 AWS 全球服务保持一致。要继续接收美国东部（弗吉尼亚州北部）以外的全球服务事件，请务必将使用美国东部（弗吉尼亚州北部）以外全球服务事件的单区域跟踪转换为多区域跟踪。如需有关捕获全球服务事件的更多信息，请参阅本章节后面部分的启用和禁用全球服务事件记录。
相比之下， CloudTrail 控制台中的事件历史记录和aws cloudtrail lookup-events命令将显示这些事件的发生 AWS 区域 地点。

您可以使用 `update-trail` 命令更改跟踪的配置设置。您还可以使用 add-tags 和 remove-tags 命令以添加和删除跟踪的标签。您只能从创建跟踪的 AWS 区域（其主区域）更新跟踪。使用时 AWS CLI，请记住您的命令在为您的个人资料配置的 AWS 区域中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

如果您已在 Amazon Security Lake 中启用 CloudTrail 管理事件，则需要至少维护一条多区域组织跟踪，并记录两者`read`以及`write`管理事件。您不能以不符合 Security Lake 要求的方式更新符合条件的跟踪。例如，通过将跟踪更改为单区域，或者关闭 `read` 或 `write` 管理事件的日志记录。

> **Note**
>
> 如果您使用 AWS CLI 或其中一个 AWS 软件开发工具包来修改跟踪，请确保跟踪的存储桶策略是 up-to-date。为了让您的存储桶自动接收来自新存储桶的事件 AWS 区域，策略必须包含完整的服务名称`cloudtrail.amazonaws.com`。有关更多信息，请参阅 适用于 Amazon S3 存储桶的政策 CloudTrail。

主题

- 将应用到一个区域的跟踪转换为应用到所有区域
- 将多区域跟踪转换为单区域跟踪
- 启用和禁用全球服务事件记录
- 启用日志文件验证
- 禁用日志文件验证

将应用到一个区域的跟踪转换为应用到所有区域

要更改现有跟踪以使其应用到所有区域，请使用 `--is-multi-region-trail` 选项。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

要确认跟踪现已应用到所有区域，请验证输出中的 IsMultiRegionTrail 元素是否为 true。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

将多区域跟踪转换为单区域跟踪

要更改现有的多区域跟踪以使其只应用于创建该跟踪的区域，请使用 --no-is-multi-region-trail 选项。

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

要确认跟踪现在只应用到一个区域，请验证输出中的 IsMultiRegionTrail 元素是否为 false。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

启用和禁用全球服务事件记录

要更改跟踪以使其不记录全球服务事件，请使用 --no-include-global-service-events 选项。

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

要确认跟踪不再记录全局服务事件，输出中的 IncludeGlobalServiceEvents 元素应显示 false。

```
{
```

```
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

要更改跟踪以使其记录全球服务事件，请使用 `--include-global-service-events` 选项。

自 2021 年 11 月 22 日起，单区域跟踪将不再接收全球服务事件，除非该跟踪已出现在美国东部（弗吉尼亚州北部）区域 us-east-1。要继续捕获全球服务事件，请将跟踪配置更新为多区域跟踪。例如，此命令将美国东部（俄亥俄州）us-east-2 中的单区域跟踪更新为多区域跟踪。将 *myExistingSingleRegionTrailWithGSE* 替换为适合您配置的相应跟踪名称。

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

由于从 2021 年 11 月 22 日起，仅在美国东部（弗吉尼亚州北部）提供全球服务事件，您还可以创建单一区域跟踪以订阅美国东部（弗吉尼亚州北部）区域 us-east-1 的全球服务事件。以下命令在 us-east-1 中创建用于接收、IAM 和事件的单区域跟踪： CloudFront AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

启用日志文件验证

要启用对跟踪的日志文件验证，可使用 `--enable-log-file-validation` 选项。摘要文件将传送到该跟踪的 Simple Storage Service（Amazon S3）存储桶。

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

要确认系统已启用日志文件验证功能，请验证输出中的 `LogFileValidationEnabled` 元素是否为 `true`。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
```

```
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

禁用日志文件验证

要禁用对跟踪的日志文件验证，请使用 --no-enable-log-file-validation 选项。

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

要确认系统已禁用日志文件验证功能，请验证输出中的 LogFileValidationEnabled 元素是否为 false。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

要使用验证日志文件 AWS CLI，请参阅 CloudTrail 使用验证日志文件的完整性 AWS CLI。

使用管理跟踪 AWS CLI

AWS CLI 包括其他几个可帮助您管理路径的命令。这些命令将标签添加到跟踪记录、获取跟踪记录状态、对跟踪记录启动和停止日志记录以及删除跟踪记录。您必须从创建跟踪的同一 AWS 区域（其主区域）运行这些命令。使用时 AWS CLI，请记住您的命令在为您的个人资料配置的 AWS 区域中运行。如果您想要在不同的区域中运行命令，可以为配置文件更改默认区域，或者与命令一起使用 --region 参数。

主题

- 将一个或多个标签添加到跟踪
- 列出一个或多个跟踪记录的标签
- 从跟踪中删除一个或多个标签
- 检索跟踪设置和跟踪状态
- 配置 CloudTrail Insights 事件选择器

- 配置事件选择器
- 配置高级事件选择器
- 停止和启动跟踪的日志记录
- 删除跟踪

将一个或多个标签添加到跟踪

要将一个或多个标签添加到现有跟踪，请运行 add-tags 命令。

以下示例向美国东部（俄亥俄）区域中 ARN 为 *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* 的跟踪记录添加了一个名为 *Owner*、值为 *Mary* 的标签。

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

如果成功，该命令不返回任何内容。

列出一个或多个跟踪记录的标签

要查看与一个或多个现有跟踪记录相关联的标签，请使用 list-tags 命令。

以下示例列出了 *Trail1* 和 *Trail2* 的标签。

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

如果成功，该命令返回类似以下内容的输出。

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "Name"
             },
             {
                 "Value": "Ohio",
                 "Key": "Location"
```

```
            }
        ]
    },
    {
        "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
        "TagsList": [
            {
                "Value": "Bob",
                "Key": "Name"
            }
        ]
    }
  ]
}
```

从跟踪中删除一个或多个标签

要从现有跟踪中删除一个或多个标签，请运行 remove-tags 命令。

以下示例从美国东部（俄亥俄）区域中 ARN 为 *arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1* 的跟踪记录删除了名为 *Location* 和 *Name* 的标签。

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

如果成功，该命令不返回任何内容。

检索跟踪设置和跟踪状态

运行describe-trails命令以检索有关 AWS 区域中跟踪的信息。以下示例返回美国东部（俄亥俄）区域中配置的跟踪记录的信息。

```
aws cloudtrail describe-trails --region us-east-2
```

如果命令成功，则将显示类似于以下内容的输出。

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
```

```
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
    }
  ]
}
```

运行 get-trail 命令检索特定跟踪的设置信息。以下示例返回名为 *my-trail* 的跟踪的设置信息。

```
aws cloudtrail get-trail - -name my-trail
```

如果成功，该命令返回类似以下内容的输出。

```
{
```

```
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

运行 `get-trail-status` 命令检索跟踪的状态。您必须从创建该命令的 AWS 区域（主区域）运行此命令，或者必须通过添加--region参数来指定该区域。

> **Note**
>
> 如果跟踪是组织跟踪，并且您是组织中的成员账户 AWS Organizations，则必须提供该跟踪的完整 ARN，而不仅仅是名称。

```
aws cloudtrail get-trail-status --name my-trail
```

如果命令成功，则将显示类似于以下内容的输出。

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

除了前面的 JSON 代码中显示的字段外，在出现 Amazon SNS 或 Simple Storage Service（Amazon S3）错误的情况下，状态还包含以下字段：

- `LatestNotificationError`. 在主题订阅失败的情况下，包含 Amazon SNS 发出的错误。
- `LatestDeliveryError`。 包含 Amazon S3 在 CloudTrail 无法将日志文件传送到存储桶时发出的错误。

配置 CloudTrail Insights 事件选择器

通过运行 put-insight-selectors 并指定 `ApiCallRateInsight` 和/或 `ApiErrorRateInsight` 作为 `InsightType` 属性的值，对跟踪记录启用 Insights 事件。要查看跟踪的 Insights 事件选择器设置，请运行 `get-insight-selectors` 命令。您必须从创建跟踪的 AWS 区域（主区域）运行此命令，或者必须通过在命令中添加--region参数来指定该区域。

> **Note**
>
> 要记录 `ApiCallRateInsight` 的 Insights 事件，跟踪必须记录 `write` 管理事件。要记录 `ApiErrorRateInsight` 的 Insights 事件，跟踪必须记录 `read` 或 `write` 管理事件。

记录 Insights 事件的示例跟踪

以下示例用于put-insight-selectors为名为 *`TrailName3`* 的跟踪创建 Insights 事件选择器。这将启用 *`TrailName3`* 个跟踪的 Insights 事件收集。Insights 事件选择器会同时记录 `ApiErrorRateInsight` 和 `ApiCallRateInsight` Insights 事件类型。

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

该示例返回为跟踪配置的 Insights 事件选择器。

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
```

```
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

示例：关闭 Insights 事件集合

以下示例用于put-insight-selectors移除名为 *TrailName3* 的跟踪的 Insights 事件选择器。清除 Insights 选择器的 JSON 字符串会禁用 *TrailName3* 个跟踪的 Insights 事件收集。

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

该示例返回为跟踪配置的现在为空的 Insights 事件选择器。

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

配置事件选择器

要查看跟踪的事件选择器设置，请运行 `get-event-selectors` 命令。您必须从创建该命令的 AWS 区域（主区域）运行此命令，或者必须使用--region参数指定该区域。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 如果跟踪是组织跟踪，并且您是组织中的成员账户 AWS Organizations，则必须提供该跟踪的完整 ARN，而不仅仅是名称。

以下示例返回跟踪的事件选择器的默认设置。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
```

```
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要创建事件选择器，请运行 `put-event-selectors` 命令。如果您想在跟踪上记录 Insights 事件，请确保事件选择器为您要用于配置跟踪的 Insights 类型启用日志记录。有关记录 Insights 事件的更多信息，请参阅 记录 Insights 事件。

当您的账户中发生事件时， CloudTrail 会评估您的跟踪配置。如果事件匹配跟踪的任何事件选择器，则跟踪将处理并记录事件。您可以为一个跟踪配置最多 5 个事件选择器和最多 250 个数据资源。有关更多信息，请参阅 记录数据事件。

主题

- 带有特定事件选择器的示例跟踪
- 记录所有管理和数据事件的示例跟踪
- 不记录 AWS Key Management Service 事件的示例跟踪
- 记录相关低容量 AWS Key Management Service 事件的示例跟踪
- 不记录 Amazon RDS 数据 API 事件的示例跟踪

带有特定事件选择器的示例跟踪

以下示例为名为的跟踪创建事件选择器，*TrailName*以包括只读和只写管理事件、两个 Amazon S3 存储桶/前缀组合的数据事件以及名为的单个函数的数据事件。 AWS Lambda *hello-world-python-function*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix","arn:aws:s3:::mybucket2/prefix2"]},{"Type": "AWS::Lambda::Function","Values":
 ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]}]}]'
```

以下示例返回为跟踪配置的事件选择器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
```

```
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

记录所有管理和数据事件的示例跟踪

以下示例为名为 *TrailName2* 的跟踪创建了一个事件选择器，其中包括所有事件，包括只读和只写管理事件，以及账户中所有 Amazon S3 存储桶、 AWS Lambda 函数和 Amazon DynamoDB 表的所有数据事件。 AWS 由于此示例使用基本事件选择器，因此它无法为开启的 S3 事件、以太坊节点上 AWS Outposts的 Amazon Managed Blockchain JSON-RPC 调用或其他高级事件选择器资源类型配置日志记录。您必须使用高级事件选择器来记录这些资源的数据事件。有关更多信息，请参阅 [配置高级事件选择器](#)。

> **Note**
>
> 如果跟踪仅应用于一个区域，则只记录该区域的事件，即使事件选择器参数指定所有 Simple Storage Service（Amazon S3）存储桶和 Lambda 函数。事件选择器仅应用于在其中创建跟踪的区域。

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
```

```
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

以下示例返回为跟踪配置的事件选择器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

不记录 AWS Key Management Service 事件的示例跟踪

以下示例为名为的跟踪创建事件选择器，*TrailName*以包括只读和只写管理事件，但排除 AWS Key Management Service (AWS KMS) 事件。由于 AWS KMS 事件被视为管理事件，而且其数量可能很大，因此，如果您有多个跟踪记录管理事件，它们可能会对您的 CloudTrail 账单产生重大影响。在

此示例中，用户已选择排除每个跟踪中的 AWS KMS 事件，但一个跟踪除外。要排除事件源，请将 ExcludeManagementEventSources 添加到事件选择器，然后在字符串值中指定事件源。

如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件记录设置。

要重新开始将 AWS KMS 事件记录到跟踪，请传递一个空数组作为的值ExcludeManagementEventSources。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

以下示例返回为跟踪配置的事件选择器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要重新开始将 AWS KMS 事件记录到跟踪，请传递一个空数组作为的值ExcludeManagementEventSources，如以下命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

记录相关低容量 AWS Key Management Service 事件的示例跟踪

以下示例为名为的跟踪创建事件选择器 *TrailName*，以包含只写管理事件和 AWS KMS 事件。由于 AWS KMS 事件被视为管理事件，而且其数量可能很大，因此，如果您有多个跟踪记录管理事件，它们可能会对您的 CloudTrail 账单产生重大影响。此示例中的用户已选择包含 W AWS KMS rit e 事件，该事件将包括DisableScheduleKey、Delete和，但不再包括大容量操作，例如EncryptDecrypt、和GenerateDataKey（这些操作现在被视为读取事件）。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

以下示例返回为跟踪配置的事件选择器。这会记录只写管理事件，包括 AWS KMS 事件。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

不记录 Amazon RDS 数据 API 事件的示例跟踪

以下示例为名为的跟踪创建事件选择器，*TrailName*以包括只读和只写管理事件，但不包括 Amazon RDS Data API 事件。由于 Amazon RDS Data API 事件被视为管理事件，而且其数量可能很大，因此，如果您有多个跟踪记录管理事件，它们可能会对您的 CloudTrail 账单产生重大影响。在此示例中，用户已选择排除每个跟踪中的 Amazon RDS 数据 API 事件，但一个跟踪除外。要排除事件源，请将 `ExcludeManagementEventSources` 添加到事件选择器，然后在字符串值中指定 Amazon RDS 数据 API 事件源：`rdsdata.amazonaws.com`。

如果选择不记录管理事件，则不会记录 Amazon RDS 数据 API 事件，并且您无法更改事件日志记录设置。

要重新开始将 Amazon RDS 数据 API 管理事件记录到跟踪中，请传递一个空数组作为值`ExcludeManagementEventSources`。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

以下示例返回为跟踪配置的事件选择器。

```
{
    "EventSelectors": [
```

```
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要重新开始将 Amazon RDS Data API 管理事件记录到跟踪中，请传递一个空数组作为的值`ExcludeManagementEventSources`，如以下命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

配置高级事件选择器

要使用高级事件选择器而非基本事件选择器来包含或排除数据事件，请在跟踪记录的详细信息页面上使用高级事件选择器。与基本事件选择器相比，高级事件选择器允许您记录更多资源类型的数据事件。基本选择器记录 S3 对象活动， AWS Lambda 函数执行活动和 DynamoDB 表。

在高级事件选择器中，构建表达式以收集有关特定资源类型的数据事件，例如 S3 存储桶、 AWS Lambda 函数、DynamoDB 表、S3 对象 Lambda 接入点、EBS 快照上的 Amazon EBS 直接 API、S3 接入点、DynamoDB 流、Lake Formation 创建的表等。 AWS Glue

有关高级事件选择器的更多信息，请参阅配置高级事件选择器。

要查看某个跟踪的高级事件选择器设置，请运行下面的 `get-event-selectors` 命令。您必须从创建跟踪的 AWS 区域（主区域）运行此命令，或者必须通过添加--region参数来指定该区域。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 如果跟踪是组织跟踪，并且您使用组织中的成员账户登录 AWS Organizations，则必须提供跟踪的完整 ARN，而不仅仅是名称。

以下示例返回跟踪的高级事件选择器的默认设置。默认情况下，不为跟踪配置高级事件选择器。

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要创建事件选择器，请运行 put-event-selectors 命令。当您的账户中发生数据事件时，CloudTrail 会评估您的跟踪配置。如果事件匹配跟踪的任何高级事件选择器，则跟踪将处理并记录事件。您可以在跟踪上配置多达 500 个条件，包括为跟踪上的所有高级事件选择器指定的所有值。有关更多信息，请参阅 记录数据事件。

主题

- 带有特定高级事件选择器的示例跟踪
- 使用自定义高级事件选择器在 Amazon S3 上记录 AWS Outposts 数据事件的示例跟踪
- 使用高级事件选择器排除 AWS Key Management Service 事件的示例路径
- 使用高级事件选择器排除 Amazon RDS 数据 API 管理事件的示例跟踪

带有特定高级事件选择器的示例跟踪

以下示例为名为的跟踪创建自定义高级事件选择器，*TrailName*以包括读取和写入管理事件（省略readOnly选择器），PutObject以及除名为的存储桶sample_bucket_name和名为的函数DeleteObject的数据事件之外的所有 Amazon S3 存储桶/前缀组合的数据事件。 AWS Lambda MyLambdaFunction由于这些都是自定义高级事件选择器，因此每组选择器都有一个描述性名称。请注意，尾随斜杠是 S3 存储桶的 ARN 值的一部分。

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
```

```
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

以下示例返回为跟踪配置的高级事件选择器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
```

```
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

使用自定义高级事件选择器在 Amazon S3 上记录 AWS Outposts 数据事件的示例跟踪

以下示例说明如何配置您的跟踪，使其包含前哨基地中 AWS Outposts 对象上的所有 Amazon S3 的所有数据事件。在此版本中，S3 在该`resources.type`字段 AWS Outposts 的事件上支持的值为`AWS::S3Outposts::Object`。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
```

```
        }
]'
```

该命令将返回以下示例输出。

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

使用高级事件选择器排除 AWS Key Management Service 事件的示例路径

以下示例为名为的跟踪创建了一个高级事件选择器，*TrailName*以包含只读和只写管理事件（省略`readOnly`选择器），但排除 AWS Key Management Service (AWS KMS) 事件。由于 AWS KMS 事件被视为管理事件，而且其数量可能很大，因此，如果您有多个跟踪记录管理事件，它们可能会对您的 CloudTrail 账单产生重大影响。

如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件日志记录设置。

要重新开始将 AWS KMS 事件记录到跟踪，请移除`eventSource`选择器，然后再次运行该命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
```

```
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

以下示例返回为跟踪配置的高级事件选择器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要再次开始将排除的事件记录到跟踪，请删除 eventSource 选择器，如以下命令中所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

使用高级事件选择器排除 Amazon RDS 数据 API 管理事件的示例跟踪

以下示例为名为的跟踪创建高级事件选择器，*TrailName*以包含只读和只写管理事件（省略`readOnly`选择器），但排除 Amazon RDS 数据 API 管理事件。要排除 Amazon RDS 数据 API 管理事件，请在`eventSource`字段的字符串值中指定 Amazon RDS 数据 API 事件源`rdsdata.amazonaws.com`。

如果您选择不记录管理事件，则不会记录 Amazon RDS 数据 API 管理事件，也无法更改 Amazon RDS 数据 API 事件记录设置。

要重新开始将 Amazon RDS 数据 API 管理事件记录到跟踪中，请移除`eventSource`选择器，然后再次运行该命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

以下示例返回为跟踪配置的高级事件选择器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
```

```
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要再次开始将排除的事件记录到跟踪，请删除 eventSource 选择器，如以下命令中所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

停止和启动跟踪的日志记录

以下命令启动和停止 CloudTrail 日志记录。

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> 在删除存储桶之前，运行 stop-logging 命令以停止向存储桶传送事件。如果您不停止记录，则 CloudTrail 会尝试在有限的时间内将日志文件传送到同名存储桶。
> 如果您停止记录或删除跟踪，则会对该跟踪禁用 CloudTrail Insights。

删除跟踪

如果您已在 Amazon Security Lake 中启用 CloudTrail 管理事件，则需要至少维护一条多区域组织跟踪，并记录两者read以及write管理事件。如果跟踪是您拥有的唯一符合此要求的跟踪，则无法将其删除，除非您在 Security Lake 中关闭 CloudTrail 管理事件。

可使用以下命令删除跟踪。您只能从创建跟踪的区域（主区域）中删除跟踪。

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

在删除跟踪时，请不要删除 Simple Storage Service（Amazon S3）存储桶或与该存储桶关联的 Amazon SNS 主题。使用 AWS Management Console AWS CLI、或服务 API 分别删除这些资源。

为组织创建跟踪

如果您在中创建了组织 AWS Organizations，则可以创建记录该组织 AWS 账户 中所有人的所有事件的跟踪。这有时称为企业跟踪记录。

组织的管理账户可以指定委托管理员来创建新的组织跟踪或管理现有的组织跟踪。有关添加委托管理员的更多信息，请参阅添加 CloudTrail 委派管理员。

组织的管理账户可以编辑账户中的现有跟踪，并将其应用于组织，从而使其成为组织跟踪。组织跟踪记录记录组织内的管理账户和所有成员账户的日志事件。有关的更多信息 AWS Organizations，请参阅 Organizat ions 术语和概念。

> **Note**
>
> 您必须使用管理账户或与组织关联的委托管理员账户登录，才能创建组织跟踪。您还必须为管理账户或委托管理员账户中的用户或角色拥有足够的权限才能创建跟踪。如果您没有足够的权限，则无法获得用于将跟踪应用于组织的选项。

使用控制台创建的所有组织跟踪都是多区域组织跟踪，用于记录组织 AWS 区域 中每个成员账户中已启用的组织跟踪的事件。要记录组织中所有 AWS 分区中的事件，请在每个分区中创建多区域组织跟踪。您可以使用创建单区域或多区域组织跟踪。 AWS CLI如果您创建单区域跟踪，则只能在该跟踪 AWS 区域（也称为主区域）中记录活动。

尽管大多数区域默认 AWS 区域 处于启用状态 AWS 账户，但您必须手动启用某些区域（也称为可选区域）。有关默认启用哪些区域的信息，请参阅《AWS Account Management 参考指南》中的启用和禁用区域之前的注意事项。有关 CloudTrail 支持的区域列表，请参阅CloudTrail 支持的区域。

创建组织跟踪时，将在属于您的组织的成员账户中创建带有您指定名称的跟踪副本。

- 如果组织跟踪适用于单区域，而跟踪的主区域不是 Opt-Region，则会在组织跟踪的主区域的每个成员账户中创建跟踪的副本。
- 如果组织跟踪是针对单区域的，而跟踪的主区域是选择区域，则会在组织跟踪的主区域中在启用该区域的成员账户中创建跟踪的副本。

- 如果组织跟踪是多区域，并且跟踪的主区域不是可选区域，则会在每个成员账户中启用的 AWS 区域每个跟踪中创建一个跟踪副本。当成员账户启用可选区域时，将在该区域的激活完成后，在新选择的区域中为该成员账户创建多区域跟踪的副本。
- 如果组织跟踪是多区域，而主区域是可选区域，则成员账户将不会向组织跟踪发送活动，除非他们选择进入创建多区域跟踪 AWS 区域 的地方。例如，如果您创建了多区域跟踪并选择欧洲（西班牙）地区作为跟踪的主区域，则只有为其账户启用了欧洲（西班牙）地区的成员账户才会将其账户活动发送到组织跟踪。

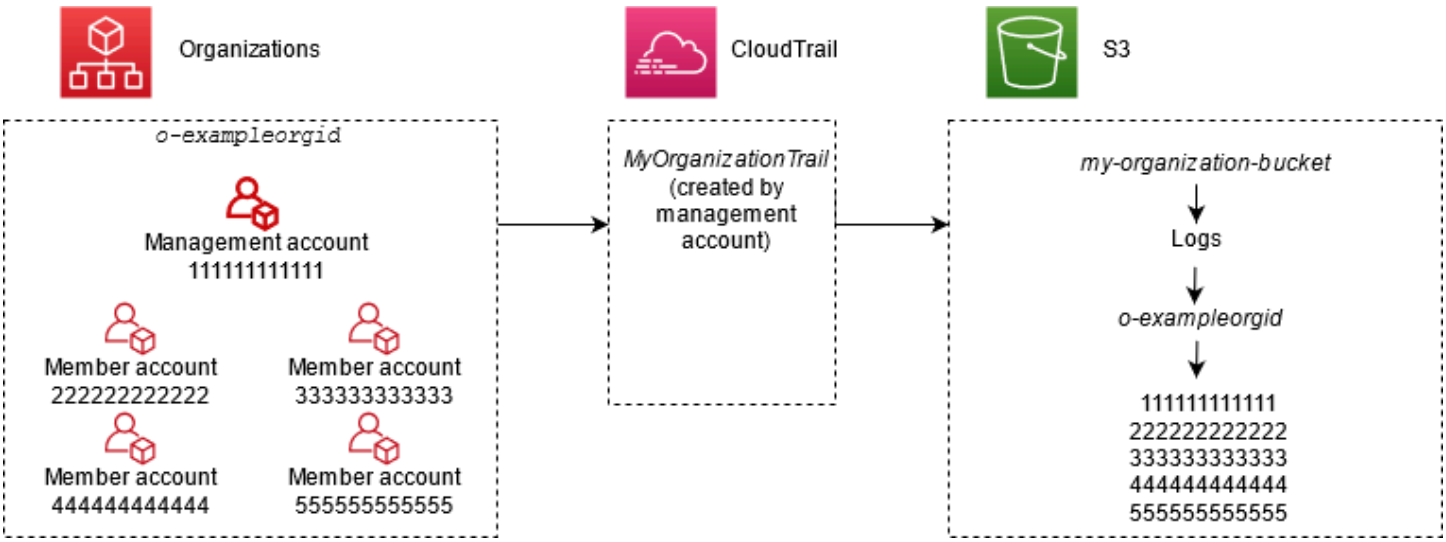
> **Note**
>
> CloudTrail 即使资源验证失败，也会在成员账户中创建组织跟踪。验证失败的示例包括：
>
> - Amazon S3 存储桶策略不正确
> - 不正确的 Amazon SNS 主题政策
> - 无法传送到 CloudWatch 日志组
> - 权限不足，无法使用 KMS 密钥进行加密
>
> 拥有 CloudTrail 权限的成员账户可以通过在 CloudTrail 控制台上查看跟踪的详细信息页面或运行 AWS CLI get-trail-status命令来查看组织跟踪的任何验证失败。

拥有成员账户 CloudTrail 权限的用户在从自己的 AWS 账户账户登录 AWS CloudTrail 控制台或运行诸如之类的 AWS CLI 命令时可以看到组织跟踪`describe-trails`。但是，成员账户中的用户没有足够的权限来删除组织跟踪、开启或关闭日志记录、更改记录的事件类型或以任何方式更改组织跟踪。

当您在控制台中创建组织跟踪或在 Organizations 中 CloudTrail 作为可信服务启用时，这会创建一个服务相关角色来在组织的成员账户中执行日志任务。此角色已命名 AWSServiceRoleForCloudTrail，并且是记录组织事件所必需 CloudTrail 的。如果向组织添加了， AWS 账户 则会向该组织添加组织跟踪和与服务相关的角色 AWS 账户，并在组织跟踪中自动开始该账户的日志记录。如果从组织中移除了， AWS 账户 则将从不再属于 AWS 账户 该组织的组织中删除组织跟踪和服务相关角色。但是，在删除账户之前创建的已删除账户的日志文件仍将保留在 Simple Storage Service（Amazon S3）存储桶（其中存储了日志文件以用于跟踪）中。

如果组织的管理账户创建了 AWS Organizations 组织跟踪，但随后被删除为该组织的管理账户，则使用其账户创建的任何组织跟踪都将成为非组织跟踪。

*############### 111111111111 ############MyOrganizationTrail## o-exampleorgid#*此跟踪将组织中所有账户的活动记录在同一 Simple Storage Service（Amazon S3）存储桶中。组织中的所有账户都可以在其跟踪列表*MyOrganizationTrail*中看到，但成员账户无法删除或修改组织跟踪。只有管理账户或委托管理员账户才能更改或删除组织的跟踪。只有管理账户才能从组织中移除成员账户。同样，默认情况下，只有管理账户才能访问跟踪的 Amazon S3 存储桶*my-organization-bucket*以及其中包含的日志。日志文件的高级存储桶结构包含一个以企业 ID 命名的文件夹，其子文件夹以企业中每个账户的账户 ID 命名。每个成员账户的事件均记录在与相应成员账户 ID 对应的文件夹中。如果成员帐户 444444444444 已从组织中删除，*MyOrganizationTrail*并且服务相关角色不再出现在 AWS 账户 444444444444 中，并且组织追踪不会为该账户记录进一步的事件。但是，444444444444 文件夹将与从组织中删除该账户之前创建的所有日志一起保留在 Simple Storage Service（Amazon S3）存储桶中。



在此示例中，管理账户中所创建跟踪的 ARN 为 `aws:cloudtrail:us-east-2:111111111111:trail/`*MyOrganizationTrail*。此 ARN 也是所有成员账户中的跟踪的 ARN。

组织跟踪记录在很多方面都类似于常规跟踪记录。您可以为组织创建多个跟踪，并选择是在所有区域还是在单区域中创建组织跟踪，以及希望在组织跟踪中记录哪些类型的事件，就像在任何其他跟踪中一样。但存在一些区别。例如，当您在控制台中创建跟踪并选择是否记录 Amazon S3 存储桶或 AWS Lambda 函数的数据事件时， CloudTrail 控制台中列出的资源仅为管理账户的资源，但您可以为成员账户中的资源添加 ARN。将记录指定成员账户资源的数据事件，而无需手动配置对这些资源的跨账户访问。有关记录管理事件、Insights 事件和数据事件的更多信息，请参阅记录管理事件记录数据事件、和记录 Insights 事件。

> **Note**
>
> 在控制台中，您可以创建多区域跟踪。这是推荐的最佳实践；在您的所有区域中记录活动 AWS 账户 有助于提高 AWS 环境的安全性。要创建单区域跟踪，请使用 AWS CLI。

当您在中的某个组织的 “活动历史记录” 中查看事件时 AWS Organizations，只能查看 AWS 账户 与您登录的组织的事件。例如，如果您使用组织管理账户登录，Event history（事件历史记录）将显示该管理账户的过去 90 天的管理事件。组织成员账户事件不会显示在管理账户的 Event history（事件历史记录）中。要查看 Event history（事件历史记录）中的会员账户事件，请使用会员账户登录。

您可以配置其他 AWS 服务，以进一步分析和处理组织跟踪 CloudTrail 日志中收集的事件数据，就像处理任何其他跟踪一样。例如，您可以使用 Amazon Athena 分析组织跟踪中的数据。有关更多信息，请参阅 AWS 与日志的服务集成 CloudTrail 。

主题

- 从成员账户跟踪转移到组织跟踪
- 准备为您的组织创建跟踪
- 在控制台中为您的组织创建跟踪
- 使用为组织创建跟踪 AWS Command Line Interface
- 故障排除

从成员账户跟踪转移到组织跟踪

如果您已经为个人成员账户配置了 CloudTrail 跟踪，但想要移至组织跟踪以记录所有账户中的事件，那么您不希望在创建组织跟踪之前删除个人成员账户跟踪而丢失事件。但是，当您有两个跟踪记录时，您会由于传递到组织跟踪记录的事件的额外副本而产生更高的成本。

为了帮助管理成本，但要避免在组织跟踪记录中开始日志传输之前丢失事件，请考虑同时保留单个成员账户跟踪记录和组织跟踪记录最多一天。这可确保组织跟踪记录所有事件，但您只会在一天内产生重复事件成本。第一天过后，您可以停止登录（或删除）任何单个会员账户跟踪记录。

准备为您的组织创建跟踪

在为贵组织创建跟踪之前，请确保正确设置贵组织的管理账户或委托管理员账户，以便创建跟踪。

- 您的组织必须先启用所有功能，然后才能为其创建跟踪。有关更多信息，请参阅启用组织中的所有功能。

- 管理账户必须具有 AWSServiceRoleForOrganizations 角色。此角色由 Organizations 在您创建组织时自动创建，并且是记录组织事件所必需的。 CloudTrail 有关更多信息，请参阅 Organizations 和服务相关角色。
- 在管理账户或委托管理员账户中创建组织跟踪的用户或角色必须拥有足够的权限才能创建组织跟踪。您必须至少将 AWSCloudTrail_FullAccess 策略或等效策略应用于该角色或用户。您还必须在 IAM 和 Organizations 中具有足够的权限，才能创建服务相关角色并启用可信访问。如果您选择使用 CloudTrail 控制台为组织跟踪创建新的 S3 存储桶， 您的保单还需要包括 `s3:PutEncryptionConfiguration` 操作，因为默认情况下，存储桶已启用服务器端加密。以下示例策略显示了所需的最低权限。

> **Note**
>
> 您不应该在所有人之间广泛共享该AWSCloudTrail_FullAccess政策 AWS 账户。相反，您应将其限制在 AWS 账户 管理员范围内，因为所收集的信息具有高度敏感性 CloudTrail。拥有此角色的用户能够关闭或重新配置他们的 AWS 账户中最敏感且最重要的审计功能。因此，您必须密切控制和监控对此策略的访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

- 要使用 AWS CLI 或 CloudTrail API 创建组织跟踪，您必须在 Organizations CloudTrail 中为启用可信访问，并且必须使用允许记录组织跟踪的策略手动创建 Amazon S3 存储桶。有关更多信息，请参阅 使用为组织创建跟踪 AWS Command Line Interface。
- 要使用现有 IAM 角色向 Amazon L CloudWatch ogs 添加对组织跟踪的监控，您必须手动修改 IAM 角色以允许将成员账户的 CloudWatch 日志传送到管理账户的日志组，如以下示例所示。CloudWatch

> **Note**
>
> 您必须使用自己账户中存在的 IAM 角色和 CloudWatch 日志组。您不能使用其他账户拥有的 IAM 角色或 CloudWatch 日志组。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
```

```
        }
    ]
}
```

您可以在 Amazon CloudWatch 登录 CloudTrail 中了解更多相关信息使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。此外，在决定为组织跟踪启用体验之前，请考虑 CloudWatch 日志的限制和服务的定价注意事项。有关更多信息，请参阅CloudWatch 日志限制和 Amazon CloudWatch 定价。

- 要在组织跟踪中记录成员账户中特定资源的数据事件，请为每项资源准备好 Amazon Resource Name（ARN）列表。创建跟踪时，成员账户资源不会显示在 CloudTrail 控制台中；您可以浏览管理账户中支持数据事件收集的资源，例如 S3 存储桶。同样，如果要在命令行中创建或更新组织跟踪时添加特定成员资源，则需要这些资源的 ARN。

> **Note**
>
> 记录数据事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

在创建组织跟踪之前，您还应该考虑查看管理账户和成员账户中已经存在多少条跟踪。 CloudTrail 限制每个区域中可以创建的跟踪数量。您在管理账户中创建组织跟踪的区域中不能超出此限制。但是，即使成员账户已达到区域中的跟踪限制，也会在成员账户中创建跟踪。虽然任何区域中的管理事件的第一个跟踪都是免费的，但其他跟踪需要付费。要降低组织跟踪记录的潜在成本，请考虑删除管理账户和成员账户中任何不需要的跟踪记录。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

企业跟踪记录安全最佳实践

作为安全最佳实践，建议您将 `aws:SourceArn` 条件密钥添加到用于企业跟踪记录的资源策略（例如 S3 存储桶、KMS 密钥或 SNS 主题的策略）。`aws:SourceArn` 的值是企业跟踪记录 ARN（或 ARN，如果您使用同一资源进行多个跟踪，例如用同一个 S3 存储桶存储多个跟踪记录的日志）。这可确保资源（例如 S3 存储桶）只接受与特定跟踪记录关联的数据。跟踪 ARN 必须使用管理账户的账户 ID。以下策略代码段显示有多个跟踪记录正在使用该资源的示例。

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

有关如何向资源策略添加条件密钥的信息，请参阅以下内容：

- 适用于 Amazon S3 存储桶的政策 CloudTrail
- 为以下各项配置 AWS KMS 密钥策略 CloudTrail
- Amazon SNS 主题政策 CloudTrail

在控制台中为您的组织创建跟踪

要从 CloudTrail 控制台创建组织跟踪，您必须以具有足够权限的管理账户或委托管理员账户中的用户或角色登录控制台。如果您未使用管理或委托管理员帐户登录，则在 CloudTrail控制台创建或编辑跟踪时，您将看不到向组织应用跟踪的选项。

您可以通过多种方式配置组织跟踪。例如，您可以为组织跟踪配置以下详细信息：

- 默认情况下，在控制台中创建跟踪时，该跟踪会记录您正在使用的 AWS 分区中的所有 AWS 区域。作为最佳实践，我们强烈建议您在所有区域中记录事件 AWS 账户。要创建单区域跟踪，请使用 AWS CLI。
- 指定是否要将跟踪应用于您的组织。默认情况下，跟踪不应用于组织。您必须选择此选项才能创建组织跟踪。
- 指定接收组织跟踪的日志文件的 Amazon S3 存储桶。您可以选择现有的 Amazon S3 桶，也可以专门为组织跟踪创建一个桶。
- 对于管理事件和数据事件，指定您要记录 Read（读取）事件、Write（写入）事件还是同时记录两者。CloudTrailInsights 事件仅记录在管理事件上。您可以通过从控制台以及成员账户（如果您指定要为其启用数据事件日志记录的每个资源的 ARN）的列表中选择资源，来指定为管理账户中这些资源记录数据事件。有关更多信息，请参阅 数据事件。

要使用创建组织跟踪 AWS Management Console

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。

   您必须以拥有足够权限的管理账户或委托管理员账户中的 IAM 身份登录，才能创建组织跟踪。
2. 选择 Trails（跟踪记录），然后选择 Create trail（创建跟踪记录）。
3. 在 Create Trail 页面上，对于 Trail name，键入一个跟踪名。有关更多信息，请参阅 命名要求。
4. 选择 Enable for all accounts in my organization（为我的组织中的所有账户启用）。如果您使用管理账户或委托管理员账户中的用户或角色登录到控制台，则只会看到此选项。要成功创建组织跟踪，请确保相应用户或角色具有足够的权限。

5. 对于 Storage location（存储位置，选择 Create new S3 bucket（创建 S3 存储桶）以创建存储桶。创建存储桶时， CloudTrail 会创建并应用所需的存储桶策略。

> **Note**
>
> 如果选择 Use existing S3 bucket（使用现有 S3 存储桶），则在 Trail log bucket name（跟踪日志存储桶名称）中指定一个存储桶，或选择 Browse（浏览）以选择存储桶。您可以选择属于任何账户的存储桶，但是，存储桶策略必须授予写入该存储桶的CloudTrail权限。有关手动编辑存储桶策略的信息，请参阅适用于 Amazon S3 存储桶的政策 CloudTrail。

为了便于查找日志，请在现有存储桶中创建一个新文件夹（也称为前缀）来存储 CloudTrail 日志。在 Prefix（前缀）字段中输入前缀。

6. 对于 Log file SSE-KMS encryption（日志文件 SSE-KMS 加密），如果您希望使用 SSE-KMS 加密而非 SSE-S3 加密对您的日志文件进行加密，请选择 Enabled（已启用）。默认值为 Enabled（已启用）。如果您未启用 SSE-KMS 加密，则将使用 SSE-S3 加密对您的日志进行加密。有关 SSE-KMS 加密的更多信息，请参阅使用具有 AWS Key Management Service 的服务器端加密（SSE-KMS）。有关 SSE-S3 加密的更多信息，请参阅配合使用服务器端加密与 Amazon S3 托管加密密钥（SSE-S3）。

   如果您启用 SSE-KMS 加密，请选择 “新建” 或 “现有”。 AWS KMS key在AWS KMS 别名中，按以下格式指定别名`alias/`*`MyAliasName`*。有关更多信息，请参阅 更新资源以使用 KMS 密钥。

> **Note**
>
> 您也可以键入其他账户的密钥 ARN。有关更多信息，请参阅 更新资源以使用 KMS 密钥。密钥策略必须 CloudTrail 允许使用密钥加密您的日志文件，并允许您指定的用户读取未加密形式的日志文件。有关手动编辑密钥政策的信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

7. 在 Additional configuration（其他配置）中，请配置以下内容。

   a. 对于 Log file validation（日志文件验证），选择 Enabled（已启用）以将日志摘要传输到您的 S3 存储桶。您可以使用摘要文件来验证您的日志文件在 CloudTrail 交付后是否没有更改。有关更多信息，请参阅 验证 CloudTrail 日志文件完整性。

b. 要传送 SNS 通知，请选择 “启用”，以便每次向您的存储桶传送日志时都会收到通知。CloudTrail 在日志文件中存储多个事件。SNS 通知针对每个日志文件而不是每个事件发送。有关更多信息，请参阅 配置 Amazon SNS 通知 CloudTrail。

如果您启用了 SNS 通知，则对于 Create a new SNS topic（创建新 SNS 主题），选择 New（新建）创建主题，或选择 Existing（现有）使用现有的主题。如果您创建的是应用到所有区域的跟踪，则针对来自所有区域的日志文件传输的 SNS 通知将发送到您创建的单个 SNS 主题中。

如果选择 “新建”，则会为您 CloudTrail 指定新主题的名称，也可以键入名称。如果选择 Existing（现有），则从下拉列表中选择一个 SNS 主题。您还可以输入来自另一个区域或来自一个具有适当权限的账户的主题的 ARN。有关更多信息，请参阅 Amazon SNS 主题政策 CloudTrail。

如果您创建一个主题，则必须订阅该主题以便获取日志文件传送的通知。您可通过 Amazon SNS 控制台进行订阅。由于通知的频率，建议您将该订阅配置为使用 Amazon SQS 队列来以编程方式处理通知。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。

8. 或者，通过选择在日志中启用，配置 CloudTrail 为将 CloudWatch 日志文件发送到CloudWatch 日志。有关更多信息，请参阅 将事件发送到 CloudWatch 日志。

> **Note**
>
> 只有管理账户才能使用控制台为组织跟踪配置 CloudWatch 日志组。授权的管理员可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 操作配置 CloudWatch 日志组。

a. 如果您启用了与 CloudWatch 日志的集成，请选择 “新建” 来创建新的日志组，或者选择 “现有” 以使用现有的日志组。如果选择 “新建”，则会为您 CloudTrail 指定新日志组的名称，也可以键入名称。

b. 如果选择 Existing（现有），则从下拉列表中选择一个日志组。

c. 选择 “新建” 创建新的 IAM 角色，以获得向日志发送 CloudWatch 日志的权限。选择 Existing（现有）以从下拉列表中选择一个现有 IAM 角色。展开 Policy document（策略文档）时，将显示新角色或现有角色的策略语句。有关该角色的更多信息，请参阅 使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档。

> **Note**
>
> 在您配置跟踪时，可以选择属于另一个账户的 S3 存储桶和 Amazon SNS 主题。但是，如果 CloudTrail 要将事件传送到 CloudWatch 日志日志组，则必须选择当前账户中存在的日志组。

9. 对于 Tags（标签），将一个或多个自定义标签（键值对）添加到跟踪中。标签可以帮助您识别您的 CloudTrail 跟踪和包含 CloudTrail 日志文件的 Amazon S3 存储桶。然后，您可以将资源组用于您的 CloudTrail 资源。有关更多信息，请参阅 AWS Resource Groups 和 标签。
10. 在 Choose log events（选择日志事件）页面中，选择要记录的事件类型。对于 Management events (管理事件)，请执行以下操作。

    a. 对于 API activity（API 活动），选择您希望跟踪记录 Read（读取）事件、Write（写入）事件，还是记录两者。有关更多信息，请参阅 管理事件。

    b. 选择 “排除 AWS KMS 事件”，从您的跟踪中筛选 AWS Key Management Service (AWS KMS) 事件。默认设置是包含所有 AWS KMS 事件。

       只有在跟踪中记录管理 AWS KMS 事件时，才可使用记录或排除事件的选项。如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件日志记录设置。

       AWS KMS 诸如`Encrypt`、`Decrypt`和之类的操作`GenerateDataKey`通常会生成大量事件（超过 99%）。这些操作现在记录为读取事件。诸如`DisableDelete`、和`ScheduleKey`（通常占事件量不到 0.5%）之类的低容量相关 AWS KMS 操作被记录为写入 AWS KMS 事件。

       如果要排除大批量事件（例如 `Encrypt`、`Decrypt` 和 `GenerateDataKey`），但仍然记录相关事件（例如 `Disable`、`Delete` 和 `ScheduleKey`），选择记录 Write（写入）管理事件，然后清除 Exclude AWS KMS events（排除 Amazon KMS 事件）复选框。

    c. 选择 Exclude Amazon RDS Data API events（排除 Amazon RDS 数据 API 事件以从跟踪中筛选出 Amazon Relational Database Service 数据 API 事件。默认设置是包含所有 Amazon RDS 数据 API 事件。有关 Amazon RDS 数据 API 事件的更多信息，请参阅 Amazon RDS Aurora 用户指南中的使用 AWS CloudTrail记录数据 API 调用。
11. 要记录数据事件，请选择 Data events（数据事件）。记录数据事件将收取额外费用。有关更多信息，请参阅AWS CloudTrail 定价。

12.

> **Important**
>
> 默认情况下，步骤 12-16 用于使用高级事件选择器配置数据事件。高级事件选择器让您可以配置更多数据事件类型，并对跟踪捕获的数据事件进行精细控制。如果您选择使用基本事件选择器，请完成 使用基本事件选择器配置数据事件设置 中的步骤，然后返回到此程序的步骤 17。

对于 Data event type（数据事件类型），选择要在其上记录数据事件的资源类型。有关可用数据事件类型的更多信息，请参阅 数据事件。

> **Note**
>
> 要记录由 Lake Formati AWS Glue on 创建的表的数据事件，请选择 La ke Formation。

13. 选择日志选择器模板。 CloudTrail 包括用于记录该资源类型的所有数据事件的预定义模板。要构建自定义日志选择器模板，请选择 Custom（自定义）。

> **Note**
>
> 为 S3 存储桶选择预定义的模板可以记录当前您 AWS 账户中的所有存储分段以及您在创建完跟踪后创建的任何存储分段的数据事件。它还允许记录您 AWS 账户中任何 IAM 身份执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的存储桶上执行的。
> 如果跟踪仅应用于一个区域，则选择记录所有 S3 存储桶的预定义模板可为跟踪所在的区域中的所有存储桶和您后来在该区域中创建的任何存储桶启用数据事件日志记录。不会为您的 AWS 账户的其他区域中的 Simple Storage Service（Amazon S3）存储桶记录数据事件。
> 如果您要为所有区域创建跟踪，则选择 Lambda 函数的预定义模板可以记录当前 AWS 账户中的所有函数以及您在完成跟踪创建后可能在任何区域创建的任何 Lambda 函数的数据事件。如果您要为单个区域创建跟踪（使用完成 AWS CLI），则此选择将启用您 AWS 账户中该区域中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
> 记录所有函数的数据事件还可以记录 AWS 账户中任何 IAM 身份执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

14. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。
15. 在 Advanced event selectors（高级事件选择器）中，为您要记录其数据事件的特定资源构建表达式。如果您使用的是预定义日志模板，则可跳过此步骤。

    a. 从下面的字段中选择。

    - **readOnly**-readOnly 可以设置为等于true或false的值。只读数据事件是不会更改资源状态的事件，例如 Get* 或 Describe* 事件。写入事件可添加、更改或删除资源、属性或构件，例如 Put*、Delete* 或 Write* 事件。要记录 read 和 write 两种事件，请不要添加 readOnly 选择器。
    - **eventName** - eventName 可以使用任何运算符。您可以使用它来包含或排除记录到的任何数据事件 CloudTrail，例如PutBucketPutItem、或GetSnapshotBlock。
    - **resources.ARN**-您可以将任何运算符与一起使用resources.ARN，但是如果您使用等于或不等于，则该值必须与您在模板中指定为的值的有效资源的 ARN 完全匹配。resources.type

      下表显示每个 resources.type 的有效 ARN 格式。

      > **Note**
      >
      > 您不能使用该resources.ARN字段筛选没有 ARN 的资源类型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* /

resources.type	resources.ARN
	arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*

resources.type	resources.ARN
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*

resources.type	resources.ARN
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必须采用以下格式之一： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必须采用以下格式之一： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*

resources.type	resources.ARN
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 对于启用了流的表，数据事件中的 resources 字段同时包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您为 resources.type 指定 AWS::DynamoDB::Table，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName在该字段上添加过滤器。

[2] 要记录特定 S3 存储桶中所有对象的所有数据事件，请使用 StartsWith 运算符，并且仅包含存储桶 ARN 作为匹配值。刻意使用尾部斜杠；切勿排除它。

[3] 要记录 S3 接入点中的所有对象的事件，建议您仅使用接入点 ARN，而不要包含对象路径，并且使用 StartsWith 或 NotStartsWith 运算符。

有关数据事件资源的 ARN 格式的更多信息，请参阅 AWS Identity and Access Management 用户指南中的操作、资源和条件键。

b. 对于每个字段，请选择 + 条件以根据需要添加任意数量的条件，所有条件总共可有最多 500 个指定值。例如，要从跟踪中记录的数据事件中排除两个 S3 存储桶的数据事件，您可以将该字段设置为 Resou rces.arn，将运算符设置为 “不以开头”，然后粘贴到 S3 存储桶 ARN 中，或者浏览您不想为其记录事件的 S3 存储桶。

要添加第二个 S3 存储桶，请选择 + 条件，然后重复上述说明，在 ARN 中粘贴或浏览到不同的存储桶。

> **Note**
>
> 对于跟踪上的所有选择器，最多可以有 500 个值。这包括选择器的多个值的数组，例如 `eventName`。如果所有选择器均为单个值，则最多可以向选择器添加 500 个条件。
> 如果您的账户中有超过 15,000 个 Lambda 函数，则在创建跟踪时无法在 CloudTrail 控制台中查看或选择所有函数。您仍可使用预定义选择器模板记录所有函数，即使这些函数未显示出来也是如此。如果您要记录特定函数的数据事件，则可手动添加一个函数 (如果您知道其 ARN)。您也可以在控制台中完成跟踪的创建，然后使用 AWS CLI 和put-event-selectors命令为特定 Lambda 函数配置数据事件记录。有关更多信息，请参阅 使用管理跟踪 AWS CLI。

c. 根据需要，选择 + Field（+ 字段）以添加其他字段。为了避免错误，请不要为字段设置冲突或重复的值。例如，不要在一个选择器中将 ARN 指定为等于某个值，然后在另一个选择器中指定 ARN 不等于相同的值。

16. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。重复步骤 12 至此步骤，为数据事件类型配置高级事件选择器。

17. 如果您希望跟踪记录见解事件，请选择 CloudTrail Insights 事件。

在 Event type（事件类型）中，选择 Insights events（Insights 事件）。在 Insights events（Insights 事件）中，选择 API call rate（API 调用率）和/或 API error rate（API 错误率）。您必须记录写入管理事件，以针对 API 调用率记录 Insights 事件。您必须记录读取或写入管理事件，以针对 API 错误率记录 Insights 事件。

CloudTrail Insights 会分析管理事件中是否存在异常活动，并在检测到异常时记录事件。默认情况下，跟踪记录不记录 Insights 事件。有关 Insights 事件的更多信息，请参阅记录 Insights 事件。记录 Insights 事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

Insights 事件将传送到另一个文件夹，该文件夹以同一 S3 存储桶命名/CloudTrail-Insight，该存储桶在跟踪详细信息页面的存储位置区域中指定。 CloudTrail为您创建新的前缀。例如，如果当前目标 S3 存储桶命名为 S3bucketName/AWSLogs/CloudTrail/，则带有新前缀的 S3 存储桶名称会命名为 S3bucketName/AWSLogs/CloudTrail-Insight/。

18. 完成选择要记录的事件类型的操作后，选择 Next（下一步）。
19. 在 Review and create（审核和重建）页面上，审核您的选择。在相关部分中选择 Edit（编辑）以更改该部分中显示的跟踪设置。在准备好创建跟踪时，选择 Create trail（创建跟踪）。
20. 新跟踪记录出现在 Trails（跟踪记录）页面上。一个组织跟踪最多可能需要 24 小时才能在所有成员账户的所有区域中创建完成。Trails（跟踪记录）页面显示您的账户中来自所有区域的跟踪记录。大约 5 分钟后， CloudTrail 发布显示组织中进行的 AWS API 调用的日志文件。您可以在指定的 Simple Storage Service（Amazon S3）存储桶中查看日志文件。

> **Note**
>
> 创建跟踪后，不能对其重命名。不过，可以删除跟踪并创建新跟踪。

后续步骤

创建您的跟踪后，您可以返回到该跟踪以进行更改：

- 通过编辑跟踪来更改跟踪的配置。有关更多信息，请参阅 更新跟踪。
- 如果需要，请配置 Amazon S3 存储桶，以允许成员账户中的特定用户读取组织的日志文件。有关更多信息，请参阅 在 AWS 账户之间共享 CloudTrail 日志文件。
- 配置 CloudTrail 为将日志文件发送到 CloudWatch 日志。有关更多信息，请参阅将事件发送到 CloudWatch 日志和中的 CloudWatch 日志项准备为您的组织创建跟踪。

> **Note**
>
> 只有管理账户才能为组织跟踪配置 CloudWatch 日志组。

- 创建表并将其用于在 Amazon Athena 中运行查询，以便分析 AWS 服务活动。有关更多信息，请参阅 Amazon Athen a 用户 CloudTrail 指南中的在控制台中创建 CloudTrail 日志表。
- 向跟踪添加自定义标签（键-值对）。
- 要创建另一个组织跟踪记录，请返回到 Trail（跟踪记录）页面并选择 Create trail（创建跟踪记录）。

> **Note**
>
> 在您配置跟踪时，可以选择属于另一个账户的 Simple Storage Service（Amazon S3）存储桶和 SNS 主题。但是，如果 CloudTrail 要将事件传送到 CloudWatch 日志日志组，则必须选择当前账户中存在的日志组。

使用为组织创建跟踪 AWS Command Line Interface

可通过使用 AWS CLI创建组织跟踪。 AWS CLI 会定期更新，添加其他功能和命令。为了帮助确保成功，请确保在开始之前已安装或更新到最新 AWS CLI 版本。

> **Note**
>
> 本节中的示例特定于创建和更新组织跟踪记录。有关使用管理跟踪 AWS CLI 的示例，请参阅使用管理跟踪 AWS CLI和使用配置 CloudWatch 日志监控 AWS CLI。使用创建或更新组织跟踪时 AWS CLI，您必须使用具有足够权限的管理账户或委托管理员账户中的 AWS CLI 配置文件。如果您要将组织跟踪转换为非组织跟踪，则必须使用组织的管理账户。
> 您必须具有足够的权限以配置用于组织跟踪的 Simple Storage Service（Amazon S3）存储桶。

创建或更新 Simple Storage Service（Amazon S3）存储桶以用于存储组织跟踪的日志文件

您必须指定一个 Simple Storage Service（Amazon S3）存储桶以接收组织跟踪的日志文件。此存储桶必须有 CloudTrail 允许将组织的日志文件放入存储桶的策略。

以下是名为的 Amazon S3 存储桶的策略示例 *myOrganizationBucket*，该存储桶归该组织的管理账户所有。将*myOrganizationBucket*、*##*、*ManagementAccountID#T railName # o-organizatid #######*

此存储桶策略包含三条语句。

- 第一条语句允许 CloudTrail 对亚马逊 S3 存储桶调用 Amazon S3 GetBucketAcl 操作。
- 第二条语句支持在跟踪仅从组织跟踪更改为该账户的跟踪时进行日志记录。
- 第三条语句支持对组织跟踪进行日志记录。

示例策略包括 Simple Storage Service（Amazon S3）存储桶策略的 aws:SourceArn 条件密钥。IAM 全局条件密钥aws:SourceArn有助于确保仅针对一个或多个特定跟踪向 S3 存储桶 CloudTrail 写入。在企业跟踪记录中，aws:SourceArn 的值必须是由管理账户拥有并使用管理账户 ID 的跟踪记录 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
```

```
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

此示例策略不允许来自成员账户的任何用户访问为组织创建的日志文件。默认情况下，组织日志文件只能由管理账户访问。有关如何允许成员账户中的 IAM 用户对 Simple Storage Service（Amazon S3）存储桶进行读取访问的信息，请参阅 在 AWS 账户之间共享 CloudTrail 日志文件。

在中 CloudTrail 作为可信服务启用 AWS Organizations

在创建组织跟踪之前，必须先启用 Organizations 中的所有功能。有关更多信息，请参阅启用组织中的所有功能，或使用管理账户中具有足够权限的配置文件运行以下命令：

```
aws organizations enable-all-features
```

启用所有功能后，必须将 Organizations 配置 CloudTrail 为可信服务。

要在 AWS Organizations 和之间创建可信服务关系 CloudTrail，请打开终端或命令行并使用管理账户中的配置文件。运行 `aws organizations enable-aws-service-access` 命令，如下例所示。

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

使用 create-trail

创建应用于所有区域的组织跟踪

要创建应用于所有区域的组织跟踪，请添加 `--is-organization-trail` 和 `--is-multi-region-trail` 选项。

> **Note**
>
> 使用创建组织跟踪时 AWS CLI，必须使用具有足够权限的管理账户或委托管理员账户中的 AWS CLI 配置文件。

以下示例中创建的组织跟踪将所有区域的日志传送到名为 *my-bucket* 的现有存储桶：

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail --is-multi-region-trail
```

要确认跟踪是否存在于所有区域中，输出中的 `IsOrganizationTrail` 和 `IsMultiRegionTrail` 参数均应设置为 `true`：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 运行 `start-logging` 命令可以为您的跟踪启动日志记录操作。有关更多信息，请参阅 停止和启动跟踪的日志记录。

将组织跟踪创建为单区域跟踪

以下命令创建一个仅在单个区域跟踪中记录事件的组织跟踪 AWS 区域，也称为单区域跟踪。记录事件的 AWS 区域是在的配置文件中指定的区域 AWS CLI。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail
```

有关更多信息，请参阅 命名要求。

示例输出：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

默认情况下，`create-trail` 命令会创建一个不启用日志文件验证的单区域跟踪。

> **Note**
>
> 运行 `start-logging` 命令可以为您的跟踪启动日志记录操作。

运行 update-trail 以更新组织跟踪

您可以运行 `update-trail` 命令更改组织跟踪的配置设置，或将单个 AWS 账户的现有跟踪应用于整个组织。请记住，您只能从在其中创建跟踪的区域运行 `update-trail` 命令。

> **Note**
>
> 如果您使用 AWS CLI 或其中一个 AWS 软件开发工具包来更新跟踪，请确保跟踪的存储桶策略是 up-to-date。有关更多信息，请参阅 使用为组织创建跟踪 AWS Command Line Interface。使用更新组织跟踪时 AWS CLI，必须使用具有足够权限的管理账户或委托管理员账户中的 AWS CLI 配置文件。如果要将组织跟踪转换为非组织跟踪，必须使用组织的管理账户，因为管理账户是所有组织资源的拥有者。
> CloudTrail 即使资源验证失败，也会更新成员账户中的组织跟踪。验证失败的示例包括：
>
> - Amazon S3 存储桶策略不正确
> - 不正确的 Amazon SNS 主题政策
> - 无法传送到 CloudWatch 日志组
> - 权限不足，无法使用 KMS 密钥进行加密
>
> 拥有 CloudTrail 权限的成员账户可以通过在 CloudTrail 控制台上查看跟踪的详细信息页面或运行 AWS CLI get-trail-status命令来查看组织跟踪的任何验证失败。

将现有跟踪应用于组织

要更改现有跟踪，使其也适用于组织而不是单个 AWS 账户，请添加`--is-organization-trail`选项，如以下示例所示。

> **Note**
>
> 使用管理账户将现有的非组织跟踪更改为组织跟踪。

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

要确认跟踪现已应用于相应组织，输出中的 `IsOrganizationTrail` 参数的值应为 `true`。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
```

```
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

在前面的示例中，已将跟踪配置为应用于所有区域 ("IsMultiRegionTrail": true)。仅应用于单区域的跟踪将在输出中显示 "IsMultiRegionTrail": false。

将应用于一个区域的组织跟踪转换为应用于所有区域

要更改现有组织跟踪以使其应用于所有区域，请添加 --is-multi-region-trail 选项，如下例中所示。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

要确认跟踪现已应用于所有区域，输出中的 IsMultiRegionTrail 参数的值应为 true。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

故障排除

本节提供有关如何解决组织跟踪问题的信息。

主题

- CloudTrail 未投递活动
- CloudTrail 没有为组织中的成员账户发送 Amazon SNS 通知

CloudTrail 未投递活动

如果 CloudTrail 没有将 CloudTrail 日志文件传送到 Amazon S3 存储桶

检查 S3 存储桶是否存在问题。

- 在 CloudTrail 控制台中，查看跟踪的详细信息页面。如果 S3 存储桶出现问题，则详细信息页面会显示一条警告，说明向 S3 存储桶交付失败。
- 从中 AWS CLI，运行get-trail-status命令。如果出现故障，命令输出将包含`LatestDeliveryError`字段，该字段显示在尝试将日志文件传送到指定存储桶时 CloudTrail 遇到的任何 Amazon S3 错误。仅当目标 S3 存储桶出现问题时才会出现此错误，超时的请求不会发生此错误。要解决此问题，请修复存储桶策略，使其 CloudTrail 可以写入存储桶；或者创建一个新的存储桶，然后调`update-trail`用指定新的存储桶。有关组织存储桶策略的信息，请参阅创建或更新用于存储组织跟踪日志文件的 Amazon S3 存储桶。

如果 CloudTrail 不是将日志传送到 CloudWatch 日志

检查 CloudWatch 日志角色策略的配置是否存在问题。

- 在 CloudTrail 控制台中，查看跟踪的详细信息页面。如果 CloudWatch 日志存在问题，则详细信息页面会显示一条警告，指示 CloudWatch 日志传输失败。
- 从中 AWS CLI，运行get-trail-status命令。如果出现故障，命令输出将包括`LatestCloudWatchLogsDeliveryError`字段，该字段显示尝试向 CloudWatch 日志传送日志时 CloudTrail 遇到的所有日志错误。 CloudWatch 要解决此问题，请修复 CloudWatch Logs 角色策略。有关 CloudWatch Logs 角色策略的信息，请参阅使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档。

如果你在组织跟踪中没有看到成员账户的活动

如果您在组织跟踪中没有看到成员账户的活动，请检查以下内容：

- 在主区域查看路线，看看它是否是可选区域

  尽管大多数区域默认 AWS 区域 处于启用状态 AWS 账户，但您必须手动启用某些区域（也称为可选区域）。有关默认启用哪些区域的信息，请参阅《AWS Account Management 参考指南》中的启用和禁用区域之前的注意事项。有关 CloudTrail 支持的区域列表，请参阅CloudTrail 支持的区域。

  如果组织跟踪是多区域，而主区域是可选区域，则成员账户将不会向组织跟踪发送活动，除非他们选择进入创建多区域跟踪 AWS 区域 的地方。例如，如果您创建了多区域跟踪并选择欧洲（西班牙）地区作为跟踪的主区域，则只有为其账户启用了欧洲（西班牙）地区的成员账户才会将其账户活动发送到组织跟踪。要解决此问题，请在组织中的每个成员账户中启用选择加入区域。有关启用可选区域的信息，请参阅AWS Account Management 参考指南中的在组织中启用或禁用区域。

- 检查组织基于资源的策略是否 CloudTrail 与服务相关角色策略冲突

  CloudTrail 使用名为的服务相关角色AWSServiceRoleForCloudTrail来支持组织跟踪。此服务相关角色 CloudTrail 允许对组织资源执行操作，例如organizations:DescribeOrganization。如果组织的基于资源的策略拒绝了服务相关角色策略中允许的操作， CloudTrail 则即使服务相关角色策略允许执行该操作，也无法执行该操作。要解决此问题，请修复组织的基于资源的策略，使其不会拒绝服务相关角色策略中允许的操作。

CloudTrail 没有为组织中的成员账户发送 Amazon SNS 通知

当具有 AWS Organizations 组织跟踪的成员账户未发送 Amazon SNS 通知时，SNS 主题策略的配置可能存在问题。 CloudTrail 即使资源验证失败，也会在成员账户中创建组织跟踪，例如，组织跟踪的 SNS 主题不包括所有成员账户 ID。如果 SNS 主题策略不正确，则会发生授权失败。

要检查跟踪的 SNS 主题策略是否存在授权失败，请执行以下操作：

- 在 CloudTrail 控制台中，查看跟踪的详细信息页面。如果授权失败，则详细信息页面会显示一条警告，SNS authorization failed并指示修复 SNS 主题策略。
- 从中 AWS CLI，运行get-trail-status命令。如果授权失败，则命令输出将包括值为的LastNotificationError字段AuthorizationError。要解决此问题，请修复 Amazon SNS 主题政策。有关 Amazon SNS 主题政策的信息，请参阅。Amazon SNS 主题政策 CloudTrail

有关 SNS 主题和订阅主题的更多信息，请参阅《亚马逊简单通知服务开发者指南》中的 Amazon SNS 入门。

查看路径的 CloudTrail Insights 事件

在跟踪上启用 CloudTrail Insights 后，您可以使用 CloudTrail控制台或查看最多 90 天的 Insights 事件 AWS CLI。本节介绍如何查看、查找和下载 Insights 事件的文件。有关使用 LookupEvents API 从 CloudTrail 事件中检索信息的信息，请参阅 AWS CloudTrail API 参考。有关 CloudTrail Insights 的更多信息，请参阅本指南记录 Insights 事件中的。

有关如何创建跟踪记录的更多信息，请参阅创建跟踪和获取和查看您的 CloudTrail 日志文件。

> **Note**
>
> 要针对 API 调用量记录 Insights 事件，跟踪必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，跟踪必须记录 `read` 或 `write` 管理事件。

主题

- 在 CloudTrail 控制台中查看跟踪的 CloudTrail Insights 事件
- 使用查看路径的 CloudTrail Insights 事件 AWS CLI

在 CloudTrail 控制台中查看跟踪的 CloudTrail Insights 事件

在跟踪上启用 CloudTrail Insights 事件后，当 CloudTrail 检测到异常 API 或错误率活动时， CloudTrail 会生成 Insights 事件并将其显示在中的控制面板和见解页面上 AWS Management Console。您可以在控制台中查看 Insights 事件，并对异常活动进行故障排除。控制台中显示了最近 90 天的 Insights 事件。您也可以使用 AWS CloudTrail 控制台下载 Insights 事件。您可以使用软件开发工具 AWS 包或以编程方式查找事件。 AWS Command Line Interface有关 CloudTrail Insights 事件的更多信息，请参阅本指南记录 Insights 事件中的。

> **Note**
>
> 要针对 API 调用量记录 Insights 事件，跟踪必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，跟踪必须记录 `read` 或 `write` 管理事件。

记录见解事件后，事件将显示在 Insights（见解）页面上达 90 天。您不能从 Insights (Insights) 页面上手动删除事件。由于您必须先创建跟踪，然后才能启用 CloudTrail Insights，因此，只要您将这些事件存储在跟踪设置中配置的 S3 存储桶中，您就可以查看记录到您的跟踪中的 Insights 事件。

使用 Amazon CloudWatch Logs 监控您的跟踪日志，并在发生特定的 Insights 事件活动时收到通知。有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

查看 Insights 事件

CloudTrail 必须在您的跟踪中启用 Insights 事件，才能在控制台中查看 Insights 事件。如果检测到异常活动，则留出最多 36 小时的时间 CloudTrail 来发布第一个 Insights 事件。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/home/。
2. 在导航窗格中，选择 Dashboard（控制面板）以查看最近的五个 Insights 事件，或选择 Insights（见解）以查看过去 90 天内在您的账户中记录的所有 Insights 事件。

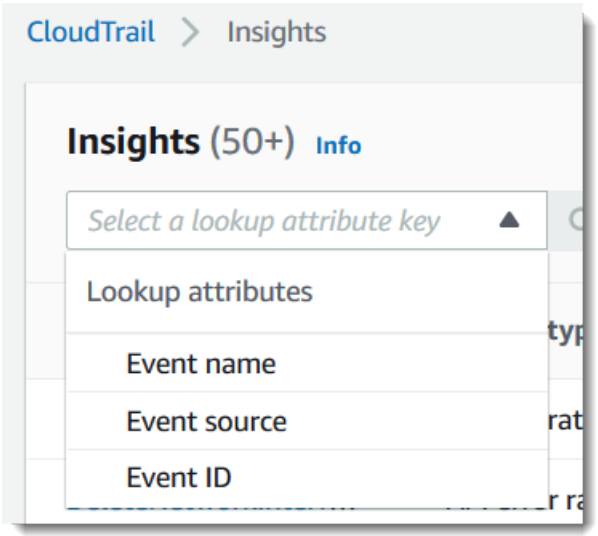
   在 Insights（见解）页面上，您可以按事件 API 源、事件名称和事件 ID 等条件筛选 Insights 事件，并将显示的事件限制为在特定时间范围内发生的事件。有关筛选 Insights 事件的更多信息，请参阅 筛选 Insights 事件。

目录

- 筛选 Insights 事件
- 查看 Insights 事件详细信息
- 缩放、平移和下载图表
- 更改图表时间跨度设置
- 下载 Insights 事件

筛选 Insights 事件

Insights（见解）中事件的默认显示按照相反的时间顺序显示事件。顶部是最新的 Insights 事件，按事件开始时间排序。下面的列表描述了可用的属性。您可以根据前三个属性进行筛选：Event name（事件名称）、Event source（事件源）和 Event ID（事件 ID）。



事件名称

事件的名称，通常是记录异常活动级别的 AWS API。

Insights 类型

CloudTrail Insights 事件的类型，可以是 API 调用率或 API 错误率。API 调用率见解类型根据基准 API 调用量分析每分钟汇总的只写管理 API 调用。API 错误率见解类型分析生成错误代码的管理 API 调用。如果 API 调用不成功，就会显示错误。

事件源

向其发出请求的 AWS 服务，例如`iam.amazonaws.com`或`s3.amazonaws.com`。在选择 Event source 筛选条件后，您可以滚动浏览事件源的列表。

事件 ID

Insights 事件的 ID。事件 ID 未显示在 Insights（见解）页表格中，但它们是您可用来筛选 Insights 事件的属性。为了生成 Insights 事件而分析的管理事件的事件 ID 与 Insights 事件的事件 ID 不同。

事件开始时间

Insights 事件的开始时间，测量方式为记录异常活动的第一分钟。此属性显示在 Insights（见解）表中，但无法在控制台中通过事件开始时间筛选。

基线平均值

API 调用率或错误率活动的正常模式。计算 Insights 事件开始前七天的基线平均值。尽管基线持续时间（ CloudTrail分析 API 正常活动的时间段）的值约为七天，但将基线持续时间 CloudTrail四舍五入为整数天，因此确切的基准持续时间可能会有所不同。

Insight 平均值

触发 Insights 事件的 API 的平均调用次数，或调用 API 时返回的特定错误的平均数。开始事件的 CloudTrail Insights 平均值是触发 Insights 事件的发生率。通常情况下，这是异常活动的第一分钟。结束事件的 Insights 平均值是在开始 Insights 事件和结束 Insights 事件之间异常活动持续时间内发生的速率。

速率变更

以百分比表示 Baseline average（基线平均值）和 Insight average（Insight 平均值）的区别。例如，如果 `AccessDenied` 发生错误的基线平均值为 1.0，并且 Insight 平均值为 3.0，那么速率变更为 300%。超过基线平均值的 Insight 平均值的速率变更在该值旁边显示向上箭头。如果因活动低于基线平均值而记录了 Insights 事件，Rate change（速率变更）在百分比旁边显示向下箭头。

如果对于所选属性或时间没有记录事件，结果列表将为空。除时间范围之外，您只能另外应用一个属性筛选条件。如果您选择另一个属性筛选条件，则将保留指定的时间范围。

以下步骤介绍如何按属性筛选。

按属性筛选

1. 要按属性筛选结果，请从下拉菜单中选择查找属性，然后在 Enter a lookup value（输入查找值）框中键入或选择值。
2. 要删除一个属性筛选条件，请选择该属性筛选条件框右侧的 X。

以下步骤介绍如何按开始日期和时间与结束日期和时间筛选。

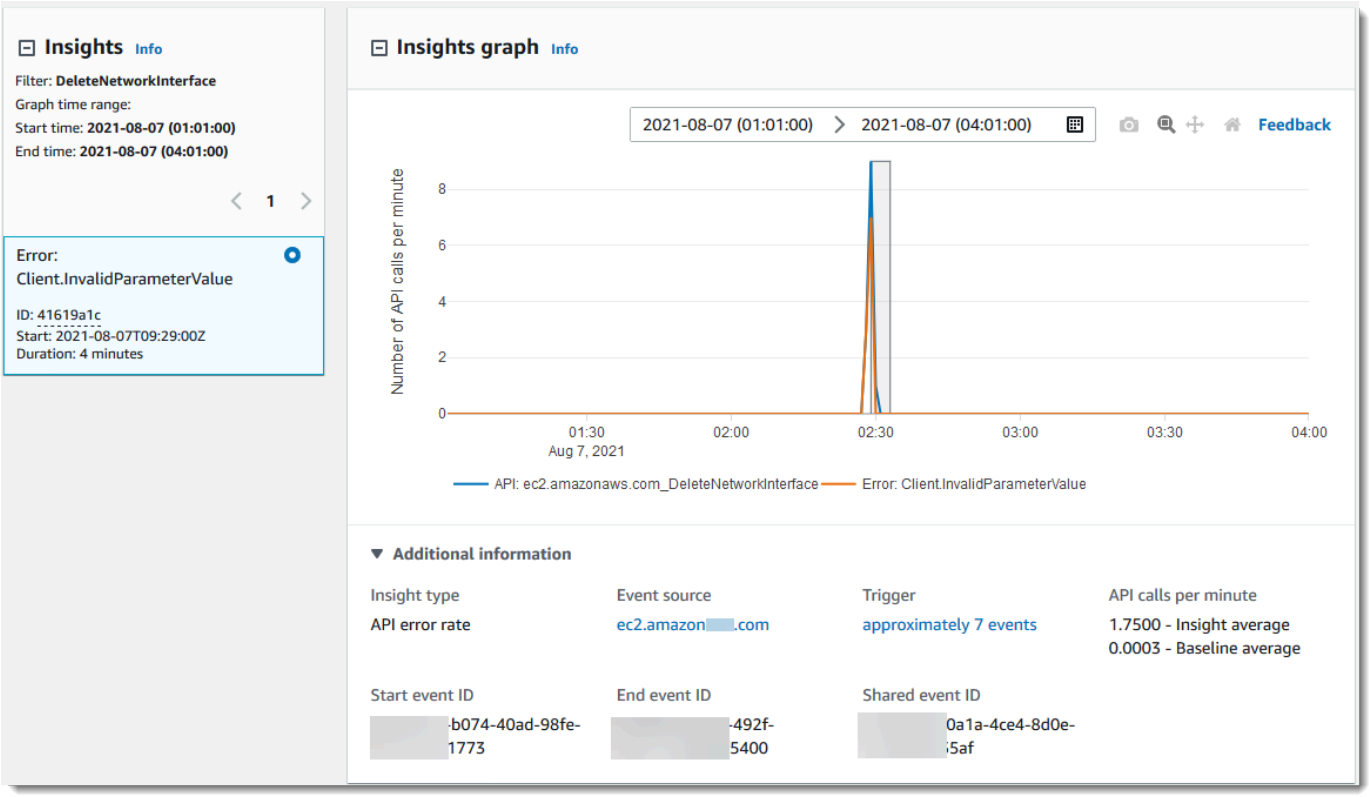
按开始日期和时间与结束日期和时间筛选

1. 要缩小您要查看的事件的时间范围，请在表格顶部的时间跨度栏上选择时间范围。预设时间范围包括 30 分钟、1 小时、3 小时或 12 小时。要指定自定义时间范围，请选择 Custom（自定义）。
2. 选择以下选项卡之一。
   - Absolute（绝对）- 供您选择具体的时间。继续执行下一步。
   - Relative to selected event（相对于所选事件）- 默认选中。让您选择相对于 Insights 事件开始时间的时间段。继续执行步骤 4。
3. 要设置 Absolute（绝对）时间范围，请执行以下操作。
   a. 在 Absolute（绝对）选项卡上，选择希望时间范围开始的日期。输入所选日期的开始时间。要手动输入日期，请使用 `yyyy/mm/dd` 格式键入日期。开始时间和结束时间使用 24 小时制，且值必须采用 `hh:mm:ss` 格式。例如，要指示开始时间为下午 6:30，请输入 **`18:30:00`**。
   b. 在日历上选择范围的结束日期，或在日历下方指定结束日期和时间。选择 应用。
4. 要设置 Relative to selected event（相对于所选事件）时间范围，请执行以下操作。
   a. 选择相对于 Insights 事件开始时间的预设时间段。预设值单位可为分钟、小时、天或周。最长相对时间周期为 12 周。
   b. 如果需要，请在预设下方的框中自定义预设值。如果老板娘，选择 Clear（清除）以重置您的更改。设置了所需的相对时间后，请选择 Apply（应用）。
5. 在 To (结束时间) 中，选择日期并指定要作为时间范围结束的时间。选择 应用。

6. 要删除一个时间范围筛选条件，请选择该 Time range (时间范围) 框右侧的日历图标，然后选择 Remove (删除)。

查看 Insights 事件详细信息

1. 选择 Insights 列表中的事件以显示其详细信息。Insights 事件的详细信息页面显示异常活动时间表的图表。



2. 将鼠标悬停在突出显示的带上，以显示图表中的每个 Insights 事件的开始时间和持续时间。

Additional information（其他信息）图表区域显示以下信息：

- 见解类型：该类型可以是 API 调用率或 API 错误率。
- 触发器：这是指向 Cloudtrail events（CloudTrail 事件）选项卡的链接，该选项卡列出了为确定发生了异常活动而分析的管理事件。
- 每分钟 API 调用数

- Baseline average（基线平均值）– 在您账户中特定区域内，大约前七天内测量的每分钟对记录 Insights 事件的 API 的典型调用速率。
- Insights average（Insights 平均值）– 触发 Insights 事件的此 API 的每分钟调用速率。启动事件的 CloudTrail Insights 平均值是触发 Insights 事件的 API 上每分钟的调用率或错误率。通常情况下，这是异常活动的第一分钟。结束事件的 Insights 平均值是在开始 Insights 事件和结束 Insights 事件之间异常活动持续时间内，每分钟 API 调用的速率。

- 事件源：记录异常数量的 API 调用或错误的 AWS 服务端点。在前面的图像中，源是 `ec2.amazonaws.com`，它是 Amazon EC2 的服务终端节点。
- 事件 ID：
  - Start event ID（开始事件 ID）– 异常活动开始时记录的 Insights 事件 ID。
  - End event ID（结束事件 ID）– 异常活动结束时记录的 Insights 事件 ID。
  - 共享事件 ID-在 Insights 事件中，共享事件 ID 是 Insights 生成的 GUID，用于唯一标识 CloudTrail Insights 事件的开始和结束对。Shared event ID（共享事件 ID）在开始和结束 Insights 事件之间是通用的，并且有助于在这两个事件建立关联以唯一地标识异常活动。

3. 选择 Attributions（归因）选项卡，可查看有关与异常活动和基准活动相关的用户身份、用户代理、API 调用率 Insights 事件和错误代码的信息。在 Attributions（归因）选项卡上的表格中显示最多五个用户身份、五个用户代理和五个错误代码，按活动计数的平均值，从最高到最低的降序排列。有关 Attributions（归因）选项卡的更多信息，请参阅本指南中的 Attributions（属性）选项卡 和 CloudTrail 见解`insightDetails`元素。
4. 在CloudTrail 事件选项卡上，查看相关事件，这些事件 CloudTrail经过分析以确定发生了异常活动。默认情况下，已对 Insights 事件名称应用了筛选条件，该名称也是相关 API 的名称。CloudTrail 事件选项卡显示在 Insights 事件的开始时间（减去一分钟）和结束时间（加一分钟）之间发生的与主题 API 相关的 CloudTrail 管理事件。

   当您在图表中选择其他 Insights 事件时，事件表中显示CloudTrail 的事件会发生变化。这些事件可帮助您执行更深入的分析，以确定 Insights 事件的可能原因以及异常 API 活动的原因。

   要显示在 Insights 事件持续时间内记录的所有 CloudTrail 事件，而不仅仅是相关 API 的事件，请关闭过滤器。
5. 选择 Insights event record（Insights 事件记录）选项卡以查看 JSON 格式的 Insights 开始和结束事件。
6. 选择链接的 Event source（事件源）将返回由该事件源筛选的 Insights（见解）页面。

缩放、平移和下载图表

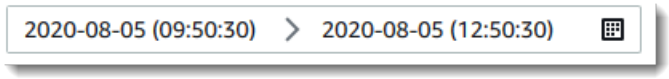
您可以使用右上角的工具栏缩放、平移和重置 Insights 事件详细信息页面上图表的轴。

从左到右，图表工具栏上的命令按钮执行以下操作：

- Download plot as a PNG (以 PNG 格式下载图表) - 下载详细信息页面上显示的图表图像，并将其保存为 PNG 格式。
- Zoom (缩放) - 拖动以选择图表上要放大的区域并更详细地查看。
- Pan (平移) - 移动图表以查看相邻的日期或时间。
- Reset axes (重置轴) - 将图表轴更改回原始状态，同时清除缩放和平移设置。

更改图表时间跨度设置

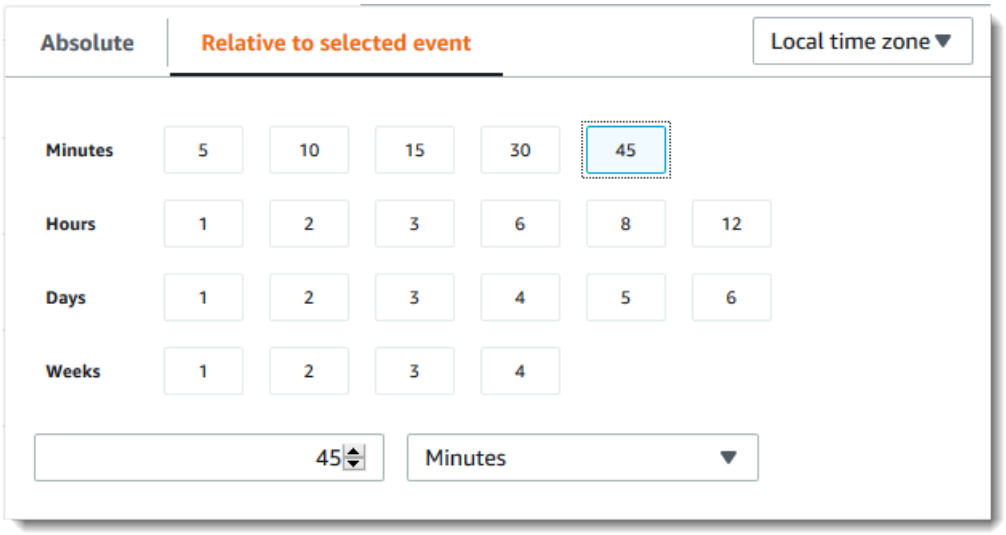
您可以更改时间跨度 - 事件显示在 x 轴上的所选持续时间 - 通过选择图表右上角的设置显示在图表中。



图表中显示的默认时间跨度取决于所选 Insights 事件的持续时间。

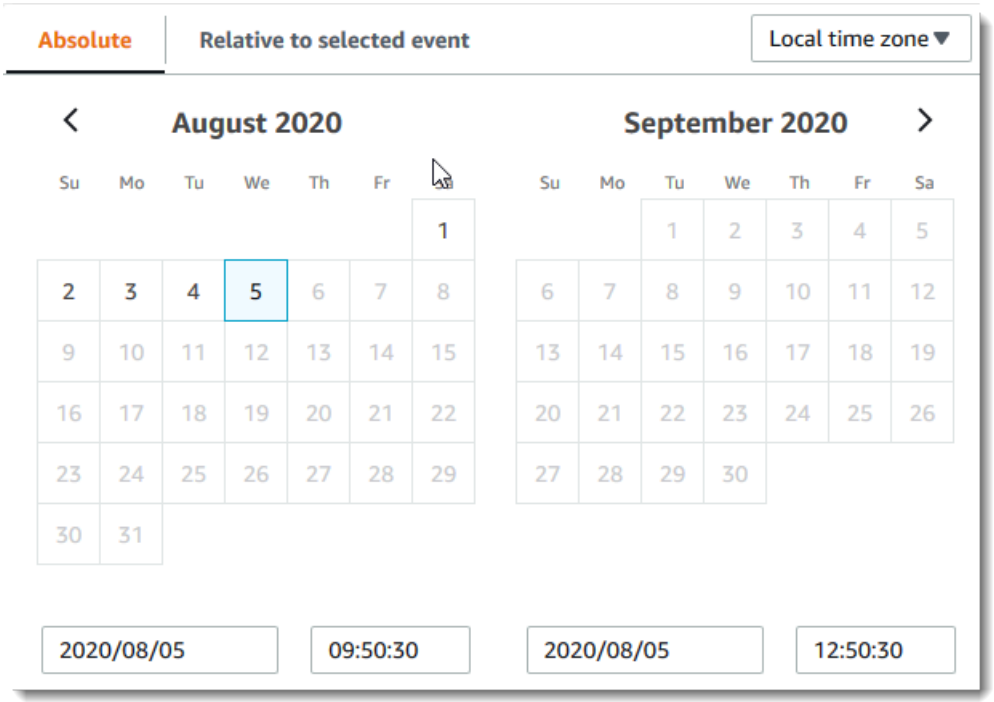
Insights 活动的持续时间	默认时间跨度
小于 4 小时	3h（三小时）
4 至 12 小时之间	12h（12 小时）
12 至 24 小时之间	1d（一天）
24 至 72 小时之间	3d（三天）
超过 72 小时	1w（一周）

您可以选择 5 分钟、30 分钟、1 小时、3 小时、12 小时或 Custom（自定义）。下图显示了 Relative to selected event（相对于所选事件）时间段，您可以在 Custom（自定义）设置中选择。相对时间段是在 Insights 事件详细信息页面上显示的所选 Insights 事件的开始和结束前后的大致时间段。



要自定义选定的预设，请在预设下方的框中指定数值和时间单位。

要指定确切的日期和时间范围，请选择 Absolute (绝对) 选项卡。如果设置绝对日期和时间范围，则需要提供开始和结束时间。有关如何设置时间的信息，请参阅本主题中的 the section called “筛选 Insights 事件”。



下载 Insights 事件

您可以采用 CSV 或 JSON 格式的文件形式下载记录的 Insights 事件历史记录。使用筛选条件和时间范围可减小您下载的文件的大小。

> **Note**
>
> CloudTrail 事件历史文件是包含可由个人用户配置的信息（例如资源名称）的数据文件。有些数据在用来读取和分析该数据的程序中有可能被解释为命令 (CSV 注入)。例如，将 CloudTrail 事件导出为 CSV 并导入到电子表格程序时，该程序可能会警告您注意安全问题。作为安全最佳实践，请禁用来自下载的事件历史记录文件中的链接或宏。

1. 指定要下载的事件的筛选条件和时间范围。例如，您可以指定事件名称 `StartInstances`，并指定时间范围为过去 3 天的活动。
2. 选择 Download events（下载事件），然后选择 Download CSV（下载 CSV）或 Download JSON（下载 JSON）。系统会提示您选择保存文件的位置。

   > **Note**
   >
   > 您的下载可能需要一点时间才能完成。要想更快地获得结果，在开始下载过程前，可使用更加具体的筛选条件或更短的时间范围来缩小结果范围。

3. 下载完成后，打开文件以查看您指定的事件。
4. 要取消下载，请选择 Cancel download (取消下载)。如果在下载完成之前取消下载，则本地计算机上的 CSV 或 JSON 文件可能只包含部分事件。

使用查看路径的 CloudTrail Insights 事件 AWS CLI

你可以通过运行aws cloudtrail lookup-events命令来查找过去 90 天的 Ins CloudTrail ights 事件。此 `lookup-events` 命令具有以下选项：

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`

- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

有关使用的一般信息 AWS Command Line Interface，请参阅《AWS Command Line Interface 用户指南》。

目录

- 先决条件
- 获取命令行帮助
- 查找 Insights 事件
- 指定要返回的 Insights 事件数量
- 按时间范围查找 Insights 事件
- 按属性查找 Insights 事件
  - 属性查找示例
- 指定下一页结果
- 从文件中获取 JSON 输入
- 查找输出字段

先决条件

- 要运行 AWS CLI 命令，必须安装 AWS CLI。有关更多信息，请参阅入门 AWS CLI。
- 确保您的 AWS CLI 版本高于 1.6.6。要验证 CLI 版本，请在命令行上运行 aws --version。
- 要为 AWS CLI 会话设置账户、区域和默认输出格式，请使用aws configure命令。有关更多信息，请参阅配置 AWS 命令行界面。
- 要针对 API 调用量记录 Insights 事件，跟踪必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，跟踪必须记录 `read` 或 `write` 管理事件。

> **Note**
>
> 这些 CloudTrail AWS CLI 命令区分大小写。

获取命令行帮助

要查看 lookup-events 的命令行帮助，请键入以下命令。

```
aws cloudtrail lookup-events help
```

查找 Insights 事件

要查看最新的 10 个 Insights 事件，请键入以下命令。

```
aws cloudtrail lookup-events --event-category insight
```

返回的事件看起来与下面的示例相似，

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.07",
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
```

```
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "userAgent",
                  "insight": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "errorCode",
```

```
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      },
      {
          "eventVersion": "1.07",
          "eventTime": "2019-10-15T21:14:00Z",
          "awsRegion": "us-east-1",
          "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
          "eventType": "AwsCloudTrailInsight",
          "recipientAccountId": "123456789012",
          "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
          "insightDetails": {
          "state": "End",
          "eventSource": "autoscaling.amazonaws.com",
          "eventName": "CompleteLifecycleAction",
          "insightType": "ApiCallRateInsight",
          "insightContext": {
            "statistics": {
              "baseline": {
                "average": 0.0000882145
              },
              "insight": {
                "average": 0.6
              },
              "insightDuration": 5,
              "baselineDuration": 11336
            },
            "attributions": [
              {
```

```
                    "attribute": "userIdentityArn",
                    "insight": [
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                        "average": 0.2
                      },
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                        "average": 0.2
                      },
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                        "average": 0.2
                      }
                    ],
                    "baseline": [
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "userAgent",
                    "insight": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "errorCode",
                    "insight": [
```

```
                    {
                      "value": "null",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "null",
                      "average": 0.0000882145
                    }
                  ]
                }
              ]
            }
          },
            "eventCategory": "Insight"
        }
    ]
}
```

有关输出中与查找相关的字段的说明，请参阅这一主题中的查找输出字段部分。有关 Insights 事件中的字段的说明，请参阅 CloudTrail 录制内容。

指定要返回的 Insights 事件数量

要指定要返回的事件数目，请键入以下命令。

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

如果未指定，则 *<integer>* 的默认值为 10。可能的值介于 1 和 50 之间。以下示例返回一个结果。

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

按时间范围查找 Insights 事件

可查找过去 90 天发生的 Insights 事件。要指定时间范围，请键入以下命令。

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>* 指定仅返回在指定时间或之后（采用 UTC）发生的 Insights 事件。如果指定的开始时间晚于指定的结束时间，则将返回错误。

`--end-time` *`<timestamp>`* 指定仅返回在指定时间或之前（采用 UTC）发生的 Insights 事件。如果指定的结束时间早于指定的开始时间，则将返回错误。

默认开始时间为过去 90 天内提供数据的最早日期。默认结束时间为在最接近当前时间发生事件的时间。

所有时间戳均采用 UTC 显示。

按属性查找 Insights 事件

要按属性进行筛选，请键入以下命令。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

您只能为每个 lookup-events 命令指定一个属性密钥-值对。以下是 `AttributeKey` 的有效 Insights 事件值。值的名称区分大小写。

- `EventId`
- `EventName`
- `EventSource`

的最大长度`AttributeValue`为 2000 个字符。在 2000 个字符限制中，以下字符（`_ ,'`、`'\\n '`、`'`、`'`）算作两个字符。

属性查找示例

以下示例命令返回 `EventName` 值为 `PutRule` 的 Insights 事件。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

以下示例命令返回 `EventId` 值为 `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002` 的 Insights 事件。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

以下示例命令返回 `EventSource` 值为 `iam.amazonaws.com` 的 Insights 事件。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

指定下一页结果

要从 lookup-events 命令获取下一页结果，请键入以下命令。

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

在此命令中，*<timestamp>* 的值来自于上一个命令输出的第一个字段。

在命令中使用 --next-token 时，您必须使用与上一个命令中相同的参数。例如，假设您运行以下命令。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

要获取下一页结果，您的下一个命令将如下所示。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

从文件中获取 JSON 输入

AWS CLI 对于某些 AWS 服务，有两个参数，即--generate-cli-skeleton和--cli-input-json，可用于生成 JSON 模板，您可以修改该模板并将其用作--cli-input-json参数的输入。本部分介绍如何将这些参数和 aws cloudtrail lookup-events 结合使用。有关更多信息，请参阅AWS CLI 骨架和输入文件。

通过从文件中获取 JSON 输入来查找 Insights 事件

1. 通过将 lookup-events 输出重定向到文件来创建与 --generate-cli-skeleton 结合使用的输入模板，如以下示例所示。

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   生成的模板文件（在本例中为 LookupEvents .txt）如下所示。

```
{
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. 可使用文本编辑器根据需要修改 JSON。JSON 输入只能包含指定的值。

> **Important**
>
> 必须先从模板中删除所有空值，然后才能使用该模板。

以下示例指定一个时间范围和要返回的结果的最大数目。

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. 要将编辑后的文件用作输入，请使用语法 `--cli-input-json file://<filename>`，如以下示例所示。

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> 您可在 `--cli-input-json` 所在的命令行中使用其他参数。

查找输出字段

事件

基于查找属性和已指定的时间范围的查找事件的列表。该事件列表按时间进行排序，最新的事件排在第一位。每个条目都包含有关查找请求的信息，并包含检索到 CloudTrail 的事件的字符串表示形式。

以下条目描述每个查找事件中的字段。

CloudTrailEvent

一个包含已返回事件的对象表示形式的 JSON 字符串。有关已返回的每个元素的信息，请参阅记录正文内容。

EventId

一个包含已返回事件的 GUID 的字符串。

EventName

一个包含已返回事件的名称的字符串。

EventSource

向其发出请求的 AWS 服务。

EventTime

事件的日期和时间（采用 UNIX 时间格式）。

资源

由已返回的事件引用的资源列表。每个资源条目指定一个资源类型和一个资源名称。

ResourceName

一个包含由事件引用的资源名称的字符串。

ResourceType

一个包含由事件引用的资源类型的字符串。如果无法确定资源类型，则返回 null。

用户名

一个包含已返回事件的账户用户名称的字符串。

NextToken

用于从上一个 `lookup-events` 命令获取下一页结果的字符串。要使用该令牌，参数必须与原始命令中的参数相同。如果输出中未显示任何 `NextToken` 条目，则不再返回结果。

有关 CloudTrail Insights 事件的更多信息，请参阅本指南记录 Insights 事件中的。

将追踪事件复制到 CloudTrail湖中

您可以将现有跟踪事件复制到 CloudTrail Lake 事件数据存储中，以创建记录到跟踪的事件的 point-in-time快照。复制跟踪事件不会干扰跟踪记录事件的功能，也不会以任何方式修改跟踪。

您可以将跟踪事件复制到为事件配置的现有 CloudTrail 事件数据存储中，也可以创建新的 CloudTrail 事件数据存储并选择复制跟踪事件选项作为事件数据存储创建的一部分。有关将跟踪事件复制到现有事件数据存储的更多信息，请参阅 使用 CloudTrail 控制台将跟踪事件复制到现有的事件数据存储中。有关创建新的事件数据存储的更多信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储。

将跟踪事件复制到 CloudTrail Lake 事件数据存储允许您对复制的事件运行查询。 CloudTrail 与事件历史记录或运行`LookupEvents`中的简单键和值查找相比，Lake 查询提供了更深入、更可自定义的事件视图。有关 CloudTrail Lake 的更多信息，请参阅与 L AWS CloudTrail ake 合作。

如果您要将跟踪事件复制到组织事件数据存储，则必须使用该组织的管理账户。您不能使用组织的委托管理员账户复制跟踪事件。

CloudTrail 湖泊事件数据存储会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价和管理 Lake 成本的信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 湖泊成本。

将跟踪事件复制到 CloudTrail Lake 事件数据存储时，会根据事件数据存储提取的未压缩数据量产生费用。

将跟踪事件复制到 CloudTrail Lake 时， CloudTrail 解压缩以 gzip（压缩）格式存储的日志，然后将日志中包含的事件复制到您的事件数据存储中。未压缩数据的大小可能大于 S3 的实际存储大小。要对未压缩数据的大小进行总体估计，可以将 S3 存储桶中日志的大小乘以 10。

您可以通过为复制的事件指定更窄的时间范围来降低成本。如果您计划仅使用事件数据存储来查询复制的事件，则可以关闭事件摄取，以免对将来的事件产生费用。有关更多信息，请参阅 AWS CloudTrail 定价 和 管理 CloudTrail 湖泊成本。

SCENARIOS（场景）

下表描述了复制跟踪事件的一些常见场景，以及如何使用控制台完成每个场景。

场景	如何在控制台中完成此操作？
无需摄取新事件即可分析和查询 CloudTrail Lake 中的历史轨迹事件	在创建事件数据存储时，创建新的事件数据存储并选择复制跟踪事件选项。创建事件数据存储时，请取消选择摄取事件（程序的步骤 15），以确保事件数据存储仅包含跟踪的历史事件，不包含未来事件。
将现有跟踪替换为 CloudTrail Lake 事件数据存储	使用与您的跟踪相同的事件选择器创建事件数据存储，以确保事件数据存储与跟踪具有相同的覆盖范围。 为避免源跟踪和目标事件数据存储之间存在重复事件，请为复制的事件选择一个早于事件数据存储创建时间的时间范围。 创建事件存储后，您可以关闭跟踪的日志记录，避免产生额外费用。

主题

- 复制跟踪事件的注意事项
- 复制跟踪事件所需的权限
- 使用 CloudTrail 控制台将跟踪事件复制到现有的事件数据存储中

复制跟踪事件的注意事项

复制跟踪事件时，请将以下因素考虑在内。

- 复制跟踪事件时， CloudTrail 使用 S3 `GetObject`API 操作检索源 S3 存储桶中的跟踪事件。有些 S3 归档存储类，例如 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Outposts 和 S3 Intelligent-Tiering Deep Archive 层，无法使用 `GetObject` 来访问。要复制存储在这些归档存储类中的跟踪事件，必须先使用 S3 `RestoreObject` 操作还原副本。有关还原已归档的对象的信息，请参阅《Amazon S3 用户指南》中的恢复已归档的对象。
- 将跟踪事件复制到事件数据存储时， CloudTrail 无论目标事件数据存储的事件类型、高级事件选择器或 AWS 区域的配置如何，都会复制所有跟踪事件。
- 在将跟踪事件复制到现有的事件数据存储之前，请确保根据您的应用场景适当配置了事件数据存储的定价选项和保留期。

  - 定价选项：定价选项决定了摄取和存储事件的成本。有关定价选项的更多信息，请参阅 AWS CloudTrail 定价和 事件数据存储定价选项。
  - 保留期：保留期限决定事件数据在事件数据存储中保存多长时间。 CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`*）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。
- 如果您要将跟踪事件复制到事件数据存储中进行调查，并且不想摄取任何未来事件，则可以停止对事件数据存储的摄取。创建事件数据存储时，请取消选择摄取事件选项（程序的步骤 15），以确保事件数据存储仅包含跟踪的历史事件，不包含未来事件。
- 在复制跟踪事件之前，请禁用任何附加到源 S3 存储桶的访问控制列表（ACL），并更新目标事件数据存储的 S3 存储桶策略。有关更新 S3 存储桶策略的更多信息，请参阅 复制跟踪事件所用的 Amazon S3 存储桶策略。有关禁用 ACL 的更多信息，请参阅为您的存储桶控制对象所有权和禁用 ACL。
- CloudTrail 仅复制源 S3 存储桶中的 Gzip 压缩日志文件中的跟踪事件。 CloudTrail 不会从未压缩的日志文件或使用 Gzip 以外的格式压缩的日志文件中复制跟踪事件。
- 为避免源跟踪和目标事件数据存储之间存在重复事件，请为复制的事件选择一个早于事件数据存储创建时间的时间范围。
- 默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的前缀，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，则必须在复制跟踪事件时选择前缀。
- 要将跟踪事件复制到组织事件数据存储，必须使用该组织的管理账户。您不能使用委托管理员账户将跟踪事件复制到组织事件数据存储。

复制跟踪事件所需的权限

在复制跟踪事件之前，请确保您拥有 IAM 角色的所有必需权限。如果您选择现有 IAM 角色来复制跟踪事件，则只需要更新 IAM 角色权限。如果您选择创建新的 IAM 角色，请为该角色 CloudTrail 提供所有必要的权限。

如果源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密存储桶中的数据。如果源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。

主题

- 复制跟踪事件所需的 IAM 权限
- 复制跟踪事件所用的 Amazon S3 存储桶策略
- 用于解密源 S3 存储桶中数据的 KMS 密钥政策

复制跟踪事件所需的 IAM 权限

复制跟踪事件时，您可以选择创建新的 IAM 角色，也可以使用现有 IAM 角色。当您选择新的 IAM 角色时， CloudTrail 会创建一个具有所需权限的 IAM 角色，您无需采取任何进一步的操作。

如果您选择现有角色，请确保 IAM 角色的策略 CloudTrail 允许从源 S3 存储桶复制跟踪事件。此部分提供所需 IAM 角色权限和信任策略的示例。

以下示例提供了权限策略，该策略 CloudTrail 允许从源 S3 存储桶复制跟踪事件。将 *myBucketNamemyAccountID*、*##*、*##*和 *eventDataStoreID* 替换为适合您的配置的值。*myAccountID* 是用于 CloudTrail Lake 的 AWS 账户 ID，它可能与 S3 存储桶的 AWS 账户 ID 不同。

将 *key-region#keyAccountID* 和 *keyID* 替换为用于加密源 S3 存储桶的 KMS 密钥的值。如果源 S3 存储桶未使用 KMS 密钥进行加密，则可省略 AWSCloudTrailImportKeyAccess 语句。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
```

```
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

以下示例提供了 IAM 信任策略，该策略 CloudTrail 允许代入 IAM 角色从源 S3 存储桶复制跟踪事件。将 *myAccountID*、*##*和 *eventDataStoreID* 替换为适合您的配置的值。*myAccountID* 是用于 CloudTrail Lake 的 AWS 账户 ID，它可能与 S3 存储桶的 AWS 账户 ID 不同。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
```

```
      }
    }
  ]
}
```

复制跟踪事件所用的 Amazon S3 存储桶策略

默认情况下，Simple Storage Service（Amazon S3）存储桶和对象都是私有的。仅资源所有者（创建存储桶的 AWS 账户）能够访问存储桶及其包含的对象。资源所有者可以通过编写访问策略来向其他资源和用户授予访问权。

在复制跟踪事件之前，必须更新 S3 存储桶策略 CloudTrail 以允许从存储桶复制跟踪事件。

您可以在 S3 存储桶策略中添加以下语句以授予这些权限。将 *roLearn* 和，*myBucketName*替换为适合您的配置的值。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

用于解密源 S3 存储桶中数据的 KMS 密钥政策

如果源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 提供从启用了 SSE-KMS 加密的 S3 存储桶复制跟踪事件所需的`kms:Decrypt`和`kms:GenerateDataKey`权限。如果源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略。更新 KMS 密钥策略 CloudTrail 允许解

密源 S3 存储桶中的数据，运行验证检查以确保事件符合 CloudTrail标准，并将事件复制到 CloudTrail Lake 事件数据存储中。

以下示例提供了 KMS 密钥策略，该策略 CloudTrail 允许解密源 S3 存储桶中的数据。将 *roLearn*、*myBucketName*、*myAccount eventDataStoreID#regi on # Id* 替换为适合您的配置的值。*myAccountID* 是用于 CloudTrail Lake 的 AWS 账户 ID，它可能与 S3 存储桶的 AWS 账户 ID 不同。

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

使用 CloudTrail 控制台将跟踪事件复制到现有的事件数据存储中

按照以下程序将跟踪事件复制到事件数据存储中。有关如何创建新的事件数据存储的信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储。

> **Note**
>
> 在将跟踪事件复制到现有的事件数据存储之前，请确保根据您的应用场景适当配置了事件数据存储的定价选项和保留期。

- 定价选项：定价选项决定了摄取和存储事件的成本。有关定价选项的更多信息，请参阅 AWS CloudTrail 定价和 事件数据存储定价选项。
- 保留期：保留期限决定事件数据在事件数据存储中保存多长时间。 CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。要确定适当的保留期，请计算要复制的最早事件（以天为单位）和要在事件数据存储中保留这些事件的天数（保留期 = *`oldest-event-in-days`*+ *`number-days-to-retain`*）的总和。例如，如果您要复制的最早事件已有 45 天，并且您想将事件在事件数据存储中再保留 45 天，则可以将保留期设置为 90 天。

要将跟踪事件复制到事件数据存储

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 控制台的左侧导航窗格中选择 T rail s。
3. 在 Trails（跟踪）页面上，选择跟踪，然后选择 Copy events to Lake（将事件复制到 Lake）。如果跟踪的源 S3 存储桶使用 KMS 密钥进行数据加密，请确保 KMS 密钥策略 CloudTrail 允许解密存储桶中的数据。如果源 S3 存储桶使用多个 KMS 密钥，则必须更新每个密钥的策略 CloudTrail 以允许解密存储桶中的数据。有关更新 KMS 密钥政策的更多信息，请参阅 用于解密源 S3 存储桶中数据的 KMS 密钥政策。
4. （可选）默认情况下， CloudTrail 仅复制 S3 存储桶`CloudTrail`前缀中包含 CloudTrail 的事件和`CloudTrail`前缀中的事件，而不检查其他 AWS 服务的前缀。如果要复制其他前缀中包含 CloudTrail 的事件，请选择 Enter S3 URI，然后选择 Browse S3 浏览到该前缀。

   S3 存储桶策略必须授予对复制跟踪事件的 CloudTrail 访问权限。有关更新 S3 存储桶策略的更多信息，请参阅 复制跟踪事件所用的 Amazon S3 存储桶策略。
5. 在“指定事件的时间范围”中，选择复制事件的时间范围。 CloudTrail 在尝试复制跟踪事件之前，请检查前缀和日志文件名以验证该名称是否包含所选开始日期和结束日期之间的日期。您可以选择 Relative range（相对范围）或者 Absolute range（绝对范围）。为避免源跟踪和目标事件数据存储之间存在重复事件，请选择一个早于事件数据存储创建时间的时间范围。

> **Note**
>
> CloudTrail 仅复制在事件数据存储保留期`eventTime`内的跟踪事件。例如，如果事件数据存储的保留期为 90 天，则 CloudTrail 不会复制任何`eventTime`超过 90 天的跟踪事件。

- 如果选择 “相对范围”，则可以选择复制过去 6 个月、1 年、2 年、7 年或自定义范围内记录的事件。 CloudTrail 复制选定时间段内记录的事件。
- 如果选择 “绝对范围”，则可以选择特定的开始和结束日期。 CloudTrail 复制在所选开始日期和结束日期之间发生的事件。

6. 对于 Delivery location（送达位置），请从下拉列表中选择目标事件数据存储。
7. 对于 Permissions（权限），请从以下 IAM 角色选项中进行选择。如果您选择现有的 IAM 角色，请验证 IAM 角色策略是否提供了必要的权限。有关更新 IAM 角色权限的更多信息，请参阅 复制跟踪事件所需的 IAM 权限。

   - 选择 Create a new role (recommended)（创建新角色（推荐））以创建新的 IAM 角色。对于 Enter IAM role name（输入 IAM 角色名称），输入角色的名称。 CloudTrail 会自动为这个新角色创建必要的权限。
   - 选择使用自定义 IAM 角色 ARN 以使用未列出的自定义 IAM 角色。对于 Enter IAM role ARN（输入 IAM 角色 ARN），输入 IAM ARN。
   - 从下拉列表中选择现有的 IAM 角色。

8. 选择 Copy events（复制事件）。
9. 系统将提示您确认复制。如果您已准备好确认，请选择 Copy trail events to Lake（将跟踪事件复制到 Lake），然后选择 Copy events（复制事件）。
10. 在 Copy details（复制详情）页面中，您可以查看复制状态并检查是否复制失败。跟踪事件复制完成后，如果复制未出错，则 Copy status（复制状态）将设置为 Completed（已完成），否则如果出错了，则设置为 Failed（失败）。

    > **Note**
    >
    > 事件复制详细信息页面上显示的详细信息不是实时的。Prefixes copied（已复制的前缀）等详细信息的实际值可能高于页面上显示的值。 CloudTrail 在事件副本的过程中以增量方式更新详细信息。

11. 如果 Copy status（复制状态）为 Failed（失败），则要先修复 Copy failures（复制失败）中显示的所有错误，然后选择 Retry copy（重试复制）。当您重试复制时，会在出现故障的位置 CloudTrail 恢复副本。

有关查看跟踪事件复制详细信息的更多信息，请参阅 事件复制详细信息。

获取和查看您的 CloudTrail 日志文件

创建跟踪并将其配置为捕获所需的日志文件后，您需要能够找到日志文件并解读其中包含的信息。

CloudTrail 将您的日志文件传输到您在创建跟踪时指定的 Amazon S3 存储桶。 CloudTrail 通常在 API 调用后的平均大约 5 分钟内传送日志。此时间并不能得到保证。有关更多信息，请参阅 AWS CloudTrail 服务等级协议。Insights 事件通常会在异常活动后 30 分钟内传递到您的存储桶。首次启用 Insights 事件后，如果检测到异常活动，请留出长达 36 小时来查看第一个 Insights 事件。

> **Note**
>
> 如果您错误配置了跟踪（例如，无法访问 S3 存储桶），则 CloudTrail 会尝试将日志文件重新传送到您的 S3 存储桶，持续 30 天，这些 attempted-to-deliver 事件将按标准费用收费。CloudTrail 为避免配置错误的跟踪产生费用，您需要删除跟踪。

主题

- 正在查找您的 CloudTrail 日志文件
- 正在下载您的 CloudTrail 日志文件

正在查找您的 CloudTrail 日志文件

CloudTrail 以 gzip 存档的形式将日志文件发布到您的 S3 存储桶。在 S3 存储桶中，日志文件的名称较为格式化，一般包含以下元素：

- 您在创建跟踪时指定的存储桶名称（可在 CloudTrail 控制台的 Trails 页面上找到）
- （可选）创建跟踪时指定的前缀
- 字符串 “AWSLogs”
- 账号
- 字符串 “CloudTrail”
- 区域标识符（如 us-west-1）
- 日志文件的发布年份（采用 YYYY 格式）
- 日志文件的发布月份（采用 MM 格式）
- 日志文件的发布日（采用 DD 格式）
- 一个字母数字字符串，用于区别该文件与覆盖相同时段的其他文件

以下示例显示完整的日志文件对象名称：

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> 对于组织跟踪，S3 存储桶中的日志文件对象名称包括路径中的组织单位 ID，如下所示：
>
> ```
> bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

要检索日志文件，可以使用 Simple Storage Service（Amazon S3）控制台、Simple Storage Service（Amazon S3）命令行界面（CLI）或 API。

使用 Simple Storage Service（Amazon S3）控制台查找您的日志文件

1. 打开 Simple Storage Service（Amazon S3）控制台。
2. 选择您指定的存储桶。
3. 在对象层次结构中导航，直到找到需要的日志文件。

   所有日志文件的扩展名都是 .gz。

您将看到一个与下面示例类似的对象层次结构，但具体存储桶名称、账户 ID、区域和日期有所不同。

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

上述对象层次结构的日志文件将与以下内容类似：

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> 您可能会收到包含一个或多个重复事件的日志文件，但这种情况不常见。在大多数情况下，重复的事件将具有相同的 `eventID`。有关 `eventID` 字段的更多信息，请参阅CloudTrail 录制内容。

正在下载您的 CloudTrail 日志文件

日志文件采用 JSON 格式。如果您安装了 JSON 查看器加载项，则可以直接在浏览器中查看这些文件。在存储桶中双击日志文件名可打开一个新的浏览器窗口或选项卡。JSON 以可读格式显示。

CloudTrail 日志文件是 Amazon S3 对象。您可以使用 Amazon S3 控制台、 AWS Command Line Interface (CLI) 或 Amazon S3 API 来检索日志文件。

有关更多信息，请参阅《亚马逊简单存储服务用户指南》中的 Amazon S3 对象概述。

下面的过程介绍如何使用 AWS Management Console下载日志文件。

下载和读取日志文件

1. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
2. 选择存储桶并选择要下载的日志文件。
3. 选择 Download 或 Download as，然后按照提示保存文件。这将以压缩格式保存文件。

   > **Note**
   >
   > 某些浏览器 (如 Chrome) 会自动为您提取日志文件。如果您的浏览器有这种功能，请跳到步骤 5。

4. 使用某种产品 (如 7-Zip) 来提取日志文件。
5. 在文本编辑器 (如 Notepad++) 中打开日志文件。

有关可显示在日志文件条目中的事件字段的更多信息，请参阅 CloudTrail 录制内容。

AWS 与第三方日志和分析专家合作，提供使用 CloudTrail 输出的解决方案。有关更多信息，请参阅AWS CloudTrail 合作伙伴。

> **Note**
>
> 您也可以使用 Event history 功能来查找过去 90 天内的创建、更新和删除 API 活动的事件。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。

配置 Amazon SNS 通知 CloudTrail

当您向 Amazon S3 存储桶 CloudTrail 发布新的日志文件时，您会收到通知。您可以使用 Amazon Simple Notification Service (Amazon SNS) 管理通知。

通知是可选的。如果您需要通知，则可以配置 CloudTrail 为在发送新日志文件时向 Amazon SNS 主题发送更新信息。要接收这些通知，可使用 Amazon SNS 订阅该主题。作为订阅者，您可将更新发送到 Amazon Simple Queue Service (Amazon SQS) 队列，这使您能够以编程方式处理这些通知。

主题

- 配置 CloudTrail 为发送通知

配置 CloudTrail 为发送通知

您可以配置跟踪以使用 Amazon SNS 主题。您可以使用 CloudTrail 控制台或 aws cloudtrail create-trailCLI 命令来创建主题。 CloudTrail 为您创建 Amazon SNS 主题并附加相应的策略，以便 CloudTrail 有权发布该主题。

您在创建 SNS 主题名称时，该名称必须满足以下要求：

- 介于 1 到 256 个字符之间
- 包含大写和小写 ASCII 字母、数字、下划线或连字符

当您为适用于所有区域的跟踪配置通知时，来自所有区域的通知都将发送到您指定的 Amazon SNS 主题。如果您有一个或多个区域特定的跟踪，须为每个区域分别创建一个主题，并单独订阅每个主题。

要接收通知，请订阅使用的一个或多个 Amazon SNS 主题。 CloudTrail 您可以使用 Amazon SNS 控制台或 Amazon SNS CLI 命令执行此操作。有关更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的订阅 Amazon SNS 主题。

> **Note**
>
> CloudTrail 当日志文件写入 Amazon S3 存储桶时会发送通知。有效账户可以生成大量通知。如果您使用电子邮件或 SMS 进行订阅，可能会收到大量消息。建议您使用 Amazon Simple Queue Service (Amazon SQS) 进行订阅，以便能以编程方式处理通知。有关更多信息，请参阅 Amazon Simple Queue Service 开发人员指南中的将 Amazon SQS 队列订阅到 Amazon SNS 主题（控制台）。

Amazon SNS 通知包含一个 JSON 对象，该对象包括一个 `Message` 字段。此 `Message` 字段列出了日志文件的完整路径，如以下示例所示：

```
{
    "s3Bucket": "your-bucket-name","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

如果多个日志文件都传输到了 Amazon S3 存储桶，则一条通知中可能包括多个日志，如以下示例所示：

```
{
    "s3Bucket": "your-bucket-name",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

如果您选择通过电子邮件接收通知，则电子邮件的正文将包含 `Message` 字段的内容。有关 JSON 结构的信息，请参阅《亚马逊简单通知服务开发者指南》中的 Fanout to Amazon SQS 队列。只有该`Message`字段显示 CloudTrail 信息。其他字段包含来自 Amazon SNS 服务的信息。

如果您使用 CloudTrail API 创建跟踪，则可以通过`CreateTrail`或`UpdateTrail`操作指定要 CloudTrail 向其发送通知的现有 Amazon SNS 主题。您必须确保该主题存在，并且该主题具有允许 CloudTrail 向其发送通知的权限。请参阅 Amazon SNS 主题政策 CloudTrail。

其他 资源

有关 Amazon SNS 主题和订阅这些主题的更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

关于管理跟踪记录的提示

- 从 2019 年 4 月 12 日开始，只有在记录事件 AWS 区域 的地方才能看到跟踪。如果您创建了一个记录所有事件的跟踪 AWS 区域，则它将在控制台中显示在您正在处理的AWS 分区 AWS 区域中的所有内容中。如果您创建的跟踪仅记录单个事件 AWS 区域，则只能在该跟踪中查看和管理该跟踪 AWS 区域。
- 要编辑列表中的跟踪，请选择跟踪名称。
- 配置至少一条适用于所有区域的跟踪，这样您就可以接收来自您所在 AWS 分区中所有区域的日志文件。
- 要记录特定区域中的事件，并将日志文件传送至同一区域中的 S3 存储桶，您可以更新要应用于单区域的跟踪。如果您要分开保留日志文件，这是很有用的。例如，您可能希望用户在特定区域管理自己的日志，或者您可能希望按区域分隔 CloudWatch 日志警报。
- 要在一个跟踪中记录来自多个 AWS 账户的事件，请考虑在中创建组织， AWS Organizations 然后创建组织跟踪。
- 创建多个跟踪记录将会产生额外成本。有关价格的更多信息，请参阅 AWS CloudTrail 定价。

管理 CloudTrail 跟踪成本

作为最佳实践，我们建议您使用可帮助您管理 CloudTrail 成本的 AWS 服务和工具。您还可以以捕获所需数据的方式配置和管理 CloudTrail 跟踪，同时保持成本效益。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

可帮助管理成本的工具

AWS 预算是一项功能 AWS Billing and Cost Management，它允许您设置自定义预算，当您的成本或使用量超过（或预计超过）预算金额时，该预算会提醒您。

在创建多条跟踪时，建议使用 AWS 预算 CloudTrail 来创建预算，这可以帮助您跟踪 CloudTrail 支出。基于成本的预算有助于提高人们对可能要支付多少使用费用的认识。 CloudTrail 当您的账单达到您定义的阈值时，预算提醒会通知您。在收到预算提醒时，可以在账单周期结束之前进行更改以管理成本。

创建预算后，您可以使用 AWS Cost Explorer 来查看您的 CloudTrail 成本如何影响您的总 AWS 账单。在 AWS Cost Explorer 中， CloudTrail 添加到服务筛选器后，您可以按地区和账户将历史 CloudTrail支出与当前 month-to-date (MTD) 支出进行比较。此功能可帮助您监控和检测每月 CloudTrail支出中的意外成本。Cost Explorer 中的其他功能使您可以将 CloudTrail 支出与特定资源级别的每月支出进行比较，从而提供有关可能导致账单成本增加或减少的原因的信息。

> **Note**
>
> 尽管您可以将标签应用于 CloudTrail 跟踪，但目前 AWS Billing 无法使用应用于跟踪的标签进行成本分配。Cost Explorer 可以显示 CloudTrail 湖泊事件数据存储和整个 CloudTrail 服务的成本。

要开始使用 AWS 预算，请打开 AWS Billing and Cost Management，然后在左侧导航栏中选择预算。我们建议您在创建预算时配置预算提醒以跟踪 CloudTrail 支出。有关如何使用 AWS 预算的更多信息，请参阅使用管理成本 AWS Budgets和最佳实践 AWS Budgets。

跟踪配置

CloudTrail 让您可以灵活地在账户中配置跟踪。您在设置过程中做出的某些决定要求您了解 CloudTrail 账单会受到的影响。以下是跟踪配置如何影响 CloudTrail 账单的示例。

多跟踪创建

每个区域内管理活动的第一份副本是免费提供的。例如，如果您的账户有 2 条单区域跟踪，一条在us-east-1单区域跟踪，另一条跟踪在内us-west-2，则不 CloudTrail 收取任何费用，因为每个相应区域中只有一个跟踪记录事件。但是，如果您的账户有多区域跟踪和额外的单区域跟踪，则单区域跟踪将产生费用，因为多区域跟踪已经记录了每个区域的事件。

如果您创建更多跟踪，将相同的管理事件传送到其他目的地，则这些后续交付会产生 CloudTrail 成本。您可以这样做，以允许不同的用户组（例如开发人员、安全人员和 IT 审计员）接收其日志文件副本。对于数据事件，所有交付都会产生 CloudTrail 费用，包括第一次交付。

在创建更多跟踪记录时，熟悉日志并了解账户中的资源所生成的事件的类型和数量尤为重要。这可以帮助您预测与账户关联的事件的数量，并计划跟踪成本。例如，在 S3 存储桶上使用 AWS KMS

托管服务器端加密 (SSE-KMS) 可能会导致在中出现大量管理事件。 AWS KMS CloudTrail跨多个跟踪记录的大量事件也会影响成本。

为了帮助限制记录到您的跟踪中的事件数量，您可以通过在 “创建跟踪” 或 “更新跟踪” 页面上选择 “排除 AWS KMS 事件” AWS KMS 或 “排除 Amazon RDS 数据 API 事件” 来筛选出 Amazon RDS 数据 API 事件。使用基本事件选择器时，您只能筛选管理事件。但是，您可以使用高级事件选择器来同时筛选管理事件和数据事件。您可以使用高级事件选择器根据 `resources.type`、`eventName`、`resources.ARN` 和 `readOnly` 字段来包含或排除数据事件，从而使您能够仅记录感兴趣的数据事件。有关配置这些字段的更多信息，请参阅 AdvancedFieldSelector。有关创建和更新跟踪记录的更多信息，请参阅本指南中的 创建跟踪 或 更新跟踪。

AWS Organizations

当您使用设置 Organizations 跟踪时 CloudTrail， CloudTrail 会将该跟踪复制到组织内的每个成员账户。除了成员账户中的任何现有跟踪记录之外，还会创建新的跟踪记录。确保组织跟踪的配置与您希望为组织中的所有账户配置跟踪的方式匹配，因为组织跟踪配置会传播到所有账户。

由于 Organizations 在每个成员账户中创建一个跟踪，因此，创建额外跟踪以收集与 Organizations 跟踪相同的管理事件的单个成员账户将收集第二个事件副本。将针对第二个副本向该账户收费。类似地，如果一个账户有一个多区域跟踪，并且在一单区域中创建第二个跟踪来收集与多区域跟踪相同的管理事件，则单区域中的跟踪将传送事件的第二个副本。第二个副本会产生费用。

另请参阅

- AWS CloudTrail 定价
- 通过以下方式管理成本 AWS Budgets
- 开始使用 Cost Explorer 成本管理服务
- 准备为您的组织创建跟踪

命名要求

本节提供有关 CloudTrail 资源、Amazon S3 存储桶和 KMS 密钥的命名要求的信息。

主题

- CloudTrail 资源命名要求
- Amazon S3 存储桶命名要求

- AWS KMS 别名命名要求

CloudTrail 资源命名要求

CloudTrail 资源名称必须满足以下要求：

- 仅包含 ASCII 字母（a-z，A-Z）、数字 (0-9)、句点 (.)、下划线 (_) 或短划线 (-)。
- 以字母或数字开头并以字母或数字结尾。
- 介于 3 到 128 个字符之间。
- 不具有相邻的句点、下划线或短划线。my-_namespace、my-\-namespace 之类的名称是无效的。
- 不能使用 IP 地址格式（例如，192.168.5.4）。

Amazon S3 存储桶命名要求

用于存储 CloudTrail 日志文件的 Amazon S3 存储桶的名称必须符合非美国标准区域的命名要求。Amazon S3 将存储桶名称定义为一个或多个标签（用句点分隔开）。有关命名规则的完整列表，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶命名规则。

以下是一些规则：

- 存储桶名称的长度介于 3 和 63 个字符之间，并且只能包含小写字母、数字、句点和短划线。
- 存储桶名称中的每个标签必须以小写字母或数字开头。
- 存储桶名称不能包含下划线、以短划线结束、包含连续句点或在句点旁边使用短划线。
- 存储桶名称不能采用 IP 地址格式 (198.51.100.24)。

> **Warning**
>
> 由于 S3 允许您的存储桶用作可公开访问的 URL，因此您选择的存储桶名称必须具有全局唯一性。如果您选择的名称已被其他一些账户用于创建存储桶，则必须使用其他名称。有关更多信息，请参阅 《Amazon Simple Storage Service 用户指南》中的存储桶限制。

AWS KMS 别名命名要求

创建时 AWS KMS key，可以选择别名来标识它。例如，您可以选择别名 “KMS-us-CloudTrail west-2” 来加密特定跟踪的日志。

别名必须满足以下要求：

- 介于 1 到 256 个（含）字符之间
- 包含字母数字字符（A-Z、a-z、0-9）、连字符 (-)、正斜杠 (/) 和下划线 (_)
- 不能以 aws 开头

有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥。

创建多个跟踪

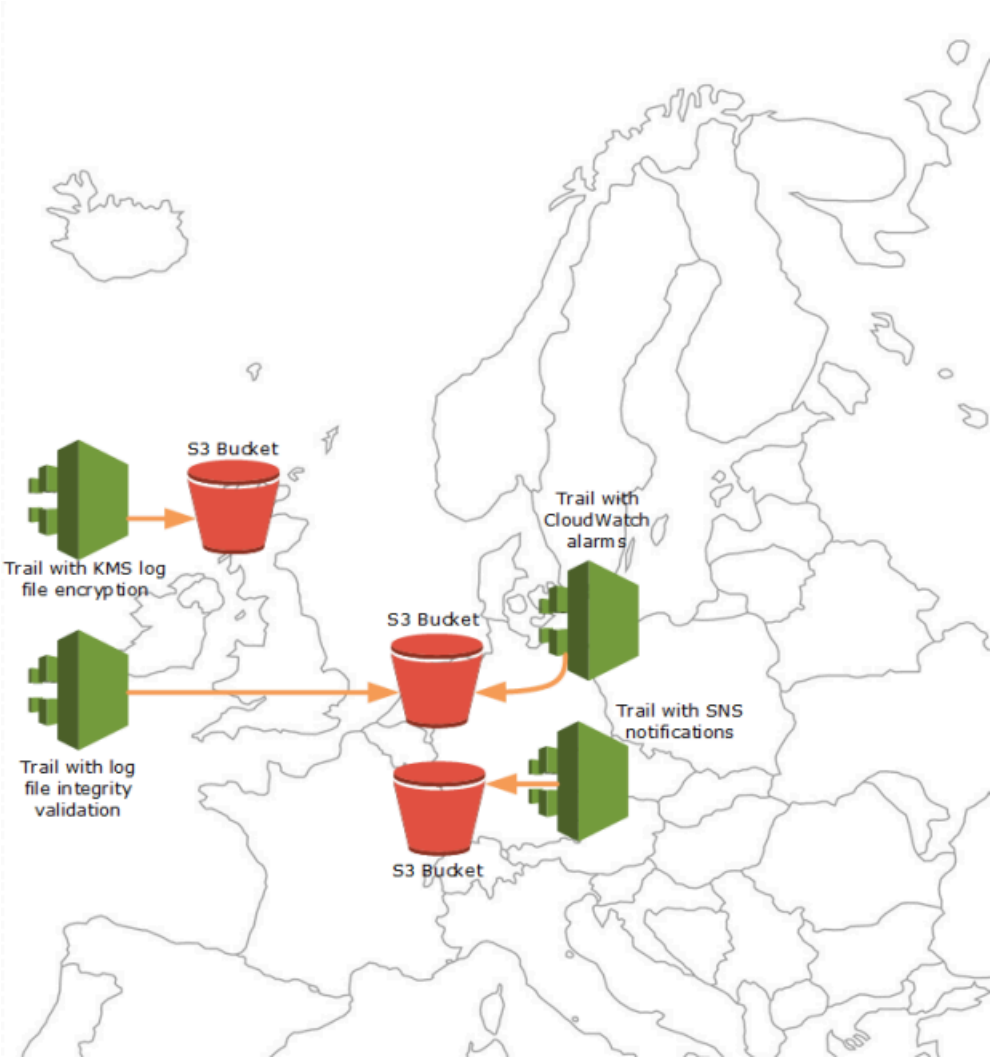
您可以使用 CloudTrail 日志文件来解决 AWS 账户中的操作或安全问题。您可以为不同用户创建跟踪，以便其创建和管理自己的跟踪。您可以将跟踪配置为将日志文件传送到单独的 S3 存储桶或共享的 S3 存储桶。

> **Note**
>
> 每个 AWS 区域 账户的管理事件的第一份副本是免费的。如果您创建更多跟踪，将相同的管理事件传送到其他目的地，则这些后续交付会产生 CloudTrail 成本。有关 CloudTrail 费用的更多信息，请参阅AWS CloudTrail 定价和管理 CloudTrail 跟踪成本。

例如，您可以具有以下用户：

- 安全管理员在欧洲（爱尔兰）区域创建跟踪并配置 KMS 日志文件的加密。此跟踪将日志文件传送到欧洲（爱尔兰）区域中的 S3 存储桶。
- IT 审计员在欧洲（爱尔兰）地区创建跟踪并配置日志文件完整性验证，以确保日志文件自 CloudTrail 交付以来没有发生变化。此跟踪配置为将日志文件传送到欧洲（法兰克福）区域中的 S3 存储桶
- 开发人员在欧洲（法兰克福）区域创建跟踪并配置 CloudWatch 警报以接收特定 API 活动的通知。此跟踪与针对日志文件完整性配置的跟踪共享同一个 S3 存储桶。
- 另一开发人员在注（法兰克福）区域中创建跟踪并配置 SNS。日志文件传输到欧洲（法兰克福）区域中的单独 S3 存储桶。

以下图像对示例进行了说明。



> **Note**
>
> 每次最多可以创建五条跟踪 AWS 区域。多区域跟踪计为每个区域一条跟踪。

您可以使用资源级权限来管理用户在上执行特定操作的能力。 CloudTrail

例如，您可以授予用户查看跟踪事件的许可，但限制其启动或者停止记录跟踪。您可以授予其他用户创建和删除跟踪的完整许可。这让您能够对跟踪和用户访问进行粒度控制。

有关资源级别许可的更多信息，请参阅示例：对针对特定跟踪记录的操作创建和应用策略。

有关多条跟踪的更多信息，请参阅CloudTrail 常见问题解答。

控制用户对 CloudTrail 跟踪的权限

AWS CloudTrail 与 AWS Identity and Access Management (IAM) 集成，可帮助您控制对 AWS 所需资源的访问权限 CloudTrail 和其他资源。 CloudTrail 这些资源的示例包括 Amazon S3 存储桶和 Amazon Simple Notification Service（Amazon SNS）主题。您可以使用 IAM 来控制哪些 AWS 用户可以创建、配置或删除 CloudTrail 跟踪、启动和停止日志记录以及访问包含日志信息的存储桶。要了解更多信息，请参阅适用于 Identity and Access 管理 AWS CloudTrail。

以下主题可帮助您了解权限、策略和 CloudTrail 安全性：

- 授予CloudTrail 管理权限
- Amazon S3 存储桶命名规则
- 适用于 Amazon S3 存储桶的政策 CloudTrail
- 使用为组织创建跟踪 AWS Command Line Interface中适用于组织跟踪的存储桶策略示例。
- Amazon SNS 主题政策 CloudTrail
- 使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)
- 复制跟踪事件所需的权限
- 指定委托管理员所需的权限
- 在 CloudTrail 控制台中创建的默认 KMS 密钥策略
- 授予在 CloudTrail 控制台上查看 AWS Config 信息的权限
- 在 AWS 账户之间共享 CloudTrail 日志文件
- 创建组织跟踪所需的权限
- 使用以前存在的 IAM 角色向 Amazon 日志添加对组织跟踪的监控 CloudWatch

AWS CloudTrail 与接口 VPC 终端节点一起使用

如果您使用亚马逊虚拟私有云（Amazon VPC）托管 AWS 资源，则可以在您的 VPC 和之间建立私有连接 AWS CloudTrail。您可以使用此连接实现 CloudTrail 与您的 VPC 上的资源进行通信，而无需通过公共互联网。

Amazon VPC 是一项 AWS 服务，可用于在您定义的虚拟网络中启动 AWS 资源。借助 VPC，您可以控制您的网络设置，如 IP 地址范围、子网、路由表和网络网关。使用 VPC 终端节点，VPC 和 AWS 服务之间的路由由 AWS 网络处理，您可以使用 IAM 策略来控制对服务资源的访问。

要将您的 VPC 连接到 CloudTrail，您需要为定义接口 VPC 终端节点 CloudTrail。接口终端节点是一个带有私有 IP 地址的 elastic network 接口，该地址用作发往受支持 AWS 服务的流量的入口点。该端点 CloudTrail 无需互联网网关、网络地址转换 (NAT) 实例或 VPN 连接即可提供可靠、可扩展的连接。有关更多信息，请参阅 Amazon VPC 用户指南中的什么是 Amazon VPC。

Interface VPC 终端节点由 AWS PrivateLink一种 AWS 技术提供支持，该技术使用带有私有 IP 地址的弹性网络接口实现 AWS 服务之间的私密通信。有关更多信息，请参阅AWS PrivateLink。

以下步骤适用于 Amazon VPC 的用户。有关更多信息，请参阅 Amazon VPC 用户指南 中的 Amazon VPC 入门。

可用性

CloudTrail 目前支持以下 AWS 区域的 VPC 终端节点：

- 美国东部（俄亥俄）
- 美国东部（弗吉尼亚州北部）
- 美国西部（北加利福尼亚）
- 美国西部（俄勒冈州）
- 非洲（开普敦）
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 亚太地区（孟买）
- 亚太地区（大阪）
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 加拿大（中部）
- 加拿大西部（卡尔加里）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）

- 欧洲地区（伦敦）
- 欧洲地区（米兰）
- 欧洲地区（巴黎）
- 欧洲（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 中东（巴林）
- 中东（阿联酋）
- 南美洲（圣保罗）
- AWS GovCloud （美国东部）
- AWS GovCloud （美国西部）

为创建 VPC 终端节点 CloudTrail

要开始在您的 VPC 中使用 CloudTrail ，请为创建一个接口 VPC 终端节点 CloudTrail。有关更多信息，请参阅 Amazon VPC 用户指南中的 AWS 服务 使用接口 VPC 终端节点访问和。

您无需更改的设置 CloudTrail。 CloudTrail AWS 服务 使用公共终端节点或私有接口 VPC 终端节点调用其他终端节点，以正在使用哪个终端节点为准。

共享子网

与任何其他 CloudTrail VPC 终端节点一样，VPC 终端节点只能由共享子网中的所有者账户创建。但是，参与者账户可以在与参与者账户共享的子网中使用 CloudTrail VPC 终端节点。有关 VPC 共享的更多信息，请参阅《Amazon VPC 用户指南》中的与其他账户共享 VPC。

AWS 账户 封闭和步道

AWS CloudTrail 持续监控和记录任何用户、角色或 AWS 服务 用户生成的账户活动事件 AWS 账户。用户可以创建 CloudTrail 跟踪，以便在他们拥有的 S3 存储桶中接收这些事件的副本。

CloudTrail 是一项基础安全服务，因此，除非用户在关闭 AWS 账户 之前明确删除了其中的跟踪，否则即使在关闭跟踪之后，用户创建的跟踪仍会继续存在并传递事件。 AWS 账户 此行为同样适用于由管理账户或委托管理员创建的组织跟踪，以及随后在组织成员账户中创建的多区域组织跟踪。这样可以确

保，当用户重新打开已关闭的账户时，可以拥有不间断的账户活动记录。它还有助于用户了解任何最终账户活动，包括删除和终止剩余的账户资源和服务。

用户可以选择在关闭跟踪之前删除跟踪 AWS 账户，或者在跟踪关闭后联系AWS Support请求删除跟踪。 AWS 账户

有关关闭的更多信息 AWS 账户，请参阅关闭 AWS 账户。

> **Note**
>
> 如果启用了 CloudTrail 日志文件验证，用户将继续收到每小时的摘要文件，这些文件表明是否创建了任何 CloudTrail 日志。
> CloudTrail 湖泊事件数据存储、用于集成的 CloudTrail 湖泊通道、 CloudTrail 服务相关渠道以及为跟踪创建的资源（例如，Amazon Log CloudWatch s 日志组和已关闭账户中存在的 Amazon S3 存储桶），遵循账户关闭的标准 AWS 行为，并在关闭后的期限（通常为 90 天）之后永久删除。

配置 CloudTrail 设置

您可以使用 CloudTrail 控制台上的 “设置” 页面来配置和查看 CloudTrail 设置。

访问 “设置” 页面

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail控制台的左侧导航窗格中选择 “设置”。
3. 根据需要查看和更新您的设置。

   可供使用的设置如下：

   - 组织委派管理员-如果您有 AWS Organizations 组织，则可以查看 CloudTrail 委派的管理员、添加授权管理员（最多三个）和移除委派的管理员。只有组织的管理账户才能添加或移除委派的管理员。

     组织的管理账户可以将组织内的任何账户分配为 CloudTrail 委托管理员，代表组织管理组织的跟踪和事件数据存储。
   - 服务相关通道— 您可以查看为您的账户创建的任何与服务相关的频道。

     AWS 服务 可以创建与服务相关的渠道来代表您接收 CloudTrail 事件。创建 AWS 服务相关频道的服务会为该频道配置高级事件选择器，并指定该频道是应用于全部 AWS 区域还是单个频道。AWS 区域

组织的委托管理员

在 AWS Organizations 组织中 CloudTrail 使用时，您可以将组织内的任何账户分配为 CloudTrail 委托管理员，代表该组织管理该组织的跟踪和事件数据存储。委派管理员是组织中的成员帐户，可以在中执行与管理帐户相同的管理任务（除非另有说明）。 CloudTrail

如果您选择委托管理员，则此成员账户将对组织中的所有组织跟踪和事件数据存储拥有管理权限。添加委托管理员不会该改变组织的跟踪或事件数据存储的管理或操作。

首次在 CloudTrail 控制台中或使用 AWS CLI 或 CloudTrail API 添加委派管理员时， CloudTrail 会检查组织的管理账户是否具有服务相关角色。如果管理账户没有服务相关角色，则为管理账户 CloudTrail 创建服务相关角色。有关服务相关角色的更多信息，请参阅将服务相关角色用于 AWS CloudTrail。

> **Note**
>
> 使用 AWS Organizations CLI 或 API 操作添加委派管理员时，如果服务相关角色不存在，则不会创建该角色。只有当您从管理账户直接调用服务时，才会创建 CloudTrail 服务相关角色，例如添加委派管理员或使用 CloudTrail 控制台或 CloudTrail API 创建组织跟踪或事件数据存储时。 AWS CLI

请注意以下因素，这些因素定义了委派管理员的操作方式 CloudTrail。

管理账户仍然是委派管理员创建的所有 CloudTrail 组织资源的所有者。

组织的管理账户仍然是授权管理员创建的任何 CloudTrail 组织资源的所有者，例如跟踪和事件数据存储。这可以在委托管理员发生更改时为组织提供连续性。

移除委派管理员账户并不会删除他们创建的任何 CloudTrail 组织资源。

移除委派管理员时，不会删除由委派管理员创建的组织跟踪和事件数据存储，因为无论 CloudTrail 组织资源是由委派的管理员还是管理账户创建的，管理账户始终充当组织资源的所有者。

一个组织最多可以有三个 CloudTrail 委托管理员。

每个组织最多可以有三个 CloudTrail 委派管理员。有关移除委托管理员的更多信息，请参阅移除 CloudTrail 委派的管理员。

下表显示了管理账户、委派管理员账户和作为 AWS Organizations 组织成员的账户的权能。

功能	管理账户	委托管理员账户	成员账户
添加或移除委托管理员账户。	是	否	否
创建组织跟踪。	是	是[1]	否
查看组织跟踪的列表。	支持	是	是
更新组织跟踪。	是	是[1、2]	否
删除组织跟踪。	支持	是	不支持
为事件或 AWS Config 配置项目创建组织 CloudTrail 事件数据存储。	支持	是	不支持

功能	管理账户	委托管理员账户	成员账户
在组织事件数据存储上启用 Insights。	是	否	否
更新组织事件数据存储。	是	是[2]	否
在组织事件数据存储上启用 Lake 查询联合身份验证[3]。	支持	是	不支持
在组织事件数据存储上禁用 Lake 查询联合身份验证。	支持	是	不支持
删除组织事件数据存储。	支持	是	不支持
将跟踪事件复制到组织事件数据存储。	是	否	否
对组织事件数据存储运行查询。	支持	是	不支持
查看组织事件数据存储的 Lake 控制面板。	支持	是	不支持

[1] 委派的管理员只能使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 操作配置 CloudWatch 日志组。调用者 CloudWatch 账户中必须同时存在日志日志组和日志角色。

[2] 只有管理账户才能将组织跟踪或事件数据存储转换为账户级跟踪或事件数据存储，或者将账户级跟踪或事件数据存储转换为组织跟踪或事件数据存储。因为组织跟踪和事件数据存储仅存在于管理账户中，所以不允许委托管理员执行这些操作。当组织跟踪或事件数据存储转换为账户级跟踪或事件数据存储时，只有管理账户才能访问跟踪或事件数据存储。

[3]只有一个委托管理员账户或管理账户才能在组织事件数据存储上启用联合身份验证。其他委托管理员账户可以使用 Lake Formation 数据共享功能查询和共享信息。任何委托管理员账户以及组织的管理账户都可以禁用联合身份验证。

主题

- 指定委托管理员所需的权限
- 添加 CloudTrail 委派管理员
- 移除 CloudTrail 委派的管理员

指定委托管理员所需的权限

分配 CloudTrail 委托管理员时，您必须拥有在中添加和删除委托管理员的权限 CloudTrail，以及以下策略声明中列出的某些 AWS Organizations API 操作和 IAM 权限。

您可以将以下声明添加到 IAM policy 的末尾以授予这些权限：

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
    "Resource": "*"
}
```

添加 CloudTrail 委派管理员

您可以添加委派管理员来管理组织的 CloudTrail 资源，例如跟踪和事件数据存储。

您可以使用 CloudTrail 控制台或为您的 AWS 组织添加 CloudTrail 委派管理员 AWS CLI。

在添加委托管理员之前，务必确保他们在组织中拥有账户，并且您已使用组织的管理账户登录。有关如何为您的组织创建新 AWS 账户的信息，请参阅在组织中创建 AWS 账户。有关如何邀请现有 AWS 账户加入您的组织的信息，请参阅邀请 AWS 账户加入您的组织。

CloudTrail console

以下过程说明如何使用 CloudTrail 控制台添加 CloudTrail 委派管理员。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 控制台的左侧导航窗格中选择 “设置”。
3. 在 Organization delegated administrators（组织的委托管理员）部分中，选择 Register administrator（注册管理员）。

4. 输入您要分配为组织跟踪和事件数据存储的 CloudTrail 委托管理员的账户的十二位数 AWS 账户 ID。
5. 选择 Register administrator（注册管理员）。

AWS CLI

以下示例添加了 CloudTrail 委派管理员。

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

如果成功，此命令不会产生任何输出。

移除 CloudTrail 委派的管理员

您可以使用 CloudTrail 控制台或删除 CloudTrail 委派的管理员 AWS CLI。

CloudTrail console

以下过程说明如何使用 CloudTrail 控制台移除 CloudTrail 委派的管理员。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 控制台的左侧导航窗格中选择 “设置”。
3. 在 Organization delegated administrators（组织的委托管理员）部分中，选择您要移除的委托管理员。
4. 选择 Remove administrator（移除管理员）。
5. 确认您要移除委托管理员，然后选择 Remove administrator（移除管理员）。

AWS CLI

以下命令删除 CloudTrail 委派的管理员。

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

如果成功，此命令不会产生任何输出。

服务相关通道

AWS 服务可以创建与服务相关的渠道来代表您接收 CloudTrail 事件。创建 AWS 服务相关频道的服务会为该频道配置高级事件选择器，并指定该频道是应用于全部 AWS 区域还是单个频道。 AWS 区域

主题

- 使用控制台查看服务相关通道
- 使用查看与服务相关的频道 AWS CLI

使用控制台查看服务相关通道

使用 CloudTrail 控制台，您可以查看有关服务创建的任何 CloudTrail 服务相关频道的信息。 AWS 如果您的账户没有任何服务相关通道，则该表为空。

可以按照以下步骤查看服务相关通道的信息。

1. 在 CloudTrail 控制台的左侧导航窗格中选择 “设置”。
2. 从服务相关通道中选择一个服务相关通道查看其详细信息。
3. 在详细信息页面上查看服务相关通道已配置好的设置。

   您可以在详细信息页面上查看以下信息：

   - 通道名称 – 通道的全称。频道名称格式`aws-service-channel/`*`AWS_service_name`*`/slc`*`AWS_service_name`*表示管理频道的 AWS 服务的名称。
   - 通道 ARN – 通道的 ARN，可在 API 请求中用来获取有关该通道的详细信息。
   - 所有区域 – 如果为所有 AWS 区域配置了通道，则该值为 `Yes`。
   - AWS 服务-管理频道的 AWS 服务的名称。
   - 管理事件 – 显示为该通道配置的所有管理事件。
   - 数据事件 – 显示为通道配置的所有数据事件。

使用查看与服务相关的频道 AWS CLI

使用 AWS CLI，您可以查看有关服务创建的任何 CloudTrail 服务相关渠道的信息。 AWS

主题

- 获取 CloudTrail 服务相关频道

- 列出所有 CloudTrail 与服务相关的频道
- AWS 服务关联渠道上的服务事件

获取 CloudTrail 服务相关频道

以下示例 AWS CLI 命令返回有关特定 CloudTrail 服务相关频道的信息，包括目标 AWS 服务的名称、为该频道配置的任何高级选择器，以及该频道是适用于所有区域还是单个区域。

您必须指定 ARN 或 `--channel` ARN 的 ID 后缀。

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

以下为响应示例。在此示例中，`AWS_service_name`表示创建频道的 AWS 服务的名称。

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
                        ]
                    }
                ]
            }
        ]
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
```

```
    ]
}
```

列出所有 CloudTrail 与服务相关的频道

以下示例 AWS CLI 命令返回有关代表您创建的所有 CloudTrail 服务相关频道的信息。可选参数包括 `--max-results`，以指定希望在单个页面上通过命令返回的最大结果数。如果结果数超过指定的 `--max-results` 值，请再次运行命令，添加返回的 `NextToken` 值来获取下一页的结果。

```
aws cloudtrail list-channels
```

以下为响应示例。在此示例中，`AWS_service_name`表示创建频道的 AWS 服务的名称。

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS 服务关联渠道上的服务事件

管理 AWS 服务关联渠道的服务可以在服务相关渠道上启动操作（例如，创建或更新服务相关频道）。CloudTrail 将这些操作记录为AWS 服务事件，并将这些事件传送到事件历史记录以及为管理事件配置的所有活动跟踪和事件数据存储中。对于这些事件，`eventType` 字段为 `AwsServiceEvent`。

以下是创建服务相关频道的 AWS 服务事件日志文件条目的示例。

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
```

```
    "eventSource":"cloudtrail.amazonaws.com",
    "eventName":"CreateServiceLinkedChannel",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"AWS Internal",
    "userAgent":"AWS Internal",
    "requestParameters":null,
    "responseElements":null,
    "requestID":"564f004c-EXAMPLE",
    "eventID":"234f004b-EXAMPLE",
    "readOnly":false,
    "resources":[
       {
          "accountId":"184434908391",
          "type":"AWS::CloudTrail::Channel",
          "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
       }
    ],
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "recipientAccountId":"111122223333",
    "eventCategory":"Management"
}
```

了解 CloudTrail 事件

中的事件 CloudTrail 是 AWS 账户中某项活动的记录。此活动可以是 IAM 身份或可由 CloudTrail监控的服务采取的操作。 CloudTrail 事件提供通过 AWS Management Console、 AWS SDK、命令行工具和其他工具进行的 API 和非 API 账户活动的历史记录。 AWS 服务

CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序出现。

有三种类型 CloudTrail 的事件：

- 管理事件
- 数据事件
- 洞察活动

默认情况下，跟踪记录和事件数据存储将记录管理事件，但不记录数据事件或 Insights 事件。

所有事件类型都使用 CloudTrail JSON 日志格式。日志包含有关您账户中的资源请求的信息，如谁发出请求、所使用的服务、执行的操作以及操作的参数。事件数据包含在 `Records` 数组中。

有关 CloudTrail 事件记录字段的信息，请参见CloudTrail 录制内容。

管理事件

管理事件提供有关对您 AWS 账户中的资源执行的管理操作的信息。这些也称为控制层面操作。示例管理事件包括：

- 配置安全性（例如， AWS Identity and Access Management `AttachRolePolicy`API 操作）。
- 注册设备（例如，Amazon EC2 `CreateDefaultVpc` API 操作）。
- 配置传送数据的规则（例如，Amazon EC2 `CreateSubnet` API 操作）。
- 设置日志记录（例如， AWS CloudTrail `CreateTrail`API 操作）。

管理事件还包括在您的账户中发生的非 API 事件。例如，当用户登录您的账户时，会 CloudTrail 记录该`ConsoleLogin`事件。有关更多信息，请参阅 捕获的非 API 事件 CloudTrail。有关 CloudTrail 记录 AWS 服务的管理事件列表，请参阅CloudTrail 支持的服务和集成。

以下示例显示了管理事件的单个日志记录。在这种情况下，名为的 IAM 用户Mary_Major运行aws cloudtrail start-logging命令调用 CloudTrail StartLogging操作，在名为的跟踪上启动日志记录过程myTrail。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
```

```
    "sessionCredentialFromConsole": "true"
}
```

在该示例中，名为 Paulo_Santos 的 IAM 用户运行 aws cloudtrail start-event-data-store-ingestion 命令调用 StartEventDataStoreIngestion 操作，开始对事件数据存储进行提取。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
```

```
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

数据事件

数据事件提供有关对在资源上或资源内执行的资源操作的信息。这些也称为数据层面操作。数据事件通常是高容量活动。

示例数据事件包括：

- 针@@ 对 S3 存储桶中对象的 Amazon S3 对象级 PutObject API 活动（例如GetObjectDeleteObject、和 API 操作）。
- AWS Lambda 函数执行活动（InvokeAPI）。
- CloudTrail PutAuditEvents用于记录外部事件的 L CloudTrail ake 频道上的活动 AWS。
- 针对主题的 Amazon SNS Publish 和 PublishBatch API 操作。

下表显示可用于跟踪和事件数据存储的数据事件类型。数据事件类型（控制台）列显示控制台中的相应选择。resources.typ **resources.type** e 值列显示您将使用或 API 指定的值，以便在跟踪或事件数据存储中包含该 AWS CLI 类型的数据事件。 CloudTrail

对于跟踪，您可以使用基本或高级事件选择器来记录 Amazon S3 对象、Lambda 函数和 DynamoDB 表（显示在表的前三行）的数据事件。您只能使用高级事件选择器来记录其余行中显示的数据事件类型。

对于事件数据存储，只能使用高级事件选择器来包含数据事件。

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon DynamoDB	表上的 Amazon DynamoDB 项目级 API 活动（例如PutItemDeleteIte	DynamoDB	AWS::DynamoDB::Table

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	m 、UpdateItem 和 API 操作）。 **Note** 对于启用了流的表，数据事件中的 resources 字段同时包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table 。如果您为 resources.type 指定 AWS::DynamoDB::Table ，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName 在该字段上添加过滤器。		

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS Lambda	AWS Lambda 函数执行活动（InvokeAPI）。	Lambda	AWS::Lambda::Function
Amazon S3	针@@ 对 S3 存储桶中对象的 Amazon S3 对象级 PutObject API 活动（例如GetObject DeleteObject 、和 API 操作）。	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 用于配置操作的 API 活动，例如对StartConfiguration Session 和的调用GetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration
AWS B2B 数据交换	用于转换器操作的 B2B 数据交换 API 活动，例如对 GetTransformerJob 和 StartTransformerJob 的调用。	B2B 数据交换	AWS::B2BI::Transformer
Amazon Bedrock	代理别名上的 Amazon Bedrock API 活动。	Bedrock 代理别名	AWS::Bedrock::AgentAlias

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	知识库上的 Amazon Bedrock API 活动。	Bedrock 知识库	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront 在 a KeyValueStore上的 API 活动	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map 命名空间上的 API 活动。	AWS Cloud Map 命名空间	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map 服务上的 API 活动。	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` 用于记录外部事件的 L CloudTrail lake 频道上的活动 AWS。	CloudTrail 频道	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	亚马逊 CodeWhisperer API 在自定义方面的活动。	CodeWhisperer 定制	`AWS::CodeWhisperer::Customization`
	个人资料上的亚马逊 CodeWhisperer API 活动。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	针对 Amazon Cognito 身份池的 Amazon Cognito API 活动。	Cognito 身份池	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	针对流的 Amazon DynamoDB API 活动	DynamoDB Streams	`AWS::DynamoDB::Stream`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) 直接 API，例如 Amazon EBS 快照上的 PutSnapshotBlock 、GetSnapshotBlock 和 ListChangedBlocks 。	Amazon EBS 直接 API	AWS::EC2::Snapshot
Amazon EMR	针对预写日志工作空间的 Amazon EMR API 活动。	EMR 预写日志工作空间	AWS::EMRWAL::Workspace
Amazon FinSpace	针对环境的 Amazon FinSpace API 活动	FinSpace	AWS::FinSpace::Environment

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS Glue	AWS Glue 在 Lake Formation 创建的表格上的 API 活动。 **Note** AWS Glue 目前仅以下区域支持表的数据事件： • 美国东部（弗吉尼亚州北部） • 美国东部（俄亥俄州） • 美国西部（俄勒冈州） • 欧洲地区（爱尔兰） • Asia Pacific（Tokyo）Region	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	探测器的亚马逊 GuardDuty API 活动。	GuardDuty 探测器	`AWS::GuardDuty::Detector`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS HealthImaging	AWS HealthImaging 数据存储上的 API 活动。	医学成像数据存储	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT 证书上@@的 API 活动。	物联网证书	`AWS::IoT::Certificate`
	AWS IoT API 在事物上的活动。	物联网的东西	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	组件版本上来自 Greengrass 核心设备的 Greengrass API 活动。 **Note** Greengrass 不会记录被拒绝访问的事件。	物联网 Greengrass 组件版本	`AWS::GreengrassV2::ComponentVersion`
	部署时来自 Greengrass 核心设备的 Greengrass API 活动。 **Note** Greengrass 不会记录被拒绝访问的事件。	物联网 Greengrass 部署	`AWS::GreengrassV2::Deployment`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS IoT SiteWise	资产上的@@ 物联网 SiteWise API 活动。	物联网 SiteWise 资产	AWS::IoTSiteWise::Asset
	时间序列上的@@ 物联网 SiteWise API 活动。	物联网 SiteWise 时间序列	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	实体上的物联网 TwinMaker API 活动。	物联网 TwinMaker 实体	AWS::IoTTwinMaker::Entity
	工作空间上 TwinMaker 的 IoT API 活动。	物联网 TwinMaker 工作空间	AWS::IoTTwinMaker::Workspace
Amazon Kendra Intelligent Ranking	针对重新评分执行计划的 Amazon Kendra Intelligent Ranking API 活动。	Kendra 排名	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces（Apache Cassandra 兼容）	表上的 Amazon Keyspaces API 活动。	卡桑德拉桌	AWS::Cassandra::Table
Amazon Kinesis Data Streams	直播中的 Kinesis Data Streams API 活动。	Kinesis 直播	AWS::Kinesis::Stream
	Kinesis Data Streams 针对直播使用者的 API 活动。	Kinesis 直播消费者	AWS::Kinesis::StreamConsumer

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon Kinesis Video Streams	Kinesis Video Streams 视频流上的 API 活动，例如GetMedia对和的调用。PutMedia	Kinesis 视频流	AWS::KinesisVideo::Stream
Amazon Managed Blockchain	针对网络的 Amazon Managed Blockchain API 活动。	托管区块链网络	AWS::ManagedBlockchain::Network
	针对 Ethereum 节点的 Amazon Managed Blockchain JSON-RPC 调用，如 eth_getBalance 或 eth_getBlockByNumber 。	托管区块链	AWS::ManagedBlockchain::Node
Amazon Neptune 图形	Neptune Graph 上的数据 API 活动，例如查询、算法或向量搜索。	Neptune 图形	AWS::NeptuneGraph::Graph
AWS Private CA	AWS Private CA 活动目录 API 活动的连接器。	AWS Private CA 活动目录连接器	AWS::PCAConnectorAD::Connector
亚马逊 Q 应用程序	亚马逊 Q 应用程序上的数据 API 活动。	亚马逊 Q 应用程序	AWS::QApps:QApp
Amazon Q Business	应用程序上的 Amazon Q Business API 活动。	Amazon Q Business 应用程序	AWS::QBusiness::Application

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	数据来源上的 Amazon Q Business API 活动。	Amazon Q Business 数据来源	`AWS::QBusiness::DataSource`
	索引上的 Amazon Q Business API 活动。	Amazon Q Business 索引	`AWS::QBusiness::Index`
	Web 体验上的 Amazon Q Business API 活动。	Amazon Q Business Web 体验	`AWS::QBusiness::WebExperience`
Amazon RDS	数据库集群上的 Amazon RDS API 活动。	RDS 数据 API-数据库集群	`AWS::RDS::DBCluster`
Amazon S3	接入点上的 Amazon S3 API 活动。	S3 接入点	`AWS::S3::AccessPoint`
	Amazon S3 对象 Lambda 接入点 API 活动，例如对和的调用。`CompleteMultipartUpload` `GetObject`	S3 对象 Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 on Outposts 对象级别 API 活动。	S3 Outposts	`AWS::S3Outposts::Object`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon SageMaker	亚马逊在终端节点上的 SageMaker InvokeEndpointWithResponseStream 活动。	SageMaker 端点	AWS::SageMaker::Endpoint
	特色商店中的亚马逊 SageMaker API 活动。	SageMaker feature store	AWS::SageMaker::FeatureGroup
	Amazon SageMaker API 在实验试用组件上的活动。	SageMaker 指标实验试验组件	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	针对平台端点的 Amazon SNS Publish API 操作。	SNS 平台端点	AWS::SNS::PlatformEndpoint
	针对主题的 Amazon SNS Publish 和 PublishBatch API 操作。	SNS 主题	AWS::SNS::Topic
Amazon SQS	消息上的 Amazon SQS API 活动。	SQS	AWS::SQS::Queue
AWS Step Functions	Step Functions API 在状态机上的活动。	Step Functions 状态机	AWS::StepFunctions::StateMachine
AWS Supply Chain	AWS Supply Chain 实例上的 API 活动。	供应链	AWS::SCN::Instance

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon SWF	域名上的@@ 亚马逊 SWF API 活动。	SWF 域名	AWS::SWF::Domain
AWS Systems Manager	控制通道上的 Systems Manager API 活动。	Systems Manager (系统管理员)	AWS::SSMMessages::ControlChannel
	托管节点上的 Systems Manager API 活动。	Systems Manager 托管式节点	AWS::SSM::ManagedNode
Amazon Timestream	针对数据库的 Amazon Timestream Query API 活动。	Timestream 数据库	AWS::Timestream::Database
	针对表的 Amazon Timestream Query API 活动。	Timestream 表	AWS::Timestream::Table
Amazon Verified Permissions	针对策略存储的 Amazon Verified Permissions API 活动。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces 瘦客户机	WorkSpaces 设备上的瘦客户端 API 活动。	瘦客户端设备	AWS::ThinClient::Device
	WorkSpaces 环境中的瘦客户端 API 活动。	瘦客户端环境	AWS::ThinClient::Environment
AWS X-Ray	追踪上@@ 的 X-Ray API 活动。	X 射线追踪	AWS::XRay::Trace

默认情况下，在您创建跟踪或事件数据存储时，未记录数据事件。要记录 CloudTrail 数据事件，必须明确添加要为其收集活动的支持的资源或资源类型。有关更多信息，请参阅 创建跟踪 和 使用控制台为事件创建 CloudTrail事件数据存储。

记录数据事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

以下示例显示了 Amazon SNS Publish 操作的数据事件的单个日志记录。


```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
```

```
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}
```

下一个示例显示了 Amazon Cognito `GetCredentialsForIdentity` 操作的数据事件的单个日志记录。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
```

```
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```

洞察活动

CloudTrail Insights 事件通过分析 CloudTrail 管理活动来捕获您 AWS 账户中异常的 API 调用率或错误率活动。Insights 事件提供相关信息，例如关联的 API、错误代码、事件时间和统计数据，以帮助您了解异常活动并对其采取措施。与在 CloudTrail 跟踪或事件数据存储中捕获的其他类型的事件不同，Insights 事件仅在 CloudTrail 检测到您的账户 API 使用情况或错误率记录的变化与账户的典型使用模式明显不同时，才会记录 Insights 事件。

可能生成 Insights 事件的活动的示例包括：

- 您的账户通常每分钟记录不超过 20 次 Simple Storage Service（Amazon S3）`deleteBucket` API 调用，但是您的账户一开始就平均每分钟记录 100 次 `deleteBucket` API 调用。在异常活动开始时记录一个 Insights 事件，并记录另一个见解事件以标记异常活动的结束。
- 您的账户通常每分钟记录 20 次对 Amazon EC2 `AuthorizeSecurityGroupIngress` API 的调用，但是您的账户开始记录对 `AuthorizeSecurityGroupIngress` 的零次调用。在异常活动开始

时记录一个 Insights 事件，10 分钟后，当异常活动结束时，将记录另一个 Insights 事件以标记异常活动的结束。

- 您的账户七天内对 AWS Identity and Access Management API、`DeleteInstanceProfile` 记录的 `AccessDeniedException` 错误通常不到一个。你的账户开始对 `DeleteInstanceProfile` API 调用每分钟平均记录 12 个 `AccessDeniedException` 错误。在异常错误率活动开始时记录一个 Insights 事件，并记录另一个 Insights 事件以标记异常活动的结束。

这些示例仅用于说明用途。根据您的使用案例，您的结果可能会有所不同。

要记录 CloudTrail Insights 事件，您必须在新的或现有的跟踪或事件数据存储上明确启用 Insights 事件。有关创建跟踪的更多信息，请参阅创建跟踪。有关创建事件数据存储的更多信息，请参阅 使用控制台为 CloudTrail Insights 事件创建事件数据存储。

将对 Insights 事件收取额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅AWS CloudTrail 定价。

CloudTrail Insights 中记录了两个事件以显示异常活动：开始事件和结束事件。下面的示例显示了一个启动见解事件的单个日志记录，该事件是在不寻常地多次调用 Application Auto Scaling API `CompleteLifecycleAction` 时发生的。对于见解事件，`eventCategory` 的值为 `Insight`。`insightDetails` 块标识事件状态、源、名称、见解类型和上下文，包括统计信息和归因。有关 `insightDetails` 块的更多信息，请参阅 CloudTrail 见解`insightDetails`元素。


```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
```

```
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
```

```
                    }]
                }]
            }
        },
        "eventCategory": "Insight"
    }
```

记录管理事件

默认情况下，跟踪记录和事件数据存储将记录管理事件，但不包含数据事件或 Insights 事件。

数据事件或 Insights 事件需额外支付费用。有关更多信息，请参阅AWS CloudTrail 定价。

目录

- 管理事件
  - 使用记录管理事件 AWS Management Console
- 读取和写入事件
- 使用 AWS Command Line Interface记录事件
  - 示例：记录跟踪的管理事件
    - 示例：使用高级事件选择器记录跟踪的管理事件
    - 示例：使用基本事件选择器记录跟踪的管理事件
  - 示例：记录事件数据存储的管理事件
- 使用 AWS 开发工具包记录事件
- 向 Amazon CloudWatch 日志发送事件

管理事件

管理事件可让您了解对 AWS 账户中的资源执行的管理操作。这些也称为控制层面操作。示例管理事件包括：

- 配置安全性（例如，IAM `AttachRolePolicy` API 操作）
- 注册设备（例如，Amazon EC2 `CreateDefaultVpc` API 操作）。
- 配置传送数据的规则（例如，Amazon EC2 `CreateSubnet` API 操作）
- 设置日志记录（例如， AWS CloudTrail `CreateTrail`API 操作）

管理事件还包括在您的账户中发生的非 API 事件。例如，当用户登录您的账户时，会 CloudTrail 记录该ConsoleLogin事件。有关更多信息，请参阅 捕获的非 API 事件 CloudTrail。

默认情况下，跟踪和事件数据存储配置为记录管理事件。

> **Note**
>
> CloudTrail 事件历史记录功能仅支持管理事件。您不能从事件历史记录中排除 AWS KMS 或 Amazon RDS Data API 事件；您应用于跟踪或事件数据存储的设置不适用于事件历史记录。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。

使用记录管理事件 AWS Management Console

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 要更新跟踪，请打开 CloudTrail 控制台的 Trails 页面并选择跟踪名称。

   要更新事件数据存储，请打开 CloudTrail 控制台的事件数据存储页面，然后选择事件数据存储名称。
3. 对于 Management events（管理事件），选择 Edit（编辑）。

   - 选择您希望跟踪或事件数据存储记录读取事件、写入事件，还是两者都记录。
   - 选择 “排除 AWS KMS 事件”，从您的跟踪或事件数据存储中筛选 AWS Key Management Service (AWS KMS) 事件。默认设置是包括所有 AWS KMS 事件。

     仅当您在跟踪或 AWS KMS 事件数据存储中记录管理事件时，才可使用记录或排除事件的选项。如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件日志记录设置。

     AWS KMS 诸如EncryptDecrypt、和之类的操作GenerateDataKey通常会生成大量事件（超过 99%）。这些操作现在记录为读取事件。诸如DisableDelete、和ScheduleKey（通常占事件量不到 0.5%）之类的低容量相关 AWS KMS 操作被记录为写入 AWS KMS 事件。

     要排除高容量事件（如EncryptDecryptGenerateDataKey、和），但仍记录相关事件（例如DisableScheduleKey、Delete和），请选择记录写入管理事件，然后清除 “排除” AWS KMS 事件复选框。
   - 选择排除 Amazon RDS Data API 事件以从跟踪或事件数据存储中筛选出 Amazon Relational Database Service Data API 事件。默认设置是包含所有 Amazon RDS 数据 API 事件。有关

Amazon RDS 数据 API 事件的更多信息，请参阅 Amazon RDS Aurora 用户指南中的使用 AWS CloudTrail记录数据 API 调用。

4. 完成后选择保存更改。

读取和写入事件

将跟踪或事件数据存储配置为记录管理事件时，可以指定是需要只读事件、只写事件还是两者都需要。

- 读取

  只读事件包括将读取您的资源但不进行更改的 API 操作。例如，只读事件包括 Amazon EC2 `DescribeSecurityGroups` 和 `DescribeSubnets` API 操作。这些操作仅返回有关 Amazon EC2 资源的信息，但不更改您的配置。

- 写入

  只写事件包括将修改（或可能修改）您的资源的 API 操作。例如，Amazon EC2 `RunInstances` 和 `TerminateInstances` API 操作将修改您的实例。

示例：为单独的跟踪记录记录读取事件和写入事件

以下示例说明如何将跟踪记录配置为将账户的日志活动拆分到单独的 S3 存储桶中：一个存储桶接收只读事件，另一个存储桶接收只写事件。

1. 您创建一个跟踪并选择一个名为 `read-only-bucket` 的 S3 存储桶来接收日志文件。然后，您更新跟踪以指定您需要 Read（读取）管理事件。
2. 您创建另一个跟踪并选择一个名为 `write-only-bucket` 的 S3 存储桶来接收日志文件。然后，您更新跟踪以指定您需要 Write（写入）管理事件。
3. Amazon EC2 `DescribeInstances` 和 `TerminateInstances` API 操作将在您的账户中执行。
4. `DescribeInstances` API 操作是只读事件，它匹配第一个跟踪的设置。跟踪将记录事件并将事件传送到 `read-only-bucket`。
5. `TerminateInstances` API 操作是只写事件，它匹配第二个跟踪的设置。跟踪将记录事件并将事件传送到 `write-only-bucket`。

使用 AWS Command Line Interface记录事件

您可以使用 AWS CLI配置跟踪或事件数据存储以记录管理事件。

主题

- 示例：记录跟踪的管理事件
- 示例：记录事件数据存储的管理事件

示例：记录跟踪的管理事件

要查看您的跟踪是否正在记录管理事件，请运行 get-event-selectors 命令。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

以下示例返回跟踪的默认设置。默认情况下，跟踪记录所有管理事件，记录所有事件源的事件，但不记录数据事件。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

您可以使用基本或高级事件选择器来记录管理事件。不能将事件选择器和高级事件选择器同时应用于跟踪。如果将高级事件选择器应用于跟踪，则所有现有的基本事件选择器都将被覆盖。以下各节提供了如何使用高级事件选择器和基本事件选择器记录管理事件的示例。

主题

- 示例：使用高级事件选择器记录跟踪的管理事件
- 示例：使用基本事件选择器记录跟踪的管理事件

示例：使用高级事件选择器记录跟踪的管理事件

以下示例为名为的跟踪创建了一个高级事件选择器，*TrailName*以包含只读和只写管理事件（省略`readOnly`选择器），但排除 AWS Key Management Service (AWS KMS) 事件。由于 AWS KMS 事件被视为管理事件，而且其数量可能很大，因此，如果您有多个跟踪记录管理事件，它们可能会对您的 CloudTrail 账单产生重大影响。

如果您选择不记录管理事件，则不会记录 AWS KMS 事件，也无法更改 AWS KMS 事件日志记录设置。

要重新开始将 AWS KMS 事件记录到跟踪，请移除`eventSource`选择器，然后再次运行该命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

以下示例返回为跟踪配置的高级事件选择器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
```

```
}
```

要再次开始将排除的事件记录到跟踪，请删除 eventSource 选择器，如以下命令中所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

下一个示例为名为的跟踪创建高级事件选择器，*TrailName*以包括只读和只写管理事件（省略readOnly选择器），但不包括 Amazon RDS 数据 API 管理事件。要排除 Amazon RDS 数据 API 管理事件，请在eventSource字段的字符串值中指定 Amazon RDS 数据 API 事件源rdsdata.amazonaws.com。

如果您选择不记录管理事件，则不会记录 Amazon RDS 数据 API 管理事件，也无法更改 Amazon RDS 数据 API 事件记录设置。

要重新开始将 Amazon RDS 数据 API 管理事件记录到跟踪中，请移除eventSource选择器，然后再次运行该命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

以下示例返回为跟踪配置的高级事件选择器。

```
{
```

```
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

要再次开始将排除的事件记录到跟踪，请删除 eventSource 选择器，如以下命令中所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

示例：使用基本事件选择器记录跟踪的管理事件

要将跟踪配置为记录管理事件，请运行 put-event-selectors 命令。以下示例说明如何配置您的跟踪以包含两个 S3 对象的所有管理事件。您可以为一个跟踪指定 1 至 5 个事件选择器。您可以为一个跟踪指定 1 至 250 个数据资源。

> **Note**
>
> 无论有多少个事件选择器，最多只能有 250 个 S3 数据资源。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

以下示例返回为跟踪配置的事件选择器。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

要从跟踪日志中排除 AWS Key Management Service (AWS KMS) 事件，请运行put-event-selectors命令并添加值为ExcludeManagementEventSources的属性kms.amazonaws.com。以下示例为名为的跟踪创建事件选择器，*TrailName*以包括只读和只写管理事件，但不包括 AWS KMS 事件。由于 AWS KMS 可能会生成大量事件，因此本示例中的用户可能希望限制事件以管理跟踪成本。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

以下示例返回为跟踪配置的事件选择器。

```
{
```

```
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

要从跟踪日志中排除 Amazon RDS 数据 API 管理事件，请运行put-event-selectors命令并添加值为ExcludeManagementEventSources的属性rdsdata.amazonaws.com。以下示例为名为的跟踪创建事件选择器，*TrailName*以包括只读和只写管理事件，但不包括 Amazon RDS 数据 API 管理事件。由于 Amazon RDS Data API 可以生成大量的管理事件，因此本示例中的用户可能希望限制事件以管理跟踪成本。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
}
```

要重新开始向跟踪记录 AWS KMS 或 Amazon RDS Data API 管理事件，请传递一个空字符串作为值ExcludeManagementEventSources，如以下命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

要将相关 AWS KMS 事件记录到跟踪（如DisableScheduleKey、Delete和），但不包括高容量 AWS KMS 事件（如EncryptDecryptGenerateDataKey、和），请记录只写管理事件，并保留记录 AWS KMS 事件的默认设置，如以下示例所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

示例：记录事件数据存储的管理事件

要查看事件数据存储是否包含管理事件，请运行 get-event-data-store 命令。

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下为响应示例。创建时间和上次更新时间采用 timestamp 格式。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
```

```
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

要创建包含所有管理事件的事件数据存储，请运行 create-event-data-store 命令。无需指定任何高级事件选择器即可包含所有管理事件。

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

要创建排除 AWS Key Management Service (AWS KMS) 事件的事件数据存储，请运行`create-event-data-store`命令并指定`eventSource`不等于`kms.amazonaws.com`。以下示例创建了一个事件数据存储，其中包含只读和只写管理事件，但不包括 AWS KMS 事件。

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
```

```
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

要创建不包括 Amazon RDS 数据 API 管理事件的事件数据存储，请运行`create-event-data-store`命令并指定`eventSource`不等于`rdsdata.amazonaws.com`。以下示例创建的事件数据存储包含只读和只写管理事件，但排除了 Amazon RDS Data API 事件。

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
```

```
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

使用 AWS 开发工具包记录事件

使用该GetEventSelectors操作来查看您的跟踪是否正在记录跟踪的管理事件。您可以将跟踪配置为通过PutEventSelectors操作记录管理事件。有关更多信息，请参阅 AWS CloudTrail API 参考。

运行该GetEventDataStore操作以查看您的事件数据存储是否包含管理事件。您可以通过运行CreateEventDataStore或UpdateEventDataStore操作将事件数据存储配置为包含管理事件。有关更多信息，请参阅 使用创建、更新和管理事件数据存储 AWS CLI 和《AWS CloudTrail API Referencehttps://docs.aws.amazon.com/awscloudtrail/latest/APIReference/》。

向 Amazon CloudWatch 日志发送事件

对于跟踪， CloudTrail 支持向 CloudWatch 日志发送数据和管理事件。当您将跟踪配置为向 CloudWatch 日志日志组发送事件时，仅 CloudTrail 发送您在跟踪中指定的事件。例如，如果您将跟踪配置为仅记录管理事件，则您的跟踪仅将管理事件传送到您的 CloudWatch 日志日志组。有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

记录数据事件

本节介绍如何使用CloudTrail 控制台和记录数据事件AWS CLI。

默认情况下，跟踪和事件数据存储不记录数据事件。记录数据事件将收取额外费用。有关更多信息，请参阅AWS CloudTrail 定价。

通过数据事件，可以了解对资源执行的或在资源内执行的资源操作。这些也称为数据层面操作。数据事件通常是高容量活动。

示例数据事件包括：

- 针@@ 对 S3 存储桶中对象的 Amazon S3 对象级 PutObject API 活动（例如GetObjectDeleteObject、和 API 操作）。
- AWS Lambda 函数执行活动（InvokeAPI）。
- CloudTrail PutAuditEvents用于记录外部事件的 L CloudTrail ake 频道上的活动 AWS。
- 针对主题的 Amazon SNS Publish 和 PublishBatch API 操作。

您可以使用高级事件选择器来创建细粒度的选择器，通过仅记录用例中感兴趣的特定事件来帮助您控制成本。例如，您可以使用高级事件选择器通过在eventName字段上添加筛选器来记录特定的 API 调用。有关更多信息，请参阅 使用高级事件选择器筛选数据事件。

> **Note**
>
> 您的跟踪记录的事件可在 Amazon 中找到 EventBridge。例如，如果您选择记录 S3 对象的数据事件而非管理事件，则您的跟踪将仅处理和记录指定 S3 对象的数据事件。这些 S3 对象的数据事件可在 Amazon 中找到 EventBridge。有关更多信息，请参阅 Amazon EventBridge 用户指南中的来自 AWS 服务的事件。

目录

- 数据事件
  - 示例：记录 Simple Storage Service（Amazon S3）对象的数据事件
  - 记录其他 AWS 账户中 S3 对象的数据事件
- 只读和只写事件
- 使用记录数据事件 AWS Management Console
- 使用记录数据事件 AWS Command Line Interface
  - 使用记录跟踪的数据事件 AWS CLI
    - 使用高级事件选择器记录事件
    - 使用高级事件选择器记录亚马逊 S3 存储桶的所有 Amazon S3 事件
    - 使用高级事件选择器记录 Simple Storage Service（Amazon S3）on AWS Outposts 事件
    - 使用基本事件选择器记录事件
  - 使用记录事件数据存储的数据事件 AWS CLI
    - 包含存储桶的所有 Amazon S3 事件
    - 包含 Amazon S3 on AWS Outposts 事件

- 使用高级事件选择器筛选数据事件
  - 筛选数据事件的依据 eventName
    - eventName使用筛选数据事件 AWS Management Console
    - eventName使用筛选数据事件 AWS CLI
  - 筛选数据事件的依据 resources.ARN
    - resources.ARN使用筛选数据事件 AWS Management Console
    - resources.ARN使用筛选数据事件 AWS CLI
  - 按readOnly值筛选数据事件
    - 使用按readOnly值筛选数据事件 AWS Management Console
    - 使用按readOnly值筛选数据事件 AWS CLI
- 记录 AWS Config 合规性的数据事件
- 使用 AWS SDK 记录数据事件
- 向 Amazon CloudWatch 日志发送事件

数据事件

下表显示可用于跟踪和事件数据存储的数据事件类型。数据事件类型（控制台）列显示控制台中的相应选择。resources.typ **`resources.type`** e 值列显示您将使用或 API 指定的值，以便在跟踪或事件数据存储中包含该 AWS CLI 类型的数据事件。 CloudTrail

对于跟踪，您可以使用基本或高级事件选择器来记录 Amazon S3 对象、Lambda 函数和 DynamoDB 表（显示在表的前三行）的数据事件。您只能使用高级事件选择器来记录其余行中显示的数据事件类型。

对于事件数据存储，只能使用高级事件选择器来包含数据事件。

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon DynamoDB	表上的 Amazon DynamoDB 项目级 API 活动（例如`PutItem`、`DeleteItem` 、`UpdateItem` 和 API 操作）。	DynamoDB	`AWS::DynamoDB::Table`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	Note 对于启用了流的表，数据事件中的 `resources` 字段同时包含 `AWS::DynamoDB::Stream` 和 `AWS::DynamoDB::Table`。如果您为 `resources.type` 指定 `AWS::DynamoDB::Table`，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请 `eventName` 在该字段上添加过滤器。		
AWS Lambda	AWS Lambda 函数执行活动（`InvokeAPI`）。	Lambda	`AWS::Lambda::Function`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon S3	针@@ 对 S3 存储桶中对象的 Amazon S3 对象级 PutObject API 活动（例如GetObject DeleteObject 、和 API 操作）。	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 用于配置操作的 API 活动，例如对StartConfiguration Session 和的调用GetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration
AWS B2B 数据交换	用于转换器操作的 B2B 数据交换 API 活动，例如对 GetTransformerJob 和 StartTransformerJob 的调用。	B2B 数据交换	AWS::B2BI::Transformer
Amazon Bedrock	代理别名上的 Amazon Bedrock API 活动。	Bedrock 代理别名	AWS::Bedrock::AgentAlias
	知识库上的 Amazon Bedrock API 活动。	Bedrock 知识库	AWS::Bedrock::KnowledgeBase

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon CloudFront	CloudFront 在 a 上的 API 活动KeyValueStore。	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map 命名空间上的 API 活动。	AWS Cloud Map 命名空间	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map 服务上的 API 活动。	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` 用于记录外部事件的 L CloudTrail ake 频道上的活动 AWS。	CloudTrail 频道	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	亚马逊 CodeWhisperer API 在自定义方面的活动。	CodeWhisperer 定制	`AWS::CodeWhisperer::Customization`
	个人资料上的亚马逊 CodeWhisperer API 活动。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	针对 Amazon Cognito 身份池的 Amazon Cognito API 活动。	Cognito 身份池	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	针对流的 Amazon DynamoDB API 活动	DynamoDB Streams	`AWS::DynamoDB::Stream`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) 直接 API，例如 Amazon EBS 快照上的 PutSnapshotBlock 、GetSnapshotBlock 和 ListChangedBlocks 。	Amazon EBS 直接 API	AWS::EC2::Snapshot
Amazon EMR	针对预写日志工作空间的 Amazon EMR API 活动。	EMR 预写日志工作空间	AWS::EMRWAL::Workspace
Amazon FinSpace	针对环境的 Amazon FinSpace API 活动	FinSpace	AWS::FinSpace::Environment

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS Glue	AWS Glue 在 Lake Formation 创建的表格上的 API 活动。 **Note** AWS Glue 目前仅以下区域支持表的数据事件： • 美国东部（弗吉尼亚州北部） • 美国东部（俄亥俄州） • 美国西部（俄勒冈州） • 欧洲地区（爱尔兰） • Asia Pacific（Tokyo）Region	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	探测器的亚马逊 GuardDuty API 活动。	GuardDuty 探测器	`AWS::GuardDuty::Detector`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS HealthImaging	AWS HealthImaging 数据存储上的 API 活动。	医学成像数据存储	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT 证书上@@的 API 活动。	物联网证书	`AWS::IoT::Certificate`
	AWS IoT API 在事物上的活动。	物联网的东西	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	组件版本上来自 Greengrass 核心设备的 Greengrass API 活动。 **Note** Greengrass 不会记录被拒绝访问的事件。	物联网 Greengrass 组件版本	`AWS::GreengrassV2::ComponentVersion`
	部署时来自 Greengrass 核心设备的 Greengrass API 活动。 **Note** Greengrass 不会记录被拒绝访问的事件。	物联网 Greengrass 部署	`AWS::GreengrassV2::Deployment`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
AWS IoT SiteWise	资产上的@@ 物联网 SiteWise API 活动。	物联网 SiteWise 资产	AWS::IoTSiteWise::Asset
	时间序列上的@@ 物联网 SiteWise API 活动。	物联网 SiteWise 时间序列	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	实体上的物联网 TwinMaker API 活动。	物联网 TwinMaker 实体	AWS::IoTTwinMaker::Entity
	工作空间上 TwinMaker 的 IoT API 活动。	物联网 TwinMaker 工作空间	AWS::IoTTwinMaker::Workspace
Amazon Kendra Intelligent Ranking	针对重新评分执行计划的 Amazon Kendra Intelligent Ranking API 活动。	Kendra 排名	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces（Apache Cassandra 兼容）	表上的 Amazon Keyspaces API 活动。	卡桑德拉桌	AWS::Cassandra::Table
Amazon Kinesis Data Streams	直播中的 Kinesis Data Streams API 活动。	Kinesis 直播	AWS::Kinesis::Stream
	Kinesis Data Streams 针对直播使用者的 API 活动。	Kinesis 直播消费者	AWS::Kinesis::StreamConsumer

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon Kinesis Video Streams	Kinesis Video Streams 视频流上的 API 活动，例如GetMedia对和的调用。PutMedia	Kinesis 视频流	AWS::KinesisVideo::Stream
Amazon Managed Blockchain	针对网络的 Amazon Managed Blockchain API 活动。	托管区块链网络	AWS::ManagedBlockchain::Network
	针对 Ethereum 节点的 Amazon Managed Blockchain JSON-RPC 调用，如 eth_getBalance 或 eth_getBlockByNumber 。	托管区块链	AWS::ManagedBlockchain::Node
Amazon Neptune 图形	Neptune Graph 上的数据 API 活动，例如查询、算法或向量搜索。	Neptune 图形	AWS::NeptuneGraph::Graph
AWS Private CA	AWS Private CA 活动目录 API 活动的连接器。	AWS Private CA 活动目录连接器	AWS::PCAConnectorAD::Connector
亚马逊 Q 应用程序	亚马逊 Q 应用程序上的数据 API 活动。	亚马逊 Q 应用程序	AWS::QApps:QApp
Amazon Q Business	应用程序上的 Amazon Q Business API 活动。	Amazon Q Business 应用程序	AWS::QBusiness::Application

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
	数据来源上的 Amazon Q Business API 活动。	Amazon Q Business 数据来源	`AWS::QBusiness::DataSource`
	索引上的 Amazon Q Business API 活动。	Amazon Q Business 索引	`AWS::QBusiness::Index`
	Web 体验上的 Amazon Q Business API 活动。	Amazon Q Business Web 体验	`AWS::QBusiness::WebExperience`
Amazon RDS	数据库集群上的 Amazon RDS API 活动。	RDS 数据 API-数据库集群	`AWS::RDS::DBCluster`
Amazon S3	接入点上的 Amazon S3 API 活动。	S3 接入点	`AWS::S3::AccessPoint`
	Amazon S3 对象 Lambda 接入点 API 活动，例如对和的调用。`CompleteMultipartUpload` `GetObject`	S3 对象 Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 on Outposts 对象级别 API 活动。	S3 Outposts	`AWS::S3Outposts::Object`

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon SageMaker	亚马逊在终端节点上的 SageMaker InvokeEndpointWithResponseStream 活动。	SageMaker 端点	AWS::SageMaker::Endpoint
	特色商店中的亚马逊 SageMaker API 活动。	SageMaker feature store	AWS::SageMaker::FeatureGroup
	Amazon SageMaker API 在实验试用组件上的活动。	SageMaker 指标实验试验组件	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	针对平台端点的 Amazon SNS Publish API 操作。	SNS 平台端点	AWS::SNS::PlatformEndpoint
	针对主题的 Amazon SNS Publish 和 PublishBatch API 操作。	SNS 主题	AWS::SNS::Topic
Amazon SQS	消息上的 Amazon SQS API 活动。	SQS	AWS::SQS::Queue
AWS Step Functions	Step Functions API 在状态机上的活动。	Step Functions 状态机	AWS::StepFunctions::StateMachine
AWS Supply Chain	AWS Supply Chain 实例上的 API 活动。	供应链	AWS::SCN::Instance

AWS 服务	描述	数据事件类型（控制台）	resources.type 值
Amazon SWF	域名上的@@ 亚马逊 SWF API 活动。	SWF 域名	AWS::SWF::Domain
AWS Systems Manager	控制通道上的 Systems Manager API 活动。	Systems Manager (系统管理员)	AWS::SSMMessages::ControlChannel
	托管节点上的 Systems Manager API 活动。	Systems Manager 托管式节点	AWS::SSM::ManagedNode
Amazon Timestream	针对数据库的 Amazon Timestream Query API 活动。	Timestream 数据库	AWS::Timestream::Database
	针对表的 Amazon Timestream Query API 活动。	Timestream 表	AWS::Timestream::Table
Amazon Verified Permissions	针对策略存储的 Amazon Verified Permissions API 活动。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces 瘦客户机	WorkSpaces 设备上的瘦客户端 API 活动。	瘦客户端设备	AWS::ThinClient::Device
	WorkSpaces 环境中的瘦客户端 API 活动。	瘦客户端环境	AWS::ThinClient::Environment
AWS X-Ray	追踪上@@ 的 X-Ray API 活动。	X 射线追踪	AWS::XRay::Trace

要记录 CloudTrail 数据事件，必须明确添加要为其收集活动的每种资源类型。有关更多信息，请参阅创建跟踪 和 使用控制台为事件创建 CloudTrail事件数据存储。

在单区域跟踪或事件数据存储上，您只能为可在该区域中访问的资源记录数据事件。尽管 S3 存储桶是全球性的，但 AWS Lambda 函数和 DynamoDB 表是区域性的。

记录数据事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

示例：记录 Simple Storage Service（Amazon S3）对象的数据事件

记录一个 S3 存储桶中的所有 S3 对象的数据事件

下面的示例演示在为一个名为 *bucket-1* 的 S3 存储桶中的所有数据事件配置日志记录时日志记录是如何工作的。在此示例中，CloudTrail 用户指定了一个空前缀，并指定了记录读取和写入数据事件的选项。

1. 用户将对象上传到 bucket-1。
2. PutObject API 操作是 Simple Storage Service（Amazon S3）对象级别的 API。它被记录为中的数据事件 CloudTrail。由于 CloudTrail 用户指定的 S3 存储桶前缀为空，因此会记录在该存储桶中任何对象上发生的事件。跟踪或事件数据存储将处理和记录事件。
3. 另一个用户将对象上传到 bucket-2。
4. PutObject API 操作发生在不是为跟踪或事件数据存储指定的 S3 存储桶中的某个对象上。跟踪或事件数据存储不会记录事件。

记录特定 S3 对象的数据事件

下面的示例演示在为特定 S3 对象配置跟踪或事件数据存储以记录事件时日志记录的工作方式。在此示例中，CloudTrail 用户指定了一个名为 b***ucket-3 # S3*** 存储桶，其前缀为 ***my-images***，并且可以选择仅记录写入数据事件。

1. 一个用户在存储桶中检测到一个以 my-images 前缀开头的对象，例如 arn:aws:s3:::bucket-3/my-images/example.jpg。
2. DeleteObject API 操作是 Simple Storage Service（Amazon S3）对象级别的 API。它在中被记录为写入数据事件 CloudTrail。事件发生在与跟踪或事件数据存储中指定的 S3 存储桶和前缀匹配的对象上。跟踪或事件数据存储将处理和记录事件。
3. 另一个用户删除了 S3 存储桶中一个带不同前缀的对象，例如 arn:aws:s3:::bucket-3/my-videos/example.avi。
4. 事件发生在与跟踪或事件数据存储中指定的前缀不匹配的对象上。跟踪或事件数据存储不会记录事件。

5. 一个用户对对象 `arn:aws:s3:::bucket-3/my-images/example.jpg` 调用 `GetObject` API 操作。
6. 虽然事件发生在跟踪或事件数据存储中指定的存储桶和前缀上，但 `GetObject` 是读取类型的 Amazon S3 对象级别 API。它被记录为读取数据事件 CloudTrail，并且跟踪或事件数据存储未配置为记录读取事件。跟踪或事件数据存储不会记录事件。

> **Note**
>
> 对于跟踪，如果记录特定 Amazon S3 存储桶的数据事件，建议不要使用将记录其数据事件的 Amazon S3 存储桶来接收在数据事件部分为跟踪指定的日志文件。使用相同的 Simple Storage Service（Amazon S3）存储桶会导致您的跟踪在日志文件每次传输到 Simple Storage Service（Amazon S3）存储桶时都记录数据事件。日志文件是按时间间隔传输的聚合事件，因此，事件与日志文件的比率不是 1:1；事件将记录到下一个日志文件中。例如，当 CloudTrail 传送日志时，`PutObject`事件会发生在 S3 存储桶上。如果还在数据事件部分中指定了 S3 存储桶，跟踪将处理 `PutObject` 事件并将其记录为数据事件。该操作是另一个 `PutObject` 事件，并且跟踪将重新处理和记录此事件。
>
> 如果您配置跟踪以记录 AWS 账户中的所有 Amazon S3 数据事件，为避免记录接收日志文件的 Amazon S3 存储桶的数据事件，请考虑配置将日志文件传输到属于其他 AWS 账户的 Amazon S3 存储桶。有关更多信息，请参阅 接收来自多个账户的 CloudTrail 日志文件。

记录其他 AWS 账户中 S3 对象的数据事件

将跟踪配置为记录数据事件时，还可以指定属于其他 AWS 账户的 S3 对象。当事件发生在指定对象上时， CloudTrail 会评估该事件是否与每个账户中的任何跟踪相匹配。如果事件与某个跟踪设置匹配，则跟踪将处理并记录该账户的事件。通常，API 调用者和资源所有者都可以接收事件。

如果您拥有一个 S3 对象并且在跟踪中指定此对象，则您的跟踪将记录在您的账户中的对象上发生的事件。由于您拥有该对象，因此您的跟踪还将在其他账户调用该对象时记录事件。

如果您在跟踪中指定一个 S3 对象，并且其他账户拥有此对象，则您的跟踪仅记录在您的账户中的此对象上发生的事件。您的跟踪不会记录其他账户中发生的事件。

示例：记录两个 AWS 账户的 Simple Storage Service（Amazon S3）对象的数据事件

以下示例显示了两个 AWS 账户如何配置 CloudTrail 以记录同一 S3 对象的事件。

1. 在您的账户中，您希望您的跟踪记录名为 owner-bucket 的 S3 存储桶中所有对象的数据事件。通过指定带空对象前缀的 S3 存储桶来配置跟踪。
2. Bob 拥有一个单独的账户，该账户已获得对 S3 存储桶的访问权限。Bob 还希望记录同一 S3 存储桶中所有对象的数据事件。对于其跟踪，他配置了跟踪并指定带空对象前缀的同一 S3 存储桶。
3. Bob 使用 PutObject API 操作将对象上传到 S3 存储桶。
4. 此事件在他的账户中发生，并且与他的跟踪设置匹配。Bob 的跟踪将处理和记录该事件。
5. 由于您拥有 S3 存储桶并且事件与您的跟踪设置匹配，因此您的跟踪也将处理和记录同一事件。由于该事件现在有两个副本（一个记录在 Bob 的跟踪中，一个记录在您的跟踪中），因此需要为数据事件的两个副本 CloudTrail 收费。
6. 您将一个对象上传到 S3 存储桶。
7. 此事件在您的账户中发生并且与您的跟踪设置匹配。您的跟踪将处理和记录此事件。
8. 由于该事件未发生在 Bob 的账户中，而且他不拥有 S3 存储桶，因此 Bob 的跟踪不会记录该事件。 CloudTrail 仅对此数据事件的一份副本收费。

示例：记录所有存储桶的数据事件，包括两个 AWS 账户使用的 S3 存储桶

以下示例显示了为在账户中收集数据事件的跟踪启用 “选择账户中的所有 S3 存储桶” 时的日志行为。AWS

1. 在您的账户中，您希望您的跟踪记录所有 S3 存储桶的数据事件。在 Data events（数据事件）中的 All current and future S3 buckets（所有当前和未来 S3 存储桶）下，您可以通过选择 Read（读取）事件、Write（写入）事件或同时选择两者，来配置跟踪。
2. Bob 拥有一个单独的账户，该账户已被授予对您账户中 S3 存储桶的访问权限。他想记录他有权访问的存储桶的数据事件。他配置他的跟踪以获取所有 S3 存储桶的数据事件。
3. Bob 使用 PutObject API 操作将对象上传到 S3 存储桶。
4. 此事件在他的账户中发生，并且与他的跟踪设置匹配。Bob 的跟踪将处理和记录该事件。
5. 由于您拥有 S3 存储桶并且事件与您跟踪的设置匹配，因此您的跟踪也将处理和记录此事件。由于该事件现在有两个副本（一个记录在 Bob 的跟踪中，一个记录在你的跟踪中），所以每个账户都要向每个账户 CloudTrail 收取一份数据事件的副本。
6. 您将一个对象上传到 S3 存储桶。
7. 此事件在您的账户中发生并且与您的跟踪设置匹配。您的跟踪将处理和记录此事件。
8. 由于该事件未发生在 Bob 的账户中，而且他不拥有 S3 存储桶，因此 Bob 的跟踪不会记录该事件。 CloudTrail 仅对您账户中此数据事件的一份副本收费。

9. 第三个用户 Mary 可以访问 S3 存储桶，并在存储桶上运行 GetObject 操作。她有一个跟踪配置为记录其账户中所有 S3 存储桶上的数据事件。因为她是 API 调用者，所以在她的跟踪中 CloudTrail 记录了一个数据事件。虽然 Bob 有权访问该存储桶，但他不是资源所有者，因此这次未在他的跟踪中记录任何事件。作为资源所有者，您在跟踪中会收到一个关于 Mary 调用的GetObject操作的事件。 CloudTrail针对数据事件的每份副本向你的账户和 Mary 的账户收费：一份在 Mary 的踪迹中，一份在你的踪迹中。

只读和只写事件

在配置跟踪或事件数据存储以记录数据事件和管理事件时，可以指定是需要只读事件、只写事件还是两者都需要。

- 读取

  Read（读取）事件包括将读取您的资源但不进行更改的 API 操作。例如，只读事件包括 Amazon EC2 DescribeSecurityGroups 和 DescribeSubnets API 操作。这些操作仅返回有关 Amazon EC2 资源的信息，但不更改您的配置。

- 写入

  Write（写入）事件包括将修改（或可能修改）您的资源的 API 操作。例如，Amazon EC2 RunInstances 和 TerminateInstances API 操作将修改您的实例。

示例：为单独的跟踪记录记录读取事件和写入事件

以下示例说明如何将跟踪记录配置为将账户的日志活动拆分到单独的 S3 存储桶中：一个存储桶接收只读事件，另一个存储桶接收只写事件。

1. 您创建一个跟踪并选择一个名为 read-only-bucket 的 S3 存储桶来接收日志文件。然后，您更新跟踪以指定您需要 Read（读取）管理事件和数据事件。
2. 您创建另一个跟踪并选择一个名为 write-only-bucket 的 S3 存储桶来接收日志文件。然后，您更新跟踪以指定您需要 Write（写入）管理事件和数据事件。
3. Amazon EC2 DescribeInstances 和 TerminateInstances API 操作将在您的账户中执行。
4. DescribeInstances API 操作是只读事件，它匹配第一个跟踪的设置。跟踪将记录事件并将事件传送到 read-only-bucket。
5. TerminateInstances API 操作是只写事件，它匹配第二个跟踪的设置。跟踪将记录事件并将事件传送到 write-only-bucket。

使用记录数据事件 AWS Management Console

以下程序介绍如何通过使用 AWS Management Console更新现有的事件数据存储或跟踪以记录数据事件。有关如何创建事件数据存储以记录数据事件的信息，请参阅 使用控制台为事件创建 CloudTrail事件数据存储。有关如何创建跟踪以记录数据事件的信息，请参阅 在控制台中创建跟踪。

对于跟踪，根据您使用的是高级事件选择器还是基本事件选择器，记录数据事件的步骤会有所不同。您可以使用高级事件选择器记录所有数据事件类型的数据事件，但是如果您使用基本事件选择器，则只能记录 Amazon S3 存储桶和存储桶对象、 AWS Lambda 函数和 Amazon DynamoDB 表的数据事件。

更新现有的事件数据存储以记录数据事件 AWS Management Console

按照以下程序更新现有的事件数据存储以记录数据事件。有关使用高级事件选择器的更多信息，请参阅本主题使用高级事件选择器筛选数据事件中的。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，在 Lake 下，选择事件数据存储。
3. 在事件数据存储页面上，选择要更新的事件数据存储。

   > **Note**
   >
   > 您只能在包含事件的事件数据存储上启用数据 CloudTrail 事件。您无法在 AWS Config 配置项目、 CloudTrail Insights CloudTrail 事件或非事件的事件数据存储上启用数据AWS 事件。

4. 在详细信息页面上的数据事件中，选择编辑。
5. 如果您尚未记录数据事件，请选择 Data events（数据事件）复选框。
6. 对于 Data event type（数据事件类型），选择要在其上记录数据事件的资源类型。
7. 选择日志选择器模板。 CloudTrail 包括用于记录该资源类型的所有数据事件的预定义模板。要构建自定义日志选择器模板，请选择 Custom（自定义）。
8. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。
9. 在 Advanced event selectors（高级事件选择器）中，为您要记录其数据事件的特定资源构建表达式。如果您使用的是预定义日志模板，则可跳过此步骤。

   a. 从下面的字段中选择。

- **readOnly**-readOnly 可以设置为等于true或false的值。只读数据事件是不会更改资源状态的事件，例如 Get* 或 Describe* 事件。写入事件可添加、更改或删除资源、属性或构件，例如 Put*、Delete* 或 Write* 事件。要记录 read 和 write 两种事件，请不要添加 readOnly 选择器。
- **eventName** - eventName 可以使用任何运算符。您可以使用它来包含或排除记录到的任何数据事件 CloudTrail，例如PutBucketGetItem、或GetSnapshotBlock。
- **resources.ARN**-您可以将任何运算符与一起使用resources.ARN，但是如果您使用等于或不等于，则该值必须与您在模板中指定为的值的有效资源的 ARN 完全匹配。resources.type

  下表显示每个 resources.type 的有效 ARN 格式。

  > **Note**
  >
  > 您不能使用该resources.ARN字段筛选没有 ARN 的资源类型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*

resources.type	resources.ARN
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-aliases/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*

resources.type	resources.ARN
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*

resources.type	resources.ARN
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必须采用以下格式之一： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必须采用以下格式之一： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclie nt: *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] 对于启用了流的表，数据事件中的 resources 字段同时包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您为 resources.type 指定 AWS::DynamoDB::Table，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName在该字段上添加过滤器。

[2] 要记录特定 S3 存储桶中所有对象的所有数据事件，请使用 StartsWith 运算符，并且仅包含存储桶 ARN 作为匹配值。刻意使用尾部斜杠；切勿排除它。

[3] 要记录 S3 接入点中的所有对象的事件，建议您仅使用接入点 ARN，而不要包含对象路径，并且使用 StartsWith 或 NotStartsWith 运算符。

有关数据事件资源的 ARN 格式的更多信息，请参阅 AWS Identity and Access Management 用户指南中的操作、资源和条件键。

b. 对于每个字段，请选择 + 条件以根据需要添加任意数量的条件，所有条件总共可有最多 500 个指定值。例如，要从事件数据存储中记录的数据事件中排除两个 S3 存储桶的数据事件，您可以将该字段设置为 Resou rces.arn，将运算符设置为 “不开头”，然后粘贴到 S3 存储桶 ARN 中，或者浏览您不想为其记录事件的 S3 存储桶。

要添加第二个 S3 存储桶，请选择 + 条件，然后重复上述说明，在 ARN 中粘贴或浏览到不同的存储桶。

> **Note**
>
> 对于事件数据存储上的所有选择器，最多可以有 500 个值。这包括选择器的多个值的数组，例如 `eventName`。如果所有选择器均为单个值，则最多可以向选择器添加 500 个条件。

c. 根据需要，选择 + Field（+ 字段）以添加其他字段。为了避免错误，请不要为字段设置冲突或重复的值。例如，不要在一个选择器中将 ARN 指定为等于某个值，然后在另一个选择器中指定 ARN 不等于相同的值。

10. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。重复步骤 6 至此步骤，为数据事件类型配置高级事件选择器。
11. 查看并验证选择后，选择保存更改。

使用高级事件选择器更新现有跟踪以记录数据事件 AWS Management Console

在中 AWS Management Console，如果您的跟踪使用高级事件选择器，则可以从记录所选资源上的所有数据事件的预定义模板中进行选择。选择了日志选择器模板后，您可以自定义模板，以仅包含最希望查看的数据事件。有关使用高级事件选择器的更多信息，请参阅本主题使用高级事件选择器筛选数据事件中的。

1. 在控制台的 “ CloudTrail 控制面板” 或 “跟踪” 页面上，选择要更新的跟踪。
2. 在详细信息页面上的数据事件中，选择编辑。
3. 如果您尚未记录数据事件，请选择 Data events（数据事件）复选框。
4. 对于 Data event type（数据事件类型），选择要在其上记录数据事件的资源类型。
5. 选择日志选择器模板。 CloudTrail 包括用于记录该资源类型的所有数据事件的预定义模板。要构建自定义日志选择器模板，请选择 Custom（自定义）。

> **Note**
>
> 为 S3 存储桶选择预定义的模板可以记录当前您 AWS 账户中的所有存储分段以及您在创建完跟踪后创建的任何存储分段的数据事件。它还允许记录您 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于其他 AWS 账户的存储桶上执行的。

如果跟踪仅应用于一个区域，则选择记录所有 S3 存储桶的预定义模板可为跟踪所在的区域中的所有存储桶和您后来在该区域中创建的任何存储桶启用数据事件日志记录。它不会在您的 AWS 账户中记录其他区域的 Amazon S3 存储桶的数据事件。
如果您要为所有区域创建跟踪，则选择 Lambda 函数的预定义模板可以记录当前 AWS 账户中的所有函数以及您在完成跟踪创建后可能在任何区域创建的任何 Lambda 函数的数据事件。如果您要为单个区域创建跟踪（对于跟踪，只能使用来完成此操作 AWS CLI），则此选择将启用您 AWS 账户中当前位于该区域的所有函数以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
记录所有功能的数据事件还可以记录 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

6. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。

7. 在 Advanced event selectors（高级事件选择器）中，为您要记录其数据事件的特定资源构建表达式。如果您使用的是预定义日志模板，则可跳过此步骤。

   a. 从下面的字段中选择。

   - **readOnly**-readOnly 可以设置为等于true或false的值。只读数据事件是不会更改资源状态的事件，例如 Get* 或 Describe* 事件。写入事件可添加、更改或删除资源、属性或构件，例如 Put*、Delete* 或 Write* 事件。要记录 read 和 write 两种事件，请不要添加 readOnly 选择器。
   - **eventName** - eventName 可以使用任何运算符。您可以使用它来包含或排除记录到的任何数据事件 CloudTrail，例如PutBucketGetItem、或GetSnapshotBlock。
   - **resources.ARN**-您可以将任何运算符与一起使用resources.ARN，但是如果您使用等于或不等于，则该值必须与您在模板中指定为的值的有效资源的 ARN 完全匹配。resources.type

     下表显示每个 resources.type 的有效 ARN 格式。

     > **Note**
     > 您不能使用该resources.ARN字段筛选没有 ARN 的资源类型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*

resources.type	resources.ARN
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*

resources.type	resources.ARN
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*

resources.type	resources.ARN
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*

resources.type	resources.ARN
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*

resources.type	resources.ARN
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必须采用以下格式之一： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	ARN 必须采用以下格式之一： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 对于启用了流的表，数据事件中的 `resources` 字段同时包含 `AWS::DynamoDB::Stream` 和 `AWS::DynamoDB::Table`。如果您为 `resources.type` 指定 `AWS::DynamoDB::Table`，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请`eventName`在该字段上添加过滤器。

[2] 要记录特定 S3 存储桶中所有对象的所有数据事件，请使用 `StartsWith` 运算符，并且仅包含存储桶 ARN 作为匹配值。刻意使用尾部斜杠；切勿排除它。

[3] 要记录 S3 接入点中的所有对象的事件，建议您仅使用接入点 ARN，而不要包含对象路径，并且使用 `StartsWith` 或 `NotStartsWith` 运算符。

有关数据事件资源的 ARN 格式的更多信息，请参阅 AWS Identity and Access Management 用户指南中的操作、资源和条件键。

b. 对于每个字段，请选择 + 条件以根据需要添加任意数量的条件，所有条件总共可有最多 500 个指定值。例如，要从跟踪中记录的数据事件中排除两个 S3 存储桶的数据事件，您可以将该字段设置为 Resou rces.arn，将运算符设置为 “不以开头”，然后粘贴到 S3 存储桶 ARN 中，或者浏览您不想为其记录事件的 S3 存储桶。

要添加第二个 S3 存储桶，请选择 + 条件，然后重复上述说明，在 ARN 中粘贴或浏览到不同的存储桶。

> **Note**
>
> 对于跟踪上的所有选择器，最多可以有 500 个值。这包括选择器的多个值的数组，例如 `eventName`。如果所有选择器均为单个值，则最多可以向选择器添加 500 个条件。

c. 根据需要，选择 + Field（+ 字段）以添加其他字段。为了避免错误，请不要为字段设置冲突或重复的值。例如，不要在一个选择器中将 ARN 指定为等于某个值，然后在另一个选择器中指定 ARN 不等于相同的值。

8. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。重复步骤 4 至此步骤，为数据事件类型配置高级事件选择器。

9. 查看并验证选择后，选择保存更改。

更新现有跟踪以使用基本事件选择器记录数据事件 AWS Management Console

按照以下程序，使用基本事件选择器更新现有跟踪以记录数据事件。

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 打开 CloudTrail 控制台的 T ra ils 页面并选择跟踪名称。

> **Note**
>
> 虽然您可以编辑现有跟踪以记录数据事件，但作为最佳实践，请考虑专门创建单独的跟踪以记录数据事件。

3. 对于 Data event（数据事件），选择 Edit（编辑）。
4. 对于 Simple Storage Service（Amazon S3）存储桶：
   a. 对于 Data event source（数据事件源），选择 S3。
   b. 您可以选择记录 All current and future S3 buckets（所有当前和未来 S3 存储桶），也可以指定单个存储桶或函数。默认情况下，记录所有当前和未来 S3 存储桶的数据事件。

      > **Note**
      >
      > 保留默认 “All current and future S3 存储桶” 选项将允许您 AWS 账户中当前的所有存储分段以及您在完成跟踪创建后创建的任何存储分段的数据事件记录。它还允许记录您 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于其他 AWS 账户的存储桶上执行的。
      > 如果您要为单个区域创建跟踪（使用完成 AWS CLI），则选择 “选择账户中的所有 S3 存储桶” 选项可为与您的跟踪位于同一区域的所有存储桶以及您稍后在该区域创建的任何存储桶启用数据事件日志记录。它不会在您的 AWS 账户中记录其他区域的 Amazon S3 存储桶的数据事件。

   c. 如果保留默认值 All current and future S3 buckets（所有当前和未来 S3 存储桶），则选择记录 Read（读取）事件、Write（写入）事件，还是记录两者。
   d. 要选择单个存储桶，请清空 All current and future S3 buckets（所有当前和未来 S3 存储桶）的 Read（读取）和Write（写入）复选框。在 Individual bucket selection（单个存储桶选择）中，浏览要在其上记录数据事件的存储桶。要查找特定存储桶，键入所需存储桶的存储桶前缀。您可以在此窗口中选择多个存储桶。选择添加存储桶，记录更多存储桶的数据事件。选择

记录 Read（读取）事件（如 `GetObject`）、Write（写入）事件（如 `PutObject`）或同时记录两种事件。

此设置优先于为各个存储桶配置的个别设置。例如，如果指定记录所有 S3 存储桶的 Read 事件，然后选择为数据事件日志记录添加一个特定存储桶，则所添加存储桶的 Read 已经是选中状态。您无法清除此选择。只能配置 Write 选项。

要从日志记录中删除存储桶，请选择 X。

5. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。
6. 对于 Lambda 函数：

   a. 对于 Data event source（数据事件源），选择 Lambda。

   b. 在 Lambda function（Lambda 函数）中，选择 All regions（所有区域）记录所有 Lambda 函数，或选择 Input function as ARN（输入函数作为 ARN）以记录特定函数上的数据事件。

   要记录 AWS 账户中的所有 Lambda 函数的数据事件，请选择 Log all current and future functions（记录所有当前和未来函数）。此设置优先于为各个函数配置的个别设置。将记录所有函数，即便这些函数未显示。

   > **Note**
   >
   > 如果为所有区域创建了一个跟踪，则此选择将为您的 AWS 账户中当前包含的所有函数以及您在创建跟踪后可能在任何区域中创建的任何 Lambda 函数启用数据事件日志记录。如果您要为单个区域创建跟踪（使用完成 AWS CLI），则此选择将启用您 AWS 账户中该区域中当前所有函数的数据事件记录，以及您在完成跟踪创建后可能在该区域创建的任何 Lambda 函数的数据事件记录。它不会为在其他区域中创建的 Lambda 函数启用数据事件日志记录。
   > 记录所有功能的数据事件还可以记录 AWS 账户中任何用户或角色执行的数据事件活动，即使该活动是在属于另一个 AWS 账户的函数上执行的。

   c. 如果选择 Input function as ARN（输入函数作为 ARN），则输入 Lambda 函数的 ARN。

   > **Note**
   >
   > 如果您的账户中有超过 15,000 个 Lambda 函数，则在创建跟踪时无法在 CloudTrail 控制台中查看或选择所有函数。您仍可以选择该选项来记录所有函数，即使未显示这些函数也是如此。如果您要记录特定函数的数据事件，则可手动添加一个函数 (如果您知道其 ARN)。您也可以在控制台中完成跟踪的创建，然后使用 AWS CLI 和put-

event-selectors命令为特定 Lambda 函数配置数据事件记录。有关更多信息，请参阅使用管理跟踪 AWS CLI。

7. 要添加需要记录数据事件的其他数据类型，请选择 Add data event type（添加数据事件类型）。
8. 对于 DynamoDB 表：
   a. 对于 Data event source（数据事件源），选择 DynamoDB。
   b. 在 DynamoDB table selection（DynamoDB 表选择）中，选择 Browse（浏览）以选择一个表，或粘贴到您有权访问的 DynamoDB 表的 ARN 中。DynamoDB 表 ARN 使用以下格式：

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   要添加另一个表，请选择 Add row（添加行），然后浏览到某个表或粘贴到您有权访问的表的 ARN 中。
9. 选择保存更改。

使用记录数据事件 AWS Command Line Interface

您可以使用 AWS CLI配置跟踪或事件数据存储以记录数据事件。

主题

- 使用记录跟踪的数据事件 AWS CLI
- 使用记录事件数据存储的数据事件 AWS CLI

使用记录跟踪的数据事件 AWS CLI

您可以使用 AWS CLI配置您的跟踪记录以记录管理事件和数据事件。

> **Note**
>
> - 请注意，如果您的账户正在记录管理事件的多个副本，将会产生费用。记录数据事件始终需要收取费用。有关更多信息，请参阅AWS CloudTrail 定价。
> - 您可以使用高级事件选择器或基本事件选择器，但不能同时使用两者。如果将高级事件选择器应用于跟踪，则所有现有的基本事件选择器都将被覆盖。
> - 如果您的跟踪使用基本的事件选择器，则您只能记录以下资源类型：

- `AWS::DynamoDB::Table`
- `AWS::Lambda::Function`
- `AWS::S3::Object`

要记录其他资源类型，您需要使用高级事件选择器。要将跟踪转换为高级事件选择器，请运行 get-event-selectors 命令以确认当前事件选择器，然后将高级事件选择器配置为与以前的事件选择器的覆盖范围相匹配，然后为要记录数据事件的任何资源类型添加选择器。

- 您可以使用高级事件选择器根据 `eventName`、`resources.ARN` 和 `readOnly` 字段的值来进行筛选，从而使您能够仅记录感兴趣的数据事件。有关配置这些字段的更多信息，请参阅 AdvancedFieldSelectorAWS CloudTrailAPI 参考和本主题使用高级事件选择器筛选数据事件中的。

要查看您的跟踪是否正在记录管理事件和数据事件，请运行 `get-event-selectors` 命令。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

该命令返回跟踪的事件选择器。

主题

- 使用高级事件选择器记录事件
- 使用高级事件选择器记录亚马逊 S3 存储桶的所有 Amazon S3 事件
- 使用高级事件选择器记录 Simple Storage Service（Amazon S3）on AWS Outposts 事件
- 使用基本事件选择器记录事件

使用高级事件选择器记录事件

> **Note**
>
> 如果将高级事件选择器应用于跟踪，则所有现有的基本事件选择器都将被覆盖。在配置高级事件选择器之前，请运行 get-event-selectors 命令以确认当前事件选择器，然后将高级事件选择器配置为与以前的事件选择器的覆盖范围相匹配，然后为要记录的任何其他数据事件添加选择器。

以下示例为名为的跟踪创建自定义高级事件选择器，*TrailName*以包括读取和写入管理事件（省略readOnly选择器），PutObject以及除名为的存储桶sample_bucket_name和名为的函数DeleteObject的数据事件之外的所有 Amazon S3 存储桶/前缀组合的数据事件。 AWS Lambda MyLambdaFunction由于这些都是自定义高级事件选择器，因此每组选择器都有一个描述性名称。请注意，尾随斜杠是 S3 存储桶的 ARN 值的一部分。

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

以下示例返回为跟踪配置的高级事件选择器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
```

```
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
```

```
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

使用高级事件选择器记录亚马逊 S3 存储桶的所有 Amazon S3 事件

> **Note**
>
> 如果将高级事件选择器应用于跟踪，则所有现有的基本事件选择器都将被覆盖。

以下示例说明如何配置您的跟踪以包含特定 S3 存储桶中的所有 Simple Storage Service（Amazon S3）对象的所有数据事件。S3 事件在 `resources.type` 字段中的值为 `AWS::S3::Object`。由于 S3 对象和 S3 存储桶的 ARN 值略有不同，因此必须为 `resources.ARN` 添加 `StartsWith` 运算符以捕获所有事件。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

该命令将返回以下示例输出。

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
```

```
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                }
            ]
        }
    ]
}
```

使用高级事件选择器记录 Simple Storage Service（Amazon S3）on AWS Outposts 事件

> **Note**
>
> 如果将高级事件选择器应用于跟踪，则所有现有的基本事件选择器都将被覆盖。

以下示例说明如何配置您的跟踪以包含您的 Outpost 中的 Outposts 对象上的所有 Simple Storage Service（Amazon S3）的所有数据事件。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

该命令将返回以下示例输出。

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

使用基本事件选择器记录事件

下面是显示基本事件选择器的 get-event-selectors 命令结果示例。默认情况下，当您使用创建跟踪时 AWS CLI，跟踪会记录所有管理事件。默认情况下，跟踪记录不记录数据事件。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

要将跟踪配置为记录管理事件和数据事件，请运行 put-event-selectors 命令。

以下示例说明如何使用基本事件选择器配置跟踪，以包含两个 S3 存储桶前缀中 S3 对象的所有管理事件和数据事件。您可以为一个跟踪指定 1 至 5 个事件选择器。您可以为一个跟踪指定 1 至 250 个数据资源。

> **Note**
>
> 如果您选择使用基本事件选择器限制数据事件，则最多只能有 250 个 S3 数据资源。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

该命令将返回为跟踪配置的事件选择器。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

使用记录事件数据存储的数据事件 AWS CLI

您可以使用 AWS CLI配置事件数据存储以包含数据事件。使用 `create-event-data-store` 命令创建新的事件数据存储以记录数据事件。使用 `update-event-data-store` 命令为现有事件数据存储更新高级事件选择器。

要查看事件数据存储是否包含数据事件，请运行 get-event-data-store 命令。

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

该命令会返回事件数据存储的设置。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

主题

- 包含存储桶的所有 Amazon S3 事件
- 包含 Amazon S3 on AWS Outposts 事件

包含存储桶的所有 Amazon S3 事件

以下示例说明如何配置事件数据存储以包含特定 S3 存储桶中所有 Amazon S3 对象的所有数据事件。S3 事件在 `resources.type` 字段中的值为 `AWS::S3::Object`。由于 S3 对象和 S3 存储桶的 ARN 值略有不同，因此必须为 `resources.ARN` 添加 `StartsWith` 运算符以捕获所有事件。

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

该命令将返回以下示例输出。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
```

```
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

包含 Amazon S3 on AWS Outposts 事件

以下示例说明如何配置事件数据存储，以包含 Outpost 中所有 Amazon S3 on Outposts 对象的全部数据事件。

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

该命令将返回以下示例输出。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
```

```
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

使用高级事件选择器筛选数据事件

本节介绍如何使用高级事件选择器来创建细粒度的选择器，这些选择器通过仅记录感兴趣的特定数据事件来帮助您控制成本。

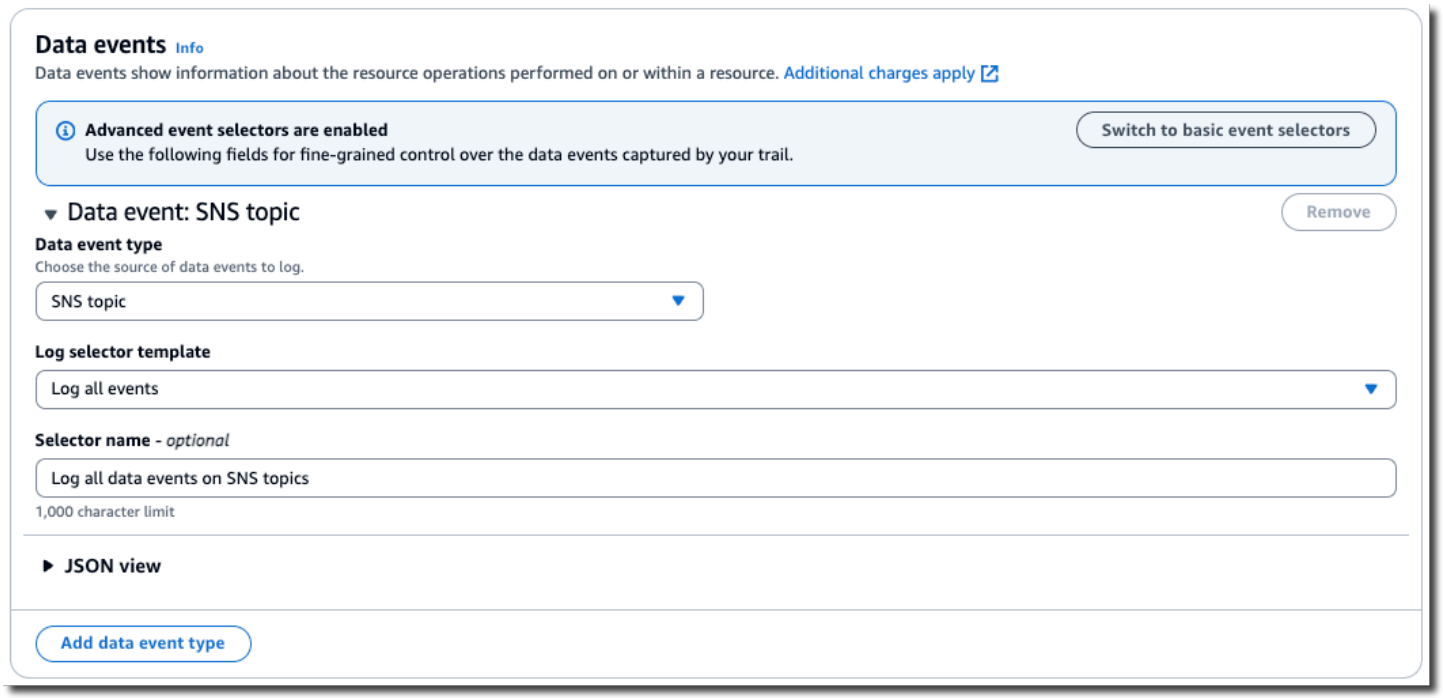
例如：

- 您可以通过在`eventName`字段上添加过滤器来包含或排除特定的 API 调用。
- 您可以通过在`resources.ARN`字段上添加过滤器来包含或排除特定资源的日志记录。例如，如果您正在记录 S3 数据事件，则可以排除对跟踪的 S3 存储桶的日志记录。
- 通过在字段上添加筛选器，您可以选择仅记录只写事件或只读事件。`readOnly`

下表提供了有关高级事件选择器的可配置字段的其他信息。

字段	必需	有效的运算符	Description
eventCategory	是	Equals	此字段设置为Data以记录数据事件。
resources.type	是	Equals	此字段用于选择要为其记录数据事件的资源类型。数据事件表显示了可能的值。
readOnly	否	Equals	这是一个可选字段，用于根据readOnly值包含或排除数据事件。true日志的值仅读取事件。false日志的值仅写入事件。如果不添加此字段，则会同时 CloudTrail 记录读取和写入事件。
eventName	否	任何	这是一个可选字段，用于筛选或筛选出记录到的任何数据事件 CloudTrail，例如或。PutBucket GetSnapshotBlock 如果您使用的是 AWS CLI，则可以通过用逗号分隔每个值来指定多个值。 如果您使用的是控制台，则可以通过为要筛选的每个eventName 值创建一个条件来指定多个值。
resources.ARN	否	任何	这是一个可选字段，用于通过提供来排除或包含特定资源的数据事件resources.ARN 。您可以将任何运算符与一起使用resources.ARN ，但是如果您使用Equals或NotEquals ，则该值必须与resoureces.type 您指定的有效资源的 ARN 完全匹配。 如果您使用的是 AWS CLI，则可以通过用逗号分隔每个值来指定多个值。 如果您使用的是控制台，则可以通过为要筛选的每个resources.ARN 值创建一个条件来指定多个值。

要使用 CloudTrail 控制台记录数据事件，请选择数据事件选项，然后在创建或更新跟踪或事件数据存储时选择感兴趣的数据事件类型。数据事件表显示了您可以在 CloudTrail 控制台上选择的可能的数据事件类型。



要使用记录数据事件 AWS CLI，请将`--advanced-event-selector`参数配置为将`eventCategory`等于，将`resources.type`值设置为等于`Data`且值等于您要记录数据事件的资源类型值。数据事件表列出了可用的资源类型。

例如，如果您想记录所有 Cognito 身份池的数据事件，则可以将`--advanced-event-selectors`参数配置为如下所示：

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
     }
]'
```

前面的示例记录了身份池上的所有 Cognito 数据事件。您可以进一步细化高级事件选择器，以筛选`eventName`、`readOnly`、和`resources.ARN`字段，以记录感兴趣的特定事件或排除不感兴趣的事件。

您可以配置高级事件选择器，以根据多个条件筛选数据事件。例如，您可以将高级事件选择器配置为记录所有 Amazon S3 PutObject 和 DeleteObject API 调用，但不包括特定 S3 存储桶的事件记录，如以下示例所示。

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
]'
```

您可以使用高级事件选择器来记录管理事件和数据事件。要记录多种资源类型的数据事件，请为要为其记录数据事件的每种资源类型添加字段选择器语句。

> **Note**
>
> Trails 可以使用基本事件选择器或高级事件选择器，但不能同时使用两者。如果将高级事件选择器应用于跟踪，则所有现有的基本事件选择器都将被覆盖。

主题

- 筛选数据事件的依据 eventName
- 筛选数据事件的依据 resources.ARN
- 按readOnly值筛选数据事件

筛选数据事件的依据 **eventName**

使用高级事件选择器，您可以根据eventName字段的值包含或排除事件。筛选eventName可以帮助控制成本，因为在记录数据事件时可以避免产生成本，从而增加对新数据 API 的支持。 AWS 服务

可以在该eventName字段中使用任何运算符。您可以使用它来筛选或筛选出记录到的任何数据事件 CloudTrail，例如或。PutBucket GetSnapshotBlock

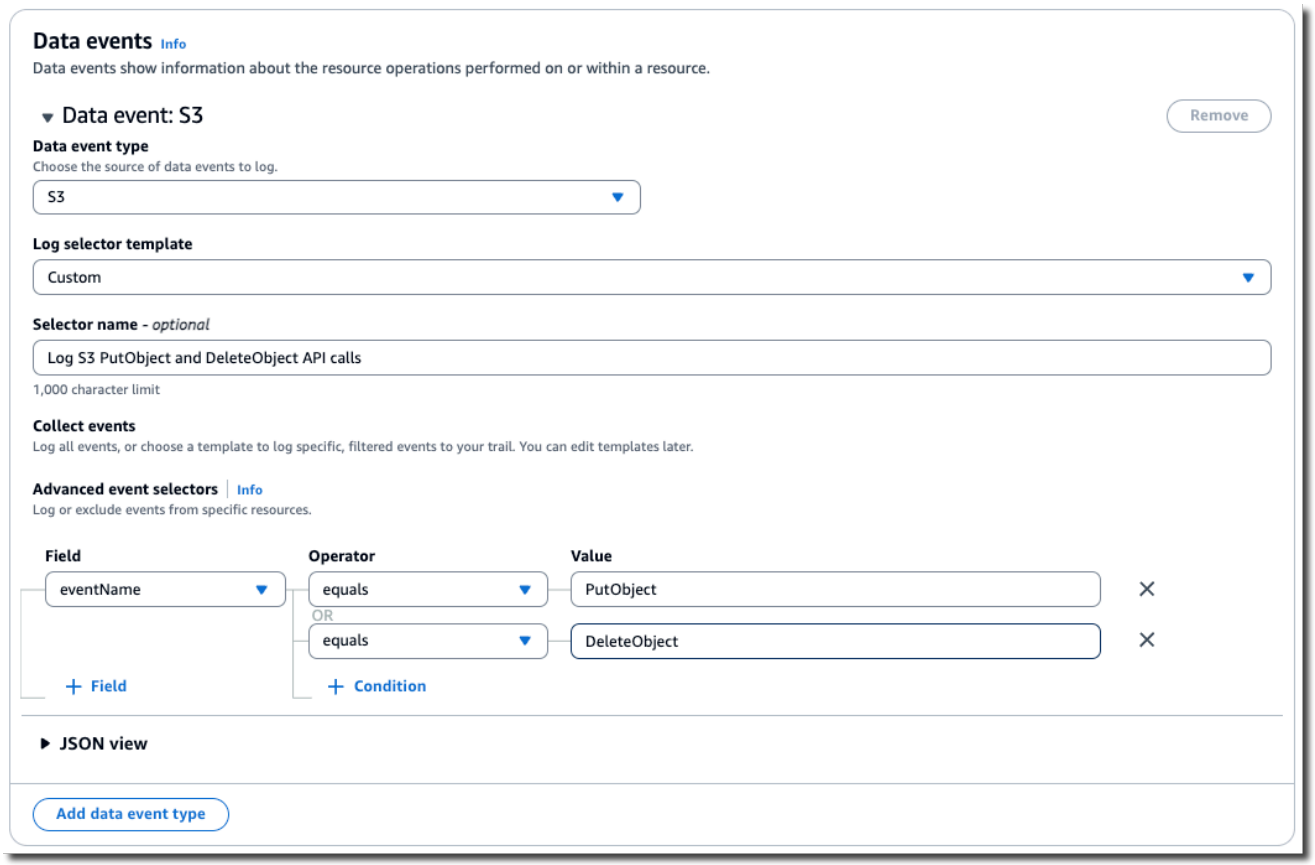
主题

- eventName使用筛选数据事件 AWS Management Console
- eventName使用筛选数据事件 AWS CLI

eventName使用筛选数据事件 AWS Management Console

按照以下步骤使用 CloudTrail 控制台对eventName字段进行筛选。

1. 按照创建跟踪过程中的步骤进行操作，或者按照创建事件数据存储过程中的步骤进行操作。
2. 按照步骤创建跟踪或事件数据存储时，请进行以下选择：
   a. 选择数据事件。
   b. 选择要记录其数据事件的数据事件类型。
   c. 对于日志选择器模板，请选择自定义。
   d. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。
   e. 在高级事件选择器中，执行以下操作以筛选：eventName
      i. 对于 “字段”，选择 “事件名称”。
      ii. 对于运算符，选择条件运算符。在此示例中，我们将选择 e quals，因为我们要记录特定的 API 调用。
      iii. 在 “值” 中，输入要筛选的事件的名称。
      iv. 要筛选其他条件eventName，请选择 + 条件。



f. 选择 +Field 可在其他字段上添加筛选器。

eventName使用筛选数据事件 AWS CLI

使用 AWS CLI，您可以对eventName字段进行筛选，以包含或排除特定事件。

以下示例记录了跟踪上的 S3 数据事件。配置--advanced-event-selectors为仅记录GetObjectPutObject、和 DeleteObject API 调用的数据事件。

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
```

```
  }
]'
```

下一个示例创建了一个新的事件数据存储，用于记录 EBS Direct API 的数据事件，但不包括 ListChangedBlocks API 调用。您可以使用update-event-data-store命令更新现有的事件数据存储。

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
         ]
    }
]'
```

筛选数据事件的依据 `resources.ARN`

使用高级事件选择器，您可以根据resources.ARN字段的值进行筛选。

您可以将任何运算符与一起使用resources.ARN，但是如果您使用Equals或NotEquals，则该值必须与您指定的resources.type值的有效资源的 ARN 完全匹配。要记录特定 S3 桶中所有对象的所有数据事件，请使用 StartsWith 运算符，并且仅包含存储桶 ARN 作为匹配值。

下表显示每个 resources.type 的有效 ARN 格式。

> **Note**
>
> 您不能使用该resources.ARN字段筛选没有 ARN 的资源类型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*

resources.type	resources.ARN
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*

resources.type	resources.ARN
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*

resources.type	resources.ARN
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必须采用以下格式之一： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必须采用以下格式之一： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*

resources.type	resources.ARN
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 对于启用了流的表，数据事件中的 resources 字段同时包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您为 resources.type 指定 AWS::DynamoDB::Table，则原定设置情况下，它将同时记录 DynamoDB 表和 DynamoDB 流事件。要排除直播事件，请eventName在该字段上添加过滤器。

[2] 要记录特定 S3 存储桶中所有对象的所有数据事件，请使用 StartsWith 运算符，并且仅包含存储桶 ARN 作为匹配值。刻意使用尾部斜杠；切勿排除它。

[3] 要记录 S3 接入点中的所有对象的事件，建议您仅使用接入点 ARN，而不要包含对象路径，并且使用 StartsWith 或 NotStartsWith 运算符。

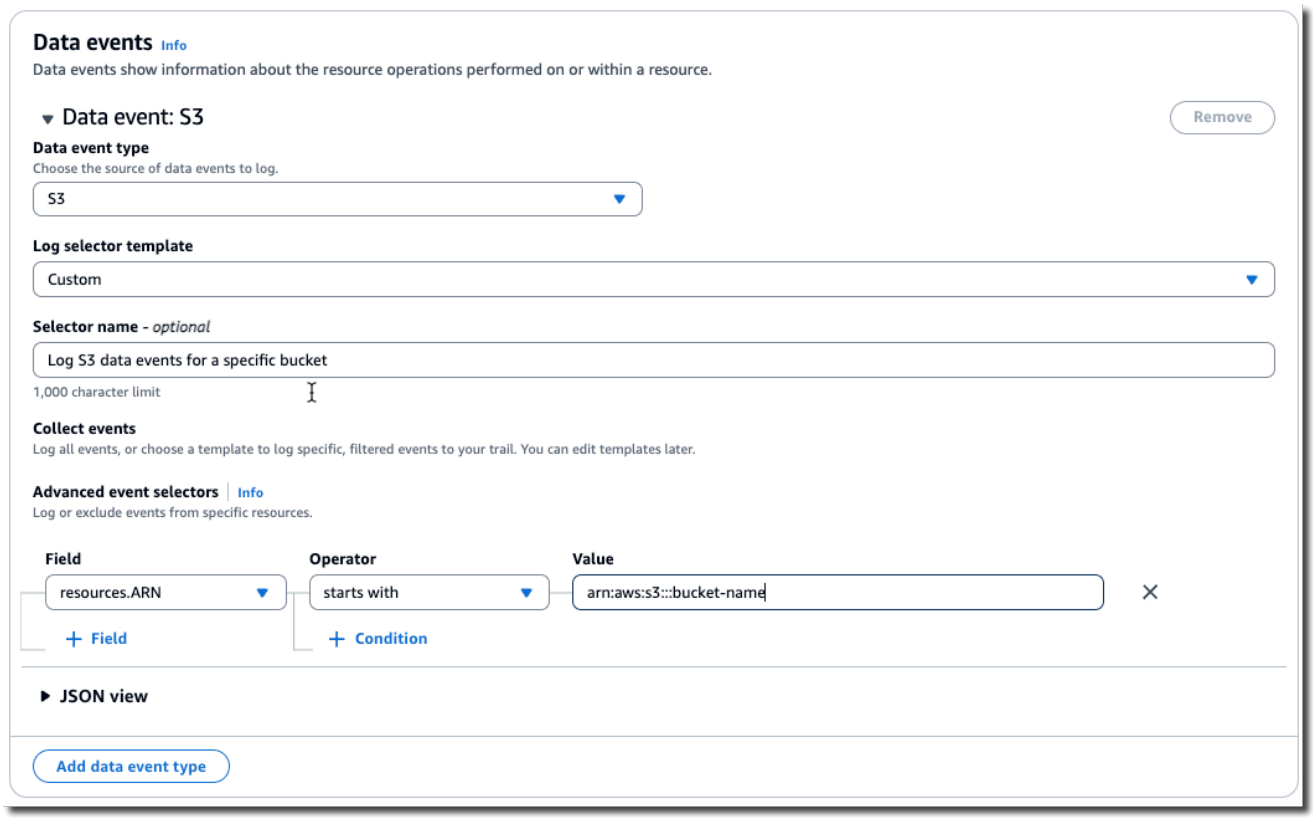
主题

- resources.ARN使用筛选数据事件 AWS Management Console
- resources.ARN使用筛选数据事件 AWS CLI

`resources.ARN`使用筛选数据事件 AWS Management Console

按照以下步骤使用 CloudTrail 控制台对`resources.ARN`字段进行筛选。

1. 按照创建跟踪过程中的步骤进行操作，或者按照创建事件数据存储过程中的步骤进行操作。
2. 按照步骤创建跟踪或事件数据存储时，请进行以下选择：
   a. 选择数据事件。
   b. 选择要记录其数据事件的数据事件类型。
   c. 对于日志选择器模板，请选择自定义。
   d. （可选）在选择器名称中，输入用于标识选择器的名称。选择器名称是高级事件选择器的描述性名称，例如“仅记录两个 S3 桶的数据事件”。选择器名称在高级事件选择器中列为 Name，展开 JSON 视图即可查看该名称。
   e. 在高级事件选择器中，执行以下操作以筛选：`resources.ARN`
      i. 对于字段，选择 resources.ARN。
      ii. 对于运算符，选择条件运算符。在此示例中，我们将选择从开始，因为我们要记录特定 S3 存储桶的数据事件。
      iii. 在值中，输入您的资源类型的 ARN（例如，arn*: aws: s3:: bucket-nam* e）。
      iv. 要筛选其他条件`resources.ARN`，请选择 + 条件。



f. 选择 +Field 可在其他字段上添加筛选器。

`resources.ARN`使用筛选数据事件 AWS CLI

使用 AWS CLI，您可以对该`resources.ARN`字段进行筛选，以记录特定 ARN 的事件或排除特定 ARN 的日志记录。

以下示例说明如何配置您的跟踪以包含特定 S3 存储桶中的所有 Simple Storage Service（Amazon S3）对象的所有数据事件。S3 事件在 `resources.type` 字段中的值为 `AWS::S3::Object`。由于 S3 对象和 S3 存储桶的 ARN 值略有不同，因此必须为 `resources.ARN` 添加 `StartsWith` 运算符以捕获所有事件。

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
```

```
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:aws:s3:::bucket_name/"] }
            ]
    }
]'
```

按**readOnly**值筛选数据事件

使用高级事件选择器，您可以根据readOnly字段的值进行筛选。

您只能在readOnly字段中使用Equals运算符。您可以将该readOnly值设置为true或false。如果不添加此字段，则会同时 CloudTrail 记录读取和写入事件。true日志的值仅读取事件。false日志的值仅写入事件。

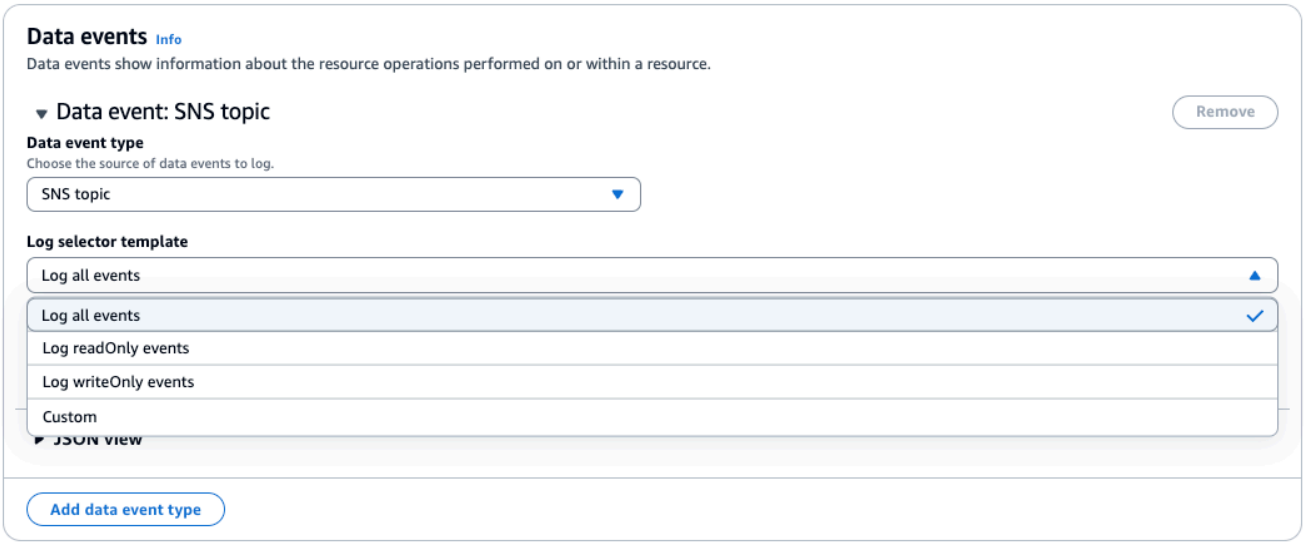
主题

- 使用按readOnly值筛选数据事件 AWS Management Console
- 使用按readOnly值筛选数据事件 AWS CLI

使用按**readOnly**值筛选数据事件 AWS Management Console

按照以下步骤使用 CloudTrail 控制台对readOnly字段进行筛选。

1. 按照创建跟踪过程中的步骤进行操作，或者按照创建事件数据存储过程中的步骤进行操作。
2. 按照步骤创建跟踪或事件数据存储时，请进行以下选择：
    a. 选择数据事件。
    b. 选择要记录其数据事件的数据事件类型。
    c. 对于日志选择器模板，请为您的用例选择相应的模板。



如果你打算这样做	选择此日志选择器模板
仅记录读取事件，不应用其他过滤器（例如，对`resources.ARN` 值进行筛选）。	记录只读事件
仅记录写入事件，不应用其他筛选器（例如，对`resources.ARN` 值进行筛选）。	记录只写事件

如果你打算这样做	选择此日志选择器模板
对readOnly值进行筛选并应用其他筛选器（例如，对resources.ARN 值进行筛选）。	自定义 在高级事件选择器中，执行以下操作以筛选该readOnly值： 记录写入事件 a. 对于字段，选择 readOnly。 b. 对于运算符，选择 equals。 c. 对于值，请输入 **false**。 d. 选择 +Field 可在其他字段上添加筛选器。 记录读取事件 a. 对于字段，选择 readOnly。 b. 对于运算符，选择 equals。 c. 对于值，请输入 **true**。 d. 选择 +Field 可在其他字段上添加筛选器。

使用按**readOnly**值筛选数据事件 AWS CLI

使用 AWS CLI，您可以对readOnly字段进行筛选。

您只能在readOnly字段中使用Equals运算符。您可以将该readOnly值设置为true或false。如果不添加此字段，则会同时 CloudTrail记录读取和写入事件。true日志的值仅读取事件。false日志的值仅写入事件。

以下示例说明如何配置您的跟踪以记录所有 Amazon S3 对象的只读数据事件。

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors '[
    {
```

```
            "Name": "Log read-only S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "readOnly", "Equals": ["true"] }
            ]
    }
]'
```

下一个示例创建了一个新的事件数据存储，该存储仅记录 EBS Direct API 的只写数据事件。您可以使用update-event-data-store命令更新现有的事件数据存储。

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName" \
--advanced-event-selectors \
'[
    {
            "Name": "Log write-only EBS Direct API data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
                { "Field": "readOnly", "Equals": ["false"] }
            ]
     }
]'
```

记录 AWS Config 合规性的数据事件

如果您使用 AWS Config 一致性包来帮助您的企业保持对正式标准的合规性，例如联邦风险与授权管理计划 (FedRAMP) 或美国国家标准与技术研究所 (NIST) 所要求的标准，则合规框架的合规包通常要求您至少记录 Amazon S3 存储桶的数据事件。合规性框架的一致性包中包括名为 cloudtrail-s3-dataevents-enabled 的托管规则，它检查您账户中的 S3 数据事件日志记录。许多未与合规性框架关联的一致性包也需要 S3 数据事件日志记录。下面是包含此规则的一致性包示例。

- Well-Architecte AWS d Framework 安全支柱的运营最佳实践
- 适用于 FDA 联邦法规第 21 篇第 11 部分的运营最佳实践
- 适用于 FFIEC 的运营最佳实践
- 适用于 FedRAMP（中等）的运营最佳实践
- 适用于 HIPAA 安全的运营最佳实践

- 适用于 K-ISMS 的运营最佳实践
- 适用于日志记录的运营最佳实践

有关中可用的一致性包样本的完整列表 AWS Config，请参阅《AWS Config 开发人员指南》中的一致性包示例模板。

使用 AWS SDK 记录数据事件

运行该GetEventSelectors操作以查看您的跟踪是否正在记录数据事件。您可以通过运行PutEventSelectors操作将跟踪配置为记录数据事件。有关更多信息，请参阅 AWS CloudTrail API 参考。

运行该GetEventDataStore操作以查看您的事件数据存储是否正在记录数据事件。通过运行CreateEventDataStore或UpdateEventDataStore操作并指定高级事件选择器，您可以将事件数据存储配置为包含数据事件。有关更多信息，请参阅 使用创建、更新和管理事件数据存储 AWS CLI 和《AWS CloudTrail API Referencehttps://docs.aws.amazon.com/awscloudtrail/latest/APIReference/》。

向 Amazon CloudWatch 日志发送事件

CloudTrail 支持向 CloudWatch 日志发送数据事件。当您将跟踪配置为向 CloudWatch 日志日志组发送事件时，仅 CloudTrail 发送您在跟踪中指定的事件。例如，如果您将跟踪配置为仅记录数据事件，则您的跟踪仅将数据事件传送到您的 CloudWatch 日志日志组。有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

记录 Insights 事件

AWS CloudTrail Insights 通过持续分析 CloudTrail 管理事件，帮助 AWS 用户识别和响应与 API 调用和 API 错误率相关的异常活动。 CloudTrail Insights 会分析您的 API 调用量和 API 错误率的正常模式（也称为基线），并在呼叫量或错误率超出正常模式时生成 Insights 事件。针对 `write` 管理 API 生成的 API 调用量的 Insights 事件，以及针对 `read` 和 `write` 管理 API 生成的 API 错误率的 Insights 事件。

> **Note**
>
> 要针对 API 调用量记录 Insights 事件，跟踪或事件数据存储必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，跟踪或事件数据存储必须记录 `read` 或 `write` 管理事件。

CloudTrail Insights 分析发生在单个区域（而不是全球区域）的管理事件。 CloudTrail Insights 事件是在生成其支持管理事件的同一区域生成的。

将对 Insights 事件收取额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关更多信息，请参阅AWS CloudTrail 定价。

目录

- 了解 Insights 事件传输情况
- 使用记录见解事件 AWS Management Console
  - 在现有跟踪上启用 CloudTrail Insights 事件
  - 在现有事件数据存储上启用 CloudTrail Insights 事件
- 使用记录见解事件 AWS Command Line Interface
  - 使用记录跟踪的见解事件 AWS CLI
  - 使用记录事件数据存储的 Insights 事件 AWS CLI
- 使用 AWS SDK 记录事件
- 跟踪的其他信息
  - 在控制台中查看跟踪的 Insights 事件
    - 筛选条件列
    - Insights graph（Insights 图表）选项卡
    - Attributions（属性）选项卡
      - 基线平均值和 Insights 平均值
    - CloudTrail “事件” 选项卡
    - Insights event record（Insights 事件记录）选项卡
  - 向 Amazon CloudWatch 日志发送跟踪事件

了解 Insights 事件传输情况

与其他 CloudTrail 捕获类型的事件不同，Insights 事件仅在 CloudTrail 检测到您的账户 API 使用量发生变化且与账户的典型使用模式明显不同时才会被记录。

在何处 CloudTrail 交付事件以及接收 Insights 事件所需的时间因跟踪和事件数据存储而异。

跟踪的 Insights 事件传输

如果您已在跟踪上启用 Insights 事件并 CloudTrail 检测到异常活动，则会将 Insigh CloudTrail ts 事件传送到您的跟踪所选目标 S3 存储桶中的/CloudTrail-Insight文件夹。首次在跟踪中启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 36 小时 CloudTrail 才能交付第一个 Insights 事件。

如果您关闭 Insights 事件记录跟踪然后重新启用 Insights 事件，或者停止并重新启动跟踪的日志记录，则如果检测到异常活动，则可能需要长达 36 小时 CloudTrail 才能重新启动 Insights 事件的交付。

事件数据存储的 Insights 事件传输

如果您已在源事件数据存储上启用 Insights 事件，则会将 Insigh CloudTrail ts 事件传送到目标事件数据存储。首次在源事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最多可能需要 7 天才能 CloudTrail 将第一个 Insights 事件传送到目标事件数据存储。

如果您关闭源事件数据存储上的 Insights 事件记录，然后重新启用 Insights 事件，或者在源事件数据存储上停止并重新启动事件摄取，则如果检测到异常活动，则最多可能需要 7 天 CloudTrail 才能重新启动 Insights 事件的交付。在 Lake 中 CloudTrail 收取 Insights 事件需要支付额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关 CloudTrail 定价的信息，请参阅AWS CloudTrail 定价。

使用记录见解事件 AWS Management Console

您可以使用控制台在跟踪或事件数据存储上启用 Insights 事件。

主题

- 在现有跟踪上启用 CloudTrail Insights 事件
- 在现有事件数据存储上启用 CloudTrail Insights 事件

在现有跟踪上启用 CloudTrail Insights 事件

使用以下步骤在现有跟踪上启用 CloudTrail Insights 事件。默认情况下，不启用 Insights 事件。

1. 在 CloudTrail 控制台的左侧导航窗格中，打开 T rail s 页面，然后选择一个跟踪名称。
2. 在 Insights events（Insights 事件）中，选择 Edit（编辑）。

> **Note**
>
> 记录 Insights 事件将收取额外费用。有关 CloudTrail 定价，请参阅AWS CloudTrail 定价。

3. 在 Event type（事件类型）中，选择 Insights events（Insights 事件）。
4. 在 Insights events（Insights 事件）中的 Choose Insights types（选择 Insights 类型）下，选择 API call rate（API 调用率）和/或 API error rate（API 错误率）。跟踪必须记录写入管理事件才能针对 API 调用率记录 Insights 事件。跟踪必须记录读取或写入管理事件才能针对 API 错误率记录 Insights 事件。
5. 选择保存更改以保存您的更改。

如果检测到异常活动，则最长可能需要 36 小时 CloudTrail 才能交付第一个 Insights 事件。

在现有事件数据存储上启用 CloudTrail Insights 事件

使用以下步骤在现有事件数据存储上启用 CloudTrail Insights 事件。默认情况下，不启用 Insights 事件。

在 Lake 中 CloudTrail 收取 Insights 事件需要支付额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关 CloudTrail 定价的信息，请参阅AWS CloudTrail 定价。

> **Note**
>
> 您只能在包含 CloudTrail 管理事件的事件数据存储上启用 CloudTrail Insights 事件。您无法在其他事件数据存储类型上启用 CloudTrail Insights 事件。

1. 在 CloudTrail 控制台左侧导航窗格的 Lake 下，选择事件数据存储。
2. 选择事件数据存储名称。
3. 在管理事件中，选择编辑。
4. 选择启用 Insights。
5. 选择 CloudTrail 将在其中提供 Insights 事件的目标事件数据存储。目标事件数据存储将根据该事件数据存储中的管理事件活动收集 Insights 事件。有关如何创建目标事件数据存储的信息，请参阅要创建记录 Insights 事件的目标事件数据存储。
6. 在选择 Insights 类型下，选择 API 调用率、API 错误率或此两者。您的事件数据存储必须记录写入管理事件，以针对 API 调用率记录 Insights 事件。您的事件数据存储必须记录读取或写入管理事件，以针对 API 错误率记录 Insights 事件。
7. 选择保存更改以保存您的更改。

如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。

使用记录见解事件 AWS Command Line Interface

您可以使用 AWS CLI配置跟踪和事件数据存储以记录 Insights 事件。

> **Note**
>
> 要针对 API 调用量记录 Insights 事件，跟踪或事件数据存储必须记录 `write` 管理事件。要针对 API 错误率记录 Insights 事件，跟踪或事件数据存储必须记录 `read` 或 `write` 管理事件。

主题

- 使用记录跟踪的见解事件 AWS CLI
- 使用记录事件数据存储的 Insights 事件 AWS CLI

使用记录跟踪的见解事件 AWS CLI

要查看您的跟踪是否正在记录 Insights 事件，请运行 `get-insight-selectors` 命令。

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

以下结果显示跟踪的默认设置。默认情况下，跟踪记录不记录 Insights 事件。`InsightType` 属性值为空，并且未指定 Insights 事件选择器，因为未启用见解事件收集。

如果您不添加 Insights 选择器，则该get-insight-selectors命令将返回以下错误消息：“调用 GetInsightSelectors 操作时出现错误 (InsightNotEnabledException)：跟踪##未启用 Insights。Edit the trail settings to enable Insights, and then try the operation again.”

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

要将跟踪配置为记录 Insights 事件，请运行 `put-insight-selectors` 命令。以下示例说明如何配置跟踪以包含 Insights 事件。Insights 选择器值可以是 `ApiCallRateInsight` 和/或 `ApiErrorRateInsight`。

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

以下结果显示为跟踪配置的 Insights 事件选择器。

```
{
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

使用记录事件数据存储的 Insights 事件 AWS CLI

要在事件数据存储上启用 Insights，必须有一个用于记录管理事件的源事件数据存储和一个用于记录 Insights 事件的目标事件数据存储。

要查看事件数据存储上是否启用了 Insights 事件，请运行 get-insight-selectors 命令。

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

要查看事件数据存储是否被配置为接收 Insights 事件或管理事件，请运行 get-event-data-store 命令。

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

以下过程向您展示如何创建目标和源事件数据存储，然后启用 Insights 事件。

1. 运行 aws cloudtrail create-event-data-store 命令创建收集 Insights 事件的目标事件数据存储。`eventCategory` 的值必须为 `Insight`。*`retention-period-days`*替换为您希望在事件数据存储中保留事件的天数。

   如果您使用 AWS Organizations 组织的管理账户登录，则如果要向委派的管理员授予对事件数据存储的访问权限，请添加`--organization-enabled`参数。

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   ```

```
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

以下为响应示例。

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

您将使用响应中的 ARN（或 ARN 的 ID 后缀）作为步骤 3 中参数 `--insights-destination` 的值。

2. 请运行 aws cloudtrail create-event-data-store 命令以创建记录管理事件的源事件数据存储。默认情况下，事件数据存储会记录所有的管理事件。您无需指定任何高级事件选择器即可记录所有管理事件。*retention-period-days*替换为您希望在事件数据存储中保留事件的天数。如果您正在创建组织事件数据存储，请包括 --organization-enabled 参数。

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

以下为响应示例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

您将使用响应中的 ARN（或 ARN 的 ID 后缀）作为步骤 3 中参数 --event-data-store 的值。

3. 请运行 put-insight-selectors 命令以启用 Insights 事件。Insights 选择器值可以是 ApiCallRateInsight 和/或 ApiErrorRateInsight。对于 --event-data-store 参数，请指定记录管理事件并将启用 Insights 的源事件数据存储的 ARN（或 ARN 的 ID 后缀）。对于

--insights-destination 参数，请指定将记录 Insights 事件的目标事件数据存储的 ARN（或 ARN 的 ID 后缀）。

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

以下结果显示为事件数据存储配置的 Insights 事件选择器。

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

首次在事件数据存储上启用 CloudTrail Insights 后，如果检测到异常活动，则最长可能需要 7 天 CloudTrail 才能交付第一个 Insights 事件。

CloudTrail Insights 分析发生在单个区域（而不是全球区域）的管理事件。 CloudTrail Insights 事件是在生成其支持管理事件的同一区域生成的。

对于组织事件数据存储， CloudTrail 分析来自每个成员账户的管理事件，而不是分析组织所有管理事件的聚合。

在 Lake 中 CloudTrail 收取 Insights 事件需要支付额外费用。如果您同时为跟踪和事件数据存储启用 Insights，则需要单独付费。有关 CloudTrail 定价的信息，请参阅AWS CloudTrail 定价。

使用 AWS SDK 记录事件

运行该GetInsightSelectors操作以查看您的跟踪或事件数据存储是否启用 Insights 事件。您可以配置您的跟踪或事件数据存储，以便通过PutInsightSelectors操作启用 Insights 事件。有关更多信息，请参阅AWS CloudTrail API 参考。

跟踪的其他信息

本部分提供特定于跟踪的其他信息。本节介绍如何从 CloudTrail 控制台的 Insights 页面查看已订阅跟踪的事件，以及如何选择将这些事件发送到 CloudWatch 日志进行监控。

主题

- 在控制台中查看跟踪的 Insights 事件
- 向 Amazon CloudWatch 日志发送跟踪事件

在控制台中查看跟踪的 Insights 事件

对于跟踪，您还可以在 CloudTrail 控制台的 Insights 页面上访问和查看 Insights 事件。有关如何在控制台中以及如何使用访问和查看 Insights 事件的更多信息 AWS CLI，请参阅本指南查看路径的 CloudTrail Insights 事件中的。

下图显示了一个跟踪 Insights 事件的示例。通过从 Dashboard (控制面板) 或 Insights (见解) 页面中选择 Insights 事件名称，可以打开 Insights 事件的详细信息页面。

如果您在跟踪上禁用 CloudTrail Insights，或者停止记录跟踪（这会禁用 CloudTrail Insights），则可能会将 Insights 事件存储在目标 S3 存储桶中，或者显示在控制台的 Insight s 页面上，该日期是您启用 Insights 的较早时间。

筛选条件列

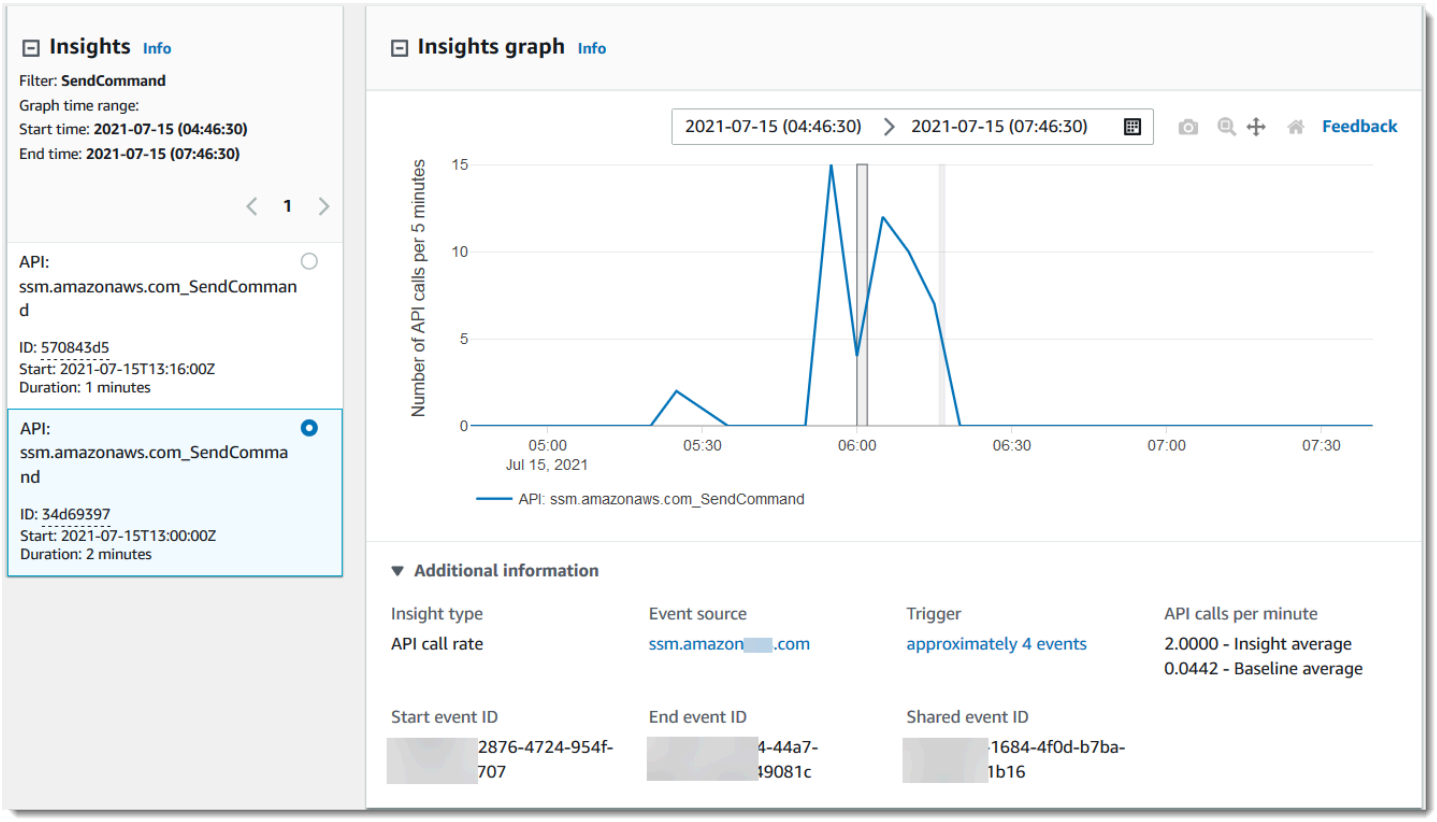
左列列出了与主题 API 相关的 Insights 事件，并且具有相同的 Insights 事件类型。通过该列，您可以选择希望了解其详细信息的 Insights 事件。在此列中选择事件时，该事件将在 Insights graph（Insights 图表）选项卡上的图形中突出显示。默认情况下， CloudTrail 应用筛选条件，将 “CloudTrail事件” 选项卡上显示的事件限制为与触发 Insights 事件的异常活动期间调用的特定 API 有关的事件。要显示在异常活动期间调用的所有 CloudTrail事件，包括与 Insights 事件无关的事件，请关闭过滤器。

Insights graph（Insights 图表）选项卡

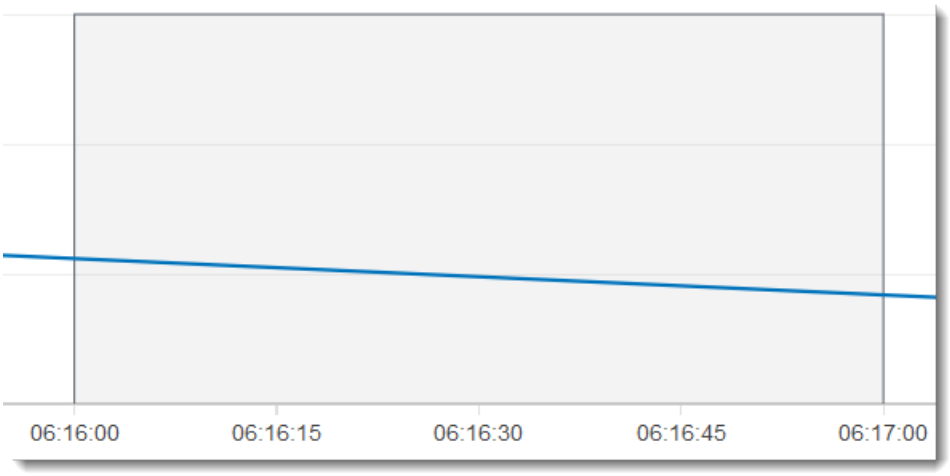
在 Insights graph（Insights 图）选项卡上，Insights 事件的详细信息页面显示在记录一个或多个 Insights 事件之前和之后的一段时间内发生的 API 调用量或错误率的图表。在图表中，Insights 事件以垂直条突出显示，条的宽度显示 Insights 事件的开始和结束时间。

在此示例中，垂直突出显示带显示账户中异常数量 AWS Systems Manager SendCommand的 API 调用。在突出显示的区域中，由于SendCommand呼叫数量超过了该账户每分钟 0.0442 次呼叫的基线平均值，因此在检测到异常活动时 CloudTrail 记录了 Insights 事件。已记录在上午 5:50 至 5:55 之间的 5 分钟内多达 15 次 SendCommand 调用的 Insights 事件。每分钟对该 API 的调用大约比该账户预期的次数多两次。在此示例中，图表的时间跨度为三小时：上午 4:30。太平洋时间 2021 年 7 月 15 日 上午 4:30 至上午 7:30。此事件的开始时间为 2021 年 7 月 15 日 上午 6:00，结束时间为两分钟后。未突出显示的结束 Insights 事件显示，该异常活动在上午 6:16 左右结束。

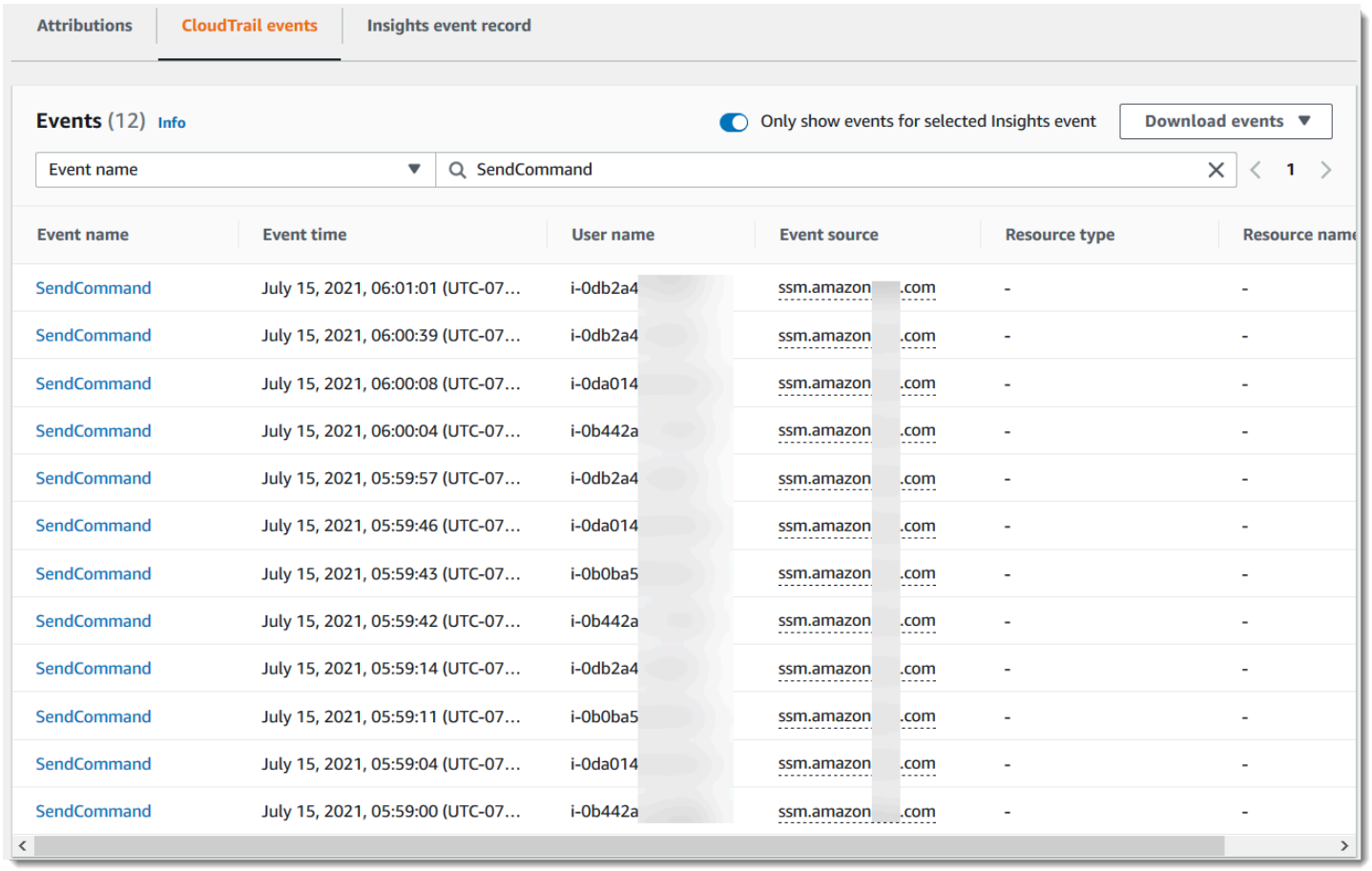
按照 Insights 事件开始前七天的时间计算基准。尽管基线持续时间（ CloudTrail 分析 API 正常活动的时间段）的值约为七天，但将基线持续时间 CloudTrail 四舍五入为整数天，因此确切的基准持续时间可能会有所不同。



您可以使用工具栏上的 Zoom（缩放）命令放大结束 Insights 事件，显示开始和结束时间。在此示例中，选择 Zoom（缩放），然后在突出显示的 Insights 事件的一边短距离拖动Zoom（缩放）光标,展开 Insights 事件并显示更多时间线详细信息。

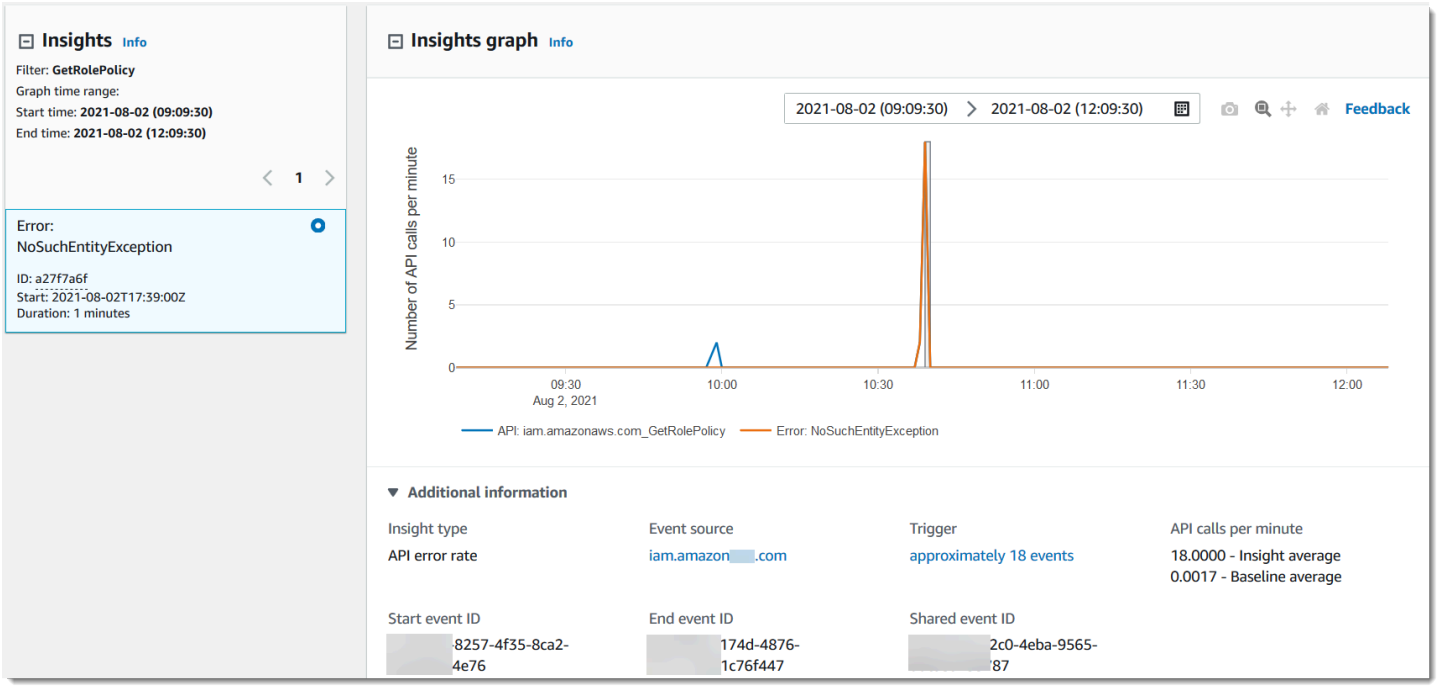


要查看经过分析以确定异常活动 CloudTrail 的事件，请打开CloudTrail 事件选项卡。在此示例中，CloudTrail 分析了 12 个事件，其中四个触发了 Insights 事件。



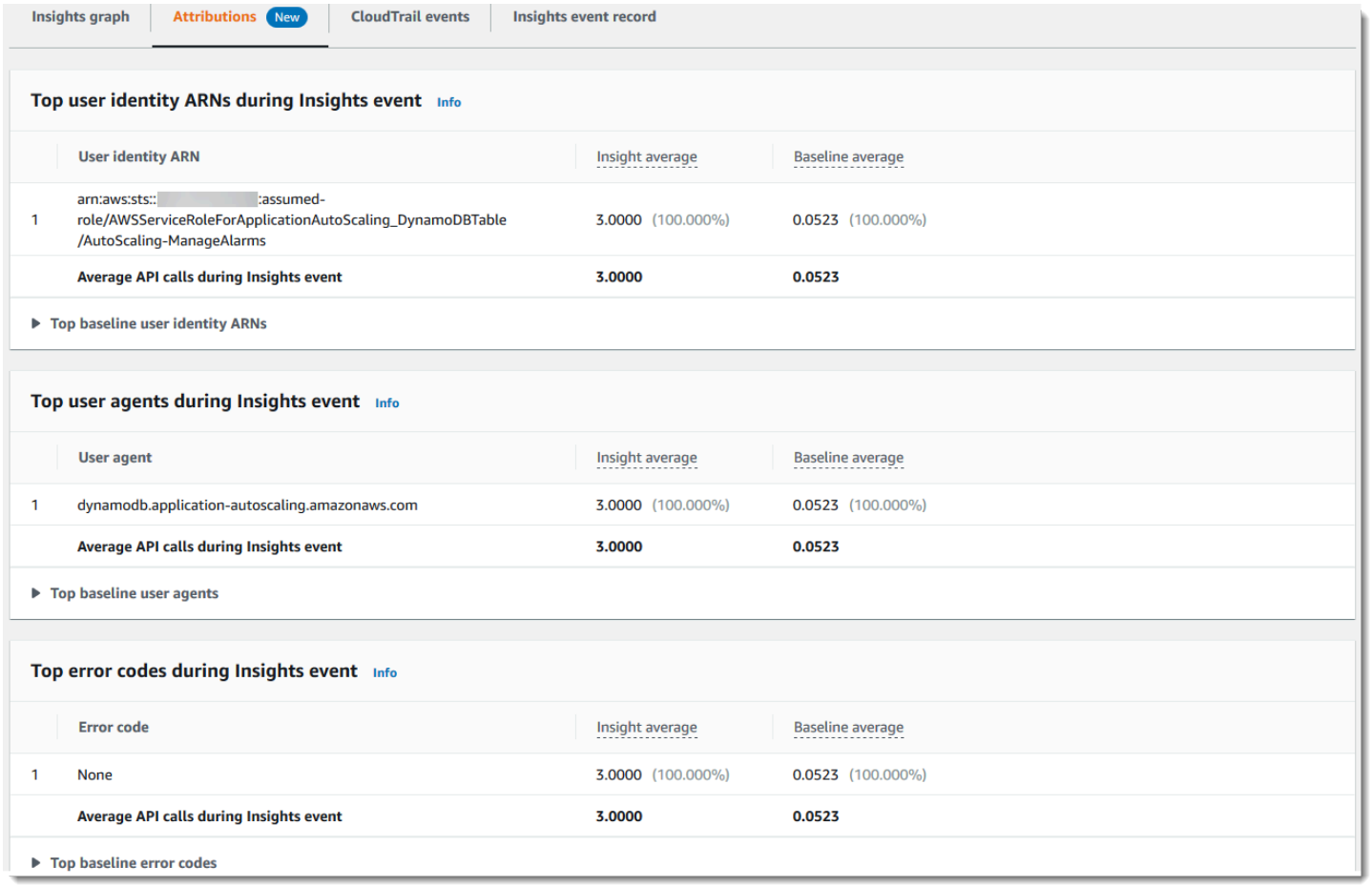
以下图片显示 API 错误率 Insights 事件的 Insights 图选项卡。突出显示的区域显示，由于 `GetRolePolicy` IAM API 调用上发生的 `NoSuchEntityException` 错误数量超出此 API 调用每分钟 0.0017 次 `NoSuchEntityException` 错误的基线平均值，在洞察期间记录了一个平均每分钟出

现 18 次错误的 Insights 事件。在本示例中，触发 Insights 事件的事件数量与 Insights 在一分钟内 18 个NoSuchEntityException错误的平均值相符。 CloudTrail 与 API 调用率图不同的是，API 错误率图显示为两条不同颜色的线：一条线衡量导致异常错误数量的 IAM API 调用（GetRolePolicy），另一条线衡量记录异常活动的错误（NoSuchEntityException）。

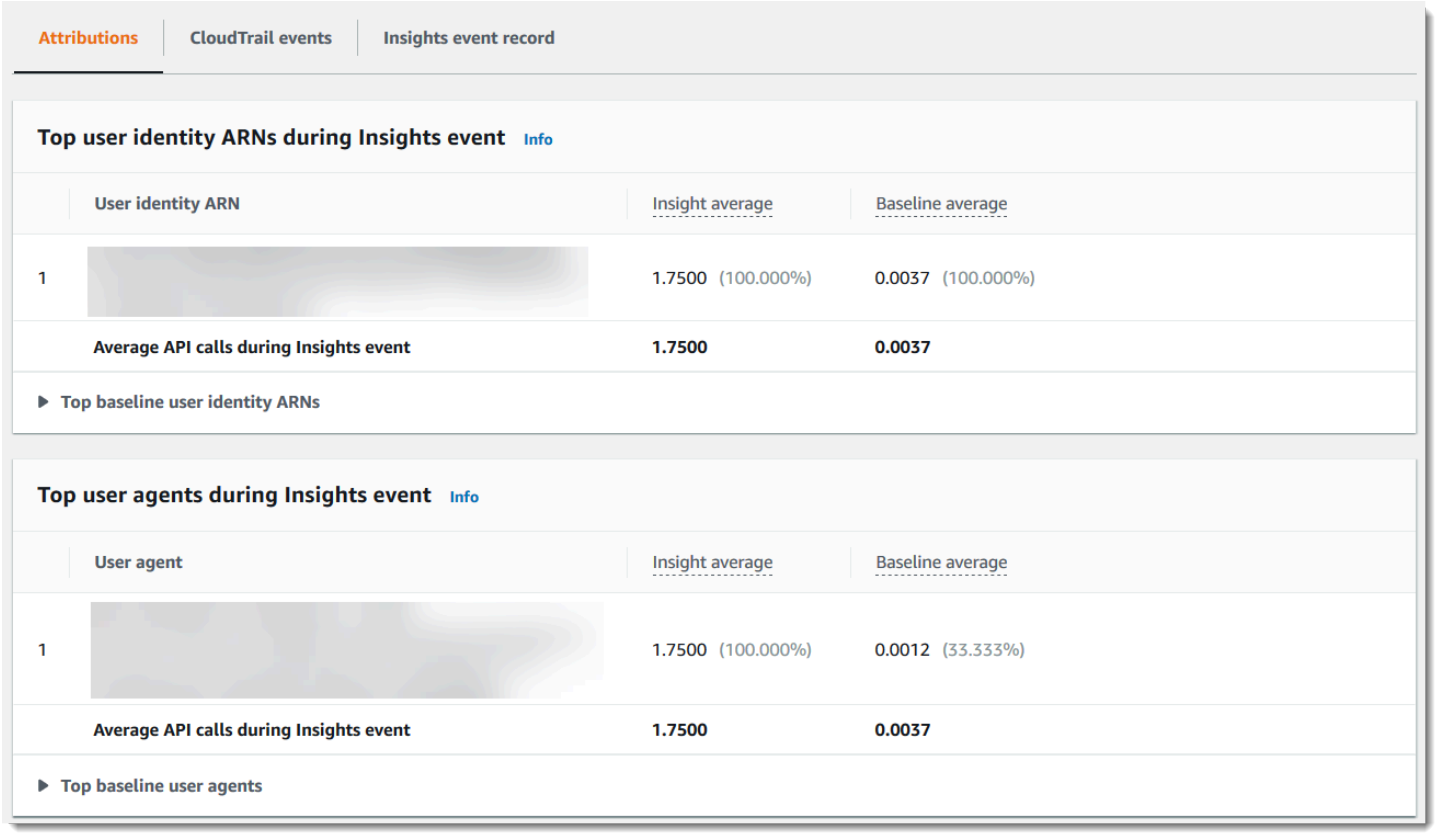


Attributions（属性）选项卡

Attributions（归因）选项卡显示有关 Insights 事件的以下信息。Attributions（归因）选项卡上的信息可以帮助您识别 Insights 活动的原因和来源。展开排名较高的基准区域，将正常时段内的用户身份、用户代理和错误代码活动与 Insights 活动期间归因的活动进行比较。Top baseline user identity ARNs（排名靠前的基准用户身份 ARN）、Top baseline user agents（排名靠前的基准用户代理）和 Top baseline error codes（排名靠前的基准错误代码）中仅显示基线平均值 – 在 Insights 事件开始时间前大约七天内按用户身份、用户代理记录的或导致错误代码的 API 事件的历史平均值。



Attributions（归因）选项卡仅显示错误率 Insights 事件中排名靠前的用户身份 ARN 和用户代理，如下图所示。错误率 Insights 事件不需要顶级错误代码。



- 排名靠前的用户身份 ARN-此表按贡献的 API 调用的平均次数降序显示了在异常活动和基准期内为 API 调用做出贡献的前五 AWS 名用户或 IAM 角色（用户身份）。引起异常活动的活动总数的平均数百分比显示在括号中。如果超过五个用户身份 ARN 涉及了异常活动，则其活动将汇总在 Other（其他）行中。
- 顶级用户代理-此表按贡献的 API 调用平均次数降序显示了用户身份在异常活动和基准期内为 API 调用做出贡献的前五个 AWS 工具。这些工具包括 AWS Management Console AWS CLI、或 AWS SDK。例如，名为 `ec2.amazonaws.com` 的用户代理表示 Amazon EC2 控制台是用于调用 API 的工具之一。引起异常活动的活动总数的平均数百分比显示在括号中。如果超过五个用户代理涉及了异常活动，则其活动将汇总在 Other（其他）行中。
- 排名靠前的错误代码 – 仅针对 API call rate（API 调用率）Insights 事件显示。此表最多显示在异常活动期间和基准期的 API 调用中发生的前五个的错误代码，按 API 调用数量从最大到最小降序排列。引起异常活动的活动总数的平均数百分比显示在括号中。如果在异常活动或基准活动期间发生了超过五个错误代码，那么它们的活动将汇总在 Other（其他）行中。

  值 None 作为排名前五的错误代码值之一，意味着很大一部分对 Insights 事件有贡献的调用不会导致错误。如果错误代码值为 None，并且表中没有其他错误代码，则 Insight average（Insights 平均值）和 Baseline average（基准平均值）列中的值与表示 Insights 事件总体的值相同。您还可以查

看显示在 Insights graph（Insights 图表）选项卡的 API calls per minute（每分钟 API 调用数）下的 Insight average（Insights 平均值）和 Baseline average（基准平均值）图例中的那些值。

基线平均值和 Insights 平均值

Baseline average（基线平均值）和 Insights average（Insights 平均值）显示排名靠前的用户身份、排名靠前的用户代理和排名靠前的错误代码。

- Baseline average（基线平均值）– 在您账户中特定区域内，大约前七天内测量的每分钟对记录 Insights 事件的 API 的典型调用速率。
- Insights average（Insights 平均值）- 触发 Insights 事件的 API 的调用或错误率。启动事件的 CloudTrail Insights 平均值是触发 Insights 事件的 API 上每分钟的调用率或错误率。通常情况下，这是异常活动的第一分钟。结束事件的 Insights 平均值是在开始 Insights 事件和结束 Insights 事件之间异常活动持续时间内，每分钟 API 调用的速率。

CloudTrail “事件” 选项卡

在CloudTrail 事件选项卡上，查看相关事件，这些事件 CloudTrail经过分析以确定发生了异常活动。默认情况下，已对 Insights 事件名称应用了筛选条件，该名称也是相关 API 的名称。要显示在异常活动期间记录的所有 CloudTrail 事件，请关闭仅显示所选 Insights 事件的事件。CloudTrail 事件选项卡显示在 Insights 事件的开始和结束时间之间发生的与主题 API 相关的 CloudTrail 管理事件。这些事件可帮助您执行更深入的分析，以确定 Insights 事件的可能原因以及异常 API 活动和错误率的原因。

Insights event record（Insights 事件记录）选项卡

与任何 CloudTrail 事件一样， CloudTrail Insights 事件是 JSON 格式的记录。Insights event record（Insights 事件记录）选项卡显示 Insights 开始和结束事件的 JSON 结构和内容，有时称为事件负载。有关 Insights 事件记录的字段和内容的更多信息，请参阅本指南中的 Insights 事件的记录字段 和 CloudTrail 见解`insightDetails`元素。

向 Amazon CloudWatch 日志发送跟踪事件

CloudTrail 支持将跟踪的 Insights 事件发送到 CloudWatch 日志。当您将跟踪配置为将 Insights 事件发送到 CloudWatch 日志日志组时， CloudTrail Insights 仅发送您在跟踪中指定的事件。例如，如果您将跟踪配置为记录管理和Insights事件，则您的跟踪会将管理事件和Insights事件传送到您的 CloudWatch 日志日志组。有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

CloudTrail 录制内容

记录的正文包含若干字段，可帮助您确定所请求的操作以及在何时何地发出请求。当 Optional (可选) 的值为 True 时，该字段仅在应用于服务、API 或事件类型时才存在。可选值 False 表示字段始终存在，或者其存在不依赖于服务、API 或事件类型。示例是 `responseElements`，它存在于可做出更改的操作（创建、更新或删除操作）的事件中。

CloudTrail 如果字段的内容超过最大字段大小，则会截断该字段。如果某个字段被截断，则 `omitted` 以值 `true` 显示。

`eventTime`

完成请求的日期和时间 [用协调世界时（UTC）表示]。事件的时间戳来自本地主机，该主机提供进行 API 调用时所在的服务 API 终端节点。例如，在美国西部（俄勒冈）地区运行的 CreateBucket API 事件将从运行 Amazon S3 终端节点 AWS 的主机上的时间开始获取其时间戳`s3.us-west-2.amazonaws.com`。通常， AWS 服务使用网络时间协议 (NTP) 来同步其系统时钟。

Since (自从)：1.0

Optional (可选)：False

`eventVersion`

日志事件格式的版本。当前版本是 1.10。

`eventVersion` 值是主要版本和次要版本，格式为 *`major_version`*.*`minor_version`*。例如，您可获得 `1.09` 的 `eventVersion` 值，其中 `1` 是主要版本，`09` 是次要版本。

CloudTrail 如果对不向后兼容的事件结构进行了更改，则会增加主版本。这包括移除已存在的 JSON 字段，或更改字段内容的表示方式（例如，日期格式）。 CloudTrail 如果更改向事件结构添加了新字段，则会增加次要版本。如果新信息对部分或全部现有事件可用，或者新信息仅可用于新事件类型，则可能会发生这种情况。应用程序可忽略新字段，以便与事件结构的新次要版本保持兼容。

如果 CloudTrail 引入了新的事件类型，但事件的结构在其他方面保持不变，则事件版本不会改变。

为确保您的应用程序能够解析事件结构，我们建议您对主要版本号执行等于比较。为确保您的应用程序预期的字段存在，我们还建议对次 greater-than-or-equal要版本进行-to 比较。次要版本中没有前导零。您可以将 *`major_version`* 和 *`minor_version`* 都解读为数字，并执行比较操作。

Since (自从)：1.0

Optional (可选)：False

`userIdentity`

有关发出请求的 IAM 身份的信息。有关更多信息，请参阅 CloudTrail 用户身份元素。

Since (自从)：1.0

Optional (可选)：False

`eventSource`

已将请求发出到的服务。此名称通常为服务名称的简短形式，不含空格但会加上 `.amazonaws.com`。例如：

- AWS CloudFormation 是`cloudformation.amazonaws.com`。
- Amazon EC2 是 `ec2.amazonaws.com`。
- Amazon Simple Workflow Service 是 `swf.amazonaws.com`。

此约定存在某些例外情况。例如，适用于 Amazon `eventSource` 的 CloudWatch 为`monitoring.amazonaws.com`。

Since (自从)：1.0

Optional (可选)：False

`eventName`

请求的操作（服务的 API 中的某个操作）。

Since (自从)：1.0

Optional (可选)：False

`awsRegion`

向 AWS 区域 其发出请求的，例如`us-east-2`。请参阅 CloudTrail 支持的区域。

Since (自从)：1.0

Optional (可选)：False

sourceIPAddress

已从中发出请求的 IP 地址。对于源自服务控制台的操作，报告的地址针对的是基础客户资源而不是控制台 Web 服务器。对于中的服务 AWS，仅显示 DNS 名称。

> **Note**
>
> 对于由 AWS发起的事件，此字段通常为 `AWS Internal/#`，其中 # 是供内部使用的编号。

Since (自从)：1.0

Optional (可选)：False

userAgent

发出请求的代理，例如、 AWS 服务 AWS Management Console、 AWS 软件开发工具包或。AWS CLI此字段的最大大小为 1 KB；超过该限制的内容将被截断。以下是值示例：

- `lambda.amazonaws.com` – 请求通过 AWS Lambda发出。
- `aws-sdk-java` – 请求通过 AWS SDK for Java发出。
- `aws-sdk-ruby` – 请求通过 AWS SDK for Ruby发出。
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— 该请求是使用 AWS CLI 安装在 Linux 上的。

> **Note**
>
> 对于源自的事件 AWS，如果 CloudTrail 知道是谁拨打 AWS 服务 了呼叫，则此字段是调用服务的事件源（例如，`ec2.amazonaws.com`）。否则，此字段为`AWS Internal/#`，其中#是用于内部目的的数字。

Since (自从)：1.0

Optional (可选)：True

errorCode

如果请求返回错误，则表示 AWS 服务错误。有关显示此字段的示例，请参阅 示例错误代码及留言记录。此字段的最大大小为 1 KB；超过该限制的内容将被截断。

Since (自从)：1.0

Optional (可选)：True

errorMessage

如果请求返回一个错误，则为该错误的描述。此消息包括授权失败的消息。 CloudTrail 捕获服务在其异常处理中记录的消息。有关示例，请参阅示例错误代码及留言记录。此字段的最大大小为 1 KB；超过该限制的内容将被截断。

> **Note**
>
> 某些 AWS 服务在活动中提供`errorCode`和`errorMessage`作为顶级字段。其他 AWS 服务在 `responseElements` 中提供错误信息。

Since (自从)：1.0

Optional (可选)：True

requestParameters

与请求一起发送的参数（如果有）。这些参数记录在相应 AWS 服务的 API 参考文档中。此字段的最大大小为 100 KB；超过该限制的内容将被截断。

Since (自从)：1.0

Optional (可选)：False

responseElements

进行更改的操作（创建、更新或删除操作）的响应元素（如果有）。如果动作 不返回响应元素，此字段是`null`。如果 操作不会更改状态（例如，请求获取或列出对象），这个元素被省略了。操作的响应元素记录在 API 参考中 相应文档 AWS 服务。此字段有最大大小 100 KB；超过该限制的内容将被截断。

该responseElements值对帮助您跟踪请求很有用 和 AWS Support。两者都x-amz-request-id和 x-amz-id-2 包含可帮助您跟踪请求的信息 AWS Support。这些值是 与服务在响应请求时返回的内容相同 启动事件，因此您可以使用它们将事件与 请求。

Since (自从)：1.0

Optional (可选)：False

additionalEventData

不是请求或响应一部分的关于事件的其他数据。此字段的最大大小为 28 KB；超过该限制的内容将被截断。

Since (自从)：1.0

Optional (可选)：True

requestID

用于标识请求的值。所调用的服务生成此值。此字段的最大大小为 1 KB；超过该限制的内容将被截断。

Since (自从)：1.01

Optional (可选)：True

eventID

生成的 GUID CloudTrail 用于唯一标识每个事件。您可以使用此值来标识单个事件。例如，您可以将此 ID 用作主键来从可搜索的数据库中检索日志数据。

Since (自从)：1.01

Optional (可选)：False

eventType

标识生了成事件记录的事件的类型。它可以是以下值之一：

- AwsApiCall - 调用了一个 API。

- AwsServiceEvent – 该服务生成了一个与跟踪相关的事件。例如，如果另一个账户使用您拥有的资源发起调用，则可能出现这种情况。
- AwsConsoleAction – 在控制台中执行了一个非 API 调用的操作。
- AwsConsoleSignIn— 您的账户（根、IAM、联合账户、SAML 或 SwitchRole）中的用户登录了。 AWS Management Console
- AwsCloudTrailInsight— 如果启用了 Insights 事件，则在 CloudTrail 检测到异常操作活动（例如资源配置峰值或突发 AWS Identity and Access Management (IAM) 操作）时 CloudTrail 生成 Insights 事件。

  AwsCloudTrailInsight 事件未使用以下字段：

  - eventName
  - eventSource
  - sourceIPAddress
  - userAgent
  - userIdentity

Since (自从)：1.02

Optional (可选)：False

apiVersion

标识与 AwsApiCall eventType 值关联的 API 版本。

Since (自从)：1.01

Optional (可选)：True

managementEvent

一个布尔值，标识该事件是否为管理事件。如果 eventVersion 为 1.06 或更高，则事件记录中将显示 managementEvent，并且事件类型为以下值之一：

- AwsApiCall
- AwsConsoleAction
- AwsConsoleSignIn
- AwsServiceEvent

Since (自从)：1.06

Optional (可选)：True

readOnly

标识此操作是否为只读操作。它可以是以下值之一：

- `true` – 操作为只读操作（例如，`DescribeTrails`）。
- `false` – 操作为只写操作（例如，`DeleteTrail`）。

Since (自从)：1.01

Optional (可选)：True

resources

事件中访问的资源列表。此字段可包含以下信息：

- 资源 ARN
- 资源拥有者的账户 ID
- 资源类型标识符，格式为：`AWS::`*`aws-service-name`*`::`*`data-type-name`*

例如，在记录 `AssumeRole` 事件时，`resources` 字段可能如下所示：

- ARN：`arn:aws:iam::123456789012:role/`*`myRole`*
- 账户 ID: `123456789012`
- 资源类型标识符：`AWS::IAM::Role`

有关带有该`resources`字段的日志示例，请参阅 AWS STS IAM 用户指南中的 CloudTrail 日志文件中的 API 事件或AWS Key Management Service 开发人员指南中的记录 AWS KMS API 调用。

Since (自从)：1.01

Optional (可选)：True

recipientAccountId

表示已收到此事件的账户 ID。`recipientAccountID` 可能与 CloudTrail 用户身份元素 `accountId` 不同。此情况会在跨账户资源访问中发生。例如，如果一个单独的账户已使用 KMS 密钥（也称为 AWS KMS key）调用 Encrypt API，则已传输到发起调用的账户的事件的 `accountId`

和 `recipientAccountID` 值将相同，而已传输到拥有 KMS 密钥的账户的事件的这两个值不相同。

Since (自从)：1.02

Optional (可选)：True

`serviceEventDetails`

确定服务事件，包括触发活动的原因和结果。有关更多信息，请参阅 AWS 服务事件。此字段的最大大小为 100 KB；超过该限制的内容将被截断。

Since (自从)：1.05

Optional (可选)：True

`sharedEventID`

生成的 GUID CloudTrail ，用于唯一标识发送到不同 AWS 账户的相同 AWS 操作中的 CloudTrail 事件。

例如，当一个账户使用AWS KMS key属于另一个账户的时，使用 KMS 密钥的账户和拥有 KMS 密钥的账户会收到针对同一操作的单独 CloudTrail 事件。为此 AWS 动作交付的每个 CloudTrail 事件都有相同的共同`sharedEventID`点, 但也有一个独特`eventID`的`recipientAccountID`.

有关更多信息，请参阅 示例 sharedEventID。

> **Note**
>
> 仅当 CloudTrail 事件传送到多个账户时，该`sharedEventID`字段才会出现。如果来电者和所有者是同一个 AWS 帐户，则只 CloudTrail 发送一个事件，并且该`sharedEventID`字段不存在。

Since (自从)：1.03

Optional (可选)：True

`vpcEndpointId`

确定从 VPC 向另一个 AWS 服务发送请求的 VPC 终端节点，如 Amazon S3。

Since (自从)：1.04

Optional (可选)：True

eventCategory

显示事件类别。用于管理LookupEvents呼叫和 Insights 活动。eventCategory

- 对于管理事件，值为 Management。
- 对于数据事件，值为 Data。
- 对于 Insights 事件，值为 Insight。

从：1.07

Optional (可选)：False

addendum

如果事件传递延迟，或者在记录事件后获得了有关现有事件的其他信息，则附录字段将显示有关事件延迟原因的信息。如果现有事件中缺少信息，则附录字段将包含缺失的信息以及缺失信息的原因。内容包括下列信息。

- **reason** - 事件或其部分内容丢失的原因。值可以是以下任何一项。
  - **DELIVERY_DELAY** – 传送事件时出现延迟。这可能是由高网络流量、连接问题或 CloudTrail 服务问题引起的。
  - **UPDATED_DATA** – 事件记录中的字段丢失或值不正确。
  - **SERVICE_OUTAGE**— 一项服务，用于 CloudTrail 记录发生中断的事件，但无法将事件记录到 CloudTrail。这种情况极为罕见。
- **updatedFields** - 由附录更新的事件记录字段。只有在原因为 UPDATED_DATA 时才提供此信息。
- **originalRequestID** - 请求的原始唯一 ID。只有在原因为 UPDATED_DATA 时才提供此信息。
- **originalEventID** - 原始事件 ID。只有在原因为 UPDATED_DATA 时才提供此信息。

从：1.08

Optional (可选)：True

sessionCredentialFromConsole

显示事件是否源于会 AWS Management Console 话。此字段不会显示出来，除非该值为 true，这意味着用于进行 API 调用的客户端是代理或外部客户端。如果使用了代理客户端，则不显示 tlsDetails 事件字段。

从：1.08

Optional (可选)：True

edgeDeviceDetails

显示有关作为请求目标的边缘设备的信息。目前，S3 Outposts 设备事件包括此字段。此字段的最大大小为 28 KB；超过该限制的内容将被截断。

从：1.08

Optional (可选)：True

tlsDetails

显示有关传输层安全 (TLS) 版本、密码套件以及服务 API 调用中使用的客户端提供的主机名的完全限定域名 (FQDN) 的信息，该主机名通常是服务端点的 FQDN。 CloudTrail如果预期信息缺失或为空，仍会记录部分 TLS 详细信息。例如，如果存在 TLS 版本和密码套件，但HOST标头为空，则事件中仍会记录可用的 TLS 详细信息。 CloudTrail

- **tlsVersion** - 请求的 TLS 版本。
- **cipherSuite** - 请求的密码套件（所用安全算法的组合）。
- **clientProvidedHostHeader** - 服务 API 调用中使用的客户端提供主机名，通常是服务端点的 FQDN。

> **Note**
>
> 在某些情况下，事件记录中不存在 tlsDetails 字段。
>
> - 如果 API 调用是由代表您进行的，则 AWS 服务 该tlsDetails字段不存在。userIdentity 元素中的 invokedBy 字段用于标识发出 API 调用的 AWS 服务 。
> - 如果 sessionCredentialFromConsole 存在且值为 true，则仅当使用外部客户端进行 API 调用时，tlsDetails 才存在于事件记录中。

从：1.08

Optional (可选)：True

Insights 事件的记录字段

以下是 Insights 事件的 JSON 结构中显示的属性，这些属性与管理或数据事件中的属性不同。

sharedEventId

A sharedEventID fo CloudTrail r Insights 事件不同于 CloudTrail事件的管理和数据类型。sharedEventID在 Insights 事件中，a sharedEventID 是 Ins CloudTrail ights 生成的 GUID，用于唯一标识 Insights 事件。 sharedEventID在 Insights 事件开始和结束 Insights 事件之间很常见，它有助于将两个事件联系起来，以唯一的方式识别异常活动。您可以将 sharedEventID 视为整体 Insights 事件 ID。

从：1.07

Optional (可选)：False

insightDetails

仅限 Insights 事件。显示有关 Insights 事件的基础触发器的信息，如事件源、用户代理、统计信息、API 名称，以及该事件是 Insights 事件的开始还是结束。有关 insightDetails 数据块的内容的更多信息，请参阅 CloudTrail 见解insightDetails元素。

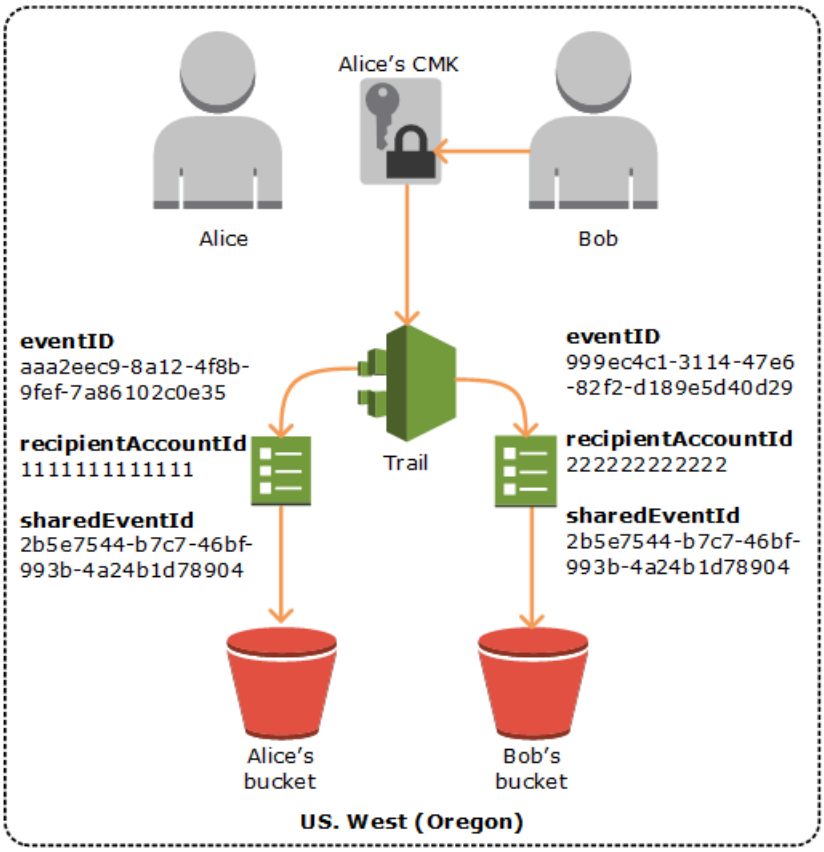
从：1.07

Optional (可选)：False

示例 sharedEventID

以下示例描述了如何为同一个操作 CloudTrail 传送两个事件：

1. Alice 有 AWS 账户 (111111111111) 并创建了一个。 AWS KMS key她是此 KMS 密钥的所有者。
2. Bob 有 AWS 账户 (222222222222)。Alice 向 Bob 提供使用该 KMS 密钥的权限。
3. 每个账户都有跟踪和单独的存储桶。
4. Bob 使用该 KMS 密钥来调用 Encrypt API。
5. CloudTrail 发送两个单独的事件。
   - 一个事件发送给 Bob。该事件显示他使用了该 KMS 密钥。
   - 一个事件发送给 Alice。该事件显示 Bob 使用了该 KMS 密钥。
   - 这些事件具有相同的 sharedEventID，但是 eventID 和 recipientAccountID 是唯一的。



在 CloudTrail Insights 中共享事件 ID

A `sharedEventID` fo CloudTrail r Insights 事件不同于 CloudTrail 事件的管理和数据类型。`sharedEventID`在 Insights 事件中，a `sharedEventID` 是 In CloudTrail sights 生成的 GUID，用于唯一标识 Insights 事件的开始和结束对。 `sharedEventID`在 Insights 事件的开始和结束之间很常见，它有助于在两个事件之间建立关联，以唯一地识别异常活动。

您可以将 `sharedEventID` 视为整体 Insights 事件 ID。

CloudTrail 用户身份元素

AWS Identity and Access Management (IAM) 提供不同类型的身份。`userIdentity` 元素包含有关发出请求的 IAM 身份的类型的详细信息，以及使用了哪些凭证。如果使用的是临时证书，则该元素显示证书是如何获取的。

目录

- 示例
- 字段

- 具有 SAML 和网络联合身份验证 AWS STS 的 API 的值
- AWS STS 来源身份

示例

userIdentity 与 IAM 用户凭证

以下示例显示使用名为 Alice 的 IAM 用户的证书发出的简单请求的 userIdentity 元素。

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

使用临时安全证书的 **userIdentity**

以下示例显示使用通过代入 IAM 角色获取的临时安全凭证发出的请求的 userIdentity 元素。该元素包含有关为获取证书而担任的角色的其他详细信息。

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
```

```
    }
}
```

代表 IAM Identity Center 用户发出的请求的 **userIdentity**

以下示例显示代表 IAM Identity Center 用户发出的请求的 userIdentity 元素。

```
"userIdentity": {
 "type": "IdentityCenterUser",
 "accountId": "123456789012",
 "onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
 },
 "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

字段

以下字段可显示在 userIdentity 元素中。

type

身份的类型。以下是可能的值：

- Root— 请求是使用您的 AWS 账户 凭据提出的。如果 userIdentity 类型为 Root，并且您为账户设置了别名，则 userName 字段包含您的账户别名。有关更多信息，请参阅您的 AWS 账户 ID 及其别名。
- IAMUser – 已使用 IAM 用户的凭证发出请求。
- AssumedRole – 已使用角色通过调用 AWS Security Token Service (AWS STS) AssumeRole API 获得的临时安全凭证发出请求。这可能包括用于 Amazon EC2 的角色和跨账户 API 访问权限。
- Role – 已由具有特定权限的持久 IAM 身份发出请求。角色会话的发出者始终为角色。有关角色的更多信息，请参阅 IAM 用户指南中的角色术语和概念。
- FederatedUser— 该请求是使用通过调用 AWS STS GetFederationTokenAPI 获得的临时安全证书发出的。sessionIssuer 元素指示是使用根还是 IAM 用户凭证调用了该 API。

  有关临时安全凭证的更多信息，请参阅《IAM 用户指南》中的临时安全凭证。
- Directory – 向目录服务发出了请求，类型未知。目录服务包括以下内容：Amazon WorkDocs 和 Amazon QuickSight。

- AWSAccount— 请求是由另一个人提出的 AWS 账户
- AWSService— 该请求是由属于 AWS 账户 的提出的 AWS 服务。例如， AWS Elastic Beanstalk 在您的账户中扮演一个 IAM 角色来 AWS 服务 代表您呼叫其他人。
- IdentityCenterUser – 代表 IAM Identity Center 用户发出的请求。
- Unknown— 请求使用 CloudTrail 无法确定的身份类型发出。

Optional (可选)：False

当使用您拥有的 IAM 角色进行跨账户访问时，日志中将显示 type 的 AWSAccount 和 AWSService。

示例：由另一个 AWS 账户启动的跨账户访问

1. 您在自己的账户中拥有一个 IAM 角色。
2. 另一个 AWS 账户切换到该角色以代入您的账户的角色。
3. 由于您拥有 IAM 角色，因此您将收到一个显示已代入此角色的其他账户的日志。type 为 AWSAccount。有关日志条目的示例，请参阅 CloudTrail 日志文件中的AWS STS API 事件。

示例：服务发起的跨账户访问 AWS

1. 您在自己的账户中拥有一个 IAM 角色。
2. AWS 服务拥有的 AWS 账户将扮演该角色。
3. 由于您拥有 IAM 角色，因此您将收到一个显示已代入此角色的 AWS 服务的日志。type 为 AWSService。

userName

已发出调用的身份的友好名称。userName 中显示的值基于 type 中的值。下表显示 type 和 userName 之间的关系：

type	userName	描述
Root（未设置别名）	不存在	如果您尚未为自己设置别名 AWS 账户，则不会显示该userName字段。有关账户别名的更多信息，请参阅您的 AWS 账户 身份证及其别名。请注

type	userName	描述
		意，userName 字段不能包含 Root，因为 Root 是身份类型而不是用户名称。
Root（已设置别名）	账户别名	有关 AWS 账户 别名的更多信息，请参阅您的 AWS 账户 身份证及其别名。
IAMUser	IAM 用户的用户名	
AssumedRole	不存在	至于 AssumedRole 类型，您可以在 **sessionIssuer** 元素的 sessionContext 中找到 userName 字段。有关示例条目，请参阅示例。
Role	用户定义	sessionContext 和 sessionIssuer 部分包含有关角色发出的会话的身份信息。
FederatedUser	不存在	sessionContext 和 sessionIssuer 部分包含有关已发出联合身份用户会话的身份的信息。
Directory	可以存在	例如，值可以是账户别名或关联 AWS 账户 ID 的电子邮件地址。
AWSService	不存在	
AWSAccount	不存在	
IdentityCenterUser	不存在	onBehalfOf 部分包含有关发出调用的 IAM Identity Center 用户 ID 和身份存储 ARN 的信息。有关 IAM Identity Center 的更多信息，请参阅《AWS IAM Identity Center 用户指南》。
Unknown	可以存在	例如，值可以是账户别名或关联 AWS 账户 ID 的电子邮件地址。

> **Note**
>
> userName 字段包含当记录的事件为错误的用户名输入导致的控制台登录失败时产生的字符串 HIDDEN_DUE_TO_SECURITY_REASONS。CloudTrail 在这种情况下不记录内容，因为文本可能包含敏感信息，如以下示例所示：
>
> - 用户不小心在用户名称字段中键入了密码。
> - 用户单击一个 AWS 账户登录页面的链接，然后键入另一个账户的账号。
> - 用户意外键入了个人电子邮件账户的账户名称、银行登录标识符或某个其他私有 ID。

Optional (可选)：True

principalId

已发出调用的实体的唯一标识符。对于使用临时安全证书发出的请求，此值包括将传递到 AssumeRole、AssumeRoleWithWebIdentity 或 GetFederationToken API 调用的会话名称。

Optional (可选)：True

arn

已发出调用的委托人的 Amazon Resource Name (ARN)。arn 的最后一个部分包含已发出调用的用户或角色。

Optional (可选)：True

accountId

拥有已授予请求权限的实体的账户。如果已使用临时安全凭证发出请求，则该账户为拥有用于获取凭证的 IAM 用户或角色的账户。

如果已使用 IAM Identity Center 授权的访问令牌发出请求，则该账户为拥有 IAM Identity Center 实例的账户。

Optional (可选)：True

accessKeyId

用于对请求签名的 访问密钥 ID。如果已使用临时安全证书发出请求，则为临时证书的访问密钥 ID。出于安全原因,accessKeyId 可能不存在，也可能显示为空字符串。

Optional (可选)：True

sessionContext

如果已使用临时安全凭证发出请求，sessionContext 会提供为这些凭证创建的会话的相关信息。当您调用任何返回临时凭证的 API 时，会创建会话。当用户在控制台中工作以及使用包含多重身份验证的 API 发出请求时，也会创建会话。此元素具有以下属性：

- creationDate – 颁发临时安全凭证时的日期和时间。用 ISO 8601 基本表示法表示。
- mfaAuthenticated – 如果将凭证用于请求的根用户或 IAM 用户还通过 MFA 设备进行身份验证，则值为 true；否则为 false。
- sourceIdentity – 请参阅本主题中的 AWS STS 来源身份。sourceIdentity 字段出现在用户代入 IAM 角色执行操作的事件中。sourceIdentity 识别发出请求的原始用户身份，无论该用户的身份是 IAM 用户、IAM 角色、通过基于 SAML 的联合身份验证进行身份验证的用户，还是通过符合 OpenID Connect（OIDC）的 Web 身份联合验证进行身份验证的用户。有关配置 AWS STS 以收集源身份信息的更多信息，请参阅 IAM 用户指南中的监控和控制使用代入角色执行的操作。
- ec2RoleDelivery - 如果凭证是由 Amazon EC2 实例元数据服务版本 1（IMDSv1）提供的，则该值为 1.0。如果凭证是使用新的 IMDS 方案提供的，则值为 2.0。

  AWS 亚马逊 EC2 实例元数据服务 (IMDS) 提供的证书包括 ec2: RoleDelivery IAM 上下文密钥。通过在 IAM 策略、资源策略 service-by-service 或 AWS Organizations 服务控制策略中使用上下文密钥作为条件，此上下文密钥便于在或 resource-by-resource 的基础上强制使用新方案。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的实例元数据和用户数据。

Optional (可选)：True

invokedBy

当请求是由诸如 Amazon EC2 Auto Scaling 或之 AWS 服务 类的公司提出请求时，发出请求的名称 AWS Elastic Beanstalk。 AWS 服务 只有在发出请求时，才会出现此字段 AWS 服务。这包括服务使用正向访问会话 (FAS)、 AWS 服务 委托人、服务相关角色或使用的服务角色发出的请求。AWS 服务

Optional (可选)：True

sessionIssuer

如果用户使用临时安全凭证发出请求，sessionIssuer 会提供有关凭证获取方式的信息。例如，如果用户通过代入角色来获取临时安全凭证，则此元素提供有关所代入角色的信息。如果用户通过使用根或 IAM 用户凭证调用 AWS STS GetFederationToken 来获取凭证，则此元素提供有关根账户或 IAM 用户的信息。此元素具有以下属性：

- type – 临时安全凭证的源，例如 Root、IAMUser 或 Role。

- userName – 已发布会话的用户或角色的友好名称。显示的值取决于 sessionIssuer 身份 type。下表显示 sessionIssuer type 和 userName 之间的关系：

sessionIssuer 类型	userName	描述
Root（未设置别名）	不存在	如果您未为账户设置别名，则 userName 字段不会出现。有关 AWS 账户 别名的更多信息，请参阅您的 AWS 账户 身份证及其别名。请注意，userName 字段不能包含 Root，因为 Root 是身份类型而不是用户名称。
Root（已设置别名）	账户别名	有关 AWS 账户 别名的更多信息，请参阅您的 AWS 账户 ID 及其别名。
IAMUser	IAM 用户的用户名	这在联合身份用户使用由 IAMUser 发布的会话时也适用。
Role	角色名称	由 IAM 用户或 Web 联合身份用户在角色会话中扮演的角色。 AWS 服务

- principalId – 已用于获取凭证的实体的内部 ID。
- arn – 已用于获取临时安全凭证的源（账户、IAM 用户或角色）的 ARN。
- accountId – 拥有已用于获取凭证的实体的账户。

Optional (可选)：True

onBehalfOf

如果请求由 IAM Identity Center 调用者发出，onBehalfOf 会提供有关发出调用的 IAM Identity Center 用户 ID 和身份存储 ARN 的信息。此元素具有以下属性：

- userId – 代表其发出调用的 IAM Identity Center 用户 ID。
- identityStoreArn – 代表其发出调用的 IAM Identity Center 身份存储的 ARN。

Optional (可选)：True

credentialId

请求的凭证 ID。只有当调用者使用持有者令牌（例如 IAM Identity Center 授权的访问令牌）时，才会设置此选项。

Optional (可选)：True

webIdFederationData

如果已使用通过 Web 身份联合验证获取的临时安全凭证发出请求，webIdFederationData 会列出有关身份提供商的信息。

此元素具有以下属性：

- federatedProvider – 身份提供商的委托人名称 (例如，适用于 Login with Amazon 的 www.amazon.com 或适用于 Google 的 accounts.google.com)。
- attributes – 提供商报告的应用程序 ID 和用户 ID (例如，适用于 Login with Amazon 的 www.amazon.com:app_id 和 www.amazon.com:user_id)。

> **Note**
>
> 省略此字段或该字段的值为空表示不存在有关身份提供者的信息。

Optional (可选)：True

具有 SAML 和网络联合身份验证 AWS STS 的 API 的值

AWS CloudTrail 支持使用安全断言标记语言 AWS Security Token Service (SAML AWS STS) 和 Web 联合身份验证进行的 logging () API 调用。当用户调用AssumeRoleWithSAML和AssumeRoleWithWebIdentityAPI 时，会 CloudTrail 记录该调用并将事件传送到您的 Amazon S3 存储桶。

这些 API 的 userIdentity 元素包含以下值。

type

身份类型。

- SAMLUser – 已使用 SAML 断言发出请求。
- WebIdentityUser – 已通过 Web 联合身份提供商发出请求。

principalId

已发出调用的实体的唯一标识符。

- 对于 SAMLUser，这是 saml:namequalifier 和 saml:sub 密钥的组合。
- 对于 WebIdentityUser，这是发布者、应用程序 ID 和用户 ID 的组合。

userName

已发出调用的身份的名称。

- 对于 SAMLUser，这是 saml:sub 密钥。
- 对于 WebIdentityUser，这是用户 ID。

identityProvider

外部身份提供商的委托人名称。只有 SAMLUser 或 WebIdentityUser 类型才显示此字段。

- 对于 SAMLUser，这是 SAML 断言的 saml:namequalifier 密钥。
- 对于 WebIdentityUser，这是 Web 联合身份验证提供商的发布者名称。它可以是您配置的提供商，如下所示：
  - Amazon Cognito 的 cognito-identity.amazon.com
  - Login with Amazon 的 www.amazon.com
  - Google 的 accounts.google.com
  - Facebook 的 graph.facebook.com

下面是 AssumeRoleWithWebIdentity 操作的示例 userIdentity 元素。

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

有关userIdentity元素的显示方式SAMLUser和WebIdentityUser类型的日志示例，请参阅使用记录 IAM 和 AWS STS API 调用 AWS CloudTrail。

AWS STS 来源身份

IAM 管理员可以配置 AWS Security Token Service 为要求用户在使用临时证书代入角色时指定其身份。sourceIdentity 字段出现在用户代入 IAM 角色或使用代入的角色执行任何操作的事件中。

sourceIdentity 字段识别发出请求的原始用户身份，无论该用户的身份是 IAM 用户、IAM 角色、使用基于 SAML 的联合身份进行身份验证的用户，还是使用符合 OpenID Connect (OIDC) 的 Web 联

合身份进行身份验证的用户。IAM 管理员配置后 AWS STS，在事件 CloudTrail 记录中的以下事件和位置中记录sourceIdentity信息：

- 用户身份代入角色时发出的AssumeRoleWithSAML、或AssumeRoleWithWebIdentity调用。AWS STS AssumeRole sourceIdentity可以在 AWS STS 通话requestParameters块中找到。
- 用户身份使用角色担任另一个角色时发出的AssumeRoleWithSAML、或AssumeRoleWithWebIdentity调用，称为角色链。 AWS STS AssumeRole sourceIdentity可以在 AWS STS 通话requestParameters块中找到。
- AWS 服务 API 调用是用户身份在担任角色并使用分配的临时凭证时进行的 AWS STS。在服务 API 事件中，sourceIdentity 可以位于 sessionContext 数据块中。例如，如果用户身份创建新 S3 存储桶，则在 CreateBucket 事件的 sessionContext 数据块中会发生 sourceIdentity。

有关如何进行配置 AWS STS 以收集源身份信息的更多信息，请参阅 IAM 用户指南中的监控和控制使用代入角色执行的操作。有关记录到 AWS STS 的事件的更多信息 CloudTrail，请参阅 IAM 用户指南 AWS CloudTrail中的使用记录 IAM 和 AWS STS API 调用。

下面是事件的示例代码段，其中显示了 sourceIdentity 字段。

示例 **requestParameters** 部分

在以下示例事件片段中，用户发出 AWS STS AssumeRole请求并设置源身份，此处用*source-identity-value-set*表示。用户代入由角色 ARN arn:aws:iam::123456789012:role/Assumed_Role 表示的角色。sourceIdentity 字段位于事件的 requestParameters 数据块中。

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
```

```
        "sourceIdentity": "source-identity-value-set",
    },
```

示例 **responseElements** 部分

在以下示例事件片段中，用户 AWS STS AssumeRole请求代入名为Developer_Role的角色并设置源身份。Admin用户代入由角色 ARN arn:aws:iam::111122223333:role/Developer_Role 表示的角色。sourceIdentity 字段显示在事件的 responseElements 和 requestParameters 数据块中。用于代入角色的临时证书、会话令牌字符串以及代入的角色 ID、会话名称和会话 ARN 与源身份一起显示在 responseElements 数据块中。

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                            EXAMPLE_SESSION_TOKEN
                            XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

示例 **sessionContext** 部分

在以下示例事件片段中，用户扮演一个名为的角色DevRole来调用 AWS 服务 API。用户设置源身份，此处用表示*source-identity-value-set*。sourceIdentity 字段位于 userIdentity 数据块中，处在事件的 sessionContext 数据块内。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

CloudTrail 见解**insightDetails**元素

AWS CloudTrail Insights 事件记录包括与其 JSON 结构中其他 CloudTrail 事件不同的字段，有时称为负载。 CloudTrail Insights 事件记录包括一个`insightDetails`块，其中包含有关 Insights 事件底层触发器的信息，例如事件源、用户身份、用户代理、历史平均值或基线、统计数据、API 名称以及该事件是 Insights 事件的开始还是结束。`insightDetails` 数据块包含以下信息。

- **`state`** - 事件是开始还是结束见解事件。该值可以是 `Start` 或 `End`。

  从：1.07

  Optional (可选)：False
- **`eventSource`**-作为异常活动来源的 AWS 服务端点，例如`ec2.amazonaws.com`。

  从：1.07

  Optional (可选)：False
- **`eventName`** - 见解事件的名称，通常是作为异常活动的源的 API 的名称。

从：1.07

Optional (可选)：False

- **insightType** - 见解事件的类型。该值可以是 ApiCallRateInsight 和/或 ApiErrorRateInsight。

  从：1.07

  Optional (可选)：False

- **insightContext** -

  有关 AWS 工具（称为用户代理）、IAM 用户和角色（称为用户身份）以及与为生成 Insights 事件而 CloudTrail 分析的事件关联的错误代码的信息。此元素还包括统计信息，显示了 Insights 事件中的异常活动与基准或正常活动对比的情况。

  从：1.07

  Optional (可选)：False

  - **statistics** - 包括有关基准的数据，或者在基准期内账户对主题 API 的典型平均调用或错误速率、在 Insights 事件的第一分钟内触发 Insights 事件的调用或错误速率、Insights 事件的持续时间（以分钟为单位）以及基准测量周期的持续时间（以分钟为单位）。

    从：1.07

    Optional (可选)：False

    - **baseline** - 在基准持续时间内，关于该账户的 Insights 事件主题 API 的平均每分钟 API 调用或错误次数，计算 Insights 事件开始之前七天内的值。

      从：1.07

      Optional (可选)：False

    - **insight** -

      对于开始 Insights 事件，此值是在异常活动开始期间的每分钟平均 API 调用或错误次数。对于结束 Insights 事件，此值是在异常活动持续期间的每分钟平均 API 调用或错误次数。

      从：1.07

      Optional (可选)：False

- **insightDuration** - 见解事件的持续时间（在主题 API 中从异常活动开始到结束的时间段），以分钟为单位。在见解事件开始和结束时都会发生 insightDuration。

  从：1.07

  Optional (可选)：False

- **baselineDuration** - 基准周期的持续时间（在主题 API 中测量正常活动的时间段），以分钟为单位。baselineDuration 至少为见解事件之前的七天时间（10080 分钟）。此字段同时出现在开始和结束见解事件中。baselineDuration 测量的结束时间始终是见解事件的开始。

  从：1.07

  Optional (可选)：False

- **attributions** - 此数据块包含有关与异常活动和基准活动相关的用户身份、用户代理和错误代码的信息。在见解事件 attributions 数据块中捕获最多五个用户身份、五个用户代理和五个错误代码，按活动计数的平均值，从最高到最低的降序排列。

  从：1.07

  Optional (可选)：True

  - **attribute** - 包含属性类型。值可以是 userIdentityArn、userAgent 或 errorCode。
    - **userIdentityArn**-显示在异常活动和基准期内导致 API 调用或错误的前五名 AWS 用户或 IAM 角色的区块。另请参阅 CloudTrail 录制内容 中的 userIdentity。

      从：1.07

      Optional (可选)：False

      - **insight** - 此数据块显示对异常活动期间进行的 API 调用有贡献的最多前五名的用户身份 ARN，按 API 调用数量从最大到最小的降序排列。它还显示了用户身份在异常活动期间进行的 API 调用的平均数量。

        从：1.07

        Optional (可选)：False

        - **value** - 对异常活动期间进行的 API 调用有贡献的排名前五的用户身份之一的 ARN。

          从：1.07

          Optional (可选)：False

- **average** - value 字段中的用户身份在异常活动期间每分钟的 API 调用或错误次数。

  从：1.07

  Optional (可选)：False

- **baseline** - 此数据块显示在正常活动期间，引发 API 调用或错误的排名前五的用户身份 ARN。它还显示了用户身份在正常活动期间记录的 API 调用或错误的平均数量。

  从：1.07

  Optional (可选)：False

  - **value** - 在正常活动期间，引发 API 调用或错误的排名前五的用户身份中某一个身份的 ARN。

    从：1.07

    Optional (可选)：False

  - **average** - 在 Insights 活动开始时间之前的七天内，value 字段中用户身份的每分钟 API 调用或错误的历史平均值。

    从：1.07

    Optional (可选)：False

- **userAgent**-一个方块，显示了在异常活动和基准期内，用户身份促成 API 调用的前五个 AWS 工具。这些工具包括 AWS Management Console AWS CLI、或 AWS SDK。另请参阅 CloudTrail 录制内容 中的 userAgent。

  从：1.07

  Optional (可选)：False

  - **insight** - 此数据块显示对异常活动期间进行的 API 调用有贡献的最多前五名的用户代理，按 API 调用数量从最大到最小的降序排列。它还显示了用户代理在异常活动期间记录的 API 调用或错误的平均数量。

    从：1.07

    Optional (可选)：False

    - **value** - 对异常活动期间进行的 API 调用有贡献的排名前五的用户代理之一。

从：1.07

Optional (可选)：False

- **average** - value 字段中的用户代理在异常活动期间，每分钟的 API 调用或错误数。

  从：1.07

  Optional (可选)：False

- **baseline** - 此数据块显示对正常活动期间进行的 API 调用贡献最大的最多前五名的用户代理。它还显示了用户代理在正常活动期间记录的 API 调用或错误的平均数量。

  从：1.07

  Optional (可选)：False

  - **value** - 在正常活动期间，引发 API 调用或错误的排名前五的用户代理之一。

    从：1.07

    Optional (可选)：False

  - **average** - 在 Insights 活动开始时间之前的七天内，value 字段中的用户代理的每分钟 API 调用或错误的历史平均值。

    从：1.07

    Optional (可选)：False

- **errorCode** - 此数据块显示在异常活动期间和基准期的 API 调用中发生的最多前五名的错误代码，按 API 调用数量从最大到最小的降序排列。另请参阅 CloudTrail 录制内容 中的 errorCode。

  从：1.07

  Optional (可选)：False

  - **insight** - 此数据块显示在异常活动期间进行的 API 调用中发生的最多前五名的错误代码，按相关 API 调用数量从最大到最小的降序排列。它还显示了在异常活动期间发生了错误的 API 调用的平均数量。

    从：1.07

    Optional (可选)：False

- **value** - 在异常活动期间进行的 API 调用中发生的排名前五的错误代码之一，例如 AccessDeniedException。

  如果触发见解事件的任何调用都不会导致错误，则此值为 null。

  从：1.07

  Optional (可选)：False

- **average** - value 字段中的错误代码在异常活动期间每分钟调用的 API 次数。

  如果错误代码值为 null，并且 insight 数据块中没有其他错误代码，则 average 的值与表现见解事件总体的 statistics 数据块中的值相同。

  从：1.07

  Optional (可选)：False

- **baseline** - 此数据块显示在正常活动期间进行的 API 调用中发生的最多前五名的错误代码。它还显示了用户代理在正常活动期间进行的 API 调用的平均数量。

  从：1.07

  Optional (可选)：False

  - **value** - 在正常活动期间进行的 API 调用中发生的排名前五的错误代码之一，例如 AccessDeniedException。

    从：1.07

    Optional (可选)：False

  - **average** - 在 Insights 活动开始时间之前的七天内，value 字段中的错误代码的每分钟 API 调用或错误的历史平均值。

    从：1.07

    Optional (可选)：False

示例 **insightDetails** 数据块

下面是在不寻常地多次调用 Application Auto Scaling API CompleteLifecycleAction 时发生的见解事件的见解事件 insightDetails 数据块示例。有关完整见解事件的示例，请参阅 洞察活动。

此示例来自开始见解事件，通过 "state": "Start" 表示。调用与见解事件关联的 API 的顶级用户身份 CodeDeployRole1、CodeDeployRole2 和 CodeDeployRole3，与其对此见解事件的平均 API 调用率以及 CodeDeployRole1 角色的基准值一起显示在 attributions 数据块中。该attributions区块还显示用户代理是codedeploy.amazonaws.com，这意味着顶级用户身份使用 AWS CodeDeploy 控制台运行 API 调用。

因为没有与为了生成见解事件而分析的事件相关的错误代码（值为 null），错误代码的 insight 平均值与整个见解事件的总体 insight 平均值相同，显示在 statistics 数据块中。

```
          "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
```

```
                    }
                  ],
                  "baseline": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "userAgent",
                  "insight": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "errorCode",
                  "insight": [
                    {
                      "value": "null",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "null",
                      "average": 0.0000882145
                    }
                  ]
                }
              ]
            }
          }
```

捕获的非 API 事件 CloudTrail

除了记录 AWS API 调用外，还可以 CloudTrail 捕获可能对您的 AWS 账户造成安全性或合规性影响或可能有助于您解决操作问题的其他相关事件。

主题

- AWS 服务事件
- AWS Management Console 登录事件

AWS 服务事件

CloudTrail 支持记录非 API 服务事件。这些事件由 AWS 服务创建，但不是由对公共 AWS API 的请求直接触发的。对于这些事件，`eventType` 字段为 `AwsServiceEvent`。

以下是客户托管密钥在 AWS Key Management Service (AWS KMS) 中自动轮换时的 AWS 服务事件场景示例。有关轮换 KMS 密钥的更多信息，请参阅轮换 KMS 密钥。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
```

```
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```

AWS Management Console 登录事件

CloudTrail 记录尝试登录 AWS Management Console、 AWS 讨论论坛和 Su AWS pport Center。所有 IAM 用户和根用户登录事件以及所有联合用户登录事件都会在 CloudTrail 日志文件中生成记录。有关查找和查看日志的信息，请参阅 正在查找您的 CloudTrail 日志文件 和 正在下载您的 CloudTrail 日志文件。

> **Note**
>
> `ConsoleLogin`事件中记录的区域因用户类型以及您使用全球还是区域终端节点登录而异。
>
> - 如果您以 root 用户身份登录，则将事件 CloudTrail 记录在 us-east-1 中。
> - 如果您使用 IAM 用户登录并使用全局终端节点，则按如下方式 CloudTrail 记录`ConsoleLogin`事件的区域：
>   - 如果浏览器中存在账户别名 cookie，则会在以下区域之一 CloudTrail 记录`ConsoleLogin`事件：us-east-2、eu-north-1 或 ap-southeast-2。这是因为控制台代理会根据用户登录位置的延迟来重定向用户。
>   - 如果浏览器中没有账户别名 cookie，则在 us-east-1 中 CloudTrail 记录该`ConsoleLogin`事件。这是因为控制台代理重定向回全局登录。
> - 如果您使用 IAM 用户登录并使用区域终端节点，则会在终端节点的相应区域中 CloudTrail 记录`ConsoleLogin`事件。有关 AWS 登录 终端节点的更多信息，请参阅AWS 登录 终端节点和配额。

主题

- IAM 用户的事件记录示例
- 根用户的示例事件记录
- 联合用户的事件记录示例

IAM 用户的事件记录示例

以下示例显示了适用于多种 IAM 用户登录方案的事件记录。

主题

- IAM 用户，未使用 MFA 而成功登录
- IAM 用户，使用 MFA 成功登录
- IAM 用户，登录失败
- IAM 用户，针对 MFA 的登录流程检查（单一 MFA 设备类型）
- IAM 用户，针对 MFA 的登录流程检查（多种 MFA 设备类型）

IAM 用户，未使用 MFA 而成功登录

以下记录显示，名为的用户在 AWS Management Console 未使用多重身份验证 (MFA) 的情况下Anaya成功登录。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
```

```
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 用户，使用 MFA 成功登录

以下记录显示，名为的 IAM 用户 AWS Management Console 使用多重身份验证 (MFA) Anaya 成功登录。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
```

```
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 用户，登录失败

以下记录显示名为 Paulo 的 IAM 用户的失败登录操作。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
```

```
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 用户，针对 MFA 的登录流程检查（单一 MFA 设备类型）

以下显示登录过程检查 IAM 用户在登录过程中是否需要多重验证 (MFA)。在此示例中，mfaType 值为 U2F MFA，表示 IAM 用户启用了单个 MFA 设备或多个相同类型的 MFA 设备 (U2F MFA)。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
```

```
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 用户，针对 MFA 的登录流程检查（多种 MFA 设备类型）

以下显示登录过程检查 IAM 用户在登录过程中是否需要多重验证 (MFA)。在此示例中，mfaType 值为 Multiple MFA Devices，表示 IAM 用户启用了多种 MFA 设备类型。

```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "IAMUser",
       "principalId": "EXAMPLE6E4XEGITWATV6R",
       "accountId": "123456789012",
       "accessKeyId": "",
       "userName": "Mary"
   },
   "eventTime": "2023-07-19T23:10:09Z",
   "eventSource": "signin.amazonaws.com",
   "eventName": "CheckMfa",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "192.0.2.0",
   "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
   "requestParameters": null,
   "responseElements": {
       "CheckMfa": "Success"
   },
   "additionalEventData": {
       "MfaType": "Multiple MFA Devices"
```

```
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

根用户的示例事件记录

以下示例显示了适用于多种 root 用户登录方案的事件记录。当您使用 root 用户登录时，将ConsoleLogin事件 CloudTrail 记录在 us-east-1 中。

主题

- 根用户，未使用 MFA 而成功登录
- 根用户，使用 MFA 成功登录
- 根用户，登录失败
- 根用户，MFA 已更改
- 根用户，密码已更改

根用户，未使用 MFA 而成功登录

以下信息显示根用户未使用多重身份验证（MFA）而成功登录的事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

根用户，使用 MFA 成功登录

以下信息显示根用户使用多重身份验证（MFA）成功登录的事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


根用户，登录失败

下面显示的是未使用 MFA 的根用户登录失败事件。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
```

```
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


根用户，MFA 已更改

下面显示的是根用户更改多重身份验证 (MFA) 设置的示例事件。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
```

```
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

根用户，密码已更改

下面显示的是根用户更改密码的示例事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
```

```
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
}
```

联合用户的事件记录示例

以下示例显示了联合用户的事件记录。联邦用户将获得临时安全证书，允许他们通过AssumeRole请求访问 AWS 资源。

以下示例显示了联合身份验证加密请求的事件。userIdentity 元素的 accessKeyId 字段中会提供原始访问密钥 ID。如果加密请求中传递了所请求的 sessionDuration，则 responseElements 中的 accessKeyId 字段会包含新的访问密钥 ID，否则会包含原始访问密钥 ID 的值。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
```

```
}
```

以下示例显示联合用户在未使用多重身份验证（MFA）的情况下成功登录的事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
```

```
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

处理 CloudTrail 日志文件

您可以对 CloudTrail 文件执行更高级的任务。

- 创建每区域多个跟踪。
- 通过将 CloudTrail 日志文件发送到 “日志” 来监控 CloudWatch 日志文件。
- 在账户间共享日志文件。
- 使用 AWS CloudTrail 处理库用 Java 编写日志处理应用程序。
- 验证您的日志文件以验证它们在交付后是否未更改 CloudTrail。

当您的账户中发生事件时， CloudTrail 会评估该事件是否与您的路径设置相匹配。只有与您的跟踪设置匹配的事件才会传输到您的 Amazon S3 存储桶和 Amazon Log CloudWatch s 日志组。

您可以对多个跟踪记录进行不同的配置，以便这些跟踪记录仅处理和记录您指定的事件。例如，一个跟踪可记录只读数据事件和管理事件，以使所有只读事件传送到一个 S3 存储桶。另一个跟踪可仅记录只写数据事件和管理事件，以使所有只写事件传送到一个单独的 S3 存储桶。

您也可以配置您的跟踪记录以拥有一个跟踪记录日志并将所有管理事件传送到一个 S3 存储桶，并配置另一个跟踪记录以记录所有数据事件并将其传送到另一个 S3 存储桶。

您可以配置您的跟踪记录以记录以下内容：

- 数据事件：通过这些事件，可以了解对资源执行的或在资源内执行的资源操作。这些也称为数据层面操作。
- 管理事件：管理事件可让您了解对 AWS 账户中的资源执行的管理操作。这些也称为控制层面操作。管理事件还包括在您的账户中发生的非 API 事件。例如，当用户登录您的账户时，会 CloudTrail 记录该`ConsoleLogin`事件。有关更多信息，请参阅 捕获的非 API 事件 CloudTrail。
- Insights 事件：见解事件捕获在您的账户中检测到的异常活动。如果您启用了 Insights 事件并 CloudTrail 检测到异常活动，则 Insights 事件会记录到您的跟踪的目标 S3 存储桶中，但会记录在不同的文件夹中。在 CloudTrail 控制台上查看 Insights 事件时，您还可以查看 Insights 事件的类型和事件时间段。与 CloudTrail 跟踪中捕获的其他类型的事件不同，Insights 事件仅在 CloudTrail 检测到您的账户 API 使用情况与账户的典型使用模式明显不同时，才会记录 Insights 事件。

  仅针对管理 API 生成 Insights 事件。有关更多信息，请参阅 记录 Insights 事件。

> **Note**
>
> CloudTrail 通常在 API 调用后的平均大约 5 分钟内传送日志。此时间并不能得到保证。有关更多信息，请参阅 AWS CloudTrail 服务等级协议。
> 如果您错误配置了跟踪（例如，无法访问 S3 存储桶），则 CloudTrail 会尝试将日志文件重新传送到您的 S3 存储桶，持续 30 天，这些 attempted-to-deliver 事件将按标准费用收费。CloudTrail 为避免配置错误的跟踪产生费用，您需要删除跟踪。

主题

- 接收来自多个区域的 CloudTrail 日志文件
- 在中管理数据一致性 CloudTrail
- 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件
- 接收来自多个账户的 CloudTrail 日志文件
- 在 AWS 账户之间共享 CloudTrail 日志文件
- 验证 CloudTrail 日志文件完整性
- CloudTrail 日志文件示例
- 使用 CloudTrail 处理库

接收来自多个区域的 CloudTrail 日志文件

您可以配置 CloudTrail 为将日志文件从多个区域传输到单个账户的单个 S3 存储桶。例如，您在美国西部（俄勒冈）区域有一个配置为将日志文件传送到 S3 存储桶的跟踪，还有一个 CloudWatch 日志日志组。当您将现有的单区域跟踪更改为记录所有区域时，会 CloudTrail 记录您账户中单个 AWS 分区中所有区域的事件。 CloudTrail 将日志文件传送到相同的 S3 存储桶和 CloudWatch 日志组。只要 CloudTrail 有权写入 S3 存储桶，多区域跟踪的存储桶就不必位于跟踪的主区域中。

要记录您账户中所有 AWS 分区中所有区域的事件，请在每个分区中创建多区域跟踪。

在控制台中，默认情况下您创建的跟踪可记录您正在使用的 AWS 分区中所有 AWS 区域 的事件。这是推荐的最佳实践。要记录单区域中的事件（不推荐），请使用 AWS CLI。要配置现有单区域跟踪以登录所有区域，必须使用 AWS CLI。

要更改现有跟踪以使其应用于所有区域，请向 update-trail 添加 `--is-multi-region-trail` 选项。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

要确认跟踪现已应用到所有区域，请验证输出中的 IsMultiRegionTrail 元素是否为 true。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 当新区域在aws分区中启动时， CloudTrail 会自动在新区域中为您创建一条与原始跟踪设置相同的跟踪。

有关更多信息，请参阅以下资源：

- 处理 CloudTrail 轨迹
- CloudTrail 常见问题

在中管理数据一致性 CloudTrail

CloudTrail 使用一种名为最终一致性的分布式计算模型。您对 CloudTrail 配置（或其他 AWS 服务）所做的任何更改，包括基于属性的访问控制 (ABAC) 中使用的标签，都需要一段时间才能从所有可能的端点中看见。有些延迟是由于世界各地将数据从服务器发送到服务器、从复制区域发送到复制区域以及从一个区域发送到另一个区域所花费的时间。 CloudTrail 还使用缓存来提高性能，但在某些情况下，这可能会增加时间。在之前缓存的数据超时之前，更改可能不可见。

您在设计应用程序时，必须考虑到这些可能的延迟。确保应用程序可以按预期工作，即使在一个位置进行的更改不能立即在其他位置可见。此类更改包括创建或更新跟踪或事件数据存储、更新事件选择器，以及启动或停止日志记录。创建或更新跟踪或事件数据存储时，会根据最新的已知配置将日志传 CloudTrail 送到 S3 存储桶或事件数据存储，直到更改传播到所有位置。

有关这会如何影响其他人的更多信息 AWS 服务，请参阅以下资源：

- Amazon DynamoDB：DynamoDB 常见问题中的什么是 DynamoDB 的一致性模型？，以及《Amazon DynamoDB 开发人员指南》中的读取一致性。
- Amazon EC2：《Amazon Elastic Compute Cloud API 参考》中的最终一致性。
- 亚马逊 EMR：在AWS 大数据博客中使用 Amazon S3 和 Amazon Elastic MapReduce 处理 ETL 工作流程时确保一致性。
- AWS Identity and Access Management (IAM)：我所做的更改并不总是立即显示在 IAM 用户指南中。
- Amazon Redshift：《Amazon Redshift 数据库开发人员指南》中的管理数据一致性。
- Amazon S3：《Amazon Simple Storage Service 用户指南》中的 Amazon S3 数据一致性模型。

使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件

您可以配置 CloudWatch 日志 CloudTrail 来监控您的跟踪日志，并在发生特定活动时收到通知。

1. 配置您的跟踪以将日志事件发送到 CloudWatch 日志。
2. 定义 CloudWatch 日志指标筛选器，以评估日志事件中是否存在术语、短语或值的匹配项。例如，您可以监控 `ConsoleLogin` 事件。
3. 为 CloudWatch 指标筛选器分配指标。
4. 创建根据您指定的阈值和时间段触发的 CloudWatch 警报。您可以配置警报，以在触发警报时发送通知，使您可以执行操作。
5. 您也可以配置 CloudWatch 为自动执行操作以响应警报。

Amazon CloudWatch 和 Amazon CloudWatch Logs 的标准定价适用。有关更多信息，请参阅 Amazon CloudWatch 定价。

有关您可以将跟踪配置为向 CloudWatch 日志发送日志的区域的更多信息，请参阅AWS 一般参考中的 Amazon CloudWatch Logs 区域和配额。

主题

- 将事件发送到 CloudWatch 日志
- 为 CloudTrail 事件创建 CloudWatch 警报：示例
- 停止 CloudTrail 向 CloudWatch 日志发送事件
- CloudWatch 的日志组和日志流命名 CloudTrail
- 使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档

将事件发送到 CloudWatch 日志

当您将跟踪配置为向 CloudWatch Logs 发送事件时，仅 CloudTrail 发送与您的跟踪设置相匹配的事件。例如，如果您将跟踪配置为仅记录数据事件，则您的跟踪仅将数据事件发送到您的 CloudWatch 日志日志组。 CloudTrail 支持向 CloudWatch 日志发送数据、见解和管理事件。有关更多信息，请参阅处理 CloudTrail 日志文件。

> **Note**
>
> 只有管理账户才能使用控制台为组织跟踪配置 CloudWatch 日志组。授权的管理员可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 操作配置 CloudWatch 日志组。

要将事件发送到 CloudWatch 日志日志组，请执行以下操作：

- 请确保您有足够的权限来创建或指定 IAM 角色。有关更多信息，请参阅 授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限。
- 如果您使用配置 CloudWatch 日志日志组 AWS CLI，请确保您有足够的权限在您指定的 CloudWatch 日志组中创建日志日志流并将 CloudTrail 事件传送到该日志流。有关更多信息，请参阅创建策略文档。
- 创建新的跟踪或指定现有的跟踪。有关更多信息，请参阅 使用控制台创建和更新跟踪。
- 创建一个日志组或指定一个现有日志组。
- 指定 IAM 角色。如果您要修改用于组织跟踪的现有 IAM 角色，则必须手动更新策略，以允许组织跟踪的日志记录。有关更多信息，请参阅此策略示例和为组织创建跟踪。
- 附加一个角色策略或者使用默认角色策略。

目录

- 使用控制台配置 CloudWatch 日志监控
  - 创建一个日志组或指定一个现有日志组
  - 指定 IAM 角色
  - 在 CloudWatch 控制台中查看事件
- 使用配置 CloudWatch 日志监控 AWS CLI
  - 创建日志组
  - 创建角色
  - 创建策略文档

- 更新跟踪
- 限制

使用控制台配置 CloudWatch 日志监控

您可以使用来配置您的跟踪 AWS Management Console ，以便将事件发送到 CloudWatch 日志进行监控。

创建一个日志组或指定一个现有日志组

CloudTrail 使用 CloudWatch 日志日志组作为日志事件的传输终端节点。可创建一个日志组或者指定一个现有日志组。

为现有跟踪创建或指定日志组

1. 请务必使用具有足够权限的管理用户或角色登录，以配置 CloudWatch 日志集成。有关更多信息，请参阅 授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限。

   > **Note**
   >
   > 只有管理账户才能使用控制台为组织跟踪配置 CloudWatch 日志组。授权的管理员可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 操作配置 CloudWatch 日志组。

2. 打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
3. 选择跟踪名称。如果您选择一个应用于所有区域的跟踪，则您将重定向到创建此跟踪的区域。可以在跟踪所在的区域创建一个日志组或者选择一个现有日志组。

   > **Note**
   >
   > 适用于所有区域的跟踪会将所有区域的日志文件发送到您指定的 CloudWatch 日志日志组。

4. 在CloudWatch 日志中，选择编辑。
5. 对于CloudWatch 日志，选择启用。
6. 在日志组名称下，选择新建创建新的日志组，或选择现有使用现有的日志组。如果选择 “新建”，则会为您 CloudTrail 指定新日志组的名称，也可以键入名称。有关命名的更多信息，请参阅 CloudWatch 的日志组和日志流命名 CloudTrail。

7. 如果选择 Existing（现有），则从下拉列表中选择一个日志组。
8. 对于角色名称，选择新建以创建新的 IAM 角色，以获得向日志发送 CloudWatch 日志的权限。选择 Existing（现有）以从下拉列表中选择一个现有 IAM 角色。展开 Policy document（策略文档）时，将显示新角色或现有角色的策略语句。有关该角色的更多信息，请参阅 使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档。

   > **Note**
   >
   > 在您配置跟踪时，可以选择属于另一个账户的 S3 存储桶和 SNS 主题。但是，如果 CloudTrail 要将事件传送到 CloudWatch 日志日志组，则必须选择当前账户中存在的日志组。

9. 选择保存更改。

指定 IAM 角色

您可以指定一个角色 CloudTrail 来代入将事件传送到日志流。

指定角色

1. 默认情况下，系统将为您指定 `CloudTrail_CloudWatchLogs_Role`。默认角色策略具有在您指定的 CloudWatch 日志组中创建日志日志流并将 CloudTrail 事件传送到该日志流所需的权限。

   > **Note**
   >
   > 如果要将此角色用于组织跟踪的日志组，则必须在创建角色后手动修改策略。有关更多信息，请参阅此策略示例和为组织创建跟踪。

   a. 要验证角色，请访问 AWS Identity and Access Management 控制台，网址为 https://console.aws.amazon.com/iam/。
   b. 选择 “角色”，然后选择 CloudTrail_ CloudWatchLogs _Rol e。
   c. 在权限选项卡中，展开策略查看其内容。
2. 您可以指定其他角色，但是如果要使用该角色向 CloudWatch 日志发送事件，则必须将所需的角色策略附加到现有角色。有关更多信息，请参阅 使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档。

在 CloudWatch 控制台中查看事件

将跟踪配置为将事件发送到 CloudWatch 日志日志组后，您可以在 CloudWatch 控制台中查看事件。CloudTrail 通常在 API 调用后的平均大约 5 分钟内将事件传送到您的日志组。此时间并不能得到保证。有关更多信息，请参阅 AWS CloudTrail 服务等级协议。

在 CloudWatch 控制台中查看事件

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在左侧导航窗格中，从日志下选择日志组。
3. 选择为您的跟踪指定的日志组。
4. 选择要查看的日志流。
5. 要查看您的跟踪记录的事件的详细信息，请选择一个事件。

> **Note**
>
> CloudWatch 控制台中的时间 (UTC) 列显示事件何时传送到您的日志组。要查看记录事件的实际时间 CloudTrail，请参阅字`eventTime`段。

使用配置 CloudWatch 日志监控 AWS CLI

您可以使用配置 AWS CLI 将事件发送 CloudTrail 到 CloudWatch 日志进行监控。

创建日志组

1. 如果您没有现有的日志组，请使用 Logs `create-log-group` 命令创建一个 CloudWatch 日志日志组作为日志事件的传输终端节点。 CloudWatch

   ```
   aws logs create-log-group --log-group-name name
   ```

   下面的示例创建一个名为 `CloudTrail/logs` 的日志组：

   ```
   aws logs create-log-group --log-group-name CloudTrail/logs
   ```

2. 检索日志组 Amazon Resource Name（ARN）。

   ```
   aws logs describe-log-groups
   ```

创建角色

为其创建一个角色 CloudTrail ，使其能够将事件发送到 CloudWatch 日志日志组。IAM `create-role` 命令接受两个参数：角色名称和代入角色策略文档 (JSON 格式) 的文件路径。您使用的策略文档`AssumeRole`授予权限 CloudTrail。`create-role` 命令可创建具有所需权限的角色。

要创建包含此策略文档的 JSON 文件，请打开文本编辑器并将以下策略内容保存到名为 `assume_role_policy_document.json` 的文件中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

运行以下命令来创建具有`AssumeRole`权限的角色 CloudTrail。

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

待命令完成后，记下输出中的角色 ARN。

创建策略文档

为创建以下角色策略文档 CloudTrail。本文档授予 CloudTrail 在您指定的 CloudWatch 日志组中创建日志日志流以及向该日志流传送 CloudTrail 事件所需的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "AWSCloudTrailCreateLogStream2014110",
```

```
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

将此策略文档保存到名为 role-policy-document.json 的文件中。

如果您要创建可能用于组织跟踪记录的策略，则需要对其进行稍微不同的配置。*######### CloudTrail ########### CloudWatch ############### CloudTrail ################ # 111111111111 ######## 111111111111 AWS ######### o-exampleorgid ######### AWS Organizations*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
```

```
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

有关组织跟踪记录的更多信息，请参阅为组织创建跟踪。

运行以下命令以将策略应用于角色。

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

更新跟踪

使用 CloudTrail`update-trail`命令使用日志组和角色信息更新跟踪。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

有关 AWS CLI 命令的更多信息，请参阅《AWS CloudTrail 命令行参考》。

限制

CloudWatch 日志和 EventBridge 每个日志允许的最大事件大小为 256 KB。尽管大多数服务事件的最大大小为 256 KB，但有些服务的事件仍然更大。 CloudTrail 不会将这些事件发送到 CloudWatch 日志或 EventBridge。

从 CloudTrail 事件版本 1.05 开始，事件的最大大小为 256 KB。这是为了帮助防止恶意行为者利用这些漏洞，并允许其他 AWS 服务（例如 L CloudWatch ogs 和）使用事件 EventBridge。

为 CloudTrail 事件创建 CloudWatch 警报：示例

本主题介绍如何为 CloudTrail 事件配置警报，并包括示例。

主题

- 先决条件
- 创建指标筛选条件，并创建警报
- 示例安全组配置更改
- 登录失 AWS Management Console 败示例
- 示例：IAM policy 更改
- 为 CloudWatch 日志警报配置通知

先决条件

在使用本主题中的示例前，您必须：

- 使用 控制台或 CLI 创建一个跟踪。
- 创建日志组，您可以在创建跟踪时执行此操作。有关创建跟踪的更多信息，请参阅创建跟踪。
- 指定或创建一个 IAM 角色， CloudTrail 该角色授予在您指定的CloudWatch 日志组中创建日志日志流以及向该日志流传送 CloudTrail 事件的权限。默认的 `CloudTrail_CloudWatchLogs_Role` 将为您执行此操作。

有关更多信息，请参阅 将事件发送到 CloudWatch 日志。本节中的示例在 Amazon CloudWatch Logs 控制台中执行。有关如何创建指标筛选条件和警报的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用筛选条件从日志事件创建指标和使用亚马逊 CloudWatch 警报。

创建指标筛选条件，并创建警报

要创建警报，您必须首先创建指标筛选条件，然后根据该筛选条件配置警报。会针对所有示例显示这些过程。有关指标筛选器语法和 CloudTrail 日志事件模式的更多信息，请参阅 A mazon Log CloudWatch s 用户指南中筛选和模式语法的 JSON 相关部分。

示例安全组配置更改

按照此过程创建 Amazon CloudWatch 警报，当安全组发生配置更改时触发该警报。

创建指标筛选条件

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，从日志下选择日志组。
3. 在日志组列表中，选择为跟踪创建的日志组。
4. 从指标筛选条件或操作菜单中选择创建指标筛选条件。
5. 在 Define pattern（定义模式）页面上的 Create filter pattern（创建筛选条件模式）中，为 Filter pattern（筛选条件模式）输入以下内容。

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. 在 Test pattern（测试模式）中，保留默认值。选择下一步。
7. 在分配指标页面上，为筛选条件名称输入 **SecurityGroupEvents**。
8. 在指标详细信息中，开启新建，然后在指标命名空间中输入 **CloudTrailMetrics**。
9. 对于指标名称，键入 **SecurityGroupEventCount**。
10. 对于指标值，键入 **1**。
11. 将 Default value（默认值）留空。
12. 选择下一步。
13. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Create metric filter（创建指标筛选条件）以创建筛选条件，或选择 Edit（编辑）返回并更改值。

创建警报

创建指标筛选器后，将打开您的 CloudTrail 跟踪 CloudWatch 日志组的日志日志组详细信息页面。按照此程序创建警报。

1. 在 Metric filters（指标筛选条件）选项卡上，找到您在 the section called “创建指标筛选条件” 中创建的指标筛选条件。填充指标筛选条件的复选框。在 Metric filters（指标筛选条件）栏中，选择 Create alarm（创建警报）。
2. 在指定指标和条件字段中输入以下内容。

a. 对于 Graph（图表），根据您在创建警报时所做的其他设置，该行设置为 **1**。
b. 对于 Metric name（指标名称），请保留当前指标名称 **SecurityGroupEventCount**。
c. 对于 Statistic（统计数据），请保留默认值 **Sum**。
d. 对于 Period（期限），请保留默认值 **5 minutes**。
e. 在 Conditions（条件）中，对于 Threshold type（阈值类型），选择 Static（静态）。
f. 对于 Whenever ***metric_name*** is（每当 metric_name 为），选择 Greater/Equal（大于/等于）。
g. 为阈值输入 **1**。
h. 在 Additional configuration（其他配置）中，保留默认值。选择下一步。

3. 在 “配置操作” 页面上，选择 “通知”，然后选择 “警报”，这表示当超过 5 分钟内 1 个更改事件的阈值并SecurityGroupEventCount处于警报状态时，将采取行动。
   a. 对于向以下 SNS 主题发送通知，选择新建主题。
   b. 输入 **SecurityGroupChanges_CloudWatch_Alarms_Topic** 作为 Amazon SNS 新主题的名称。
   c. 在将接收通知的电子邮件端点中，输入您希望在触发此警报时接收通知的用户的电子邮件地址。用逗号分隔电子邮件地址。

      每位电子邮件收件人会收到电子邮件，要求他们确认他们想要订阅 Amazon SNS 主题。
   d. 选择创建主题。
4. 对于此示例，跳过其他操作类型。选择下一步。
5. 在 Add name and description（添加名称和描述）页面上，输入警报的易识别名称以及描述。在此示例中，请输入 **Security group configuration changes** 作为名称，**Raises alarms if security group configuration changes occur** 作为说明。选择下一步。
6. 在 Preview and create（预览和重建）页面上，审核您的选择。选择 Edit（编辑）以进行更改，或选择 Create alarm（创建警报）以创建警报。

   创建警报后， CloudWatch 打开 “警报” 页面。在有关 SNS 主题的所有电子邮件收件人都确认他们想要订阅 SNS 通知之前，警报的 Actions（操作）列一直显示 Pending confirmation（待确认）。

登录失 AWS Management Console 败示例

按照此过程创建 Amazon CloudWatch 警报，该警报将在五分钟内出现三次或更多 AWS Management Console 登录失败时触发。

创建指标筛选条件

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，从日志下选择日志组。
3. 在日志组列表中，选择为跟踪创建的日志组。
4. 从指标筛选条件或操作菜单中选择创建指标筛选条件。
5. 在 Define pattern（定义模式）页面上的 Create filter pattern（创建筛选条件模式）中，为 Filter pattern（筛选条件模式）输入以下内容。

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. 在 Test pattern（测试模式）中，保留默认值。选择下一步。
7. 在分配指标页面上，为筛选条件名称输入 **ConsoleSignInFailures**。
8. 在指标详细信息中，开启新建，然后在指标命名空间中输入 **CloudTrailMetrics**。
9. 对于指标名称，键入 **ConsoleSigninFailureCount**。
10. 对于指标值，键入 **1**。
11. 将 Default value（默认值）留空。
12. 选择下一步。
13. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Create metric filter（创建指标筛选条件）以创建筛选条件，或选择 Edit（编辑）返回并更改值。

创建警报

创建指标筛选器后，将打开您的 CloudTrail跟踪 CloudWatch 日志组的日志日志组详细信息页面。按照此程序创建警报。

1. 在 Metric filters（指标筛选条件）选项卡上，找到您在 the section called “创建指标筛选条件” 中创建的指标筛选条件。填充指标筛选条件的复选框。在 Metric filters（指标筛选条件）栏中，选择 Create alarm（创建警报）。
2. 在 Create Alarm（创建警报）页面上的 Specify metric and conditions（指定指标和条件）中，输入以下内容：
   a. 对于 Graph（图表），根据您在创建警报时所做的其他设置，该行设置为 **3**。
   b. 对于 Metric name（指标名称），请保留当前指标名称 **ConsoleSigninFailureCount**。
   c. 对于 Statistic（统计数据），请保留默认值 **Sum**。

d. 对于 Period（期限），请保留默认值 **5 minutes**。

e. 在 Conditions（条件）中，对于 Threshold type（阈值类型），选择 Static（静态）。

f. 对于 Whenever ***metric_name*** is（每当 metric_name 为），选择 Greater/Equal（大于/等于）。

g. 为阈值输入 **3**。

h. 在 Additional configuration（其他配置）中，保留默认值。选择下一步。

3. 在配置操作页面上，对于通知，选择警报，这表示当超过 5 分钟内 3 个更改事件的阈值并ConsoleSigninFailureCount处于警报状态时，将采取行动。

a. 对于向以下 SNS 主题发送通知，选择新建主题。

b. 输入 **ConsoleSignInFailures_CloudWatch_Alarms_Topic** 作为 Amazon SNS 新主题的名称。

c. 在将接收通知的电子邮件端点中，输入您希望在触发此警报时接收通知的用户的电子邮件地址。用逗号分隔电子邮件地址。

每位电子邮件收件人会收到电子邮件，要求他们确认他们想要订阅 Amazon SNS 主题。

d. 选择创建主题。

4. 对于此示例，跳过其他操作类型。选择下一步。

5. 在 Add name and description（添加名称和描述）页面上，输入警报的易识别名称以及描述。在此示例中，请输入 **Console sign-in failures** 作为名称，**Raises alarms if more than 3 console sign-in failures occur in 5 minutes** 作为说明。选择下一步。

6. 在 Preview and create（预览和重建）页面上，审核您的选择。选择 Edit（编辑）以进行更改，或选择 Create alarm（创建警报）以创建警报。

创建警报后， CloudWatch 打开 “警报” 页面。在有关 SNS 主题的所有电子邮件收件人都确认他们想要订阅 SNS 通知之前，警报的 Actions（操作）列一直显示 Pending confirmation（待确认）。

示例：IAM policy 更改

按照此过程创建 Amazon CloudWatch 警报，该警报将在调用 API 以更改 IAM 策略时触发。

创建指标筛选条件

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。

2. 在导航窗格中，选择日志。

3. 在日志组列表中，选择为跟踪创建的日志组。
4. 选择 Actions（操作），然后选择 Create metric filter（创建指标筛选条件）。
5. 在 Define pattern（定义模式）页面上的 Create filter pattern（创建筛选条件模式）中，为 Filter pattern（筛选条件模式）输入以下内容。

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. 在 Test pattern（测试模式）中，保留默认值。选择下一步。
7. 在分配指标页面上，为筛选条件名称输入 **IAMPolicyChanges**。
8. 在指标详细信息中，开启新建，然后在指标命名空间中输入 **CloudTrailMetrics**。
9. 对于指标名称，键入 **IAMPolicyEventCount**。
10. 对于指标值，键入 **1**。
11. 将 Default value（默认值）留空。
12. 选择下一步。
13. 在 Review and create（审核和重建）页面上，审核您的选择。选择 Create metric filter（创建指标筛选条件）以创建筛选条件，或选择 Edit（编辑）返回并更改值。

创建警报

创建指标筛选器后，将打开您的 CloudTrail跟踪 CloudWatch 日志组的日志日志组详细信息页面。按照此程序创建警报。

1. 在 Metric filters（指标筛选条件）选项卡上，找到您在 the section called “创建指标筛选条件” 中创建的指标筛选条件。填充指标筛选条件的复选框。在 Metric filters（指标筛选条件）栏中，选择 Create alarm（创建警报）。
2. 在 Create Alarm（创建警报）页面上的 Specify metric and conditions（指定指标和条件）中，输入以下内容：
   a. 对于 Graph（图表），根据您在创建警报时所做的其他设置，该行设置为 **1**。
   b. 对于 Metric name（指标名称），请保留当前指标名称 **IAMPolicyEventCount**。

c. 对于 Statistic（统计数据），请保留默认值 **Sum**。

d. 对于 Period（期限），请保留默认值 **5 minutes**。

e. 在 Conditions（条件）中，对于 Threshold type（阈值类型），选择 Static（静态）。

f. 对于 Whenever ***metric_name*** is（每当 metric_name 为），选择 Greater/Equal（大于/等于）。

g. 为阈值输入 **1**。

h. 在 Additional configuration（其他配置）中，保留默认值。选择下一步。

i.

3. 在配置操作页面上，对于通知，选择警报，这表示当超过 5 分钟内 1 个更改事件的阈值且 IAM PolicyEventCount 处于警报状态时，将采取该操作。

   a. 对于向以下 SNS 主题发送通知，选择新建主题。

   b. 输入 **IAM_Policy_Changes_CloudWatch_Alarms_Topic** 作为 Amazon SNS 新主题的名称。

   c. 在将接收通知的电子邮件端点中，输入您希望在触发此警报时接收通知的用户的电子邮件地址。用逗号分隔电子邮件地址。

      每位电子邮件收件人会收到电子邮件，要求他们确认他们想要订阅 Amazon SNS 主题。

   d. 选择创建主题。

4. 对于此示例，跳过其他操作类型。选择下一步。

5. 在 Add name and description（添加名称和描述）页面上，输入警报的易识别名称以及描述。在此示例中，请输入 **IAM Policy Changes** 作为名称，**Raises alarms if IAM policy changes occur** 作为说明。选择下一步。

6. 在 Preview and create（预览和重建）页面上，审核您的选择。选择 Edit（编辑）以进行更改，或选择 Create alarm（创建警报）以创建警报。

   创建警报后， CloudWatch 打开 “警报” 页面。在有关 SNS 主题的所有电子邮件收件人都确认他们想要订阅 SNS 通知之前，警报的 Actions（操作）列一直显示 Pending confirmation（待确认）。

为 CloudWatch 日志警报配置通知

您可以将 CloudWatch 日志配置为在触发警报时发送通知 CloudTrail。这样，您就可以对事件中捕获并由 CloudWatch 日志检测到的关键操作 CloudTrail事件做出快速响应。 CloudWatch 使用亚马逊简单通知服务 (SNS) Simple Notification Service 发送电子邮件。有关更多信息，请参阅CloudWatch 用户指南中的设置 Amazon SNS 通知。

停止 CloudTrail 向 CloudWatch 日志发送事件

您可以通过更新跟踪以禁用 CloudWatch CloudWatch 日志设置来停止向 Amazon Logs 发送 AWS CloudTrail 事件。

停止向 CloudWatch 日志（控制台）发送事件

停止向 CloudWatch 日志发送 CloudTrail 事件

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择 Trails（跟踪记录）。
3. 选择要禁用 CloudWatch 日志集成的跟踪的名称。
4. 在CloudWatch 日志中，选择编辑。
5. 取消选中启用复选框。
6. 选择保存更改。

停止向 CloudWatch 日志发送事件 (CLI)

您可以通过运行update-trail命令来移除作为传输终端节点的 CloudWatch 日志组。以下命令将日志组 ARN 和日志角色 ARN 的值替换为空值，从而从跟踪配置中清除日志组 CloudWatch 和角色 ARN。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch 的日志组和日志流命名 CloudTrail

Amazon CloudWatch 会将您为 CloudTrail 事件创建的日志组与您在某个区域中的任何其他日志组一起显示。建议您使用可帮助您轻松地将该日志组与其他日志组区分开的日志组名称。例如，**`CloudTrail/logs`**。

命名日志组时请遵循以下准则：

- 日志组名称在 AWS 账户的某个区域内必须是唯一的。
- 日志组名称的长度可介于 1 和 512 个字符之间。
- 日志组名称包含以下字符：a-z、A-Z、0-9、“_”（下划线）、“-”（连字符）、“/”（正斜杠）、“.”（句点）和“#”（井号）。

CloudTrail ######################account_ID _ CloudTrail _ trail_ region#

> **Note**
>
> 如果 CloudTrail 日志量很大，则可能会创建多个日志流来将日志数据传送到您的日志组。*# ############### CloudTrail ########account_ID _ trail _ region CloudTrail _ ###*

有关 CloudWatch 日志组的更多信息，请参阅 Amazon 日志用户指南和 Amazon Lo CloudWatch g s API 参考CreateLogGroup中的使用 CloudWatch 日志组和日志流。

使用 CloudWatch 日志 CloudTrail 进行监控的角色策略文档

本节介绍 CloudTrail 角色向 Log CloudWatch s 发送日志事件所需的权限策略。在配置为发送事件时，可以将策略文档附加 CloudTrail 到角色，如中所述将事件发送到 CloudWatch 日志。您也可以使用 IAM 创建角色。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务或创建 IAM 角色 (AWS CLI)。

以下示例策略文档包含在您指定的日志组中创建 CloudWatch 日志流以及将 CloudTrail 事件传送到美国东部（俄亥俄州）地区的日志流所需的权限。（这是适用于默认 IAM 角色 `CloudTrail_CloudWatchLogs_Role` 的默认策略。）

> **Note**
>
> 防混淆副手不适用于 CloudWatch 日志监控的角色策略。角色策略不支持使用`aws:SourceArn`和`aws:SourceAccount`。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
```

```
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

如果您要创建可能用于组织跟踪记录的策略，则需要根据为该角色创建的默认策略对其进行修改。*### ###### CloudTrail ##### l og_group_nam e ###################### CloudTrail ################ 111111111111 ######## 111111111111 AWS ################ o-exampleorgid #### CloudWatch AWS Organizations*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
```

```
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

有关组织跟踪记录的更多信息，请参阅为组织创建跟踪。

接收来自多个账户的 CloudTrail 日志文件

您可以让 AWS 账户 将多个日志文件 CloudTrail 传输到单个 Amazon S3 存储桶中。例如，您有四个 AWS 账户 账户 ID 为 111111111111、222222222222、333333333333 和 444444444444，并且您想要配置为将所有四个账户中的日志文件传输到属于账户 111111111111 的存储桶。 CloudTrail 要完成此操作，请依次完成以下步骤：

1. 在目标存储桶所属的账户（此示例中为 111111111111）中创建跟踪。不要为任何其他账户创建跟踪。

   有关说明，请参阅在控制台中创建跟踪。
2. 更新目标存储桶的存储桶政策，向其授予跨账户权限。 CloudTrail

   有关说明，请参阅设置适用于多个账户的存储桶策略。
3. 在要为其记录活动的其他账户（此示例中为 222222222222、333333333333 和 444444444444）中创建跟踪。在每个账户中创建跟踪时，指定属于您在步骤 1 中指定的账户（此示例中为 111111111111）的 Amazon S3 存储桶。有关说明，请参阅在其他账户中创建跟踪。

> **Note**
>
> 如果您选择启用 SSE-KMS 加密，KMS 密钥策略必须 CloudTrail 允许使用该密钥加密您的日志文件，并允许您指定的用户读取未加密形式的日志文件。有关手动编辑密钥政策的信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

为其他账户调用的数据事件修订存储桶拥有者账户 ID

过去，如果在 Amazon S3 CloudTrail 数据事件 API 调用者中启用了数据事件，则会在数据事件中 CloudTrail 显示 S3 存储桶拥有者的账户 ID（例如PutObject）。 AWS 账户 即使存储桶拥有者账户没有启用 S3 数据事件，也会出现这种情况。

现在，如果满足以下两个条件，则 CloudTrail 删除resources区块中 S3 存储桶所有者的账户 ID：

- 数据事件 API 调用来自不同 AWS 账户 于 Amazon S3 存储桶拥有者的人。
- API 调用程序收到了一个仅适用于该调用程序账户的 AccessDenied 错误。

在其上面进行 API 调用的资源的拥有者仍收到完整的事件。

以下事件记录片段是一个预期行为的示例。在 Historic 片段中，将向不同账户中的 API 调用程序显示 S3 存储桶拥有者的账户 ID 123456789012。在当前行为示例中，不会显示存储桶拥有者的账户 ID。

```
# Historic

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

以下是当前的行为。

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
```

```
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

主题

- 设置适用于多个账户的存储桶策略
- 在其他账户中创建跟踪

设置适用于多个账户的存储桶策略

要使存储桶接收来自多个账户的日志文件，其存储桶策略必须授予从您指定的所有账户写入日志文件的 CloudTrail 权限。这意味着您必须修改目标存储桶的存储桶策略，以授予从每个指定账户写入日志文件的 CloudTrail 权限。

> **Note**
>
> 出于安全原因，未经授权的用户无法创建包含 `AWSLogs/` 作为 `S3KeyPrefix` 参数的跟踪记录。

修改存储桶权限，以便可以从多个账户接收这些文件

1. AWS Management Console 使用拥有存储桶的账户（在本示例中为 111111111111）登录，然后打开 Amazon S3 控制台。
2. 选择用于 CloudTrail 传送日志文件的存储桶，然后选择权限。
3. 在 Bucket policy（存储桶策略）下，选择 Edit（编辑）。
4. 修改现有策略以便为要将其日志文件传输到此存储桶的每个额外账户添加一个行。参阅以下示例策略并记下指定另一个账户 ID 的带下划线的 `Resource` 行。作为安全最佳实践，请将 `aws:SourceArn` 条件密钥添加到 Simple Storage Service（Amazon S3）存储桶策略。这有助于防止未经授权访问您的 S3 存储桶。如果您有现有跟踪记录，请务必添加一个或多个条件密钥。

   > **Note**
   >
   > AWS 账户 ID 是一个十二位数字，包括前导零。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
              "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
            ]
          }
       }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ],
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
```

```
}
```

在其他账户中创建跟踪

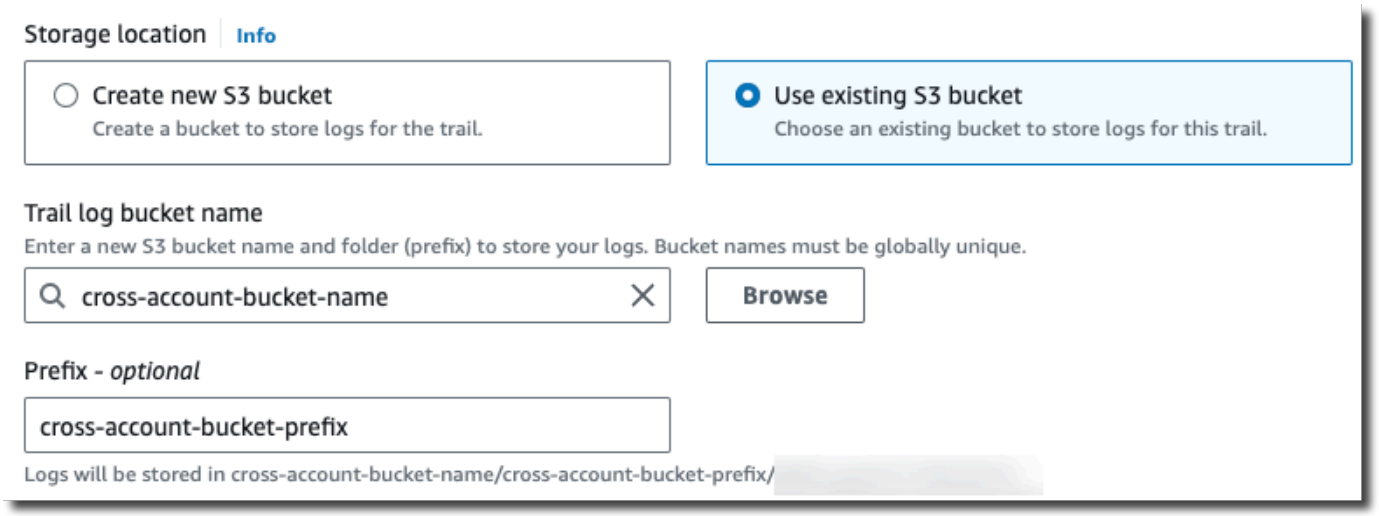
您可以使用控制台或创建其他跟踪 AWS 账户 并将其日志文件聚合 AWS CLI 到一个 Amazon S3 存储桶中。或者，您可以创建组织跟踪以记录 AWS 账户 属于组织的所有成员 AWS Organizations。有关更多信息，请参阅 为组织创建跟踪。

使用控制台在其他 AWS 账户中创建跟踪

您可以使用 CloudTrail 控制台在其他账户中创建跟踪。

1. AWS Management Console 使用您要为其创建跟踪的账户登录。按照 在控制台中创建跟踪 中的步骤，使用控制台创建跟踪。
2. 对于 Storage location（存储位置），选择 Use existing S3 bucket（使用现有 S3 存储桶）。使用文本框输入您用于跨账户存储日志文件的存储桶的名称。

> **Note**
>
> 存储桶策略必须授予对其进行写入的 CloudTrail 权限。有关手动编辑存储桶策略的信息，请参阅设置适用于多个账户的存储桶策略。



3. 在前缀中，输入您用于跨账户存储日志文件的前缀。如果您选择使用与您在存储桶策略中指定的前缀不同的前缀，则必须编辑目标存储桶的存储桶策略， CloudTrail 以允许使用此新前缀将日志文件写入存储桶。

使用 CLI 在其他 AWS 账户中创建跟踪

您可以使用 AWS 命令行工具在其他账户中创建跟踪，并将其日志文件聚合到一个 Amazon S3 存储桶中。有关这些工具的更多信息，请参阅《AWS CLI 命令参考》中的 cloudtrail。

使用 create-trail 命令创建跟踪，并指定以下内容：

- `--name` 指定跟踪的名称。
- `--s3-bucket-name` 指定您用于跨账户存储日志文件的 Amazon S3 存储桶。
- `--s3-prefix` 指定日志文件传输路径的前缀（可选）。
- `--is-multi-region-trail`指定此跟踪将记录您所在分区中所有 AWS 区域的事件。

您可以为账户运行 AWS 资源的每个区域创建一个跟踪。

以下示例命令说明如何使用 AWS CLI为您的附加账户创建跟踪。要将这些账户的日志文件传送到您在第一个账户（此示例中为 111111111111）中创建的存储桶，请在 `--s3-bucket-name` 选项中指定存储桶名称。Simple Storage Service（Amazon S3）存储桶名称具有全局唯一性。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail
```

当您运行该命令时，将显示与以下内容类似的输出：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

有关使用 AWS 命令行工具 CloudTrail 的更多信息，请参阅CloudTrail 命令行参考。

在 AWS 账户之间共享 CloudTrail 日志文件

本节介绍如何在多个 AWS 账户之间共享 CloudTrail 日志文件。您用于在两者之间共享日志的方法 AWS 账户 取决于您的 S3 存储桶的配置。下面是是共享日志文件的选项：

- 强制存储桶拥有者 – S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权并禁用或启用访问控制列表（ACL）。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对数据的访问权限。设置强制存储桶拥有者选项后，访问权限将通过存储桶策略进行管理，用户无需代入角色。
- 代入角色以共享日志文件 – 如果您尚未选择强制存储桶拥有者设置，则用户需要代入角色才能访问您的 S3 存储桶中的日志文件。

通过代入角色在账户之间共享日志文件

> **Note**
>
> 本部分仅适用于未使用强制存储桶拥有者设置的 Amazon S3 存储桶。

本节介绍如何 AWS 账户 通过扮演角色在多个 CloudTrail 日志文件之间共享日志文件，并描述共享日志文件的场景。

- 方案 1：向生成了已放置到 Amazon S3 存储桶中的日志文件的账户授予只读访问权。
- 方案 2：向可以为您分析日志文件的第三方账户授予访问您的 Amazon S3 存储桶中的所有日志文件的权限。

要授予对 Amazon S3 存储桶中的日志文件的只读访问权

1. 为您要与之共享日志文件的每个账户创建一个 IAM 角色。您必须是管理员才能授予权限。

   创建角色时，请执行以下操作:

   - 选择其他 AWS 账户 选项。
   - 输入要授予访问权的账户的 12 位数账户 ID。
   - 如果您希望用户在代入角色之前提供多重验证，请选中 Require MFA 框。
   - 选择 AmazonS3 ReadOnlyAccess 政策。

> **Note**
>
> 默认情况下，AmazonS3 ReadOnlyAccess 政策授予您账户中所有 Amazon S3 存储桶的检索和列出权限。

有关 IAM 角色的权限管理的详细信息，请参阅 IAM 用户指南中的 IAM 角色。

2. 创建一个访问策略，该策略向要与之共享日志文件的账户授予只读访问权。
3. 指示每个账户代入一个角色来检索日志文件。

要使用第三方账户授予对日志文件的只读访问权

1. 为您要与之共享日志文件的第三方账户创建一个 IAM 角色。您必须是管理员才能授予权限。

   创建角色时，请执行以下操作:

   - 选择其他 AWS 账户 选项。
   - 输入要授予访问权的账户的 12 位数账户 ID。
   - 输入外部 ID 以便额外控制可代入角色的用户。有关更多信息，请参阅 IAM 用户指南中的如何在向第三方授予对您的 AWS 资源的访问权限时使用外部 ID。
   - 选择 AmazonS3 ReadOnlyAccess 政策。

   > **Note**
   >
   > 默认情况下，AmazonS3 ReadOnlyAccess 政策授予您账户中所有 Amazon S3 存储桶的检索和列出权限。

2. 创建一个访问策略，该策略向要与之共享日志文件的第三方账户授予只读访问权。
3. 指示第三方账户代入一个角色来检索日志文件。

以下部分介绍了有关这些步骤的更多详细信息。

主题

- 创建用于向自己的账户授予访问权限的访问策略
- 创建用于向第三方授予访问权限的访问策略

- 代入角色
- 停止在 AWS 账户之间共享 CloudTrail 日志文件

创建用于向自己的账户授予访问权限的访问策略

作为 Amazon S3 存储桶的所有者，您可以完全控制向其 CloudTrail 写入其他账户日志文件的 Amazon S3 存储桶。您想将每个业务部门的日志文件共享回创建它们的业务部门。但您不希望部门能够读取任何其他部门的日志文件。

例如，要与账户 B 而非账户 C 共享账户 B 的日志文件，您必须在您的账户中创建一个新的 IAM 角色，指定账户 B 是受信任的账户。此角色信任策略指定可信任账户 B 来代入由您的账户创建的角色，与以下示例类似。如果使用控制台创建角色，则将自动创建信任策略。如果您使用 SDK 创建角色，则必须将信任策略作为参数提供给 `CreateRole` API。如果您使用 CLI 创建角色，则必须在 `create-role` CLI 命令中指定信任策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

您还必须创建访问策略来指定账户 B 只能从账户 B 将其日志文件写入到的位置进行读取。访问策略将类似于以下内容。请注意，资源 ARN 包括账户 B 的十二位数账户 ID，以及您在聚合过程中为账户 B 开启时指定的前缀（如果有）。 CloudTrail 有关指定前缀的更多信息，请参阅在其他账户中创建跟踪。

> **Important**
>
> 您必须确保访问策略中的前缀与您在账户 B 开启时指定的前缀完全相同。如果不是，则必须编辑账户中的 IAM 角色访问策略以包含账户 B 的实际前缀。如果角色访问策略中的前缀与

您在账户 B CloudTrail 中开启时指定的前缀不完全相同，则账户 B 将无法访问其日志文件。CloudTrail

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

对任何其他账户使用上述过程。

在创建每个用户的角色并指定相应的信任和访问策略后，以及在每个账户的管理员向该账户中的 IAM 用户授予访问权后，账户 B 或账户 C 中的 IAM 用户可以编程方式代入角色。

有关更多信息，请参阅 代入角色。

创建用于向第三方授予访问权限的访问策略

您必须为第三方账户创建单独的 IAM 角色。在创建角色时， AWS 会自动创建信任关系，以指定将信任第三方账户来代入角色。此角色的访问策略指定了该账户可执行的操作。有关创建角色的更多信息，请参阅创建 IAM 角色。

例如，由创建的信任关系 AWS 指定第三方账户（本例中为账户 Z）受信任来担任您创建的角色。以下是信任策略的示例：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole"
    }]
}
```

如果您在为第三方账户创建角色时指定了外部 ID，则您的访问策略将包含一个添加的 Condition 元素，该元素将测试由该账户分配的唯一 ID。此测试在代入角色时执行。以下示例访问策略包含 Condition 元素。

有关更多信息，请参阅 IAM 用户指南中的如何在向第三方授予 AWS 资源访问权限时使用外部 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-
account-Z"}}
    }]
}
```

您还必须为您的账户创建访问策略来指定第三方账户可读取 Amazon S3 存储桶中的所有日志。访问策略应类似于以下示例。Resource 值结尾处的通配符（*）表示第三方账户可访问已获得相应访问权的 S3 存储桶中的任何日志文件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

在为第三方账户创建角色并指定相应的信任关系和访问策略后，第三方账户中的 IAM 用户必须以编程方式代入角色才能读取存储桶中的日志文件。有关更多信息，请参阅 代入角色。

代入角色

您必须指定一个单独的 IAM 用户来代入自己在每个账户中创建的各个角色，还必须确保每个 IAM 用户都拥有相应权限。

IAM 用户和角色

在创建必要的角色和策略后，您必须在要与之共享文件的每个账户中指定一个 IAM 用户。每个 IAM 用户均以编程方式代入相应的角色以访问日志文件。当用户代入角色时， AWS 会向该用户返回临时安全凭证。此类凭证可用于发出列出、检索、复制或删除日志文件的请求，具体取决于与角色关联的访问策略所授予的权限。

有关使用 IAM 身份的更多信息，请参阅 IAM 身份（用户、组和角色）。

主要区别在于，您在每个方案中为每个 IAM 角色创建的访问策略。

- 在方案 1 中，访问策略只允许每个账户读取其自己的日志文件。有关更多信息，请参阅 创建用于向自己的账户授予访问权限的访问策略。
- 在方案 2 中，访问策略允许第三方账户读取已聚合到 Amazon S3 存储桶中的所有日志文件。有关更多信息，请参阅 创建用于向第三方授予访问权限的访问策略。

为 IAM 用户创建权限策略

要执行角色允许的操作，IAM 用户必须拥有调用 AWS STS AssumeRoleAPI 的权限。您必须编辑每个用户的策略，以授予他们相应的权限。也就是说，在附加到 IAM 用户的策略中设置资源元素。以下示例演示了另一个账户中的 IAM 用户的策略，此策略允许该用户代入账户 A 之前创建的一个名为 Test 的角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

编辑客户托管策略（控制台）

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 在策略列表中，选择要编辑的策略的名称。您可以使用搜索框筛选策略列表。
4. 选择权限选项卡，然后选择编辑。
5. 请执行以下操作之一：

   - 选择可视化选项以更改您的策略，而无需了解 JSON 语法。您可以更改策略中的每个权限块的服务、操作、资源或可选条件。也可以导入一个策略以在您的策略底部添加其他权限。完成更改后，选择下一步以继续。
   - 选择 JSON 选项，然后在 JSON 文本框中键入或粘贴文本以修改您的策略。也可以导入一个策略以在您的策略底部添加其他权限。解决策略验证过程中生成的任何安全警告、错误或常规警告，然后选择下一步。

> **Note**
>
> 您可以随时在可视化和 JSON 编辑器选项卡之间切换。不过，如果您进行更改或在可视化编辑器中选择下一步，IAM 可能会调整策略结构以针对可视化编辑器进行优化。有关更多信息，请参阅《IAM 用户指南》中的调整策略结构。

6. 在查看并保存页面上，查看此策略中定义的权限，然后选择保存更改以保存您的工作。
7. 如果管理型策略已达到最大版本数（5 个），选择保存更改将显示对话框。要保存您的新版本，策略最旧的非默认版本将被移除并替换为该新版本。（可选）您也可以将新版本设置为策略的默认版本。

   选择保存更改以保存您的新策略版本。

正在呼叫 AssumeRole

用户可以通过创建一个应用程序来代入角色，该应用程序调用 AWS STS `AssumeRole`API 并传递角色会话名称、要代入的角色的 Amazon 资源编号 (ARN) 以及可选的外部 ID。创建要代入的角色的账户将定义角色会话名称。外部 ID（如果有）由第三方账户定义，并且将传递给拥有账户以便在创建角色时将此 ID 包含在内。有关更多信息，请参阅 IAM 用户指南中的如何在向第三方授予对您的 AWS 资源的访问权限时使用外部 ID。您可以通过打开 IAM 控制台从账户 A 检索 ARN。

使用 IAM 控制台在账户 A 中查找 ARN 值

1. 选择 Roles
2. 选择要检查的角色。
3. 在摘要部分中查找角色 ARN。

AssumeRole API 会返回临时证书，用于访问拥有账户的资源。在此示例中，您要访问的资源是 Amazon S3 存储桶以及该存储桶所包含的日志文件。该临时证书拥有您在角色访问策略中定义的权限。

以下 Python 示例（使用 AWS SDK for Python (Boto)）将说明如何调用 `AssumeRole` 以及如何使用返回的临时安全证书来列出由账户 A 控制的所有 Simple Storage Service（Amazon S3）存储桶。

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
```

```
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

停止在 AWS 账户之间共享 CloudTrail 日志文件

要停止与他人共享日志文件 AWS 账户，请删除您为该账户创建的角色。有关如何删除角色的信息，请参阅删除角色或实例配置文件。

验证 CloudTrail 日志文件完整性

要确定日志文件在 CloudTrail 传送后是被修改、删除还是未更改，可以使用 CloudTrail 日志文件完整性验证。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。您可以使用 AWS CLI 在文件 CloudTrail 交付地点验证文件。

为什么使用它？

在安全和事故调查中，经验证的日志文件非常重要。例如，通过经验证的日志文件，您可以十分确定日志文件本身未更改，或者特定用户凭证执行了特定 API 活动。 CloudTrail 日志文件完整性验证过程还可以让您知道日志文件是否已被删除或更改，或者肯定地断言在给定时间段内没有向您的账户发送任何日志文件。

工作方式

启用日志文件完整性验证后， CloudTrail 会为其提供的每个日志文件创建一个哈希值。每隔一小时，CloudTrail 还会创建并传送一个文件，该文件引用了过去一小时的日志文件，并包含每个文件的哈希值。此文件称为摘要文件。 CloudTrail 使用公钥和私钥对的私钥签署每个摘要文件。交付后，您可以使用公钥来验证摘要文件。 CloudTrail 对每个密钥对使用不同的密钥对 AWS 区域。

摘要文件将与您的 CloudTrail 日志文件传输到与您的跟踪关联的 Amazon S3 存储桶。如果您的日志文件从所有区域或多个账户传输到单个 Amazon S3 存储桶，则 CloudTrail 会将来自这些区域和账户的摘要文件传送到同一个存储桶中。

摘要文件放在与日志文件不同的文件夹中。摘要文件与日志文件分开放置，您就可以执行细粒度安全策略，允许现有日志处理解决方案继续运行，无需进行修改。每个摘要文件还包含之前摘要文件（如果存在）的数字签名。当前摘要文件的签名位于摘要文件 Simple Storage Service（Amazon S3）对象的元数据属性中。有关摘要文件内容的更多信息，请参阅CloudTrail 摘要文件结构。

存储日志文件和摘要文件

您可以安全、耐用、廉价地将 CloudTrail 日志文件和摘要文件无限期地存储在 Amazon S3 或 S3 Glacier 中。为增强存储在 Simple Storage Service（Amazon S3）中的摘要文件的安全性，您可以使用 Simple Storage Service（Amazon S3）MFA 删除。

启用验证并验证文件

要启用日志文件完整性验证，可以使用 AWS Management Console AWS CLI、或 CloudTrail API。启用日志文件完整性验证允许 CloudTrail 将摘要日志文件传输到您的 Amazon S3 存储桶，但不能验证文件的完整性。有关更多信息，请参阅 为启用日志文件完整性验证 CloudTrail。

要验证 CloudTrail 日志文件的完整性，您可以使用 AWS CLI 或创建自己的解决方案。 AWS CLI 将在文件 CloudTrail 交付地点对文件进行验证。如果您要验证已移到其他位置（Simple Storage Service（Amazon S3）或别处）的日志，您可以创建自己的验证工具。

有关使用验证日志的信息 AWS CLI，请参阅 CloudTrail 使用验证日志文件的完整性 AWS CLI。有关开发 CloudTrail 日志文件验证的自定义实现的信息，请参阅 CloudTrail 日志文件完整性验证的自定义实现。

为启用日志文件完整性验证 CloudTrail

您可以使用 AWS Management Console、 AWS 命令行界面 (AWS CLI) 或 CloudTrail API 启用日志文件完整性验证。 CloudTrail 大约一小时后开始交付摘要文件。

AWS Management Console

要使用 CloudTrail 控制台启用日志文件完整性验证，请在创建或更新跟踪时为 “启用日志文件验证” 选项选择 “是”。默认情况下会对新的跟踪记录启用此功能。有关更多信息，请参阅 使用控制台创建和更新跟踪。

AWS CLI

要使用启用日志文件完整性验证 AWS CLI，请将`--enable-log-file-validation`选项与 create-t rail 或 up date-trail 命令一起使用。要禁用日志文件完整性验证，请使用 `--no-enable-log-file-validation` 选项。

示例

下面的 `update-trail` 命令启用日志文件验证并开始将摘要文件传送到指定跟踪的 Simple Storage Service（Amazon S3）存储桶中。

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

要使用 CloudTrail API 启用日志文件完整性验证，请在调用`CreateTrail`或`true`时将`EnableLogFileValidation`请求参数设置为`UpdateTrail`。

有关更多信息，请参阅 AWS CloudTrail API 参考`UpdateTrail`中的`CreateTrail`和。

CloudTrail 使用验证日志文件的完整性 AWS CLI

要使用验证日志 AWS Command Line Interface，请使用 CloudTrail `validate-logs`命令。此命令使用提交到 Simple Storage Service（Amazon S3）存储桶的摘要文件执行验证。有关摘要文件的信息，请参阅 CloudTrail 摘要文件结构。

AWS CLI 允许您检测以下类型的更改：

- 修改或删除 CloudTrail 日志文件
- 修改或删除 CloudTrail 摘要文件
- 上述两者的修改或删除

> **Note**
>
> 仅 AWS CLI 验证摘要文件引用的日志文件。有关更多信息，请参阅 检查特定文件是否由传送 CloudTrail。

先决条件

要使用验证日志文件的完整性 AWS CLI，必须满足以下条件：

- 您必须联机连接到 AWS。
- 您必须拥有包含摘要文件和日志文件的 Simple Storage Service（Amazon S3）存储桶的读取访问权限。
- 摘要和日志文件不得从 CloudTrail 交付它们的原始 Amazon S3 位置移出。

> **Note**
>
> AWS CLI无法验证下载到本地磁盘的日志文件。有关自行创建验证工具的指南，请参阅 CloudTrail 日志文件完整性验证的自定义实现。

validate-logs

语法

validate-logs 采用下面的语法形式。括号内为可选参数。

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> validate-logs 命令与特定区域相关。必须指定--region全局选项才能验证特定日志的日志 AWS 区域。

Options

validate-logs 提供以下命令行选项。--trail-arn 和 --start-time 为必需选项。组织跟踪还需要 --account-id 选项。

--start-time

指定将验证在指定 UTC 时间戳值当时或之后提交的日志文件。示例：2015-01-08T05:21:42Z。

--end-time

（可选）指定将验证在指定 UTC 时间戳值当时或之前提交的日志文件。默认值为当前 UTC 时间 (Date.now())。示例：2015-01-08T12:31:41Z。

> **Note**
>
> 对于指定的时间范围，validate-logs 命令只检查其对应的摘要文件引用的日志文件。不检查 Simple Storage Service（Amazon S3）存储桶中的任何其他日志文件。有关更多信息，请参阅 检查特定文件是否由传送 CloudTrail。

--s3-bucket

（可选）指定存储摘要文件的 Simple Storage Service（Amazon S3）存储桶。如果未指定存储桶名称，则 AWS CLI 将通过调用来检索存储桶名称DescribeTrails()。

--s3-prefix

（可选）指定表示摘要文件存储位置的 Simple Storage Service（Amazon S3）前缀。如果未指定，则 AWS CLI 将通过调用来检索它DescribeTrails()。

> **Note**
>
> 仅在当前前缀不同于指定时间范围期间使用的前缀时，才应使用此选项。

--account-id

也可选择指定用于验证日志的账户。组织跟踪需要此参数来验证组织内特定账户的日志。

--trail-arn

指定要验证的跟踪的 Amazon Resource Name（ARN）。跟踪 ARN 遵循的格式。

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> 要获取跟踪的 ARN，您可以先使用 describe-trails 命令，然后再运行 validate-logs。
> 如果在您指定的时间范围内日志文件被提交到多个存储桶，而您需要将对日志文件的验证限制在一个存储桶，则除了跟踪 ARN，您可能还需要指定存储桶的名称和前缀。

`--verbose`

（可选）输出指定时间范围内的每个日志文件或摘要文件的验证信息。输出指示文件保持不变还是发生过修改或已删除。在非详细模式（默认）下，仅当验证失败时才返回信息。

示例

下面的示例验证从指定起始时间到当前时间的日志文件，使用为当前跟踪配置的 Simple Storage Service（Amazon S3）存储桶并指定详细输出。

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

validate-logs 的工作原理

`validate-logs` 命令从验证指定时间范围内最新的摘要文件开始。首先，它验证摘要文件是否已从其声明的所属位置下载。换句话说，如果 CLI 从 S3 位置 `p1` 下载摘要文件 `df1`，则 validate-logs 会验证 `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`。

如果摘要文件的签名有效，则它检查摘要文件中引用的每个日志的哈希值。之后，此命令按时间倒序连续验证之前的摘要文件及其引用的日志文件。它继续进行这一操作，直到到达指定的 `start-time` 值或摘要链结束为止。如果有摘要文件缺失或无效，则此命令在输出中指出无法验证的时间范围。

验证结果

验证结果从摘要头开始，采用以下格式：

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

主输出的每行包含单个摘要文件或日志文件的验证结果，格式如下：

```
<Digest file | Log file> <S3 path> <Validation Message>
```

下表描述了可能会出现的日志文件和摘要文件的验证消息。

文件类型	验证消息	描述
Digest file	valid	摘要文件签名有效。可以检查所引用的日志文件。仅详细模式包含此消息。

文件类型	验证消息	描述
Digest file	INVALID: has been moved from its original location	检索摘要文件的 S3 存储桶或 S3 对象与摘要文件中记录的 S3 存储桶或 S3 对象位置不匹配。
Digest file	INVALID: invalid format	摘要文件格式无效。无法验证与摘要文件表示的时间范围对应的日志文件。
Digest file	INVALID: not found	找不到摘要文件。无法验证与摘要文件表示的时间范围对应的日志文件。
Digest file	INVALID: public key not found for fingerprint ##	找不到与摘要文件中记录的指纹对应的公有密钥。无法验证摘要文件。
Digest file	INVALID: signature verification failed	摘要文件签名无效。摘要文件无效，无法验证其引用的日志文件，也无法确定其中所列的 API 活动。
Digest file	INVALID: Unable to load PKCS #1 key with fingerprint ##	无法加载含有指定指纹的 DER 编码公有密钥（PKCS #1 格式），无法验证摘要文件。
Log file	valid	日志文件已验证且自提交以来未发生过修改。仅详细模式包含此消息。
Log file	INVALID: hash value doesn't match	日志文件的哈希值不匹配。日志文件在传送后已被修改 CloudTrail。
Log file	INVALID: invalid format	日志文件格式无效。无法验证日志文件。
Log file	INVALID: not found	找不到日志文件，无法验证。

输出包含有关返回结果的摘要信息。

示例输出

详细

下面的示例 validate-logs 命令使用 --verbose 标志并生成后面的示例输出。[...] 表示示例输出已省略。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid
```

```
Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

非详细

下面的示例 validate-logs 命令不使用 --verbose 标志。在后面的示例输出中，出现一个错误。只返回了头、错误和摘要信息。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

检查特定文件是否由传送 CloudTrail

要检查存储桶中的特定文件是否由传送 CloudTrail，请在包含该文件的时间段内以详细模式运行validate-logs。如果文件出现在的输出中validate-logs，则该文件由传送 CloudTrail。

CloudTrail 摘要文件结构

每个摘要文件均包含前一小时提交到您的 Simple Storage Service（Amazon S3）存储桶的日志文件的名称，这些日志文件的哈希值，以及前一日志文件的数字签名。最新摘要文件的签名存储在摘要文件对象的元数据属性中。数字签名和哈希值用于验证日志文件和摘要文件本身的完整性。

摘要文件位置

摘要文件提交到 Simple Storage Service（Amazon S3）存储桶位置，语法如下。

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> 对于组织跟踪记录，存储桶位置还包括组织单位 ID，如下所示：
>
> ```
> s3://s3-bucket-name/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

示例摘要文件内容

以下示例摘要文件包含 CloudTrail 日志信息。

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
```

```
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```

摘要文件字段描述

下面是摘要文件中每个字段的描述：

`awsAccountId`

已为其发送摘要文件的 AWS 账户 ID。

`digestStartTime`

摘要文件所涵盖的起始 UTC 时间范围，以日志文件交付的时间为参考。 CloudTrail这意味着，如果时间范围是 [Ta, Tb]，则摘要包含在 Ta 与 Tb 之间提交给客户的所有日志文件。

`digestEndTime`

摘要文件所涵盖的 UTC 结束时间范围，以日志文件交付的时间为参考。 CloudTrail这意味着，如果时间范围是 [Ta, Tb]，则摘要包含在 Ta 与 Tb 之间提交给客户的所有日志文件。

`digestS3Bucket`

已将最新摘要文件传送到的 Simple Storage Service（Amazon S3）存储桶的名称。

`digestS3Object`

最新摘要文件的 Simple Storage Service（Amazon S3）对象密钥（即，Simple Storage Service（Amazon S3）存储桶位置）。字符串中的前两个区域显示摘要文件是从哪个区域提交的。

最后的区域（your-trail-name 之后）是跟踪的主区域。主区域是创建跟踪的区域。如果是多区域跟踪，主区域可能不是提交摘要文件的区域。

`newestEventTime`

摘要的日志文件中的所有事件中最近事件的 UTC 时间。

`oldestEventTime`

摘要的日志文件中的所有事件中最早事件的 UTC 时间。

> **Note**
>
> 如果摘要文件延迟提交，则 `oldestEventTime` 的值将早于 `digestStartTime` 的值。

`previousDigestS3Bucket`

上一个摘要文件传送到的 Simple Storage Service（Amazon S3）存储桶。

`previousDigestS3Object`

上一个摘要文件的 Simple Storage Service（Amazon S3）对象密钥（即，Simple Storage Service（Amazon S3）存储桶位置）。

`previousDigestHashValue`

前一摘要文件的未压缩内容的十六进制编码哈希值。

`previousDigestHashAlgorithm`

用于对前一摘要文件进行哈希处理的哈希算法的名称。

`publicKeyFingerprint`

与用于对摘要文件进行签名的私有密钥相匹配的公有密钥的十六进制编码指纹。您可以使用 AWS CLI 或 CloudTrail API 检索与摘要文件对应的时间范围内的公钥。对于返回的公有密钥，其指纹

与此值匹配的公有密钥可用于验证摘要文件。有关检索摘要文件公钥的信息，请参阅 AWS CLI `list-public-keys`命令或 CloudTrail `ListPublicKeys`API。

> **Note**
>
> CloudTrail 每个区域使用不同的私钥/公钥对。每个摘要文件都使用对其区域唯一的私钥进行签名。因此，当您验证来自特定区域的摘要文件时，必须从同一区域检索其相应公钥。

`digestSignatureAlgorithm`

用于对摘要文件进行签名的算法。

`logFiles.s3Bucket`

日志文件的 Simple Storage Service（Amazon S3）存储桶的名称。

`logFiles.s3Object`

最新日志文件的 Simple Storage Service（Amazon S3）对象密钥。

`logFiles.newestEventTime`

日志文件中最近事件的 UTC 时间。此时间还与日志文件本身的时间戳相对应。

`logFiles.oldestEventTime`

日志文件中最早事件的 UTC 时间。

`logFiles.hashValue`

未压缩日志文件内容的十六进制编码哈希值。

`logFiles.hashAlgorithm`

用于对日志文件进行哈希处理的哈希算法。

启动摘要文件

启动日志文件完整性验证时，将生成一个启动摘要文件。重新启动日志文件完整性验证（通过禁用后重新启用日志文件完整性验证，或者通过停止记录然后在启用验证时重新启动记录）时，也将生成一个启动摘要文件。在启动摘要文件中，与前一摘要文件相关的以下字段将为空：

- previousDigestS3Bucket
- previousDigestS3Object
- previousDigestHashValue
- previousDigestHashAlgorithm
- previousDigestSignature

“空”摘要文件

CloudTrail 即使在摘要文件所代表的一小时内您的账户中没有 API 活动，也会提供摘要文件。如果需要确定在摘要文件报告的小时内未提交日志文件，这非常有用。

下面的示例说明当未出现 API 活动时记录了 1 小时的摘要文件的内容。注意，摘要文件内容最后的 logFiles:[ ] 字段为空。

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
```

```
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```

摘要文件的签名

摘要文件的签名信息位于 Simple Storage Service（Amazon S3）摘要文件对象的两个对象元数据属性中。每个摘要文件都有下面的元数据项：

- `x-amz-meta-signature`

  摘要文件签名的十六进制编码值。下面是示例签名：

  ```
  3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
  28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
  05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
  ```

- `x-amz-meta-signature-algorithm`

  下面是用于生成摘要签名的算法示例值：

  `SHA256withRSA`

摘要文件链

每个摘要文件都包含对其先前摘要文件的引用，这一事实实现了“链接”，允许诸如之类的 AWS CLI 验证工具检测摘要文件是否已被删除。通过它，在指定时间范围内的摘要文件可以从最近开始往前连续检查。

> **Note**
>
> 禁用日志文件完整性验证后，摘要文件链将在一小时后中断。 CloudTrail 不会为在禁用日志文件完整性验证期间传送的日志文件创建摘要文件。例如，如果您在 1 月 1 日中午启用日志文件完整性验证，在 1 月 2 日中午禁用它，在 1 月 10 日中午再次启用它，则不会为从 1 月 2 日中午到 1 月 10 日中午之间提交的日志文件创建摘要文件。每当您停止 CloudTrail 记录或删除跟踪时，这同样适用。

如果您的跟踪的 S3 存储桶策略配置错误或服务 CloudTrail 出现意外中断，则可能无法收到全部或部分摘要文件。要确认您的跟踪是否有任何摘要传送错误，请运行get-trail-status命令并检查LatestDigestDeliveryError参数是否有错误。在交付问题得到解决（例如，通过修复存储桶策略）后， CloudTrail 将尝试重新传送任何丢失的摘要文件。在重新交付期间，摘要文件可能会乱序交付，因此链条可能会暂时显得中断。

如果日志记录停止或跟踪被删除， CloudTrail 将提供最终的摘要文件。此摘要文件包含有关所有剩余日志文件的信息，所涵盖的事件直至（包含）StopLogging 事件。

CloudTrail 日志文件完整性验证的自定义实现

由于 CloudTrail 使用行业标准、公开可用的加密算法和哈希函数，因此您可以创建自己的工具来验证 CloudTrail 日志文件的完整性。启用日志文件完整性验证后，会将摘要文件 CloudTrail 传送到您的 Amazon S3 存储桶。您可以使用这些文件实现自己的验证解决方案。有关摘要文件的更多信息，请参阅CloudTrail 摘要文件结构。

本主题介绍如何为摘要文件签名，然后详述了要对摘要文件及其引用的日志文件实现验证解决方案所需采取的步骤。

了解 CloudTrail 摘要文件的签名方式

CloudTrail 摘要文件使用 RSA 数字签名进行签名。对于每个摘要文件，执行以下 CloudTrail操作：

1. 创建一个字符串，以基于指定的摘要文件字段进行数据签名（在下一章节中讲解）。
2. 获取区域唯一的私钥。
3. 将此字符串的 SHA-256 哈希值和私钥传递给 RSA 签名算法（生成数字签名）。
4. 将签名的字节代码编码成十六进制格式。
5. 将此数字签名放入 Simple Storage Service（Amazon S3）摘要文件对象的 x-amz-meta-signature 元数据属性中。

数据签名字符串的内容

用于数据签名的字符串中包含以下 CloudTrail 对象：

- UTC 扩展格式的摘要文件结束时间戳（如 2015-05-08T07:19:37Z）
- 当前摘要文件的 S3 路径
- 当前摘要文件的 SHA-256 哈希值（十六进制编码）
- 之前摘要文件的十六进制编码签名

本文档的稍后部分提供了计算此字符串的格式和作为示例的字符串。

自定义验证实现步骤

实现自定义验证解决方案时，您需要先验证摘要文件，然后再验证其引用的日志文件。

验证摘要文件

要验证摘要文件，您需要其签名、与用于对其进行签名的私钥对应的公钥以及您计算的数据签名字符串。

1. 获取摘要文件。
2. 验证已从摘要文件的原始位置检索了摘要文件。
3. 获取摘要文件的十六进制编码签名。
4. 获取与用于对摘要文件进行签名的私钥对应的公钥的十六进制编码指纹。
5. 检索与摘要文件对应的时间范围的公钥。
6. 从检索到的公钥中，选择指纹与摘要文件中的指纹匹配的公钥。
7. 使用摘要文件哈希值及其他摘要文件字段，重新创建用于验证摘要文件签名的数据签名字符串。
8. 将此字符串的 SHA-256 哈希值、公钥及签名作为参数传递给 RSA 签名验证算法，以验证签名。如果结果为 true，则摘要文件有效。

验证日志文件

如果摘要文件有效，则验证摘要文件引用的每个日志文件。

1. 为验证日志文件的完整性，系统会计算未压缩内容的 SHA-256 哈希值并将结果与摘要中记录的十六进制日志文件哈希值进行比较。如果哈希值匹配，则日志文件有效。
2. 通过使用当前摘要文件中包含的有关前一个摘要文件的信息，连续验证前一个摘要文件及其对应的日志文件。

以下部分详细介绍了这些步骤。

A. 获取摘要文件

第一步是获取最新的摘要文件，验证您已从其来源位置检索到它，然后验证其数字签名并获取公钥的指纹。

1. 例如，使用 S3 GetObject或 Amazons3Client 类，从您的 Amazon S3 存储桶中获取要验证的时间范围内的最新摘要文件。
2. 检查用于检索此文件的 S3 存储桶和 S3 对象是否与摘要文件中记录的 S3 存储桶 S3 对象位置匹配。
3. 接下来，从 Simple Storage Service（Amazon S3）中摘要文件对象的 `x-amz-meta-signature` 元数据属性获取摘要文件的数字签名。
4. In the digest file, get the fingerprint of the public key whose private key was used to sign the digest file from the `digestPublicKeyFingerprint` field。

B. 检索用于验证摘要文件的公钥

要获取用于验证摘要文件的公钥，您可以使用 AWS CLI 或 CloudTrail API。在这两种情况下，您都需要指定要验证的摘要文件的时间范围（即，起始时间和结束时间）。对于您指定的时间范围，可能会返回一个或多个公钥。返回的密钥的有效时间范围可能会发生重叠。

> **Note**
>
> 由于每个区域 CloudTrail 使用不同的私钥/公钥对，因此每个摘要文件都使用其区域独有的私钥进行签名。因此，当您验证来自特定区域的摘要文件时，必须从同一区域检索其公钥。

使用检 AWS CLI 索公钥

要使用检索摘要文件的公钥 AWS CLI，请使用`cloudtrail list-public-keys`命令。此命令采用以下格式：

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

start-time 和 end-time 参数为 UTC 时间戳且是可选的。如果未指定，则使用当前时间，且返回当前有效的一个或多个公钥。

示例响应

响应是代表所返回的一个或多个密钥的 JSON 对象的列表：

```
{
    "publicKeyList": [
```

```
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

使用 CloudTrail API 检索公钥

要使用 CloudTrail API 检索摘要文件的公钥，请将开始时间和结束时间值传递给 `ListPublicKeys` API。`ListPublicKeys` API 返回与用于在指定时间范围对摘要文件进行签名的私钥对应的公钥。对于每个公钥，此 API 还返回相应的指纹。

`ListPublicKeys`

本部分介绍 `ListPublicKeys` API 的请求参数和响应元素。

> **Note**
>
> ListPublicKeys 的二进制字段的编码可能随时发生变化。

请求参数

名称	描述
StartTime	（可选）以 UTC 为单位指定查找 CloudTrail 摘要文件公钥的时间范围的起始时间。如果 StartTime 未指定，则使用当前时间，并返回当前的公钥。 类型: DateTime
EndTime	（可选）以 UTC 为单位指定查找 CloudTrail 摘要文件公钥的时间范围的结束时间。如果 EndTime 未指定，则使用当前时间。 类型: DateTime

响应元素

PublicKeyList - PublicKey 对象数组，包含：

名称	描述
Value	DER 编码的公钥值（采用 PKCS #1 格式）。 类型：Blob
ValidityStartTime	公钥有效的起始时间。 类型: DateTime
ValidityEndTime	公钥有效的结束时间。 类型: DateTime
Fingerprint	公钥的指纹。指纹可用于识别验证摘要文件所必需的公钥。 类型：字符串

C. 选择要用于验证的公钥

从 `list-public-keys` 或 `ListPublicKeys` 返回的公钥中，选择指纹与摘要文件的 `digestPublicKeyFingerprint` 字段中记录的指纹匹配的公钥。此即为用于验证摘要文件的公钥。

D. 重新创建数据签名字符串

现在，您有了摘要文件的签名及关联公钥，接下来，您需要计算数据签名字符串。算出数据签名字符串后，您就有了验证签名所需的输入。

数据签名字符串采用以下格式：

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

之后是示例 `Data_To_Sign_String`。

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

重新创建此字符串后，您即可验证摘要文件。

E. 验证摘要文件

将重新创建的数据签名字符串的 SHA-256 哈希值、数字签名和公钥传给 RSA 签名验证算法。如果输出为 true，则已验证摘要文件签名，且摘要文件有效。

F. 验证日志文件

验证摘要文件后，您可以验证其引用的日志文件。摘要文件包含日志文件的 SHA-256 哈希值。如果其中一个日志文件在 CloudTrail 交付后被修改，则 SHA-256 哈希值将发生变化，并且摘要文件的签名将不匹配。

下面的内容介绍如何验证日志文件：

1. 使用摘要文件的 `logFiles.s3Bucket` 和 `logFiles.s3Object` 字段中的 S3 位置信息对日志文件执行 `S3 Get` 操作。
2. 如果 `S3 Get` 操作成功，则按照以下步骤循环访问摘要文件的 logFiles 数组中列出的日志文件：
   a. 从摘要文件中相应日志的 `logFiles.hashValue` 字段检索文件的原始哈希值。
   b. 使用 `logFiles.hashAlgorithm` 中指定的哈希算法计算未压缩的日志文件内容的哈希值。
   c. 比较您生成的哈希值和摘要文件中日志的哈希值。如果哈希值匹配，则日志文件有效。

G. 验证其他摘要和日志文件

在每个摘要文件中，以下字段提供前一个摘要文件的位置和签名：

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

使用此信息顺序访问之前的摘要文件，按照前述部分中的步骤验证每个摘要文件的签名及其引用的日志文件。唯一的区别在于：对于之前的摘要文件，您不需要从摘要文件对象的 Simple Storage Service（Amazon S3）元数据属性检索数字签名。`previousDigestSignature` 字段提供了前一个摘要文件的签名。

您可以一直向前进行此操作，直到到达起始的摘要文件，或摘要文件链断开，以先到者为准。

离线验证摘要和日志文件

离线验证摘要和日志文件时，您通常可以按照前述部分中介绍的流程进行。但是，您必须考虑到以下方面：

处理最新的摘要文件

最新（即“当前”）摘要文件的数字签名位于摘要文件对象的 Simple Storage Service（Amazon S3）元数据属性中。在离线情况下，当前摘要文件的数字签名不可用。

对于这种情况，有两种处理方式：

- 由于前一个摘要文件的数字签名位于当前摘要文件中，因此请从 next-to-last 摘要文件开始验证。使用这种方法时，不会验证最新的摘要文件。

- 作为预备步骤，从摘要文件对象的元数据属性获取当前摘要文件的签名，然后将其安全地离线存储。这样，除了链中前面的文件，此最新的摘要文件也可得到验证。

路径解决方案

已下载的摘要文件中的字段（如 `s3Object` 和 `previousDigestS3Object`）仍将指向日志文件和摘要文件的 Simple Storage Service（Amazon S3）在线位置。离线解决方案必须找到一种方法，将它们重新路由到已下载的日志和摘要文件的当前路径。

公钥

要进行离线验证，首先必须在线获取验证给定时间范围内的日志文件所需的所有公钥（例如，通过调用 `ListPublicKeys` 实现），然后将它们安全地离线存储。每当您需要验证超出指定的初始时间范围的其他文件时，都必须重复执行这一步。

示例验证代码段

以下示例片段提供了用于验证 CloudTrail 摘要和日志文件的基本代码。此框架代码未指定在线/离线条件；也就是说，由您决定是否实现在线连接到 AWS的代码。建议在实现中使用 Java Cryptography Extension (JCE) 和 Bouncy Castle 作为安全提供程序。

示例代码段：

- 如何创建用于验证摘要文件签名的数据签名字符串。
- 如何验证摘要文件签名。
- 如何验证日志文件哈希值。
- 用于验证摘要文件链的代码结构。

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;
```

```
public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
as part of the data to sign
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
 ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:
```

```
                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
                    messageDigest.update(logFileContent);
```

```
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
 Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
 match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
 Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail 日志文件示例

CloudTrail 监控您账户的事件。如果您创建跟踪，它会将这些事件作为日志文件传送到您的 Simple Storage Service（Amazon S3）存储桶。如果您在 CloudTrail Lake 中创建事件数据存储，则事件将记录到您的事件数据存储中。事件数据存储不使用 S3 存储桶。

主题

- CloudTrail 日志文件名格式
- 日志文件示例

CloudTrail 日志文件名格式

CloudTrail 对于传输到您的 Amazon S3 存储桶的日志文件对象，使用以下文件名格式：

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYY、MM、DD、HH 和 mm 为日志文件传输时间中表示年、月、日、小时和分钟的数字。小时为 24 小时格式。Z 表示时间采用 UTC 格式。

  > **Note**
  >
  > 在特定时间传输的日志文件可包含在该时间前的任何时刻编写的记录。

- 日志文件名称的 16 字符 UniqueString 部分用于防止覆盖文件。它没有意义，日志处理软件应忽略它。
- FileNameFormat 为文件的编码。目前，这是 json.gz（一个采用压缩 gzip 格式的 JSON 文本文件）。

示例 CloudTrail 日志文件名

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

日志文件示例

一个日志文件包含一条或多条记录。以下是日志代码段的示例，其中显示开始日志文件创建的操作记录。

有关 CloudTrail 事件记录字段的信息，请参见CloudTrail 录制内容。

目录

- Amazon EC2 日志示例
- IAM 日志示例
- 示例错误代码及留言记录
- CloudTrail 洞察事件日志示例

Amazon EC2 日志示例

Amazon Elastic Compute Cloud（Amazon EC2）在 AWS Cloud中提供大小可调的计算容量。您可以启动虚拟服务器，配置安全性和联网，并管理存储。Amazon EC2 还可快速扩展或缩减以处理需求变化或使用高峰，从而减少对预测服务器流量的需求。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南。

以下示例显示，一位名为 Mateo 的 IAM 用户对实例 i-EXAMPLE56126103cb 和 i-EXAMPLEaff4840c22 执行了 aws ec2 start-instances 命令，从而调用了 Amazon EC2 StartInstances 操作。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
```

```
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

以下示例显示，一位名为 Nikki 的 IAM 用户执行了 aws ec2 stop-instances 命令，从而调用了 Amazon EC2 StopInstances 操作，以停止两个实例。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
```

```
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

以下示例显示，一位名为 Arnav 的 IAM 用户执行了 aws ec2 create-key-pair 命令，从而调用了 CreateKeyPair 操作。请注意，responseElements包含密钥对的哈希值，并 AWS 删除了密钥材料。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

IAM 日志示例

AWS Identity and Access Management (IAM) 是一项 Web 服务，可帮助您安全地控制对 AWS 资源的访问。借助 IAM，您可以集中管理控制用户可访问哪些 AWS 资源的权限。可以使用 IAM 来控制谁通过了身份验证（准许登录）并获得授权（具有z权限）来使用资源。有关更多信息，请参阅 IAM 用户指南。

以下示例显示，名为 Mary 的 IAM 用户执行了 aws iam create-user 命令，从而调用了 CreateUser 操作，以创建名为 Richard 的新用户。

```
{"Records": [{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
```

```
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

以下示例显示，名为 Paulo 的 IAM 用户执行了 aws iam add-user-to-group 命令，从而调用了 AddUserToGroup 操作，以将名为 Jane 的用户添加到 Admin 组。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

以下示例显示，名为 Saanvi 的 IAM 用户执行了 aws iam create-role 命令，从而调用了 CreateRole 操作，以创建角色。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
```

```
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


示例错误代码及留言记录

以下示例显示，名为 Terry 的 IAM 用户执行了 aws cloudtrail update-trail 命令，从而调用了 UpdateTrail 操作，以更新名为 myTrail2 的跟踪，但未找到跟踪名称。日志在 errorCode 和 errorMessage 中显示了此错误。


```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
```

```
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail 洞察事件日志示例

以下示例显示了 CloudTrail Insights 事件日志。实际上，Insights 事件是一对事件，它们标记异常的写管理 API 活动或错误响应活动周期的开始和结束。`state` 字段显示是在异常活动期间的开始还是结束时记录事件。事件名称与 CloudTrail 分析管理事件以确定发生了异常活动的 AWS Systems Manager API 的名称相同。`UpdateInstanceInformation`尽管开始事件和结束事件具有唯一的 `eventID` 值，但它们也有一个由该对使用的 `sharedEventID` 值。见解事件显示 `baseline`、正常活动模式、`insight` 或触发开始见解事件的平均异常活动；在结束事件中，还显示见解事件持续时间内平均异常活动的 `insight` 值。有关 CloudTrail Insights 的更多信息，请参阅记录 Insights 事件。

```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
```

```
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

使用 CloudTrail 处理库

CloudTrail 处理库是一个 Java 库，它提供了一种处理 AWS CloudTrail 日志的简便方法。您可以提供有关 CloudTrail SQS 队列的配置详细信息，并编写用于处理事件的代码。剩下的就交给 CloudTrail 处理库了。它会轮询您的 Amazon SQS 队列，读取和解析队列消息，下载 CloudTrail 日志文件，解析日志文件中的事件，并将事件作为 Java 对象传递到您的代码。

CloudTrail 处理库具有高度的可扩展性和容错能力。它可以并行处理日志文件，以便您可以根据需要处理任意数量的日志。它会处理与网络超时和无法访问的资源相关的网络故障。

以下主题向您展示如何使用 CloudTrail 处理库来处理 Java 项目中的 CloudTrail 日志。

该库是作为Apache许可的开源项目提供的，可在以下网址获得：。 GitHub https://github.com/aws/aws-cloudtrail-processing-library库源包括可用作您自己的项目基础的示例代码。

主题

- 最低要求

- 处理 CloudTrail 日志
- 高级主题
- 其他 资源

最低要求

要使用 CloudTrail 处理库，必须具备以下条件：

- AWS SDK for Java 1.11.830
- Java 1.8（Java SE 8）

处理 CloudTrail 日志

要在 Java 应用程序中处理 CloudTrail 日志，请执行以下操作：

1. 将 CloudTrail 处理库添加到您的项目中
2. 配置 CloudTrail 处理库
3. 实施事件处理器
4. 实例化和运行处理执行程序

将 CloudTrail 处理库添加到您的项目中

要使用 CloudTrail 处理库，请将其添加到 Java 项目的类路径中。

目录

- 将库添加到 Apache Ant 项目
- 将库添加到 Apache Maven 项目
- 将库添加到 Eclipse 项目
- 将库添加到 IntelliJ 项目

将库添加到 Apache Ant 项目

将 CloudTrail 处理库添加到 Apache Ant 项目中

1. 从以下地址下载或克隆 CloudTrail 处理库源代码 GitHub：

- https://github.com/aws/ aws-cloudtrail-processing-library

2. 从源构建 .jar 文件，如自述文件中所述：

```
mvn clean install -Dgpg.skip=true
```

3. 将生成的 .jar 文件复制到您的项目中，并将它添加到您项目的 build.xml 文件中。例如：

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

将库添加到 Apache Maven 项目

CloudTrail 处理库可用于 Apache Maven。您可以将其添加到您的项目，方法是：在项目的 pom.xml 文件中编写单个依赖项。

将 CloudTrail 处理库添加到 Maven 项目

- 打开您的 Maven 项目的 pom.xml 文件，并添加如下依赖项：

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

将库添加到 Eclipse 项目

将 CloudTrail 处理库添加到 Eclipse 项目中

1. 从以下地址下载或克隆 CloudTrail 处理库源代码 GitHub：

- https://github.com/aws/ aws-cloudtrail-processing-library

2. 从源构建 .jar 文件，如自述文件中所述：

```
mvn clean install -Dgpg.skip=true
```

3. 将生成的 aws-cloudtrail-processing-library -1.6.1.jar 复制到项目中的某个目录中（通常）。`lib`
4. 在 Eclipse Project Explorer 中右键单击您的项目名称，选择 Build Path，然后选择 Configure。
5. 在 Java Build Path 窗口中，选择 Libraries 选项卡。
6. 选择添加 JAR... 然后导航到你复制的路径 aws-cloudtrail-processing-library -1.6.1.jar。
7. 选择 OK 以完成将 `.jar` 添加到您的项目的过程。

将库添加到 IntelliJ 项目

将 CloudTrail 处理库添加到 IntelliJ 项目中

1. 从以下地址下载或克隆 CloudTrail 处理库源代码 GitHub：
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 从源构建 .jar 文件，如自述文件中所述：

```
mvn clean install -Dgpg.skip=true
```

3. 从 File 中，选择 Project Structure。
4. 选择 Modules，然后选择 Dependencies。
5. 选择 + JARS or Directories，然后转至您构建 `aws-cloudtrail-processing-library-1.6.1.jar` 的路径。
6. 选择 Apply，然后选择 OK 以完成将 `.jar` 添加到您的项目的过程。

配置 CloudTrail 处理库

您可以通过创建在运行时加载的类路径属性文件来配置 CloudTrail 处理库，也可以手动创建`ClientConfiguration`对象并设置选项。

提供属性文件

您可以编写向您的应用程序提供配置选项的类路径属性文件。以下示例文件显示了您可设置的选项：

```
# AWS access key. (Required)
```

```
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

以下参数为必需参数：

- `sqsUrl`— 提供从中提取 CloudTrail通知的 URL。如果不指定此值，则 `AWSCloudTrailProcessingExecutor` 会引发 `IllegalStateException`。
- `accessKey` – 您账户的唯一标识符，例如 AKIAIOSFODNN7EXAMPLE。

- `secretKey`— 你账户的唯一标识符，例如 wjalrxutnfemi/k7mdeng/ CYEXAMPLEKEY bPxRfi。

`accessKey`和`secretKey`参数提供您访问库的 AWS 凭据，以便库可以 AWS 代表您进行访问。

其他参数的默认值由库设置。有关更多信息，请参阅 AWS CloudTrail Processing Library 参考。

创建一个 ClientConfiguration

您可以通过在 `ClientConfiguration` 对象上设置选项来提供针对 `AWSCloudTrailProcessingExecutor` 的选项，而不是在类路径属性中设置选项，如下面的示例所示：

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

实施事件处理器

要处理 CloudTrail 日志，必须实现接收 CloudTrail 日志数据的。`EventsProcessor`以下是一个实施示例：

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

在实现时`EventsProcessor`，您需要实现`AWSCloudTrailProcessingExecutor`用于向您发送 CloudTrail 事件的`process()`回调。事件在 `CloudTrailClientEvent` 对象的列表中提供。

该CloudTrailClientEvent对象提供了一个CloudTrailEvent和CloudTrailEventMetadata，你可以用它来读取 CloudTrail 事件和交付信息。

该简单示例会输出传递到 SampleEventsProcessor 的每个事件的事件信息。在您自己的实现中，您可以按照所需方式处理日志。只要 AWSCloudTrailProcessingExecutor 有事件要发送并仍在运行，它就会继续将事件发送至您的 EventsProcessor。

实例化和运行处理执行程序

在您编写EventsProcessor并设置 CloudTrail 处理库的配置值（在属性文件中或通过使用ClientConfiguration类）之后，您可以使用这些元素来初始化和使用AWSCloudTrailProcessingExecutor。

用于**AWSCloudTrailProcessingExecutor**处理 CloudTrail 事件

1. 实例化 AWSCloudTrailProcessingExecutor.Builder 对象。 Builder 的构造函数采用一个 EventsProcessor 对象和一个类路径属性文件名。
2. 调用 Builder 的 build() 工厂方法，以配置并获取 AWSCloudTrailProcessingExecutor 对象。
3. 使用 AWSCloudTrailProcessingExecutor's start() 和 m stop() ethods 开始和结束 CloudTrail 事件处理。

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

高级主题

主题

- 筛选要处理的事件

- 处理数据事件
- 报告进度
- 处理错误

筛选要处理的事件

默认情况下，您的 Amazon SQS 队列的 S3 存储桶中的所有日志及其包含的所有事件均会发送到您的 EventsProcessor。P CloudTrail rocessing Library 提供了可选接口，您可以实现这些接口来筛选用于获取 CloudTrail 日志的源并筛选您有兴趣处理的事件。

SourceFilter

您可以实施 SourceFilter 接口，以选择是否要处理来自提供的源的日志。SourceFilter 声明单个调用方法 filterSource()，该方法接收一个 CloudTrailSource 对象。要阻止源中的事件被处理，请从 false () 返回 filterSource()。

在库轮询 Amazon SQS 队列中的日志之后， CloudTrail 处理库会调用该filterSource()方法。在库启动日志的事件筛选或处理之前会发生此事。

以下是一个实施示例：

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());
```

```
    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

如果您未提供自己的 SourceFilter，则会使用 DefaultSourceFilter，这样将允许处理所有源 (它总是返回 true)。

EventFilter

您可以实现EventFilter接口来选择是否向您的发送 CloudTrail事件EventsProcessor。EventFilter声明一个接收CloudTrailEvent对象的filterEvent()单个回调方法。要阻止事件被处理，请从 false () 返回 filterEvent()。

CloudTrail 处理库会在库轮询 Amazon SQS 队列中的日志并进行源筛选之后调用该filterEvent()方法。这在库开始处理日志的事件之前发生。

请参阅下面的实施示例：

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

如果您未提供自己的 EventFilter，则会使用 DefaultEventFilter，这样将允许处理所有事件 (它总是返回 true)。

处理数据事件

CloudTrail 处理数据事件时，它会保留原始格式的数字，无论是整数 (int) 还是float（包含十进制的数字）。在数据事件字段中包含整数的事件中， CloudTrail 历史上会将这些数字作为浮点数进行处理。当前，通过保留这些字段的原始格式来 CloudTrail 处理这些字段中的数字。

作为最佳实践，为避免破坏自动化，请灵活使用任何用于处理或筛选 CloudTrail 数据事件的代码或自动化，并允许两者兼int而有float格式的数字。为获得最佳效果，请使用 CloudTrail 处理库 1.4.0 或更高版本。

以下示例代码段显示了 float 格式的数字 2.0，用于数据事件的 ResponseParameters数据块中的 desiredCount 参数。

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

以下示例代码段显示了 int 格式的数字 2，用于数据事件的 ResponseParameters数据块中的 desiredCount 参数。

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

报告进度

实现ProgressReporter接口以自定义 CloudTrail 处理库进度报告。 ProgressReporter声明了两个方法：reportStart()和reportEnd()，它们在以下操作的开头和结尾处被调用：

- 轮询来自 Amazon SQS 的消息
- 分析来自 Amazon SQS 的消息
- 正在处理日志 Amazon SQS 来源 CloudTrail
- 删除来自 Amazon SQS 的消息
- 正在下载 CloudTrail 日志文件
- 处理 CloudTrail 日志文件

这两种方法均会收到一个 `ProgressStatus` 对象，该对象包含有关已执行操作的信息。`progressState` 成员包含标识当前操作的 `ProgressState` 枚举的一个成员。此成员可以包含 `progressInfo` 成员中的其他信息。此外，您从 `reportStart()` 返回的任何对象都会传递给 `reportEnd()`，以便您能够提供上下文信息，例如事件开始处理时的时间。

下面是一个实施示例，该示例提供了有关完成操作所需时间的信息：

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

如果您未实施自己的 `ProgressReporter`，则将改用 `DefaultExceptionHandler` (它会输出正在运行的状态的名称)。

处理错误

您可使用 ExceptionHandler 接口在日志处理期间发生异常时提供特殊处理。ExceptionHandler 声明单个调用方法 handleException()，该方法将接收一个带有关于已发生异常的上下文的 ProcessingLibraryException 对象。

您可以使用传入的 ProcessingLibraryException 的 getStatus() 方法来查明发生异常时所执行的操作，并获取有关该操作的状态的附加信息。ProcessingLibraryException 派生自 Java 的标准 Exception 类，因此您也可以通过调用任一 Exception 方法来检索有关异常的信息。

请参阅下面的实施示例：

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

如果您未提供自己的 ExceptionHandler，则改用 DefaultExceptionHandler (它会输出标准错误消息)。

> **Note**
>
> 如果deleteMessageUponFailure参数为true，则 CloudTrail 处理库不区分一般异常和处理错误，并且可能会删除队列消息。
>
> 1. 例如，使用 SourceFilter 按时间戳筛选消息。
> 2. 但是，您没有访问接收 CloudTrail 日志文件的 S3 存储桶所需的权限。由于您没有所需的权限，因此会引发 AmazonServiceException。 CloudTrail 处理库将其封装在CallBackException.

3. `DefaultExceptionHandler` 会将其记录为错误，但不会确定根本原因，这个原因就是您没有所需的权限。 CloudTrail 处理库将此视为处理错误并删除该消息，即使该消息包含有效的 CloudTrail 日志文件也是如此。

如果您要用 `SourceFilter` 来筛选消息，请验证您的 `ExceptionHandler` 是否可将服务异常与处理错误区分开。

其他 资源

有关 CloudTrail 处理库的更多信息，请参阅以下内容：

- CloudTrail 处理库 GitHub 项目，其中包括演示如何实现 CloudTrail 处理库应用程序的示例代码。
- CloudTrail 处理库 Java Package 文档。

安全性 AWS CloudTrail

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用的合规计划 AWS CloudTrail，请参阅按合规计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 CloudTrail。以下主题向您介绍如何进行配置 CloudTrail 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 CloudTrail 资源。

主题

- 中的数据保护 AWS CloudTrail
- 适用于 Identity and Access 管理 AWS CloudTrail
- 合规性验证 AWS CloudTrail
- 韧性在 AWS CloudTrail
- 中的基础设施安全 AWS CloudTrail
- 防止跨服务混淆代理
- 中的安全最佳实践 AWS CloudTrail
- 使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)

中的数据保护 AWS CloudTrail

分 AWS 担责任模型适用于中的数据保护 AWS CloudTrail。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API CloudTrail 或 SDK 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或 AWS SDK 的情况。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

默认情况下， CloudTrail 事件日志文件使用 Amazon S3 服务器端加密 (SSE) 进行加密。您也可以选择使用 AWS Key Management Service (AWS KMS) 密钥加密日志文件。您可以将日志文件在 存储桶中存储任意长的时间。您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。如果您想接收有关日志文件传送和验证的通知，可以设置 Amazon SNS 通知。

以下安全最佳实践也涉及以下方面的数据保护 CloudTrail：

- 使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)
- 适用于 Amazon S3 存储桶的政策 CloudTrail
- 验证 CloudTrail 日志文件完整性
- 在 AWS 账户之间共享 CloudTrail 日志文件

由于 CloudTrail 日志文件存储在 Amazon S3 的一个或多个存储桶中，因此您还应查看《亚马逊简单存储服务用户指南》中的数据保护信息。有关更多信息，请参阅 Amazon S3 中的数据保护。

适用于 Identity and Access 管理 AWS CloudTrail

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 CloudTrail 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 AWS CloudTrail 与 IAM 配合使用
- 基于身份的策略示例 AWS CloudTrail
- AWS CloudTrail 基于资源的策略示例
- 适用于 Amazon S3 存储桶的政策 CloudTrail
- 适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略
- Amazon SNS 主题政策 CloudTrail
- 对 AWS CloudTrail 身份和访问进行故障排除
- 将服务相关角色用于 AWS CloudTrail
- AWS 的托管策略 AWS CloudTrail

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 CloudTrail。

服务用户-如果您使用 CloudTrail 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 CloudTrail 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问中的功能 CloudTrail，请参阅对 AWS CloudTrail 身份和访问进行故障排除。

服务管理员-如果您负责公司的 CloudTrail 资源，则可能拥有完全访问权限 CloudTrail。您的工作是确定您的服务用户应访问哪些 CloudTrail 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何将 IAM 与配合使用 CloudTrail，请参阅如何 AWS CloudTrail 与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理访问权限 CloudTrail。要查看您可以在 IAM 中使用的 CloudTrail 基于身份的策略示例，请参阅。基于身份的策略示例 AWS CloudTrail

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 - 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界

的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。

- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS CloudTrail 与 IAM 配合使用

在使用 IAM 管理访问权限之前 CloudTrail，请先了解哪些可用的 IAM 功能 CloudTrail。

您可以搭配使用的 IAM 功能 AWS CloudTrail

IAM 功能	CloudTrail 支持
基于身份的策略	是
基于资源的策略	部分
策略操作	是
策略资源	是
策略条件键（特定于服务）	否
ACL	否
ABAC（策略中的标签）	部分
临时凭证	是

IAM 功能	CloudTrail 支持
转发访问会话（FAS）	是
服务角色	是
服务相关角色	是

要全面了解 CloudTrail 以及其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 CloudTrail

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM 策略。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

基于身份的策略示例 CloudTrail

要查看 CloudTrail 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS CloudTrail

内部基于资源的政策 CloudTrail

支持基于资源的策略	部分

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

CloudTrail 支持在用于与 CloudTrail Lake 外部事件源集成的频道上使用基于资源的策略。 AWS用于该通道的基于资源的策略将定义哪些主体实体（账户、用户、角色和联合用户）可以针对该通道调用 `PutAuditEvents`，以将事件传送到目标事件数据存储。有关创建与 CloudTrail Lake 集成的更多信息，请参阅与外部的事件源创建集成 AWS。

示例

要查看 CloudTrail 基于资源的策略的示例，请参阅AWS CloudTrail 基于资源的策略示例。

的政策行动 CloudTrail

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 CloudTrail 操作列表，请参阅《服务授权参考》 AWS CloudTrail中定义的操作。

正在执行的策略操作在操作前 CloudTrail 使用以下前缀：

```
cloudtrail
```

例如，要授予某人使用 `ListTags` API 操作列出跟踪的标签的权限，您应将 `cloudtrail:ListTags` 操作纳入他们的策略中。策略语句必须包含 `Action` 或 `NotAction` 元素。 CloudTrail 定义了它自己的一组操作，这些操作描述了您可以使用此服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
      "cloudtrail:RemoveTags
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 Get 开头的所有操作，包括以下操作：

```
"Action": "cloudtrail:Get*"
```

的政策资源 CloudTrail

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 CloudTrail 资源类型及其 ARN 的列表，请参阅《服务授权参考》 AWS CloudTrail中的 “由定义的资源”。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 AWS CloudTrail定义的操作。

在中 CloudTrail，有三种资源类型：跟踪、事件数据存储和频道。每种资源均有相关联的唯一 Amazon Resource Name (ARN)。在策略中，您可以使用 ARN 来标识该策略适用的资源。 CloudTrail 目前不支持其他资源类型，这些资源有时被称为子资源。

CloudTrail 跟踪资源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

CloudTrail 事件数据存储资源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

CloudTrail 频道资源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

有关 ARN 格式的更多信息，请参阅 A mazon 资源名称 (ARN) 和 AWS 服务命名空间。

例如，对于标识为 *123456789012* 的，要在您的语句中指定位于美国东部（俄亥俄州）地区的名为 *My-Trail* 的跟踪，请使用以下 ARN： AWS 账户

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

要在其中指定属于特定账户的所有跟踪 AWS 区域，请使用通配符 (*)：

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

某些 CloudTrail 操作（例如创建资源的操作）无法对特定资源执行。在这些情况下，您必须使用通配符 (*)。

```
"Resource": "*"
```

许多 CloudTrail API 操作涉及多个资源。例如，`CreateTrail` 需要一个 Amazon S3 存储桶来存储日志文件，因此用户必须拥有写入存储桶的权限。要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
```

的策略条件密钥 CloudTrail

支持特定于服务的策略条件密钥	否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

CloudTrail 不定义自己的条件键，但它支持使用一些全局条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 CloudTrail 条件键列表，请参阅《服务授权参考》 AWS CloudTrail中的条件密钥。要了解可以使用条件键的操作和资源，请参阅操作定义者 AWS CloudTrail。

输入的 ACL CloudTrail

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC with CloudTrail

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是

ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

尽管您可以为 CloudTrail 资源附加标签，但 CloudTrail 仅支持基于标签控制对 CloudTrail Lake 事件数据存储和频道的访问权限。您无法基于标签控制对跟踪记录的访问权限。

您可以为 CloudTrail 资源附加标签或在请求中传递标签 CloudTrail。有关为 CloudTrail 资源添加标签的更多信息，请参阅创建跟踪和。使用创建、更新和管理跟踪 AWS CLI

将临时证书与 CloudTrail

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

转发访问会话 CloudTrail

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

CloudTrail 的服务角色

支持服务角色	是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 CloudTrail 功能。只有在 CloudTrail 提供操作指导时才编辑服务角色。

的服务相关角色 CloudTrail

支持服务相关角色	是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

CloudTrail 支持与 AWS Organizations集成的服务相关角色。创建组织跟踪或事件数据存储需要用到此角色。组织跟踪和事件数据存储组织 AWS 账户 中所有人的日志事件。有关创建或管理 CloudTrail服务相关角色的更多信息，请参阅将服务相关角色用于 AWS CloudTrail。

基于身份的策略示例 AWS CloudTrail

默认情况下，用户和角色无权创建或修改 CloudTrail资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源

执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM policy。

有关由定义的操作和资源类型的详细信息 CloudTrail，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》 AWS CloudTrail中的操作、资源和条件密钥。

主题

- 策略最佳实践
- 示例：允许和拒绝针对指定跟踪的操作
- 示例：对针对特定跟踪记录的操作创建和应用策略
- 示例：拒绝基于标签创建或删除事件数据存储的访问权限
- 使用 CloudTrail控制台
- 允许用户查看他们自己的权限
- 为 CloudTrail 用户授予自定义权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 CloudTrail 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM

Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

CloudTrail 没有可以在策略声明Condition元素中使用的特定于服务的上下文密钥。

示例：允许和拒绝针对指定跟踪的操作

以下示例演示了一个策略，该策略允许具有此策略的用户查看跟踪的状态和配置，并为名为 *My-First-Trail* 的跟踪启动和停止日志记录。这条步道是在美国东部（俄亥俄州）地区（其所在地区）创建的，编号为 *123 AWS ##* 456789012。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

以下示例演示了一项策略，该策略明确拒绝对任何未命名为 *My-First-* Trail 的跟踪 CloudTrail 执行操作。

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

示例：对针对特定跟踪记录的操作创建和应用策略

您可以使用权限和策略来控制用户对 CloudTrail 跟踪执行特定操作的能力。

例如，您不想公司开发人员组中的用户开始或停止对特定跟踪的日志记录。但是，您可能想授予他们在跟踪中执行 DescribeTrails 和 GetTrailStatus 操作的权限。您希望开发人员组的用户能够对自己管理的跟踪记录执行 StartLogging 或 StopLogging 操作。

您可以创建两条策略语句，然后将它们附加到您在 IAM 中创建的开发人员组。有关 IAM 中的组的更多信息，请参阅 IAM 用户指南中的 IAM 组。

在第一条策略中，您拒绝对您指定的跟踪 ARN 执行 StartLogging 和 StopLogging 操作。在下面的示例中，跟踪 ARN 为 arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
```

```
    ]
}
```

在第二个策略中，允许对所有 CloudTrail 资源GetTrailStatus执行DescribeTrails和操作：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

如果开发人员组中的用户尝试针对您在第一条策略中指定的跟踪启动或停止日志记录，该用户会收到拒绝访问异常。该开发人员组中的用户可针对自己创建和管理的跟踪记录启动和停止日志记录。

以下示例显示了在名为的配置文件中 AWS CLI 配置的开发者组devgroup。首先，devgroup 的用户运行 describe-trails 命令。

```
$ aws --profile devgroup cloudtrail describe-trails
```

该命令成功完成并返回以下输出：

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
```

```
            "S3BucketName": "myS3bucket ",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

然后，该用户针对您在第一条策略中指定的跟踪运行 get-trail-status 命令。

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

该命令成功完成并返回以下输出：

```
{
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

接下来，devgroup 组中的一位用户针对同一个跟踪运行 stop-logging 命令。

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

该命令返回拒绝访问异常，示例如下：

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

该用户针对同一个跟踪运行 start-logging 命令。

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

该命令再次返回拒绝访问异常，示例如下：

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

示例：拒绝基于标签创建或删除事件数据存储的访问权限

在如下策略示例中，如果以下条件一条都无法满足，使用 CreateEventDataStore 创建事件数据存储的权限将被拒绝：

- 事件数据存储自身并没有应用 stage 标签键。
- 阶段标签的值不是 alpha、beta、gamma 或 prod。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

在以下策略示例中，如果事件数据存储有 stage 标签且值为 prod，使用 DeleteEventDataStore 删除事件数据存储的权限将被拒绝。类似策略可以帮助保护事件数据存储免遭意外删除。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

使用 CloudTrail控制台

要访问 AWS CloudTrail 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 CloudTrail 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

授予CloudTrail 管理权限

要允许 IAM 角色或用户管理 CloudTrail 资源，例如跟踪、事件数据存储或频道，您必须授予执行与 CloudTrail 任务相关的操作的明确权限。在大多数情况下，您可以使用包含预定义权限的 AWS 托管策略。

> **Note**
>
> 您授予用户执行 CloudTrail 管理任务的权限与将日志文件传输到 Amazon S3 存储桶或向 Amazon SNS 主题发送通知 CloudTrail 所需的权限不同。有关这些权限的更多信息，请参阅适用于 Amazon S3 存储桶的政策 CloudTrail。
> 如果您配置与 Amazon CloudWatch Logs 的集成，则 CloudTrail 还需要一个可以代入的角色来向 Amazon Lo CloudWatch gs 日志组传送事件。您必须创建 CloudTrail 使用的角色。有关更

多信息，请参阅 授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限 和 将事件发送到 CloudWatch 日志。

以下 AWS 托管策略可用于 CloudTrail：

- AWSCloudTrail_FullAccess— 此政策提供对 CloudTrail 资源 CloudTrail 操作的完全访问权限，例如跟踪、事件数据存储和频道。此策略提供创建、更新和删除 CloudTrail 跟踪、事件数据存储和频道所需的权限。

  该策略还提供管理 Amazon S3 存储桶、日志日志组和 CloudWatch 跟踪的 Amazon SNS 主题的权限。但是，`AWSCloudTrail_FullAccess`托管策略不提供删除 Amazon S3 存储桶、日志组或 Amazon SNS 主题的权限。 CloudWatch 有关其他人的托管策略的信息 AWS 服务，请参阅《AWS 托管策略参考指南》。

  > **Note**
  >
  > 本AWSCloudTrail_FullAccess政策不打算在您之间广泛共享 AWS 账户。拥有此角色的用户能够关闭或重新配置他们的 AWS 账户账户中最敏感且最重要的审计功能。因此，您只能将此策略应用于账户管理员。您必须严格控制和监控此策略的使用。

- AWSCloudTrail_ReadOnlyAccess— 此策略授予查看 CloudTrail 控制台的权限，包括最近的事件和事件历史记录。此策略还支持查看现有跟踪、事件数据存储和通道。拥有此策略的角色和用户可以下载事件历史记录，但他们无法创建或更新跟踪、事件数据存储或通道。

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

其他 资源

要详细了解如何使用 IAM 向身份（例如用户和角色）授予对您账户中资源的访问权限，请参阅 IAM 用户指南中的如何设置 IAM 和AWS 资源访问管理。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

为 CloudTrail 用户授予自定义权限

CloudTrail 策略向与之合作的用户授予权限 CloudTrail。如果您需要向用户授予不同的权限，则可以将 CloudTrail 策略附加到 IAM 群组或用户。您可以编辑策略，使之包括或排除特定权限。您还可以创建自己的自定义策略。策略是一些 JSON 文档，它们定义了允许用户执行的操作以及允许用户对哪些资源执行这些操作。有关特定示例，请参阅 示例：允许和拒绝针对指定跟踪的操作 和 示例：对针对特定跟踪记录的操作创建和应用策略。

目录

- 只读访问权限
- 完全 访问
- 授予在 CloudTrail 控制台上查看 AWS Config 信息的权限
- 授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限
- 其他信息

只读访问权限

以下示例显示了授予对 CloudTrail 跟踪的只读访问权限的策略。这等同于托管策略 AWSCloudTrail_ReadOnlyAccess。它对用户授予查看跟踪信息的权限，而不是创建或更新跟踪记录的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:Get*",
                "cloudtrail:Describe*",
                "cloudtrail:List*",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

在这些策略语句中，Effect 元素指定是允许还是拒绝操作。Action 元素列出了允许用户执行的特定操作。Resource元素列出了允许用户对其执行这些操作的 AWS 资源。对于控制 CloudTrail 操作访问权限的策略，Resource元素通常设置为*，通配符表示 “所有资源”。

Action 元素中的值对应于服务支持的 API。操作前面有表示它们指的是 CloudTrail 动作。cloudtrail:您可以在 Action 元素中使用 * 通配符，如以下示例所示：

- "Action": ["cloudtrail:*Logging"]

  这允许所有以 “Logging”（StartLogging，StopLogging）结尾的 CloudTrail 操作。
- "Action": ["cloudtrail:*"]

  这允许所有 CloudTrail 操作，但不允许对其他 AWS 服务执行操作。
- "Action": ["*"]

  这允许所有 AWS 操作。此权限适合授予充当您账户的 AWS 管理员的用户。

只读策略不对用户授予执行 CreateTrail、UpdateTrail、StartLogging 和 StopLogging 操作的权限。具有此策略的用户不能够创建跟踪记录、更新跟踪记录或启用和关闭日志记录。有关 CloudTrail 操作列表，请参阅 AWS CloudTrail API 参考。

完全 访问

以下示例显示了授予对的完全访问权限的策略 CloudTrail。这等同于托管策略 AWSCloudTrail_FullAccess。它授予用户执行所有 CloudTrail 操作的权限。它还允许用户在 Amazon S3 中记录数据事件 AWS Lambda，管理 Amazon S3 存储桶中的文件，管理 CloudWatch 日志监控 CloudTrail 日志事件的方式，以及在用户关联的账户中管理 Amazon SNS 主题。

> **Important**
>
> 该AWSCloudTrail_FullAccess政策或同等权限不打算在您的 AWS 账户中广泛共享。具有此角色或同等访问权限的用户可以禁用或重新配置其 AWS 账户中最敏感和最重要的审计功能。因此，此策略应仅应用于账户管理员，并且此策略的使用应受到密切控制和监控。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

授予在 CloudTrail 控制台上查看 AWS Config 信息的权限

您可以在 CloudTrail 控制台上查看事件信息，包括与该事件相关的资源。对于这些资源，您可以选择 AWS Config 图标在 AWS Config 控制台中查看该资源的时间表。将此政策附加到您的用户，以授予他们只读 AWS Config 访问权限。该策略不对他们授予在 AWS Config中更改设置的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

有关更多信息，请参阅 使用 AWS Config查看引用的资源。

授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限

如果您有足够的权限，则可以在 CloudTrail 控制台中查看和配置向 CloudWatch 日志发送的事件。这些权限可能超出了为 CloudTrail管理员授予的权限。将此策略附加到将配置和管理与 CloudWatch 日志CloudTrail集成的管理员。该策略不直接向他们授予 CloudWatch 日志中 CloudTrail 或日志中的权限，而是授予创建和配置角色所需的权限，以便成功 CloudTrail将事件传送到您的 CloudWatch 日志组。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。

其他信息

要详细了解如何使用 IAM 向身份（例如用户和角色）授予对您账户中资源的访问权限，请参阅 IAM 用户指南中的AWS 资源入门和访问管理。

AWS CloudTrail 基于资源的策略示例

CloudTrail 支持用于 La CloudTrail ke 集成的 CloudTrail 渠道的基于资源的权限策略。有关创建与 CloudTrail Lake 集成的更多信息，请参阅与外部的事件源创建集成 AWS。

该策略所需的信息由集成类型决定。

- 对于方向集成， CloudTrail 要求策略包含合作伙伴的 AWS 账户 ID，并要求您输入合作伙伴提供的唯一外部 ID。 CloudTrail 使用 CloudTrail 控制台创建集成时，会自动将合作伙伴的 AWS 账户 ID 添加到资源策略中。请参阅合作伙伴的文档，了解如何获取保单所需的 AWS 账户 号码。
- 对于解决方案集成，您必须至少指定一个 AWS 账户 ID 作为委托人，并且可以选择输入外部 ID 以防止副手感到困惑。

以下是对基于资源的策略的要求：

- 该策略中定义的资源 ARN 必须与该策略附加到的通道 ARN 相匹配。
- 该策略仅包含一项操作：`cloudtrail-data:PutAuditEvents`

- 该策略至少包含一个语句。该策略最多可以包含 20 个语句。
- 每个语句至少包含一个主体。一个语句最多可以包含 50 个主体。

除非该策略拒绝通道所有者访问资源，否则该所有者可以针对该通道调用 PutAuditEvents API。

主题

- 示例：为主体提供通道访问权限
- 示例：使用外部 ID 防范混淆代理

示例：为主体提供通道访问权限

以下示例向拥有 ARN 的委托人授予权限 arn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root，以及arn:aws:iam::123456789012:root使用 ARN 在 CloudTrail 频道上调用 PutAuditEventsAPI 的权限。arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

示例：使用外部 ID 防范混淆代理

以下示例将使用外部 ID 来解决和防范混淆代理。混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。

集成合作伙伴会创建要在策略中使用的外部 ID，然后在创建集成的过程中向您提供该外部 ID。该值可以是任意唯一字符串，如密码或账号。

如果对 PutAuditEventsAPI 的调用包含策略中定义的外部 ID 值 `arn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root`，则该示例`arn:aws:iam::123456789012:root`向拥有 ARN 的委托人授予在 CloudTrail 频道资源上调用 PutAuditEvents API 的权限。

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "uniquePartnerExternalID"
                }
            }
        }
    ]
}
```

适用于 Amazon S3 存储桶的政策 CloudTrail

默认情况下，Simple Storage Service（Amazon S3）存储桶和对象都是私有的。仅资源所有者（创建存储桶的 AWS 账户）能够访问存储桶及其包含的对象。资源所有者可以通过编写访问策略来向其他资源和用户授予访问权。

要创建或修改 Simple Storage Service（Amazon S3）存储桶以接收企业跟踪记录的日志文件，您必须修改存储桶策略。有关更多信息，请参阅 使用为组织创建跟踪 AWS Command Line Interface。

要将日志文件传送到 S3 存储桶， CloudTrail 必须具有所需的权限，并且不能将其配置为申请方付款存储桶。

CloudTrail 为您在策略中添加以下字段：

- 允许的 SID
- 存储桶名称
- 的服务主体名称 CloudTrail
- 存储日志文件的文件夹的名称，包括存储桶名称、前缀（如果您已指定）和您的 AWS 账户 ID

作为安全最佳实践，请将 `aws:SourceArn` 条件密钥添加到 Simple Storage Service（Amazon S3）存储桶策略。IAM 全局条件密钥`aws:SourceArn`有助于确保仅针对一个或多个特定的跟踪 CloudTrail 写入 S3 存储桶。`aws:SourceArn` 的值始终是使用存储桶存储日志的跟踪记录（或跟踪记录 ARN 数组）的 ARN。确保将 `aws:SourceArn` 条件密钥添加到现有跟踪记录的 S3 存储桶策略。

以下策略 CloudTrail 允许将日志文件写入支持的存储桶 AWS 区域。将 *myBucketName[OptionalPrefix]/*、*myAccountID#regi on* 和 T *railName #########*的值。

S3 存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

有关的更多信息 AWS 区域，请参阅CloudTrail 支持的区域。

目录

- 指定用于 CloudTrail 日志传输的现有存储桶
- 从其他账户接收日志文件
- 创建或更新 Simple Storage Service（Amazon S3）存储桶以用于存储组织跟踪的日志文件
- Simple Storage Service（Amazon S3）存储桶策略问题排查
  - Simple Storage Service（Amazon S3）策略配置常见错误
  - 更改现有存储桶的前缀
- 其他 资源

指定用于 CloudTrail 日志传输的现有存储桶

如果您将现有 S3 存储桶指定为日志文件传输的存储位置，则必须将允许 CloudTrail 写入该存储桶的策略附加到该存储桶。

> **Note**
>
> 最佳做法是使用专用 S3 存储桶存储 CloudTrail 日志。

将所需的 CloudTrail 策略添加到 Amazon S3 存储桶

1. 打开 Amazon S3 控制台，网址为：https://console.aws.amazon.com/s3/。
2. 选择要将日志文件传送 CloudTrail 到哪个存储桶，然后选择 “权限”。
3. 选择编辑。
4. 将 S3 bucket policy 复制到 Bucket Policy Editor 窗口。用您的存储桶名称、前缀和账号替换斜体占位符。如果您在创建跟踪时指定了前缀，请在此处包含该前缀。前缀是 S3 对象键的可选附加内容，可在存储桶中创建类似于文件夹的组织结构。

   > **Note**
   >
   > 如果现有存储桶已附加了一个或多个策略，请添加用于 CloudTrail 访问该策略的声明。评估生成的权限集，确保它们适合于访问存储桶的用户。

从其他账户接收日志文件

您可以配置 CloudTrail 为将来自多个 AWS 账户的日志文件传送到单个 S3 存储桶。有关更多信息，请参阅 接收来自多个账户的 CloudTrail 日志文件。

创建或更新 Simple Storage Service（Amazon S3）存储桶以用于存储组织跟踪的日志文件

您必须指定一个 Simple Storage Service（Amazon S3）存储桶以接收组织跟踪的日志文件。此存储桶必须有 CloudTrail 允许将组织的日志文件放入存储桶的策略。

以下是名为的 Amazon S3 存储桶的策略示例 *myOrganizationBucket*，该存储桶归该组织的管理账户所有。将*myOrganizationBucket*、*##*、*ManagementAccountID#T railName # o-organizatid #######*

此存储桶策略包含三条语句。

- 第一条语句允许 CloudTrail 对亚马逊 S3 存储桶调用 Amazon S3 `GetBucketAcl` 操作。

- 第二条语句支持在跟踪仅从组织跟踪更改为该账户的跟踪时进行日志记录。
- 第三条语句支持对组织跟踪进行日志记录。

示例策略包括 Simple Storage Service（Amazon S3）存储桶策略的 aws:SourceArn 条件密钥。IAM 全局条件密钥aws:SourceArn有助于确保仅针对一个或多个特定的跟踪 CloudTrail 写入 S3 存储桶。在企业跟踪记录中，aws:SourceArn 的值必须是由管理账户拥有并使用管理账户 ID 的跟踪记录 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
```

```
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

此示例策略不允许来自成员账户的任何用户访问为组织创建的日志文件。默认情况下，组织日志文件只能由管理账户访问。有关如何允许成员账户中的 IAM 用户对 Simple Storage Service（Amazon S3）存储桶进行读取访问的信息，请参阅 在 AWS 账户之间共享 CloudTrail 日志文件。

Simple Storage Service（Amazon S3）存储桶策略问题排查

以下部分说明如何对 S3 存储桶策略进行问题排查。

Simple Storage Service（Amazon S3）策略配置常见错误

在创建或更新跟踪的过程中创建新存储桶时，会将所需的权限 CloudTrail附加到您的存储桶。存储桶策略使用服务主体名称"cloudtrail.amazonaws.com"，该名称允许 CloudTrail 为所有区域传送日志。

如果没有 CloudTrail 为某个区域传送日志，则您的存储桶可能有一个较旧的策略，该策略为每个区域指定 CloudTrail 账户 ID。此策略仅 CloudTrail允许传输指定区域的日志。

作为最佳实践，请更新策略以使用 CloudTrail 服务主体的权限。为此，请用服务委托方的名称 ("cloudtrail.amazonaws.com") 替换账户 ID ARN。这 CloudTrail 允许为当前和新区域传送日志。作为安全最佳实践，请将 aws:SourceArn 或 aws:SourceAccount 条件密钥添加到 Simple Storage Service（Amazon S3）存储桶策略。这有助于防止未经授权的账户访问您的 S3 存储桶。如果您有现有跟踪记录，请务必添加一个或多个条件密钥。以下示例展示了建议的策略配置。将 *myBucketName[OptionalPrefix]/*、*myAccountID#regi on* 和 T *railName #########*的值。

Example 具有服务委托方名称的存储桶策略示例

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

更改现有存储桶的前缀

如果您尝试添加、修改或删除从跟踪记录接收日志的 S3 存储桶的日志文件前缀，可能会收到以下错误消息：There is a problem with the bucket policy。存储桶策略包含错误的前缀会阻碍跟踪向存储桶传送日志。要解决此问题，请使用 Amazon S3 控制台更新存储桶策略中的前缀，然后使用 CloudTrail控制台为跟踪中的存储桶指定相同的前缀。

更新 Simple Storage Service（Amazon S3）存储桶的日志文件前缀

1. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
2. 选择要修改其前缀的存储桶，然后选择 Permissions（权限）。
3. 选择编辑。
4. 在存储桶策略中，在 `s3:PutObject` 操作下编辑 `Resource` 条目，根据需要添加、修改或删除日志文件 *`prefix/`*。

```
"Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
```

5. 选择保存。
6. 打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
7. 选择跟踪，并在 Storage location 中点击铅笔图标来编辑存储桶的设置。
8. 对于 S3 bucket，选择要更改前缀的存储桶。
9. 对于 Log file prefix，更新前缀，使其与您在存储桶策略中输入的前缀相符。
10. 选择保存。

其他 资源

有关 S3 存储桶和策略的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的使用存储桶策略。

适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略

默认情况下，Simple Storage Service（Amazon S3）存储桶和对象都是私有的。仅资源所有者（创建存储桶的 AWS 账户）能够访问存储桶及其包含的对象。资源所有者可以通过编写访问策略来向其他资源和用户授予访问权。

要将 CloudTrail Lake 查询结果传送到 S3 存储桶， CloudTrail 必须具有所需的权限，并且不能将其配置为申请方付款存储桶。

CloudTrail 为您在策略中添加以下字段：

- 允许的 SID
- 存储桶名称
- 的服务主体名称 CloudTrail

作为安全最佳实践，请将 `aws:SourceArn` 条件密钥添加到 Simple Storage Service（Amazon S3）存储桶策略。IAM 全局条件密钥`aws:SourceArn`有助于确保仅针对事件数据存储 CloudTrail 写入 S3 存储桶。

以下策略 CloudTrail 允许将查询结果从支持的存储桶传送到存储桶 AWS 区域。将 *myBucketName*“*myAccountID*” 和 “*myQueryRunning##*” 替换为适合您的配置的值。*myAccountID* 是用于的 AWS 账户 ID CloudTrail，它可能与 S3 存储桶的 AWS 账户 ID 不同。

> **Note**
>
> 如果您的存储桶策略包含 KMS 密钥的声明，我们建议您使用完全限定的 KMS 密钥 ARN。如果您改用 KMS 密钥别名，则会在请求者的账户中 AWS KMS 解析密钥。这一行为可能导致使用属于请求者而不是存储桶拥有者的 KMS 密钥来加密数据。
> 如果这是组织事件数据存储，则事件数据存储 ARN 必须包含管理账户的 AWS 账户 ID。这是因为管理账户保留对所有组织资源的所有权。

S3 存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

目录

- 为 La CloudTrail ke 查询结果指定现有存储桶
- 其他 资源

为 La CloudTrail ke 查询结果指定现有存储桶

如果您将现有 S3 存储桶指定为 CloudTrail Lake 查询结果交付的存储位置，则必须向该存储桶附加允许将查询结果传送 CloudTrail 到该存储桶的策略。

> **Note**
>
> 作为最佳实践，请使用专用 S3 存储桶获取 CloudTrail Lake 查询结果。

将所需的 CloudTrail 策略添加到 Amazon S3 存储桶

1. 打开 Amazon S3 控制台，网址为：https://console.aws.amazon.com/s3/。
2. 选择 CloudTrail 要在其中传送 Lake 查询结果的存储桶，然后选择 Permissi on s。
3. 选择编辑。
4. 将 S3 bucket policy for query results 复制到 Bucket Policy Editor 窗口。将斜体占位符替换为您的存储桶、区域和账户 ID 的名称。

> **Note**
>
> 如果现有存储桶已附加了一个或多个策略，请添加用于 CloudTrail 访问该策略的声明。评估生成的权限集，以确保其适用于访问存储桶的用户。

其他 资源

有关 S3 存储桶和策略的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的使用存储桶策略。

Amazon SNS 主题政策 CloudTrail

要向 SNS 主题发送通知， CloudTrail 必须具有所需的权限。 CloudTrail当您在控制台中创建或更新跟踪时创建 Amazon SNS 主题时，会自动为该 CloudTrail 主题附加所需的权限。

> **Important**
>
> 作为安全最佳实践，为了限制对 SNS 主题的访问，强烈建议您在创建或更新跟踪以发送 SNS 通知后，手动编辑附加到 SNS 主题的 IAM policy 以添加条件键。有关更多信息，请参阅本主题中的the section called “SNS 主题策略的安全最佳实践”。

CloudTrail 为您在策略中添加以下语句，其中包含以下字段：

- 允许的 SID。
- 的服务主体名称 CloudTrail。
- SNS 主题，包括区域、账户 ID 和主题名称。

以下策略 CloudTrail 允许从支持的区域发送有关日志文件传输的通知。有关更多信息，请参阅 CloudTrail 支持的区域。这是在创建或更新跟踪并选择启用 SNS 通知时附加到新的或现有 SNS 主题策略的默认策略。

SNS 主题策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
        }
    ]
}
```

要使用 AWS KMS加密的 Amazon SNS 主题发送通知，您还必须通过在的策略中添加以下声明来启用事件源 CloudTrail () 和加密主题之间的兼容性。 AWS KMS key

KMS 密钥策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

有关更多信息，请参阅启用来自 AWS 服务的事件源和加密主题之间的兼容性。

目录

- SNS 主题策略的安全最佳实践
- 指定要发送通知的现有主题
- SNS 主题策略问题排查
  - CloudTrail 未发送某个地区的通知
  - CloudTrail 未为组织中的成员账户发送通知
- 其他 资源

SNS 主题策略的安全最佳实践

默认情况下， CloudTrail 附加到您的 Amazon SNS 主题的 IAM 政策声明允许 CloudTrail 服务委托人向由 ARN 标识的 SNS 主题发布内容。为帮助防止攻击者访问您的 SNS 主题并代表主题收件人发送通知， CloudTrail 请手动编辑您的 CloudTrail SNS 主题策略，以便在所附的策略声明中添加`aws:SourceArn`条件密钥。 CloudTrail此密钥的值是跟踪记录的 ARN，或使用 SNS 主题的跟踪记录 ARN 数组。因为它既包括特定跟踪记录 ID，也包括拥有该跟踪记录的账户的 ID，所以它将 SNS 主题限制为仅可访问那些有权限管理该跟踪记录的账户。在向 SNS 主题策略添加条件密钥之前，请从控制台的跟踪设置中获取 SNS 主题名称。 CloudTrail

`aws:SourceAccount` 支持条件密钥，但不建议使用。

将 **`aws:SourceArn`** 条件键添加到您的 SNS 主题策略

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择跟踪设置中显示的 SNS 主题，然后选择 Edit（编辑）。
4. 展开 Access policy (访问策略)。
5. 在 Access policy（访问策略）JSON 编辑器中，查找类似于以下示例的数据块。

```
    {
```

```
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. 为条件添加新数据块 `aws:SourceArn`，如以下示例中所示。值 `aws:SourceArn` 是您要向 SNS 发送通知的跟踪的 ARN。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. 完成 SNS 主题策略的编辑后，选择 Save changes（保存更改）。

将 **aws:SourceAccount** 条件键添加到您的 SNS 主题策略

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择跟踪设置中显示的 SNS 主题，然后选择 Edit（编辑）。
4. 展开 Access policy (访问策略)。
5. 在 Access policy（访问策略）JSON 编辑器中，查找类似于以下示例的数据块。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. 为条件添加新数据块 aws:SourceAccount，如以下示例中所示。的值aws:SourceAccount是拥有 CloudTrail 跟踪的账户的 ID。此示例限制只有能够登录 AWS 账户 123456789012 的用户才能访问 SNS 主题。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. 完成 SNS 主题策略的编辑后，选择 Save changes（保存更改）。

指定要发送通知的现有主题

您可以在 Amazon SNS 控制台中手动将 Amazon SNS 主题的权限添加到您的主题策略中，然后在控制台中指定该主题。 CloudTrail

手动更新 SNS 主题策略

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 选择 Topics，然后选择主题。
3. 选择 “编辑”，然后向下滚动到 “访问策略”。

4. 添加SNS topic policy包含相应区域、账户 ID 和主题名称值的声明。
5. 如果您的主题是加密主题，则必须 CloudTrail 允许拥有`kms:GenerateDataKey*`和`kms:Decrypt`权限。有关更多信息，请参阅 Encrypted SNS topic KMS key policy。
6. 选择保存更改。
7. 返回 CloudTrail 控制台并指定跟踪的主题。

SNS 主题策略问题排查

以下部分说明如何对 SNS 主题策略进行问题排查。

方案：

- CloudTrail 未发送某个地区的通知
- CloudTrail 未为组织中的成员账户发送通知

CloudTrail 未发送某个地区的通知

在创建或更新跟踪的过程中创建新主题时，会将所需的权限 CloudTrail 附加到您的主题。主题策略使用服务主体名称`"cloudtrail.amazonaws.com"`，该名称允许 CloudTrail 向所有区域发送通知。

如果 CloudTrail 不是针对某个地区发送通知，则您的主题可能有一个较旧的政策，该政策为每个区域指定了 CloudTrail 账户 ID。此政策仅 CloudTrail 允许向指定区域发送通知。

以下主题策略仅允许 CloudTrail 向指定的九个区域发送通知：

Example 具有账户 ID 的主题策略

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
```

```
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

此策略使用基于个人 CloudTrail 账户 ID 的权限。要为新区域传送日志，您必须手动更新策略以包含该地区的 CloudTrail账户 ID。例如，由于 CloudTrail 增加了对美国东部（俄亥俄州）地区的支持，因此您必须更新政策才能为该地区添加账户 ID ARN：。`"arn:aws:iam::475085895292:root"`

作为最佳实践，请更新策略以使用 CloudTrail 服务主体的权限。为此，请用服务委托方的名称 (`"cloudtrail.amazonaws.com"`) 替换账户 ID ARN。

这 CloudTrail 允许发送当前和新区域的通知。以下是前一策略的更新版本：

Example 具有服务委托方名称的主题策略

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

验证策略具有正确的值：

- 在 `Resource` 字段中，指定主题所有者的账号。如果主题是由您创建的，请指定您的账号。
- 为区域和 SNS 主题名称指定适当的值。

CloudTrail 未为组织中的成员账户发送通知

当具有 AWS Organizations 组织跟踪的成员账户未发送 Amazon SNS 通知时，SNS 主题策略的配置可能存在问题。 CloudTrail 即使资源验证失败，也会在成员账户中创建组织跟踪，例如，组织跟踪的 SNS 主题不包括所有成员账户 ID。如果 SNS 主题策略不正确，则会发生授权失败。

要检查跟踪的 SNS 主题策略是否存在授权失败，请执行以下操作：

- 在 CloudTrail 控制台中，查看跟踪的详细信息页面。如果授权失败，则详细信息页面会显示一条警告，`SNS authorization failed`并指示修复 SNS 主题策略。
- 从中 AWS CLI，运行get-trail-status命令。如果授权失败，则命令输出将包括值为的`LastNotificationError`字段`AuthorizationError`。

其他 资源

有关 SNS 主题和订阅这些主题的更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

对 AWS CloudTrail 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 CloudTrail 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 CloudTrail
- 我无权执行 iam:PassRole
- 我想允许我以外的人 AWS 账户 访问我的 CloudTrail 资源
- 我无权执行 iam:PassRole
- 在尝试创建组织跟踪或事件数据存储时，我遇到了 NoManagementAccountSLRExistsException 异常

我无权在以下位置执行操作 CloudTrail

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `cloudtrail:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 `mateojackson` 用户的策略，以允许使用 `cloudtrail:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当 `mateojackson` IAM 用户尝试使用控制台查看有关跟踪的详细信息，但其账户没有相应的 CloudTrail 托管策略（AWSCloudTrail_FullAccess或 AWSCloudTrail_ReadOnlyAccess）或等效权限时，就会出现以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他在控制台中访问跟踪信息和状态。

如果您使用具有AWSCloudTrail_FullAccess托管策略或其等效权限的 IAM 用户或角色登录，并且无法配置跟踪 AWS Config 或 Amazon CloudWatch Logs 集成，则可能缺少与这些服务集成所需的权限。有关更多信息，请参阅 授予在 CloudTrail 控制台上查看 AWS Config 信息的权限 和 授予在 CloudTrail 控制台上查看和配置 Amazon CloudWatch 日志信息的权限。

我无权执行 `iam:PassRole`

如果您收到错误消息，提示您无权执行`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 CloudTrail。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户`marymajor`尝试使用控制台在中执行操作时，会出现以下示例错误 CloudTrail。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 CloudTrail 资源

您可以创建一个角色并在多个角色之间共享 CloudTrail 信息 AWS 账户。有关更多信息，请参阅 在 AWS 账户之间共享 CloudTrail 日志文件。

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解是否 CloudTrail 支持这些功能，请参阅如何 AWS CloudTrail 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户存取之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

我无权执行 `iam:PassRole`

如果您收到错误消息，提示您无权执行`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 CloudTrail。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户`marymajor`尝试使用控制台在中执行操作时，会出现以下示例错误 CloudTrail。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

在尝试创建组织跟踪或事件数据存储时，我遇到了 `NoManagementAccountSLRExistsException` 异常

如果管理账户没有服务相关角色，就会引发 `NoManagementAccountSLRExistsException` 异常。使用 AWS Organizations AWS CLI 或 API 操作添加委托管理员时，如果服务相关角色不存在，则不会创建该角色。

当您使用组织的管理账户添加委派管理员或在 CloudTrail 控制台中创建组织跟踪或事件数据存储时，或者使用 AWS CLI 或 CloudTrail API， CloudTrail 会自动为您的管理账户创建服务相关角色（如果尚不存在）。

如果您尚未添加委托管理员，请使用 CloudTrail 控制台 AWS CLI 或 CloudTrail API 添加委派管理员。有关添加委派管理员的更多信息，请参阅添加 CloudTrail 委派管理员和 RegisterOrganizationDelegatedAdmin(API)。

如果您已经添加了委托管理员，请使用管理账户在 CloudTrail 控制台中创建组织跟踪或事件数据存储，或者使用 AWS CLI 或 CloudTrail API。有关创建组织跟踪的更多信息，请参阅在控制台中为您的组织创建跟踪使用为组织创建跟踪 AWS Command Line Interface、和 CreateTrail(API)。

将服务相关角色用于 AWS CloudTrail

AWS CloudTrail 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 CloudTrail服务相关角色由服务预定义 CloudTrail ，包括该服务代表您呼叫他人 AWS 服务 所需的所有权限。

服务相关角色使设置变得 CloudTrail 更加容易，因为您不必手动添加必要的权限。 CloudTrail 定义其服务相关角色的权限，除非另有定义，否则 CloudTrail 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 CloudTrail

CloudTrail 使用名为的服务相关角色 AWSServiceRoleForCloudTrail— 此服务关联角色用于支持组织跟踪和组织事件数据存储。

AWSServiceRoleForCloudTrail 服务相关角色信任以下服务来代入该角色：

- `cloudtrail.amazonaws.com`

此角色用于支持在中创建和管理 CloudTrail 组织跟踪和 CloudTrail Lake 组织事件数据存储 CloudTrail。有关更多信息，请参阅 为组织创建跟踪。

附加到该角色的CloudTrailServiceRolePolicy策略 CloudTrail 允许对指定资源完成以下操作：

- 对所有 CloudTrail 资源执行的操作：
  - `All`
- 对所有 AWS Organizations 资源执行的操作：
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- CloudTrail 服务主体对所有 Organizations 资源执行的操作，用于列出该组织的委派管理员：
  - `organizations:ListDelegatedAdministrators`
- 在组织事件数据存储上禁用 Lake 联合身份验证的操作：
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为创建服务相关角色 CloudTrail

您无需手动创建服务相关角色。当您创建组织跟踪或组织事件数据存储，或者在 CloudTrail 控制台中添加委派管理员时，或者使用 AWS CLI 或 API 操作时， CloudTrail会为您创建服务相关角色（如果尚不存在）。

如果删除此服务相关角色，然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。当您创建组织跟踪或组织事件数据存储或添加委派管理员时， CloudTrail 会再次为您创建服务相关角色。

编辑的服务相关角色 CloudTrail

CloudTrail 不允许您编辑AWSServiceRoleForCloudTrail服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除的服务相关角色 CloudTrail

您无需手动删除该 AWSServiceRoleForCloudTrail 角色。如果从 Or AWS 账户 ganizations 组织中移除了，则该AWSServiceRoleForCloudTrail角色将自动从该组织中删除 AWS 账户。如果不从组织中移除账户，则无法将策略从组织管理账户中的 AWSServiceRoleForCloudTrail 服务相关角色中分离或移除。

您也可以使用 IAM 控制台、 AWS CLI 或 AWS API 手动删除服务相关角色。为此，您必须先手动清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 CloudTrail 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

要删除 AWSServiceRoleForCloudTrail 角色正在使用的某个资源，您可以执行下列操作之一：

- AWS 账户 从 Organizations 中的组织中删除。
- 更新跟踪以使其不再是组织跟踪。有关更多信息，请参阅 更新跟踪。
- 更新事件数据存储，使其不再为组织事件数据存储。有关更多信息，请参阅 使用控制台更新事件数据存储。
- 删除跟踪。有关更多信息，请参阅 删除跟踪。
- 删除事件数据存储。有关更多信息，请参阅 使用控制台删除事件数据存储。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除AWSServiceRoleForCloudTrail服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

CloudTrail 服务相关角色支持的区域

CloudTrail 支持在所有 AWS 区域 地方使用服务相关角色，而 CloudTrail 且 Organizations 都可用。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

AWS 的托管策略 AWS CloudTrail

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用 AWS 托管策略。这

些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅《IAM 用户指南》中的适用于工作职能的AWS 托管式策略。

AWS 托管策略：**AWSCloudTrail_ReadOnlyAccess**

将AWSCloudTrail_ReadOnlyAccess策略附加到其角色的用户身份可以在跟踪 CloudTrail、Lake 事件数据存储或 CloudTrail Lake 查询中执行只读`Describe*`操作，例如、、和操作。`Get*` `List*`

AWS 托管策略：**AWSServiceRoleForCloudTrail**

该CloudTrailServiceRolePolicy政策 AWS CloudTrail 允许代表您对组织跟踪和组织事件数据存储执行操作。该策略包括描述和列出组织中的组织账户和委托管理员所需的 AWS Organizations 权限。 AWS Organizations

此策略还包括在组织事件数据存储上禁用 Lake Fed eration 所需的 AWS Lake Formation 权限 AWS Glue 和权限。

此政策附加到允许代表您执行操作 CloudTrail 的AWSServiceRoleForCloudTrail服务相关角色。您无法将此策略附加到您的用户、组或角色。

CloudTrail AWS 托管策略的更新

查看有关 AWS 托管策略更新的详细信息 CloudTrail。要获得有关此页面更改的自动提醒，请订阅该页面上的 RSS feed。 CloudTrail 文档历史记录

更改	描述	日期
`CloudTrailServiceRolePolicy` – 对现有策略的更新	更新了策略，以允许在禁用联合身份验证时对组织事件数据存储执行以下操作：	2023 年 11 月 26 日

更改	描述	日期
	• glue:DeleteTable • lakeformation:DeregisterResource	
AWSCloudTrail_ReadOnlyAccess – 更新了现有策略	CloudTrail 将AWSCloudTrailReadOnlyAccess 策略的名称更改为AWSCloudTrail_ReadOnlyAccess 。此外，策略中的权限范围已缩小为 CloudTrail 操作。它不再包含 Amazon S3 或 AWS Lambda 操作权限。 AWS KMS	2022 年 6 月 6 日
CloudTrail 开始跟踪更改	CloudTrail 开始跟踪其 AWS 托管策略的更改。	2022 年 6 月 6 日

合规性验证 AWS CloudTrail

AWS CloudTrail 作为多个合规计划的一部分，第三方审计师对安全性和 AWS 合规性进行评估。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业指导方针和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS CloudTrail

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。如果您特别需要跨更远的地理距离复制 CloudTrail 日志文件，则可以将跨区域复制用于跟踪 Amazon S3 存储桶，这样可以跨不同区域的存储桶自动异步复制对象。 AWS

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，还 CloudTrail 提供多项功能来帮助支持您的数据弹性和备份需求。

记录所有 AWS 区域事件的跟踪和事件数据存储

将跟踪应用于所有 AWS 区域时， CloudTrail 会在您所在AWS 分区的所有其他区域 AWS 区域 中创建配置相同的跟踪。 AWS 添加新区域时，将在新区域中自动创建该跟踪配置。

创建多区域事件数据存储时， CloudTrail 会收集您账户 AWS 区域 中所有发生的事件。

CloudTrail 日志数据的版本控制、生命周期配置和对象锁定保护

由于 CloudTrail 使用 Amazon S3 存储桶来存储日志文件，因此您还可以使用 Amazon S3 提供的功能来帮助满足您的数据弹性和备份需求。有关更多信息，请参阅 Amazon S3 中的故障恢复能力。

中的基础设施安全 AWS CloudTrail

作为一项托管服务 AWS CloudTrail ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用 CloudTrail 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全性协议 (TLS)。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

以下安全最佳实践还涉及以下方面的基础架构安全 CloudTrail：

- 考虑使用 Amazon VPC 终端节点进行跟踪访问。
- 考虑使用 Amazon VPC 终端节点进行 Amazon S3 存储桶访问。有关更多信息，请参阅使用存储桶策略控制来自 VPC 终端节点的访问。
- 识别并审计所有包含 CloudTrail 日志文件的 Amazon S3 存储桶。考虑使用标签来帮助识别您的 CloudTrail 跟踪和包含 CloudTrail日志文件的 Amazon S3 存储桶。然后，您可以将资源组用于您的 CloudTrail 资源。有关更多信息，请参阅 AWS Resource Groups。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务

（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况， AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用aws:SourceArn和aws:SourceAccount全局条件上下文密钥来限制为资源 AWS CloudTrail 提供其他服务的权限。如果您只希望将一个资源与跨服务访问相关联，请使用 aws:SourceArn。如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 aws:SourceAccount。

防范混淆代理问题最有效的方法是使用 aws:SourceArn 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (*) 的 aws:SourceArn 全局上下文条件键。例如，"arn:aws:cloudtrail:*:*AccountID*:trail/*"。包含通配符时，您还必须使用 StringLike 条件运算符。

aws:SourceArn 的值必须是正在使用该资源的跟踪、事件数据存储或通道的 ARN。

以下示例显示了如何使用中的aws:SourceArn和aws:SourceAccount全局条件上下文键 CloudTrail 来防止出现混淆的副手问题:适用于 CloudTrail Lake 查询结果的 Amazon S3 存储桶策略.

中的安全最佳实践 AWS CloudTrail

AWS CloudTrail 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

主题

- CloudTrail 侦探安全最佳实践
- CloudTrail 预防性安全最佳实践

CloudTrail 侦探安全最佳实践

创建跟踪

要持续记录您的 AWS 账户中的事件，您必须创建跟踪。尽管在不创建跟踪的情况下在 CloudTrail 控制台中为管理事件 CloudTrail 提供 90 天的事件历史记录信息，但它不是永久记录，也不能提供有关所有可能的事件类型的信息。要获得持续记录以及包含您指定的所有事件类型的记录，您必须创建跟踪，它将日志文件传送到您指定的 Simple Storage Service（Amazon S3）存储桶。

为了帮助管理您的 CloudTrail 数据，可以考虑创建一个记录所有管理事件的跟踪 AWS 区域，然后创建其他跟踪来记录资源的特定事件类型，例如 Amazon S3 存储桶活动或 AWS Lambda 函数。

以下是您可以采取的一些步骤：

- 为您的 AWS 账户创建跟踪记录。
- 为企业创建跟踪记录。

将路径应用于所有人 AWS 区域

要获得您 AWS 账户中的 IAM 身份或服务所发生事件的完整记录，应将每个跟踪配置为全部记录事件 AWS 区域。通过全部记录事件 AWS 区域，您可以确保您的 AWS 账户中发生的所有事件都被记录下来，无论这些事件发生在哪个 AWS 区域。这包括记录全球服务事件，这些事件记录到该服务的特定 AWS 区域。当您创建适用于所有区域的跟踪时，会 CloudTrail 记录每个区域的事件并将 CloudTrail 事件日志文件传送到您指定的 S3 存储桶。如果您在创建应用于所有区域的跟踪后又添加了一个 AWS 区域，则该新区域会自动包括在内，该区域中的事件也将被记录。这是您在 CloudTrail 控制台中创建跟踪时的默认选项。

以下是您可以采取的一些步骤：

- 为您的 AWS 账户创建跟踪记录。
- 更新现有跟踪记录以记录所有 AWS 区域中的事件。
- 使用中的multi-region-cloud-trail启用规则，实施持续的侦探控制，以帮助确保创建的所有 AWS 区域跟踪都记录所有事件。 AWS Config

启用 CloudTrail 日志文件完整性

在安全和取证调查中，经验证的日志文件非常重要。例如，通过经验证的日志文件，您可以十分确定日志文件本身未更改，或者特定 IAM 身份凭证执行了特定 API 活动。 CloudTrail 日志文件完整性验证过程还可以让您知道日志文件是否已被删除或更改，或者肯定地断言在给定时间段内没有向您的账户发送任何日志文件。 CloudTrail 日志文件完整性验证使用行业标准算法：SHA-256 用于哈希，SHA-256 使用 RSA 进行数字签名。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail日志文件在计算上是不可行的。有关更多信息，请参阅 启用验证并验证文件。

与 Amazon CloudWatch 日志集成

CloudWatch 日志允许您监控和接收捕获的特定事件的警报 CloudTrail。发送到 CloudWatch 日志的事件是配置为由您的跟踪记录的事件，因此请确保您已将一个或多个跟踪配置为记录您感兴趣监控的事件类型（管理事件和/或数据事件）。

例如，您可以监控密钥安全和与网络相关的管理事件，例如AWS Management Console 登录失败事件。

以下是您可以采取的一些步骤：

- 查看示例CloudWatch日志集成。 CloudTrail
- 配置您的跟踪以将事件发送到 CloudWatch 日志。
- 考虑实施持续的侦探控制，通过使用中的cloud-trail-cloud-watch启用-logs 的规则，帮助确保所有跟踪都将事件发送到 CloudWatch 日志进行监控。 AWS Config

使用亚马逊 GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可帮助您保护您的账户、容器、工作负载和 AWS 环境中的数据。通过使用机器学习 (ML) 模型以及异常和威胁检测功能，可以 GuardDuty 持续监控不同的日志源，以识别环境中的潜在安全风险和恶意活动，并确定其优先级。

例如，如果它检测到通过实例启动角色专为 Amazon EC2 实例创建但正在从其中的其他账户使用的证书，则 GuardDuty 会检测到潜在的证书泄露。 AWS有关更多信息，请参阅 Amazon GuardDuty 用户指南。

使用 AWS Security Hub

使用监控您的使用情况， CloudTrail 因为它与安全最佳实践有关AWS Security Hub。Security Hub 使用侦测性安全控件来评估资源配置和安全标准，以帮助您遵守各种合规框架。有关使用 Security Hub 评估 CloudTrail 资源的更多信息，请参阅《AWS Security Hub 用户指南》中的AWS CloudTrail 控件。

CloudTrail 预防性安全最佳实践

的以下最佳做法 CloudTrail 可以帮助防止安全事件。

记录到专用和集中式 Simple Storage Service（Amazon S3）存储桶

CloudTrail 日志文件是 IAM 身份或 AWS 服务所执行操作的审计日志。这些日志的完整性、完全性和可用性对于进行取证和审计至关重要。通过登录到专用和集中化的 Simple Storage Service（Amazon S3）存储桶，您可以强制实施严格的安全控制、访问和责任划分。

以下是您可以采取的一些步骤：

- 创建一个单独的 AWS 账户作为日志存档账户。如果您使用 AWS Organizations，请在组织中注册此账户，并考虑创建组织跟踪来记录组织中所有 AWS 账户的数据。
- 如果您不使用 Organizations，但想要记录多个 AWS 账户的数据，请创建一个跟踪以记录此日志存档帐户中的活动。将对此账户的访问权限限制为仅限应该对账户和审计数据具有访问权限的可信管理用户。
- 在创建跟踪的过程中，无论是组织跟踪还是单个 AWS 账户的跟踪，都要创建一个专用 Amazon S3 存储桶来存储该跟踪的日志文件。
- 如果您想记录多个 AWS 账户的活动，请修改存储桶策略以允许记录和存储您想要记录 AWS 账户活动的所有账户的日志 AWS 文件。
- 如果您没有使用组织跟踪记录，请在所有 AWS 账户中创建跟踪，同时在日志存档账户中指定 Simple Storage Service（Amazon S3）存储桶。

使用带有 AWS KMS 托管密钥的服务器端加密

默认情况下，传送 CloudTrail 到您的 S3 存储桶的日志文件使用服务器端加密和 KMS 密钥 (SSE-KMS) 进行加密。要将 SSE-KMS 与配合使用 CloudTrail，您需要创建并管理 KMS 密钥 AWS KMS key，也称为 KMS 密钥。

> **Note**
>
> 如果您使用 SSE-KMS 和日志文件验证，并且您已修改您的 Simple Storage Service（Amazon S3）存储桶策略以仅允许 SSE-KMS 加密文件，您将无法创建利用该存储桶的跟踪记录，除非您修改存储桶策略以专门允许 AES256 加密，如以下示例策略行所示。
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

以下是您可以采取的一些步骤：

- 查看使用 SSE-KMS 加密您的日志文件的优点。
- 创建一个 KMS 密钥用来加密日志文件。
- 为您的跟踪记录配置日志文件加密。
- 考虑实施持续的侦探控制，以帮助确保所有跟踪都使用中的规则使用 SSE-KMS 加密日志文件。cloud-trail-encryption-enabled AWS Config

将条件键添加到默认 Amazon SNS 主题策略

当您配置跟踪以向 Amazon SNS 发送通知时，CloudTrail 会在您的 SNS 主题访问策略中添加一条允许向 SNS 主题 CloudTrail 发送内容的策略声明。作为安全最佳实践，我们建议在 CloudTrail 策略声明中添加`aws:SourceArn`（或可选`aws:SourceAccount`）条件密钥。这有助于防止未经授权的账户访问您的 SNS 主题。有关更多信息，请参阅 Amazon SNS 主题政策 CloudTrail。

对您存储日志文件的 Simple Storage Service（Amazon S3）存储桶实施最低权限访问

CloudTrail 将事件跟踪到您指定的 Amazon S3 存储桶。这些日志文件包含 IAM 身份和 AWS 服务所采取的操作的审计日志。这些日志的完整性和完全性对于进行审计和取证至关重要。为了帮助确保完整性，在创建或修改对用于存储 CloudTrail 日志文件的任何 Amazon S3 存储桶的访问权限时，应遵守最低权限原则。

执行以下步骤：

- 查看您在其中存储日志文件的任何和所有存储桶的 Simple Storage Service（Amazon S3）存储桶策略，如有必要，可对其进行调整以删除任何不必要的访问权限。如果您使用 CloudTrail 控制台创建跟踪，则会为您生成此存储桶策略，但也可以手动创建和管理。
- 作为安全最佳实践，请务必手动将 `aws:SourceArn` 条件密钥添加到存储桶策略。有关更多信息，请参阅 适用于 Amazon S3 存储桶的政策 CloudTrail。
- 如果您使用同一 Amazon S3 存储桶来存储多个 AWS 账户的日志文件，请按照接收多个账户的日志文件的指导进行操作。
- 如果您使用组织跟踪记录，请确保遵循组织跟踪记录的指南，然后在 使用为组织创建跟踪 AWS Command Line Interface 中审核组织跟踪记录的 Simple Storage Service（Amazon S3）存储桶的策略示例。
- 查看 Simple Storage Service（Amazon S3）安全文档和用于保护存储桶的示例演练。

在存储日志文件的 Amazon S3 存储桶上启用 MFA 删除

配置多重身份验证（MFA）后，尝试更改存储桶版本控制状态或删除存储桶中的对象版本时，需要进行额外的身份验证。这样，即使某个用户获得有权永久删除 Amazon S3 对象的 IAM 用户的密码，您仍然能够防止可能破坏日志文件的操作。

以下是您可以采取的一些步骤：

- 请查看《Amazon Simple Storage Service 用户指南》中的 MFA 删除指南。
- 添加 Simple Storage Service（Amazon S3）存储桶策略以请求 MFA。

> **Note**
>
> 不能将 MFA 删除与生命周期配置一起使用。有关生命周期配置以及如何与其他配置交互的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的生命周期和其他存储桶配置。

配置存储日志文件的 Simple Storage Service（Amazon S3）存储桶上的生命周期管理

CloudTrail 跟踪的默认设置是无限期地将日志文件存储在为跟踪配置的 Amazon S3 存储桶中。您可以使用 Simple Storage Service（Amazon S3）对象生命周期管理规则来定义您自己的保留策略，以更好地满足您的业务和审计需求。例如，您可能要将时间超过一年的日志文件存档到 Amazon Glacier，或者在经过一定时间之后删除日志文件。

> **Note**
>
> 启用了多重身份验证（MFA）的存储桶上不支持生命周期配置。

限制对 AWSCloudTrail_FullAccess策略的访问权限

拥有该AWSCloudTrail_FullAccess策略的用户可以禁用或重新配置其 AWS 账户中最敏感和最重要的审计功能。本政策不打算被广泛共享或广泛应用于您 AWS 账户中的 IAM 身份。将本政策的适用范围限制在尽可能少的个人，即您希望担任 AWS 账户管理员的个人。

使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)

默认情况下，通过使用服务器端加密和 KMS 密钥 (SSE-KMS) 对传输 CloudTrail 到您的存储桶的日志文件进行加密。如果您未启用 SSE-KMS 加密，则您的日志将使用 SSE-S3 加密进行加密。

> **Note**
>
> 启用服务器端加密将使用 SSE-KMS 加密日志文件而不加密摘要文件。摘要文件使用 Simple Storage Service（Amazon S3）托管加密密钥（SSE-S3）加密。
> 如果您使用带有 S3 存储桶密钥的现有 S3 存储桶，则 CloudTrail 必须获得密钥策略中的许可才能使用 AWS KMS 操作`GenerateDataKey`和`DescribeKey`。如果未在密钥策略中授予 `cloudtrail.amazonaws.com` 这些权限，则无法创建或更新跟踪。

要将 SSE-KMS 与配合使用 CloudTrail，您需要创建并管理 KMS 密钥，也称为。AWS KMS key您可以为密钥附加策略，以确定哪些用户可以使用该密钥来加密和解密日志文件 CloudTrail 。通过 S3 可实现无缝解密。当密钥的授权用户读取 CloudTrail 日志文件时，S3 会管理解密，授权用户可以读取未加密形式的日志文件。

这种方法有以下优势：

- 您可以自行创建和管理 KMS 密钥加密密钥。
- 您可以使用单个 KMS 密钥对所有区域中的多个账户的日志文件进行加密和解密。
- 您可以控制谁可以使用您的密钥来加密和解密日志文件 CloudTrail 。您可以根据自己的要求，将密钥的权限分配给组织中的用户。
- 安全性更高。使用此功能时，为了读取日志文件，需要以下权限：
  - 用户必须对包含日志文件的存储桶具有 S3 读取权限。
  - 用户还必须应用了允许通过 KMS 密钥策略解密权限的策略或角色。
- 由于 S3 会自动解密来自有权使用 KMS 密钥的用户的请求的日志文件，因此日志文件的 SSE-KMS 加密与读取 CloudTrail 日志数据的应用程序向后兼容。 CloudTrail

> **Note**
>
> 您选择的 KMS 密钥必须与接收您的日志文件的 Amazon S3 存储桶在同一 AWS 区域创建。例如，如果日志文件将存储在美国东部（俄亥俄）区域的存储桶中，则必须在该区域中创建一个 KMS 密钥，或者选择一个在该区域中创建的 KMS 密钥。要验证 S3 存储桶的区域，请在 Simple Storage Service（Amazon S3）控制台中检查其属性。

启用日志文件加密

> **Note**
>
> 如果您在 CloudTrail 控制台中创建 KMS 密钥，则会为您 CloudTrail 添加所需的 KMS 密钥策略部分。如果您在 IAM 控制台中创建了密钥，或者 AWS CLI 需要手动添加所需的策略部分，请按照以下步骤操作。

要为 CloudTrail 日志文件启用 SSE-KMS 加密，请执行以下高级步骤：

1. 创建 KMS 密钥。

   - 有关使用创建 KMS 密钥的信息 AWS Management Console，请参阅AWS Key Management Service 开发人员指南中的创建密钥。
   - 有关使用创建 KMS 密钥的信息 AWS CLI，请参阅创建密钥。

   > **Note**
   >
   > 您选择的 KMS 密钥必须与接收日志文件的 S3 存储桶位于同一个区域。要验证某个 S3 存储桶的区域，请在 S3 控制台中检查该存储桶的属性。

2. 在密钥中添加 CloudTrail 允许加密和用户解密日志文件的策略部分。

   - 有关将包含在策略中的内容的信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

   > **Warning**
   >
   > 请务必在策略中为需要读取日志文件的所有用户包含解密权限。如果在将密钥添加到跟踪配置前未执行此步骤，则无解密权限的用户将无法读取加密的文件，直至您向他们授予这些权限。

   - 有关使用 IAM 控制台编辑策略的信息，请参阅 AWS Key Management Service 开发人员指南中的编辑密钥策略。
   - 有关使用将策略附加到 KMS 密钥的信息 AWS CLI，请参阅put-key-policy。

3. 更新您的跟踪以使用您修改其策略的 KMS 密钥 CloudTrail。

   - 要使用 CloudTrail 控制台更新您的跟踪配置，请参阅更新资源以使用 KMS 密钥。
   - 要使用更新您的跟踪配置 AWS CLI，请参阅使用启用和禁用 CloudTrail 日志文件加密 AWS CLI。

CloudTrail 还支持 AWS KMS 多区域密钥。有关多区域密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的使用多区域密钥。

下一节介绍与您的 KMS 密钥策略一起使用所需的策略部分 CloudTrail。

授予创建 KMS 密钥的权限

您可以授予用户使用该`AWSKeyManagementServicePowerUser`策略创建 AWS KMS key 的权限。

授予权限以创建 KMS 密钥

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 选择您要授予权限的组或用户。
3. 选择 Permissions，然后选择 Attach Policy。
4. 搜索 AWSKeyManagementServicePowerUser，选择该策略，然后选择 Attach policy（附加策略）。

   现在该用户有权创建 KMS 密钥了。有关创建策略的更多信息，请参阅 IAM 用户指南中的创建 IAM 策略。

为以下各项配置 AWS KMS 密钥策略 CloudTrail

您可以通过三种方式创建： AWS KMS key

- 控制 CloudTrail 台
- AWS 管理控制台
- 的 AWS CLI

> **Note**
>
> 如果您在 CloudTrail 控制台中创建 KMS 密钥，则会为您 CloudTrail 添加所需的 KMS 密钥策略。您无需手动添加策略声明。请参阅 在 CloudTrail 控制台中创建的默认 KMS 密钥策略。

如果您在 AWS 管理或中创建 KMS 密钥 AWS CLI，则必须在密钥中添加策略部分，以便可以将其与一起使用 CloudTrail。该策略必须 CloudTrail 允许使用密钥加密您的日志文件和事件数据存储，并允许您指定的用户读取未加密形式的日志文件。

请参阅以下资源：

- 要使用创建 KMS 密钥 AWS CLI，请参阅创建密钥。
- 要编辑的 KMS 密钥策略 CloudTrail，请参阅AWS Key Management Service 开发人员指南中的编辑密钥策略。
- 有关如何 CloudTrail 使用的技术细节 AWS KMS，请参阅《AWS Key Management Service 开发人员指南》 AWS KMS中的 “AWS CloudTrail 使用方式”。

与一起使用必填的 KMS 密钥策略部分 CloudTrail

如果您使用 AWS 管理控制台或创建了 KMS 密钥 AWS CLI，则必须至少在 KMS 密钥策略中添加以下语句才能使用 CloudTrail。

主题

- 跟踪所需的 KMS 密钥策略元素
- 事件数据存储所需的 KMS 密钥策略元素

跟踪所需的 KMS 密钥策略元素

1. 启用 CloudTrail 日志加密权限。请参阅 授予加密权限。
2. 启用 CloudTrail 日志解密权限。请参阅 授予解密权限。如果您通过 S3 存储桶密钥使用现有 S3 存储桶，则需要 `kms:Decrypt` 权限才能创建或更新启用了 SSE-KMS 加密的跟踪。
3. 启用 CloudTrail 以描述 KMS 密钥属性。请参阅 启用 CloudTrail 以描述 KMS 密钥属性。

作为安全最佳实践，请将 `aws:SourceArn` 条件密钥添加到 KMS 密钥策略。IAM 全局条件密钥`aws:SourceArn`有助于确保仅 CloudTrail 将 KMS 密钥用于特定的一个或多个跟踪。`aws:SourceArn` 的值始终是使用 KMS 密钥的跟踪记录 ARN（或跟踪记录 ARN 数组）。确保将 `aws:SourceArn` 条件密钥添加到现有跟踪记录的 KMS 密钥策略。

也支持 `aws:SourceAccount` 条件密钥，但不推荐使用。`aws:SourceAccount` 的值是跟踪记录拥有者的账户 ID，或用于企业跟踪记录的管理账户 ID。

> **Important**
>
> 向 KMS 密钥策略添加新部分时，不要更改策略中任何已存在的部分。
> 如果在跟踪上启用了加密，并且禁用了 KMS 密钥，或者 KMS 密钥策略配置不正确 CloudTrail，则 CloudTrail 无法传送日志。

事件数据存储所需的 KMS 密钥策略元素

1. 启用 CloudTrail 日志加密权限。请参阅 授予加密权限。
2. 启用 CloudTrail 日志解密权限。请参阅 授予解密权限。
3. 授予用户和角色使用 KMS 密钥对事件数据存储数据进行加密和解密的权限。

在您创建事件数据存储并使用 KMS 密钥对其进行加密时，或者针对使用 KMS 密钥加密的事件数据存储运行查询时，您应该拥有对 KMS 密钥的写入权限。KMS 密钥策略必须具有访问权限 CloudTrail，并且 KMS 密钥应可供对事件数据存储进行操作（例如查询）的用户管理。

4. 启用 CloudTrail 以描述 KMS 密钥属性。请参阅 启用 CloudTrail 以描述 KMS 密钥属性。

在适用于事件数据存储的 KMS 密钥策略中，不支持 `aws:SourceArn` 和 `aws:SourceAccount` 条件密钥。

> **Important**
>
> 向 KMS 密钥策略添加新部分时，不要更改策略中任何已存在的部分。
> 如果在事件数据存储上启用了加密，并且禁用或删除了 KMS 密钥，或者 KMS 密钥策略配置不正确 CloudTrail，则 CloudTrail无法将事件传送到您的事件数据存储。

授予加密权限

Example CloudTrail 允许代表特定账户加密日志

CloudTrail 需要明确的权限才能代表特定账户使用 KMS 密钥加密日志。要指定账户，请将以下所需语句添加到您的 KMS 密钥策略，并将 *account-id*、*region* 和 *trailName* 替换为与您的配置相应的值。您可以向该`EncryptionContext`部分添加其他账户 ID，使这些账户 CloudTrail 能够使用您的 KMS 密钥加密日志文件。

作为安全最佳实践，请将 `aws:SourceArn` 条件密钥添加到适用于跟踪的 KMS 密钥策略。IAM 全局条件密钥`aws:SourceArn`有助于确保仅 CloudTrail 将 KMS 密钥用于特定的一个或多个跟踪。

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
```

```
            "StringLike": {
                "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
            }
        }
}
```

用于加密 CloudTrail Lake 事件数据存储日志的 KMS 密钥的策略不能使用条件密钥`aws:SourceArn`或`aws:SourceAccount`。以下是适用于事件数据存储的 KMS 密钥策略的示例。

```
{
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

以下示例策略声明说明了另一个账户如何使用您的 KMS 密钥加密 CloudTrail 日志。

场景

- 您的 KMS 密钥位于账户 *111111111111* 中。
- 您和账户 *222222222222* 都将加密日志。

在该策略中，您将一个或多个使用您的密钥加密的账户添加到 CloudTrailEncryptionContext。这仅限 CloudTrail 于使用您的密钥加密您指定的账户的日志。如果向账户 *222222222222* 的根账户授予加密日志的权限时，会将权限委托给账户管理员，以便加密该账户中其他用户所需的权限。账户管理员只需更改与这些 IAM 用户关联的策略，即可实现此目的。

作为安全最佳实践，请将 `aws:SourceArn` 条件密钥添加到 KMS 密钥策略。IAM 全局条件密钥`aws:SourceArn`有助于确保仅对指定的跟踪 CloudTrail 使用 KMS 密钥。但事件数据存储的 KMS 密钥政策并不支持此条件。

KMS 密钥策略语句：

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

有关编辑用于的 KMS 密钥策略的更多信息 CloudTrail，请参阅 AWS Key Management Service 开发人员指南中的编辑密钥策略。

授予解密权限

在将 KMS 密钥添加到 CloudTrail 配置中之前，请务必向所有需要解密权限的用户授予解密权限。拥有加密权限但没有解密权限的用户无法读取加密日志。如果您通过 S3 存储桶密钥使用现有 S3 存储桶，则需要 `kms:Decrypt` 权限才能创建或更新启用了 SSE-KMS 加密的跟踪。

启用 CloudTrail 日志解密权限

必须授予密钥用户显式权限才能读取 CloudTrail 已加密的日志文件。为使用户能够读取加密日志，请向您的 KMS 密钥政策添加下面的必需语句（修改 `Principal` 部分，从而为您希望能够利用您的 KMS 密钥执行解密操作的每个主体添加一行）。

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
```

```
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

以下是允许 CloudTrail 服务主体解密跟踪日志所需的示例策略。

```
{
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

与 La CloudTrail ke 事件数据存储一起使用的 KMS 密钥的解密策略类似于以下内容。指定为 `Principal` 的值的用户或角色 ARN，需要解密权限才能创建或更新事件数据存储、运行查询或获取查询结果。

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

以下是允许 CloudTrail 服务主体解密事件数据存储日志所需的示例策略。

```
{
      "Sid": "Allow CloudTrail to decrypt an event data store",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

允许您账户中的用户使用您的 KMS 密钥解密跟踪日志

示例

此策略语句演示如何允许您账户中的用户或角色使用您的密钥读取您账户的 S3 存储桶中的加密日志。

Example 场景

- 您的 KMS 密钥、S3 存储桶以及 IAM 用户 Bob 均位于账户 *111111111111* 中。
- 您授予 IAM 用户 Bob 解密 S3 存储桶中 CloudTrail 日志的权限。

在密钥策略中，您可以为 IAM 用户 Bob 启用 CloudTrail 日志解密权限。

KMS 密钥策略语句：

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

允许其他账户中的用户使用您的 KMS 密钥解密跟踪日志

您可以允许其他账户中的用户使用您的 KMS 密钥解密跟踪日志，而非事件数据存储日志。需要对密钥策略执行的更改取决于 S3 存储桶位于您的账户还是其他账户中。

允许其他账户中的存储桶用户解密日志

示例

此策略声明演示如何让其他账户中的 IAM 用户或角色使用您的密钥读取其他账户的 S3 存储桶中的加密日志。

场景

- 您的 KMS 密钥位于账户 *111111111111* 中。
- IAM 用户 Alice 和 S3 存储桶均位于账户 *222222222222* 中。

在这种情况下，您 CloudTrail 授予解密账户下日志的权限*222222222222*，并授予 Alice 的 IAM 用户策略使用账户中的密钥*KeyA*的权限。*111111111111*

KMS 密钥策略语句：

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Alice 的 IAM 用户策略声明：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

允许其他账户中的用户解密您的桶中的跟踪日志

Example

此策略演示其他账户如何使用您的密钥读取您的 S3 存储桶中的加密日志。

Example 场景

- 您的 KMS 密钥和 S3 存储桶均位于账户 *111111111111* 中。
- 从您的存储桶读取日志的用户位于账户 *222222222222* 中。

要启用此场景，您需要为账户中的 IAM 角色CloudTrailReadRole启用解密权限，然后向其他账户授予代入该角色的权限。

KMS 密钥策略语句：

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRole信托实体政策声明：

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

有关编辑用于的 KMS 密钥策略的信息 CloudTrail，请参阅AWS Key Management Service 开发人员指南中的编辑密钥策略。

启用 CloudTrail 以描述 KMS 密钥属性

CloudTrail 需要能够描述 KMS 密钥的属性。要启用此功能，请将下面的必需语句原样添加到您的 KMS 密钥策略中。除了您指定的其他权限之外，此语句不授予 CloudTrail 任何权限。

作为安全最佳实践，请将 aws:SourceArn 条件密钥添加到 KMS 密钥策略。IAM 全局条件密钥aws:SourceArn有助于确保仅 CloudTrail 将 KMS 密钥用于特定的一个或多个跟踪。

```
{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

有关编辑 KMS 密钥策略的更多信息，请参阅 AWS Key Management Service 开发人员指南中的编辑密钥策略。

在 CloudTrail 控制台中创建的默认 KMS 密钥策略

如果您在 CloudTrail 控制台 AWS KMS key 中创建，则会自动为您创建以下策略。该策略允许以下权限：

- 允许 KMS 密钥的 AWS 账户 （根）权限。
- CloudTrail 允许加密 KMS 密钥下的日志文件并描述 KMS 密钥。
- 允许指定账户中的所有用户解密日志文件。
- 允许指定账户中的所有用户为 KMS 密钥创建 KMS 别名。
- 为创建跟踪的账户的账户 ID 启用跨账户日志解密。

主题

- CloudTrail Lake 事件数据存储的默认 KMS 密钥策略
- 用于跟踪的默认 KMS 密钥策略

CloudTrail Lake 事件数据存储的默认 KMS 密钥策略

以下是为您在 La CloudTrail k AWS KMS key e 中的事件数据存储中使用的默认策略。

```
{
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores. Created
 ${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
```

```
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

用于跟踪的默认 KMS 密钥策略

以下是为您在跟踪中使用的创建的默认策略。 AWS KMS key

> **Note**
>
> 该策略包含一条语句，允许使用 KMS 密钥跨账户解密日志文件。

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:root",
```

```
                    "arn:aws:iam::account-id:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
```

```
                }
            }
        }
    ]
}
```

更新资源以使用 KMS 密钥

在 AWS CloudTrail 控制台中，更新跟踪或事件数据存储以使用密 AWS Key Management Service 钥。请注意，使用自己的 KMS 密钥会产生加密和解密 AWS KMS 费用。有关更多信息，请参阅AWS Key Management Service 定价。

主题

- 更新跟踪以使用 KMS 密钥
- 更新事件数据存储以使用 KMS 密钥

更新跟踪以使用 KMS 密钥

要更新跟踪以使用您修改过的 CloudTrail，请在 CloudTrail 控制台中完成以下步骤。 AWS KMS key

> **Note**
>
> 按照以下过程更新跟踪将使用 SSE-KMS 加密日志文件，但不加密摘要文件。摘要文件使用 Simple Storage Service（Amazon S3）托管加密密钥（SSE-S3）加密。
> 如果您使用带有 S3 存储桶密钥的现有 S3 存储桶，则 CloudTrail 必须获得密钥策略中的许可才能使用 AWS KMS 操作`GenerateDataKey`和`DescribeKey`。如果未在密钥策略中授予 `cloudtrail.amazonaws.com` 这些权限，则无法创建或更新跟踪。

要使用更新跟踪 AWS CLI，请参阅使用启用和禁用 CloudTrail 日志文件加密 AWS CLI。

更新跟踪以使用 KMS 密钥

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 选择 Trails（跟踪记录），然后选择跟踪记录名称。
3. 在 General details（一般详细信息）中，选择 Edit（编辑）。

4. 对于 Log file SSE-KMS encryption（日志文件 SSE-KMS 加密），如果您希望使用 SSE-KMS 加密而非 SSE-S3 加密对您的日志文件进行加密，请选择 Enabled（已启用）。默认值为 Enabled（已启用）。如果您未启用 SSE-KMS 加密，则将使用 SSE-S3 加密对您的日志进行加密。有关 SSE-KMS 加密的更多信息，请参阅将服务器端加密与 AWS Key Management Service (SSE-KMS) 一起使用。有关 SSE-S3 加密的更多信息，请参阅配合使用服务器端加密与 Amazon S3 托管加密密钥（SSE-S3）。

   选择 Existing（现有）以使用 AWS KMS key更新您的跟踪。选择与接收日志文件的 S3 存储桶位于同一个区域的 KMS 密钥。要验证 S3 存储桶的区域，请在 S3 控制台中查看其属性。

   > **Note**
   >
   > 您也可以键入其他账户的密钥 ARN。有关更多信息，请参阅 更新资源以使用 KMS 密钥。密钥策略必须 CloudTrail 允许使用密钥加密您的日志文件，并允许您指定的用户读取未加密形式的日志文件。有关手动编辑密钥政策的信息，请参阅为以下各项配置 AWS KMS 密钥策略 CloudTrail。

   在 AWS KMS Ali as 中，按格式指定您更改策略以供使用的别名`alias/`*`MyAliasName`*。CloudTrail有关更多信息，请参阅 更新资源以使用 KMS 密钥。

   您可以键入别名、ARN 或全局唯一密钥 ID。如果该 KMS 密钥属于另一账户，请验证密钥策略对您授予了使用它的权限。值可以是以下格式之一：

   - 别名：`alias/`*`MyAliasName`*
   - 别名 ARN：`arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
   - 密钥 ARN：`arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-1234567890`
   - 全局唯一密钥 ID：`12345678-1234-1234-1234-123456789012`

5. 选择 Update trail（更新跟踪）。

   > **Note**
   >
   > 如果您选择的 KMS 密钥被禁用或正等待删除，则不能使用该 KMS 密钥保存跟踪。您可以启用该 KMS 密钥或选择另一个。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的密钥状态：对您的 KMS 密钥产生的影响。

更新事件数据存储以使用 KMS 密钥

要更新事件数据存储以使用您修改过的 CloudTrail，请在 CloudTrail 控制台中完成以下步骤。 AWS KMS key

要使用更新事件数据存储 AWS CLI，请参阅使用更新事件数据存储 AWS CLI。

> **Important**
>
> 禁用或删除 KMS 密钥或移除对密钥的 CloudTrail 权限可以 CloudTrail 防止将事件提取到事件数据存储中，并阻止用户查询使用该密钥加密的事件数据存储中的数据。在将事件数据存储与 KMS 密钥关联后，将无法移除或更改 KMS 密钥。在禁用或删除与事件数据存储配合使用的 KMS 密钥之前，请删除或备份您的事件数据存储。

更新事件数据存储以使用 KMS 密钥

1. 登录 AWS Management Console 并打开 CloudTrail 控制台，网址为 https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择 Lake 中的 Event data stores（事件数据存储）。选择要更新的事件数据存储。
3. 在 General details（一般详细信息）中，选择 Edit（编辑）。
4. 如果未启用加密选项，则选择使用自己的 AWS KMS key，以使用自己的 KMS 密钥来加密日志文件。

   选择 Existing（现有），以使用您的 KMS 密钥更新事件数据存储。选择与事件数据存储位于同一个区域内的 KMS 密钥。不支持来自其他账户的密钥。

   在 Enter AWS KMS Alias 中，按以下格式指定您更改策略以供使用的别名`alias/`*`MyAliasName`*。 CloudTrail有关更多信息，请参阅 更新资源以使用 KMS 密钥。

   您可以选择别名，也可以使用全局唯一的密钥 ID。值可以是以下格式之一：

   - 别名：`alias/`*`MyAliasName`*
   - 别名 ARN：`arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
   - 密钥 ARN：`arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-123456789`0
   - 全局唯一密钥 ID：`12345678-1234-1234-1234-123456789012`

5. 选择保存更改。

> **Note**
>
> 如果您选择的 KMS 密钥被禁用或正等待删除，则不能使用该 KMS 密钥来保存事件数据存储配置。您可以启用该 KMS 密钥，也可以选择另一个密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的密钥状态：对您的 KMS 密钥产生的影响。

使用启用和禁用 CloudTrail 日志文件加密 AWS CLI

本主题介绍如何使用启用和禁用 SSE-KMS 日志文件加密。 CloudTrail AWS CLI有关背景信息，请参阅使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)。

主题

- 使用启用 CloudTrail 日志文件加密 AWS CLI
- 使用禁用 CloudTrail 日志文件加密 AWS CLI

使用启用 CloudTrail 日志文件加密 AWS CLI

- 为跟踪启用日志文件加密
- 为事件数据存储启用日志文件加密

为跟踪启用日志文件加密

1. 使用 AWS CLI创建密钥。您创建的密钥必须与接收您的 CloudTrail 日志文件的 S3 存储桶位于同一区域。在此步骤中，您可以使用 AWS KMS create-key命令。
2. 获取现有的密钥策略，以便您可以对其进行修改以供使用 CloudTrail。您可以使用 AWS KMS get-key-policy命令检索密钥策略。
3. 在密钥策略中添加必填部分，以便 CloudTrail 可以加密和用户可以解密您的日志文件。确保为需要阅读日志文件的所有用户授予解密权限。请勿更改策略的现有部分。有关要包含的策略部分的信息，请参阅 为以下各项配置 AWS KMS 密钥策略 CloudTrail。
4. 使用 AWS KMS put-key-policy命令将修改后的 JSON 策略文件附加到密钥。
5. 使用`--kms-key-id`参数运行 CloudTrail `create-trail`或`update-trail`命令。此命令将启用日志加密。

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

--kms-key-id参数指定您修改其策略的密钥 CloudTrail。它可以是以下格式中的任意一种：

- 别名。例如：alias/MyAliasName
- 别名 ARN。例如：arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- 密钥 ARN。例如：arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012
- 全局唯一密钥 ID。例如：12345678-1234-1234-1234-123456789012

以下为响应示例：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "my-bucket-name"
}
```

如果存在 KmsKeyId 元素，则表示已启用日志文件加密功能。加密的日志文件应在 5 分钟左右出现在您的存储桶中。

为事件数据存储启用日志文件加密

1. 使用 AWS CLI创建密钥。您创建的密钥必须与事件数据存储位于同一区域。对于此步骤，请运行 AWS KMS create-key命令。
2. 获取要编辑的现有密钥策略以供使用 CloudTrail。您可以通过运行 AWS KMS get-key-policy命令来获取密钥策略。
3. 在密钥策略中添加必填部分，以便 CloudTrail 可以加密和用户可以解密您的日志文件。确保为需要阅读日志文件的所有用户授予解密权限。请勿更改策略的现有部分。有关要包含的策略部分的信息，请参阅 为以下各项配置 AWS KMS 密钥策略 CloudTrail。
4. 通过运行 AWS KMS put-key-policy命令将编辑后的 JSON 策略文件附加到密钥。

5. 运行 CloudTrail `create-event-data-store`或`update-event-data-store`命令，然后添加`--kms-key-id`参数。此命令将启用日志加密。

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

`--kms-key-id`参数指定您修改其策略的密钥 CloudTrail。它可以是以下四种格式中的任意一种：

- 别名。例如：`alias/MyAliasName`
- 别名 ARN。例如：`arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- 密钥 ARN。例如：`arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- 全局唯一密钥 ID。例如：`12345678-1234-1234-1234-123456789012`

以下为响应示例：

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

如果存在 KmsKeyId 元素，则表示已启用日志文件加密功能。加密的日志文件应在 5 分钟左右出现在您的事件数据存储中。

使用禁用 CloudTrail 日志文件加密 AWS CLI

要停止加密针对跟踪的日志，请运行 update-trail，并向 kms-key-id 参数传递一个空字符串：

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

以下为响应示例：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

如果不存在 KmsKeyId 值，则表示已停用日志文件加密功能。

> **Important**
>
> 您无法停止针对事件数据存储的日志文件加密。

文档历史记录

下表描述了对的文档所做的重要更改 AWS CloudTrail。要获得本文档的更新通知，您可以订阅 RSS 源。

- API 版本：2013-11-01
- 最新文档更新：2024-05-30

变更	说明	日期
已更新的文档	添加了描述如何使用高级事件选择器筛选数据事件的部分。有关更多信息，请参阅使用高级事件选择器筛选数据事件。	2024年5月29日
新增功能	现在，您可以使用高级事件选择器在 Amazon Kinesis Data Streams 流和直播使用者上记录 CloudTrail 数据事件。有关更多信息，请参阅数据事件。	2024年5月21日
已更新的文档	更新了CloudTrail 湖泊支持区域页面，添加了亚太地区（海得拉巴）区域（ap-south-2）、欧洲（苏黎世）区域（eu-central-2）和以色列（特拉维夫）区域（il-central-1）。	2024 年 5 月 16 日
新增功能	现在，您可以使用高级事件选择器在 AWS Step Functions 状态机上记录 CloudTrail 数据事件。有关更多信息，请参阅数据事件。	2024 年 5 月 16 日
已更新的文档	添加了有关使用查看 CloudTrail 成本和使用情况的部分 AWS Cost Explorer。有关更多	2024 年 5 月 14 日

	信息，请参阅使用查看您的 CloudTrail 费用和使用情况 AWS Cost Explorer。	
新增功能	现在，您可以使用高级事件选择器在 Amazon Q 应用程序上记录 CloudTrail 数据事件。有关更多信息，请参阅数据事件。	2024 年 5 月 1 日
已更新的文档	对用户指南部分和页面标题进行了总体组织改进，其中包括以下内容：将 CloudTrail 日志事件参考页面的标题更改为了解 CloudTrail 事件，并添加了对管理事件、数据事件和 Insights 事件的描述。将 “设置” 页面的标题更改为 CloudTrail “配置设置”。已将日志数据事件、日志管理事件和日志分析事件页面移至了解 CloudTrail 事件部分。已将CloudTrail日志文件示例页面移至CloudTrail 日志文件部分。添加了单独的页面，列出了 CloudTrail Lake 事件数据存储、查询和集成的 AWS CLI命令。	2024 年 4 月 10 日
已更新的文档	更新了支持CloudTrail 湖泊的区域页面，添加了欧洲（西班牙）区域 (eu-south-2)。	2024 年 4 月 10 日

增加了服务支持	此版本支持 AWS 控制目录。有关更多信息，请参阅日志控制目录 API 调用的AWS 服务主题 CloudTrail和使用的日志 AWS 控制目录 API 调用 AWS CloudTrail。	2024 年 4 月 8 日
增加了服务支持	此版本支持 AWS 截止日期云。有关更多信息，请参阅 AWS 服务 的主题 CloudTrail。	2024 年 4 月 2 日
新增功能	AWS CloudTrail 活动版本现在是 1.10。有关更多信息，请参阅CloudTrail 录制内容。	2024 年 3 月 26 日
增加了服务支持	此版本支持 AWS Billing Conductor。有关更多信息，请参阅AWS 服务 主题 CloudTrail和使用记录 AWS Billing Conductor API 调用 AWS CloudTrail。	2024 年 3 月 12 日
新增功能	现在，您可以使用高级事件选择器在 AWS X-Ray 跟踪和 AWS Systems Manager 托管节点上记录 CloudTrail 数据事件。有关更多信息，请参阅数据事件。	2024 年 3 月 7 日
新增功能	现在，您可以使用高级事件选择器在亚马逊简单工作流服务 (Amazon SWF) Simple SWF Service 域上记录 CloudTrail 数据事件。有关更多信息，请参阅数据事件。	2024年2月14日

新增功能	CloudTrail 添加了 `ListInsightsMetricData` API。`ListInsightsMetricData` API 会返回已启用 Insights 的跟踪的 Insights 指标数据。有关更多信息，请参阅 AWS CloudTrail API 参考ListInsightsMetricData中的。	2024年2月6日
新增功能	现在，您可以使用高级事件选择器记录 AWS IoT AWS IoT SiteWise、和 CloudTrail AWS AppConfig 的数据事件。有关更多信息，请参阅数据事件。	2024 年 1 月 4 日
新增功能	现在，您可以使用高级事件选择器记录 CloudTrail 数据事件。 AWS IoT Greengrass 有关更多信息，请参阅数据事件。	2023 年 12 月 22 日
新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即加拿大西部（卡尔加里）地区。有关更多信息，请参阅CloudTrail 支持的区域。	2023 年 12 月 20 日
新增功能	现在，您可以使用高级事件选择器记录亚马逊密钥空间（适用于 Apache Cassandra）、AWS IoT TwinMaker Amazon RDS CloudTrail 的数据事件。AWS Supply Chain 有关更多信息，请参阅数据事件。	2023 年 12 月 20 日

更新了 AWS 托管策略	更新了 CloudTrailServiceRolePolicy 托管策略，以允许在禁用联合身份验证时对组织事件数据存储执行以下操作：`glue:DeleteTable` 和 `lakeformation:DeregisterResource` 。	2023 年 11 月 26 日
新增功能	现在，您可以联合 CloudTrail 湖泊事件数据存储以查看与数据目录中的事件数据存储相关的元数据，并使用 Amazon Athena 对事件数据运行 SQL 查询。 AWS Glue 存储在 AWS Glue 数据目录中的表元数据让 Athena 查询引擎知道如何查找、读取和处理您要查询的数据。有关更多信息，请参阅联合事件数据存储。	2023 年 11 月 26 日
新增功能	现在，您可以使用高级事件选择器记录 CloudTrail 数据事件。 AWS Cloud Map 有关更多信息，请参阅记录数据事件。	2023 年 11 月 16 日
新增功能	现在，您可以使用高级事件选择器在 Amazon SQS 消息上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 11 月 16 日

新增功能	CloudTrail Lake 现在为事件数据存储提供两种定价选项：一年可延期保留定价和七年保留定价。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。在此版本之前，所有事件数据存储都使用七年期保留定价选项。您可以使用CloudTrail 控制台或 UpdateEventDataStoreAPI 操作将事件数据存储从使用七年保留定价选项切换为使用一年可延期保留定价选项。AWS CLI有关定价选项的更多信息，请参阅 AWS CloudTrail 定价和事件数据存储定价选项。	2023 年 11 月 15 日
新增功能	现在，你可以在 La CloudTrail ke 中收集 Insights 事件。AWS CloudTrail Insights 通过持续分析 CloudTrail 管理事件，帮助 AWS 用户识别和响应与 API 调用和 API 错误率相关的异常活动。要在 CloudTrail Lake 中收集 Insights 事件，您需要一个用于记录管理事件并启用 Insights 的源事件数据存储，以及一个目标事件数据存储库，用于根据源事件数据存储中的异常管理事件活动收集 Insights 事件。有关更多信息，请参阅为 CloudTrail Insights 事件创建事件数据存储和记录 Insights 事件。	2023 年 11 月 9 日

增加了服务支持	此版本支持 AWS Launch Wizard。有关更多信息，请参阅AWS 服务 主题 CloudTrail和使用记录 AWS Launch Wizard API 调用 AWS CloudTrail。	2023 年 11 月 8 日
增加了服务支持	此版本支持 Amazon Bedrock。有关更多信息，请参阅AWS 服务 主题 CloudTrail并使用记录 Amazon Bedrock API 调用 AWS CloudTrail。	2023 年 10 月 23 日
新增功能	现在，您可以使用高级事件选择器在 Amazon CodeWhisperer 自定义项上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 10 月 18 日
新增功能	现在，您可以使用高级事件选择器在 Amazon Timestream 数据库和表中记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 9 月 28 日
新增功能	现在，您可以使用高级事件选择器在 Amazon SNS 主题和平台终端节点上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 9 月 28 日
已更新的文档	添加了表格，显示 AWS Organizations 组织内的管理账户、委派管理员账户和成员账户可以执行的任务 CloudTrail。有关更多信息，请参阅组织的委托管理员。	2023 年 9 月 25 日

增加了服务支持	此版本支持 AWS Marketplace 协议。有关更多信息，请参阅 API 调用 CloudTrail和日志协议 API 调用的AWS 服务主题 AWS CloudTrail。	2023 年 9 月 1 日
新增功能	现在，您可以使用高级事件选择器在 Amazon Kinesis 视频流和亚马逊 SageMaker 终端节点上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 8 月 31 日
增加了服务支持	此版本支持 AWS 应用程序转换服务。 AWS 应用程序转换服务是用于.NET 的 AWS 微服务提取器等服务使用的后端服务。有关更多信息，请参阅 CloudTrail支持的服务和集成。	2023 年 8 月 26 日
新增功能	现在，您可以使用高级事件选择 AWS Private CA 器在 Active Directory 的 Connector 上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 8 月 24 日
已更新的文档	添加了新的 CloudTrail Lake 场景，以展示如何使用创建事件数据存储、查看 CloudTrail Lake 控制面板、将跟踪事件复制到事件数据存储、查看和运行示例查询，以及如何将查询结果保存到 Amazon S3 存储桶 AWS Management Console。有关更多信息，请参阅 CloudTrailLake 场景	2023 年 8 月 16 日

新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即以色列（特拉维夫）地区。有关更多信息，请参阅CloudTrail 支持的区域。	2023 年 8 月 1 日
增加了服务支持	此版本支持 AWS HealthImaging。有关更多信息，请参阅CloudTrail支持的服务和集成以及使用 AWS CloudTrail记录 AWS HealthImaging API 调用。	2023 年 7 月 26 日
新增功能	现在，您可以使用高级事件选择器在 AWS HealthImaging 数据存储中记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 7 月 26 日
新增功能	现在，您可以使用高级事件选择器在 AWS Systems Manager 控制通道和 Amazon Managed Blockchain 网络上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 6 月 21 日
新增功能	现在，您可以使用aws cloudtrail verify-query-results命令验证 CloudTrail Lake 保存的查询结果。有关更多信息，请参阅使用 AWS CLI验证保存的查询结果。	2023 年 6 月 21 日

增加了服务支持	此版本支持 Amazon Verified Permissions。有关更多信息，请参阅CloudTrail支持的服务和集成以及使用记录亚马逊已验证的权限 API 调用 AWS CloudTrail。	2023 年 6 月 13 日
新增功能	现在，您可以使用 CloudTrail Lake 仪表板在事件数据存储中可视化事件。有关更多信息，请参阅查看 Lake 控制面板。	2023 年 6 月 13 日
新增功能	现在，您可以使用高级事件选择器在 Amazon 验证权限策略存储中记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 6 月 13 日
新增功能	现在，您可以使用高级事件选择器在 Amazon CodeWhisperer 个人资料上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 6 月 6 日
新增功能	现在，您可以在事件数据存储上启动和停止 CloudTrail 事件摄取。有关使用控制台停止事件提取的信息，请参阅停止事件数据存储提取事件。有关使用停止事件摄取的信息 AWS CLI，请参阅停止对事件数据存储进行提取。	2023 年 6 月 2 日

新增功能	现在，您可以使用高级事件选择器在 Amazon EMR 预写日志工作空间上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 5 月 31 日
增加了服务支持	此版本支持 Amazon Security Lake。有关更多信息，请参阅CloudTrail支持的服务和集成以及使用记录 Amazon Security Lake API 调用 AWS CloudTrail。	2023 年 5 月 30 日
已更新的文档	更新了 CloudTrail 用户身份元素主题，增加了代表 IAM Identity Center 用户提出的请求的示例和字段描述。有关更多信息，请参阅 CloudTrail userIdentity 元素。	2023 年 5 月 23 日
已更新的文档	此更新支持 CloudTrail处理库的以下补丁版本： aws-cloudtrail-processing-library-1.6.1.jar。有关更多信息，请参阅上的 “使用 CloudTrail 处理库” 和 “CloudTrail 处理库” GitHub。	2023 年 5 月 23 日
新增功能	CloudTrail Lake 现在支持 Presto 的所有功能和运算符。有关更多信息，请参阅 L CloudTrail ake SQL 限制。	2023 年 5 月 9 日

新增功能	现在，您可以使用高级事件选择器在 Amazon GuardDuty 探测器上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件和使用记录 Amazon GuardDuty API 调用 AWS CloudTrail。	2023 年 3 月 30 日
已更新的文档	添加了新章节，旨在介绍如何为事件数据存储创建用户定义的成本分配标签。有关更多信息，请参阅为 CloudTrail Lake 事件数据存储创建用户定义的成本分配标签。	2023 年 3 月 24 日
增加了服务支持	此版本支持 AWS 电信网络生成器 (AWS TNB)。有关更多信息，请参阅CloudTrail支持的服务和集成以及使用记录 AWS Telco Network Builder API 调用。 AWS CloudTrail	2023 年 2 月 21 日
新增功能	现在，您可以使用高级事件选择器在 Amazon Cognito 身份池上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 2 月 15 日
已更新的文档	添加了有关 La CloudTrail ke 可用学习资源的新章节。有关更多信息，请参阅学习资源。	2023 年 2 月 9 日

新增功能	现在，您可以使用外部的事件源创建 CloudTrail Lake 集成。AWS您可以记录和存储来自您的混合环境中任何来源的用户活动数据，如本地或云中托管的内部或 SaaS 应用程序、虚拟机或容器。有关更多信息，请参阅创建与 AWS外部事件源的集成。	2023 年 1 月 31 日
新增功能	现在，您可以使用高级事件选择器记录有关 CloudTrail 湖泊频道 CloudTrail `PutAuditEvents` 活动的 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2023 年 1 月 31 日
新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即亚太地区（墨尔本）地区。有关更多信息，请参阅CloudTrail 支持的区域。	2023 年 1 月 24 日
已更新的文档	中添加了有关管理数据一致性的新章节 CloudTrail，请参阅中的管理数据一致性 CloudTrail。	2023 年 1 月 18 日
新增功能	现在，您可以使用高级事件选择器在 Amazon SageMaker 功能库中记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2022 年 12 月 27 日

增加了服务支持	此版本支持 AWS Marketplace Discovery。请参阅 AWS CloudTrail 支持的服务和集成。	2022 年 12 月 15 日
新增功能	现在，您可以使用高级事件选择器在 Amazon SageMaker 指标实验试用组件上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2022 年 12 月 15 日
新增功能	现在，您可以创建包含 AWS Config 配置项目的事件数据存储，并使用事件数据存储来调查对生产环境的不合规更改。有关更多信息，请参阅为 AWS Config 配置项目创建事件数据存储。	2022 年 11 月 28 日
新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即亚太地区（海得拉巴）地区。有关更多信息，请参阅CloudTrail 支持的区域。	2022 年 11 月 22 日
新增功能	现在，您可以使用高级事件选择器记录 Amazon FinSpace 环境中的 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2022 年 11 月 18 日
新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即欧洲（西班牙）地区。有关更多信息，请参阅CloudTrail 支持的区域。	2022 年 11 月 16 日

新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即欧洲（苏黎世）地区。有关更多信息，请参阅CloudTrail 支持的区域。	2022 年 11 月 9 日
新增功能	AWS Organizations 组织的管理账户现在可以添加委派管理员来管理该组织的 CloudTrail 跟踪和事件数据存储。有关更多信息，请参阅组织的委托管理员。	2022 年 11 月 7 日
新增功能	现在，您可以为 CloudTrail Lake 事件数据存储启用 AWS Key Management Service 加密。有关更多信息，请参阅创建事件数据存储。	2022 年 11 月 7 日
新增功能	现在，您可以在运行查询时将 CloudTrail Lake 查询结果保存到 Amazon S3 存储桶中。有关运行查询的更多信息，请参阅 Run a query and save query results（运行查询并保存查询结果）。有关下载查询结果的更多信息，请参阅 Get and download saved query results（获取和下载已保存的查询结果）。	2022 年 10 月 21 日
新增功能	现在，您可以将 CloudTrail 跟踪事件复制到 CloudTrail Lake 事件数据存储中。有关更多信息，请参阅将跟踪事件复制到 CloudTrail Lake。	2022 年 9 月 19 日

已更新的文档	添加了 L CloudTrail ake 支持的亚马逊 CloudWatch 指标列表。有关更多信息，请参阅支持的 CloudWatch 指标。	2022 年 9 月 16 日
新增功能	现在，您可以使用查看 CloudTrail 与服务相关的频道。 AWS CLI有关更多信息，请参阅使用查看服务相关频道。 CloudTrail AWS CLI	2022 年 9 月 9 日
新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即中东 (UAE) 地区。有关更多信息，请参阅CloudTrail 支持的区域。	2022 年 8 月 30 日
更改的功能	CloudTrail 已将托管策略的名称更改`AWSCloudTrailReadOnlyAccess` 为`AWSCloudTrail_ReadOnlyAccess` 。此策略中的权限范围已缩小。默认情况下，该策略不再授予列出所有 Amazon S3 存储桶、 AWS Lambda 函数或 AWS KMS 别名的权限。有关更多信息，请参阅只读访问权限。	2022 年 6 月 6 日

更改的功能	作为安全最佳实践，现在您可以将 `aws:SourceArn` 或 `aws:SourceAccount` 条件密钥添加到 Simple Storage Service（Amazon S3）存储桶策略中的 `s3:GetBucketAcl` ACL 检查数据块。有关更多信息，请参阅为其配置 Amazon S3 存储桶策略 CloudTrail。	2022 年 5 月 11 日
更改的功能	从 2022 年 2 月 24 日起，在任何源于使用代理客户端的 AWS Management Console 会话的事件中，都 AWS CloudTrail 开始更改`userAgent` 和`sourceIPAddress` 字段的值。对于这些事件，CloudTrail将`userAgent` 和`sourceIPAddress` 字段的值替换为`AWS Internal`。CloudTrail进行了此项更改，以标准化其在所有 AWS 服务中记录服务操作信息的方式。有关更多信息，请参阅CloudTrail 录制内容。	2022 年 4 月 12 日
增加了服务支持	此版本支持 Amazon GameSparks。请参阅 AWS CloudTrail 支持的服务和集成。	2022 年 3 月 24 日
增加了服务支持	此版本支持 E AWS App Mesh nvoy 管理服务。请参阅 AWS CloudTrail 支持的服务和集成。	2022 年 3 月 18 日

已更新的文档	已为 L CloudTrail ake 添加了新的查询示例，这是一项新功能，可让您对事件运行精细的多字段 SQL 查询。此外，已向 `DescribeQuery` 和 `GetQueryResults` 操作的查询元数据结果添加新的字段 `BytesScanned` 。有关更多信息，请参阅使用 CloudTrail Lake。	2022 年 3 月 4 日
更改的功能	CloudTrail 现在，如果满足以下两个条件，则会在数据事件`resources` 块中移除 Amazon S3 存储桶拥有者的账户 ID：数据事件 API 调用来自与 Amazon S3 存储桶拥有者不同的 AWS 账户，API 调用者收到了仅针对调用者账户的`AccessDenied` 错误。有关更多信息，请参阅为其他账户调用的数据事件修订存储桶拥有者账户 ID。	2022 年 3 月 3 日
已更新的文档	此更新支持 CloudTrail 处理库的以下版本：增加了对实现自定义 S3 管理器的支持，增加了对记录文件解析相关异常的事件的支持，支持解析中的可选`errorCode` 字段`insightDetails` ，并更新了账户 ID 解析正则表达式以接受非数字值。有关更多信息，请参阅上的“使用 CloudTrail 处理库”和“CloudTrail处理库” GitHub。	2022 年 1 月 28 日

新增功能	CloudTrail 引入了 CloudTrail Lake，这是一项新功能，可让您对事件运行细粒度的多字段 SQL 查询。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。有关更多信息，请参阅使用 CloudTrail Lake。	2022 年 1 月 5 日
新区域支持	CloudTrail 将支持范围扩大到一个新的区域，即亚太地区（雅加达）区域。有关更多信息，请参阅CloudTrail 支持的区域。	2021 年 12 月 13 日
增加了服务支持	此版本支持 Amazon WorkSpaces Web。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 12 月 3 日
新增功能	现在，您可以使用高级事件选择器在 Lake Formation 创建的 AWS Glue 表上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2021 年 11 月 30 日
更改的功能	作为安全最佳实践，您现在可以在密钥策略和 Amazon S3 存储桶策略中添加`aws:SourceArn` 或`aws:SourceAccount` 条件 AWS KMS 密钥。有关更多信息，请参阅为配置 AWS KMS 密钥策略 CloudTrail和配置 Amazon S3 存储桶策略 CloudTrail。	2021 年 11 月 15 日

增加了服务支持	此版本支持 AWS 弹性中心。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 11 月 10 日
新增功能	提供了一个新的 CloudTrail Insights 事件类型：错误率 Insights 事件。错误率 Insights 事件捕获您账户中 API 调用上发生的错误的异常活动。有关更多信息，请参阅记录跟踪记录的 Insights 事件。	2021 年 11 月 10 日
新增功能	现在，您可以使用高级事件选择器在 DynamoDB 流上记录 CloudTrail 数据事件。有关更多信息，请参阅记录数据事件。	2021 年 9 月 22 日
新增功能	现在，您可以记录 Simple Storage Service（Amazon S3）接入点上的数据事件。您可以使用高级事件选择器记录 Simple Storage Service（Amazon S3）接入点数据事件。有关更多信息，请参阅记录数据事件。	2021 年 8 月 24 日

更改的功能	当您配置跟踪以向 Amazon SNS 发送通知时，CloudTrail 会在您的 SNS 主题访问策略中添加一条允许向 SNS 主题 CloudTrail 发送内容的策略声明。作为安全最佳实践，我们建议在 CloudTrail 策略声明中添加`aws:SourceArn` 或`aws:SourceAccount` 条件密钥。有关更多信息，请参阅 Amazon SNS 主题政策。 CloudTrail	2021 年 8 月 16 日
增加了服务支持	此版本支持 Amazon Route 53 应用程序恢复控制器。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 7 月 27 日
新增功能	现在，您可以记录在 EBS 快照上运行的 Amazon EBS 直接 API 的数据事件。您可以使用高级事件选择器记录 Amazon EBS 直接 API 数据事件。有关更多信息，请参阅记录数据事件。	2021 年 7 月 27 日
更改的功能	CloudTrail 处理数据事件时，它会保留原始格式的数字，无论是整数 () 还是整数 (`int`)。`float`在数据事件字段中包含整数的事件中，CloudTrail 历史上会将这些数字作为浮点数进行处理。现在，CloudTrail 保留数据事件中整数的原始格式。有关更多信息，请参阅使用 CloudTrail 处理库。	2021 年 7 月 13 日

新增功能	现在，您可以从跟踪记录中排除 Amazon RDS 数据 API 管理事件。有关更多信息，请参阅记录跟踪的管理事件。	2021 年 7 月 1 日
增加了服务支持	此版本支持 AWS BugBust。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 6 月 24 日
增加了服务支持	此版本支持 Amazon Managed Grafana 和 Amazon Managed Service for Prometheus。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 6 月 2 日
增加了服务支持	此版本支持 AWS App Runner。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 5 月 18 日
增加了服务支持	此版本支持 AWS Systems Manager 事件管理器。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 5 月 10 日
已更新的文档	此更新描述了 AWS Config 一致性包的数据事件记录要求，尤其是 HIPAA 或 FedRAMP 等合规框架。有关更多信息，请参阅记录数据事件。	2021 年 5 月 7 日
增加了服务支持	此版本支持 Service Quotas 和 Amazon EBS 直接 API。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 4 月 13 日

新增功能	在 IAM 管理员进行配置后 AWS STS，当用户担任 IAM 角色或使用代入的角色执行任何操作时，将`sourceIdentity` 信息 CloudTrail 记录在事件中。有关更多信息，请参阅 CloudTrail userIdentity 元素。	2021 年 4 月 13 日
已更新的文档	此更新记录了某些 CloudTrail事件记录字段中内容的限制（以千字节 (KB) 为单位）。有关更多信息，请参阅CloudTrail 录制内容。	2021 年 4 月 8 日
新增功能	在 IAM 管理员进行配置后 AWS STS，当用户担任 IAM 角色或使用代入的角色执行任何操作时，将`sourceIdentity` 信息 CloudTrail 记录在事件中。有关更多信息，请参阅 CloudTrail userIdentity 元素。	2021 年 4 月 6 日
新增功能	现在，您可以记录 Amazon DynamoDB 表上的数据事件。您可以使用事件选择器或高级事件选择器记录 DynamoDB 数据事件。有关更多信息，请参阅记录数据事件。	2021 年 3 月 23 日
增加了服务支持	此版本支持 Amazon Managed Workflows for Apache Airflow。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 3 月 22 日

新增功能	如果您选择使用高级事件选择器，则您现在可以记录 S3 对象 Lambda 接入点上的数据事件。有关更多信息，请参阅记录数据事件。	2021 年 3 月 18 日
增加了服务支持	此版本支持 AWS 故障注入模拟器。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 3 月 15 日
新增功能	如果您选择使用高级事件选择器，则您现在可以记录 Amazon Managed Blockchain 中的 Ethereum 节点上的数据事件。有关更多信息，请参阅记录数据事件。	2021 年 3 月 1 日
增加了服务支持	此版本支持 Amazon Managed Blockchain 以及预览版 Ethereum for Managed Blockchain。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 2 月 4 日
增加了服务支持	此版本支持 AWS Amplify。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 2 月 3 日
增加了服务支持	此版本支持 Amazon Lookout for Metrics。请参阅 AWS CloudTrail 支持的服务和集成。	2021 年 2 月 1 日

已更新的文档	此更新支持 CloudTrail 处理库的以下补丁版本：更新用户指南中的.jar 文件引用以使用最新版本 aws-cloudtrail-processing-library -1.4.0.jar。有关更多信息，请参阅上的“使用 CloudTrail 处理库”和“CloudTrail处理库” GitHub。	2021 年 1 月 12 日
新增功能	现在，您可以记录 AWS Outposts上的 Simple Storage Service（Amazon S3）的数据事件。有关更多信息，请参阅记录数据事件。	2020 年 12 月 21 日
增加了服务支持	此版本支持 Amazon Lookout for Equi AWS Well-Architected Tool pment 和亚马逊定位服务。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 12 月 16 日
增加了服务支持	此版本支持 AWS IoT Greengrass V2。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 12 月 15 日
增加了服务支持	此版本支持 Amazon EMR on EKS。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 12 月 10 日
增加了服务支持	此版本支持 Audi AWS t Manager 和 Amazon HealthLake。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 12 月 8 日

增加了服务支持	此版本支持 Amazon Lookout for Vision。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 12 月 1 日
新增功能	AWS CloudTrail 活动版本现在是 1.08。版本 1.08 为引入了新的字段。 CloudTrail有关更多信息，请参阅CloudTrail 录制内容。	2020 年 11 月 24 日
新增功能	AWS CloudTrail 为数据事件引入了高级事件选择器。高级事件选择器允许更精细地控制记录到跟踪中的数据事件。您可以包含或排除特定 AWS 资源的数据事件，并在这些资源上选择特定 API 以记录到您的跟踪。有关更多信息，请参阅记录数据事件。	2020 年 11 月 24 日
增加了服务支持	此版本支持 AWS Network Firewall。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 11 月 17 日
增加了服务支持	此版本支持 T AWS rusted Advisor。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 10 月 22 日
已更新的文档	为根用户登录事件添加了两个新的事件记录示例。有关更多信息，请参阅 AWS 控制台登录事件。	2020 年 10 月 13 日

更改的功能	`AWSCloudTrail_FullAccess` 策略中的权限已缩小范围。此策略不再允许您删除 Amazon SNS 主题或 Simple Storage Service（Amazon S3）存储桶，并且移除了 `getObject` 操作。有关更多信息，请参阅为 CloudTrail 用户授予自定义权限。	2020 年 9 月 29 日
已更新的文档	此更新支持 CloudTrail 处理库的以下补丁版本：更新用户指南中的.jar 文件引用以使用最新版本 aws-cloudtrail-processing-library -1.3.0.jar。有关更多信息，请参阅上的“使用 CloudTrail 处理库” 和“CloudTrail处理库” GitHub。	2020 年 8 月 28 日
增加了服务支持	此版本支持 AWS Outposts。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 8 月 28 日
新增功能	AWS CloudTrail Insights 为 CloudTrail 洞察事件引入了归因字段 归因字段显示与触发 Insights 事件的异常活动相关的排名靠前的用户身份、用户代理和错误代码。为便于比较，归因字段还显示与正常活动或基线活动相关的排名靠前的用户身份、用户代理和错误代码。有关更多信息，请参阅记录跟踪的 Insights 事件。	2020 年 8 月 13 日

新增功能	该 AWS CloudTrail 控制台采用了全新的外观，旨在使其更易于使用。 AWS CloudTrail 用户指南已更新，其中包含有关如何在控制台中执行任务（例如创建跟踪、更新跟踪和下载事件历史记录）的过程的更改。	2020 年 8 月 13 日
增加了服务支持	此版本支持 Amazon Interactive Video Service。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 7 月 15 日
增加了服务支持	此版本支持 Amazon Honeycode。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 6 月 24 日
增加了服务支持	此版本支持 Amazon Macie。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 5 月 19 日
增加了服务支持	此版本支持 Amazon Kendra。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 5 月 13 日
增加了服务支持	此版本支持 AWS IoT SiteWise。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 4 月 29 日
增加了区域支持	此版本支持一个附加区域：欧洲地区（米兰）。请参阅 AWS CloudTrail 支持的区域。	2020 年 4 月 28 日

增加了服务和区域支持	此版本支持 Amazon AppFlow。请参阅 AWS CloudTrail 支持的服务和集成。此外，还增加了对非洲（开普敦）区域的支持。请参阅 AWS CloudTrail 支持的区域。	2020 年 4 月 22 日
新增功能	诸如`EncryptDecrypt`、和之类的大容量 AWS KMS 操作现在`GenerateDataKey` 被记录为读取事件。如果您选择记录跟踪中的所有 AWS KMS 事件，并选择记录写入管理事件，则您的跟踪会记录相关 AWS KMS 操作`Disable`，例如、`Delete`和`ScheduleKey` 。	2020 年 4 月 7 日
增加了服务支持	此版本支持 Amazon CodeGuru Reviewer。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 2 月 7 日
增加了服务支持	本版本支持 Amazon Managed Apache Cassandra Service。请参阅 AWS CloudTrail 支持的服务和集成。	2020 年 1 月 17 日
增加了服务支持	此版本支持 Amazon Connect。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 12 月 13 日

已更新的文档	此更新支持 CloudTrail 处理库的以下补丁版本：更新用户指南中的.jar 文件引用以使用最新版本 aws-cloudtrail-processing-library -1.2.0.jar。有关更多信息，请参阅上的“使用 CloudTrail 处理库”和“CloudTrail处理库” GitHub。	2019 年 11 月 21 日
新增功能	此版本支持 AWS CloudTrail Insights，可帮助您检测账户中的异常活动。请参阅记录跟踪的 Insights 事件。	2019 年 11 月 20 日
新增功能	此版本添加了一个用于从跟踪中筛选 AWS Key Management Service 事件的选项。创建跟踪。	2019 年 11 月 20 日
增加了服务支持	此版本支持 AWS CodeStar 通知。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 11 月 7 日
新增功能	无论您使用 CloudTrail 控制台还是 API CloudTrail，此版本都支持在中创建跟踪时添加标签。此版本添加了两个新的 API，`GetTrail` 和 `ListTrails` 。	2019 年 11 月 1 日
增加了服务支持	此版本支持 AWS App Mesh。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 10 月 17 日
增加了服务支持	此版本支持 Amazon Translate。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 10 月 17 日

文档更新	“不支持的服务” 主题已恢复并更新，仅包括那些当前未在 CloudTrail其中记录事件的 AWS 服务。请参阅 CloudTrail 不支持的服务。	2019 年 10 月 7 日
文档更新	该文档已更新，其中包含对 `AWSCloudTrailFullAccess` 策略的更改。已更新一个策略示例，该示例显示了与 `AWSCloudTrailFullAccess` 等效的权限，以将可对其执行 `iam:PassRole` 操作的资源限制为那些与以下条件语句匹配的资源：`"iam:PassedToService": "cloudtrail.amazonaws.com"` 。请参阅 AWS CloudTrail 基于身份的策略示例。	2019 年 9 月 24 日
文档更新	文档已更新为新主题 “管理 CloudTrail 成本”，以帮助您在预算范围内获取所需的日志数据。 CloudTrail	2019 年 9 月 3 日
增加了服务支持	此版本支持 AWS Control Tower。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 8 月 13 日
增加了区域支持	此版本支持一个附加区域：中东（巴林）。请参阅 AWS CloudTrail 支持的区域。	2019 年 7 月 29 日

文档更新	文档已更新，其中包含有关安全性的信息 CloudTrail。请参阅 AWS CloudTrail中的安全性。	2019 年 7 月 3 日
增加了服务支持	此版本支持 AWS Ground Station。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 6 月 6 日
增加了服务支持	此版本支持 AWS IoT Things Graph。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 6 月 4 日
增加了服务支持	此版本支持 Amazon AppStream 2.0。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 4 月 25 日
增加了区域支持	此版本支持一个附加区域：亚太地区（香港）。请参阅 AWS CloudTrail 支持的区域。	2019 年 4 月 24 日
增加了服务支持	本版本支持适用于 Apache Flink 的亚马逊托管服务。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 3 月 22 日
增加了服务支持	此版本支持 AWS Backup。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 2 月 4 日
增加了服务支持	此版本支持 Amazon WorkLink。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 1 月 23 日

增加了服务支持	此版本支持 AWS Cloud9。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 1 月 21 日
增加了服务支持	此版本支持 AWS Elemental MediaLive。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 1 月 19 日
增加了服务支持	此版本支持 Amazon Comprehend。请参阅 AWS CloudTrail 支持的服务和集成。	2019 年 1 月 18 日
增加了服务支持	此版本支持 AWS Elemental MediaPackage。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 12 月 21 日
增加了区域支持	此版本支持一个附加区域：欧洲（斯德哥尔摩）。请参阅 AWS CloudTrail 支持的区域。	2018 年 12 月 11 日
文档更新	文档已使用有关受支持和不受支持的服务的信息进行更新。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 12 月 3 日
增加了服务支持	此版本支持 Res AWS ource Access Manager (AWS RAM)。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 11 月 20 日
更新了功能	此版本支持在中 CloudTrail 创建用于记录组织中所有 AWS 账户的事件的跟踪 AWS Organizations。请参阅为组织创建跟踪。	2018 年 11 月 19 日

增加了服务支持	此版本支持 Amazon Pinpoint SMS 和语音 API。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 11 月 16 日
增加了服务支持	此版本支持 AWS IoT Greengrass。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 10 月 29 日
已更新的文档	此更新支持 CloudTrail 处理库的以下补丁版本：更新用户指南中的.jar 文件引用以使用最新版本 aws-cloudtrail-processing-library -1.1.3.jar。有关更多信息，请参阅上的“使用 CloudTrail 处理库”和“CloudTrail处理库” GitHub。	2018 年 10 月 18 日
新增功能	此版本支持在 Event history (事件历史记录) 中使用额外的筛选条件。请参阅在 CloudTrail 控制台中查看 CloudTrail 事件。	2018 年 10 月 18 日
新增功能	此版本支持使用 Amazon Virtual Private Cloud (Amazon VPC) 在您的 VPC 与 AWS CloudTrail之间建立私有连接。参见AWS CloudTrail 与接口 VPC 终端节点配合使用。	2018 年 8 月 9 日
增加了服务支持	此版本支持 Amazon Data Lifecycle Manager。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 7 月 24 日

增加了服务支持	此版本支持 Amazon MQ。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 7 月 19 日
增加了服务支持	此版本支持 AWS 移动 CLI。请参阅 AWS CloudTrail 支持的服务和集成。	2018 年 6 月 29 日
AWS CloudTrail 可通过 RSS 提要获取文档历史记录通知	现在，您可以通过订阅 RSS 提要来接收有关 AWS CloudTrail 文档更新的通知。	2018 年 6 月 29 日

早期更新

下表描述了 2018 年 6 月 29 日 AWS CloudTrail 之前的文档发布历史。

更改	描述	发行日期
增加了服务支持	此版本支持 Amazon RDS Performance Insights。有关更多信息，请参阅CloudTrail 支持的服务和集成。	2018 年 6 月 21 日
新增功能	此版本支持在事件历史记录中记录所有 CloudTrail 管理事件。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。	2018 年 6 月 14 日
增加了服务支持	此版本支持 AWS Billing and Cost Management。请参阅 CloudTrail 支持的服务和集成。	2018 年 6 月 7 日
增加了服务支持	此发布版支持 Amazon Elastic Container Service for Kubernetes (Amazon EKS)。请参阅 CloudTrail 支持的服务和集成。	2018 年 6 月 5 日
已更新的文档	此更新支持 CloudTrail处理库的以下补丁版本： • 更新用户指南中的.jar 文件引用以使用最新版本 aws-cloudtrail-processing-library -1.1.2.jar。	2018 年 5 月 16 日

更改	描述	发行日期
	有关更多信息，请参阅上使用 CloudTrail 处理库的“CloudTrail 处理库” GitHub。	
增加了服务支持	此版本支持 AWS Billing and Cost Management。请参阅 CloudTrail 支持的服务和集成。	2018 年 6 月 7 日
增加了服务支持	此发布版支持 Amazon Elastic Container Service for Kubernetes (Amazon EKS)。请参阅 CloudTrail 支持的服务和集成。	2018 年 6 月 5 日
已更新的文档	此更新支持 CloudTrail处理库的以下补丁版本： • 更新用户指南中的.jar 文件引用以使用最新版本 aws-cloudtrail-processing-library -1.1.2.jar。 有关更多信息，请参阅上使用 CloudTrail 处理库的“CloudTrail 处理库” GitHub。	2018 年 5 月 16 日
增加了服务支持	此版本支持 AWS X-Ray。请参阅 CloudTrail 支持的服务和集成。	2018 年 4 月 25 日
增加了服务支持	此版本支持 AWS IoT 分析。请参阅 CloudTrail 支持的服务和集成。	2018 年 4 月 23 日
增加了服务支持	此版本支持 Secrets Manager。请参阅 CloudTrail 支持的服务和集成。	2018 年 4 月 10 日
增加了服务支持	此版本支持 Amazon Rekognition。请参阅 CloudTrail 支持的服务和集成。	2018 年 4 月 6 日
增加了服务支持	此版本支持 AWS 私有证书颁发机构 (PCA)。请参阅 CloudTrail 支持的服务和集成。	2018 年 4 月 4 日

更改	描述	发行日期
新增功能	此版本支持使用 Amazon Athena 更轻松地搜索 CloudTrail 日志文件。您可以直接从 CloudTrail 控制台自动创建用于查询日志的表，并使用这些表在 Athena 中运行查询。有关更多信息，请参阅CloudTrail 支持的服务和集成和在 CloudTrail控制台中创建 CloudTrail 日志表。	2018 年 3 月 15 日
增加了服务支持	此版本支持 AWS AppSync。请参阅 CloudTrail 支持的服务和集成。	2018 年 2 月 13 日
增加了区域支持	此版本支持一个附加区域：ap-northeast-3，亚太地区（大阪）。请参阅 CloudTrail 支持的区域。	2018 年 2 月 12 日
增加了服务支持	此版本支持 AWS Shield。请参阅 CloudTrail 支持的服务和集成。	2018 年 2 月 12 日
增加了服务支持	此版本支持 Amazon SageMaker。请参阅 CloudTrail 支持的服务和集成。	2018 年 1 月 11 日
增加了服务支持	此版本支持 AWS Batch。请参阅 CloudTrail 支持的服务和集成。	2018 年 1 月 10 日
新增功能	此版本支持将活动历史记录中 CloudTrail 可用的账户活动时间延长至 90 天。您还可以自定义列的显示以改善 CloudTrail 事件的视图。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。	2017 年 12 月 12 日
增加了服务支持	此版本支持 Amazon WorkMail。请参阅 CloudTrail 支持的服务和集成。	2017 年 12 月 12 日
增加了服务支持	此版本支持 Alexa for Business AWS Elemental MediaConvert、 AWS Elemental MediaStore和。请参阅 CloudTrail 支持的服务和集成。	2017 年 12 月 1 日
增加了功能和文档	此版本支持记录 AWS Lambda 函数的数据事件。 有关更多信息，请参阅 记录数据事件。	2017 年 11 月 30 日

更改	描述	发行日期
增加了功能和文档	此版本支持记录 AWS Lambda 函数的数据事件。 有关更多信息，请参阅 记录数据事件。	2017 年 11 月 30 日
增加了功能和文档	此版本支持对 CloudTrail 处理库的以下更新： • 添加了对管理事件的布尔标识的支持。 • 将 CloudTrail 活动版本更新到 1.06。 有关更多信息，请参阅上使用 CloudTrail 处理库的“CloudTrail 处理库” GitHub。	2017 年 11 月 30 日
增加了服务支持	此版本支持 AWS Glue。请参阅 CloudTrail 支持的服务和集成。	2017 年 11 月 7 日
新文档	此发布版添加了新主题中的配额 AWS CloudTrail。	2017 年 10 月 19 日
已更新的文档	此版本更新了 Amazon Athena、Amazon Elastic Container Regi AWS CodeBuild stry 和 CloudTrail 事件历史记录中支持的 API 的文档。 AWS Migration Hub	2017 年 10 月 13 日
增加了服务支持	此版本支持 Amazon Chime。请参阅 CloudTrail 支持的服务和集成。	2017 年 9 月 27 日
增加了功能和文档	此版本支持为您的 AWS 账户中的所有 Amazon S3 存储桶配置数据事件记录。请参阅 记录数据事件。	2017 年 9 月 20 日
增加了服务支持	此版本支持 Amazon Lex。请参阅 CloudTrail 支持的服务和集成。	2017 年 8 月 15 日
增加了服务支持	此版本支持 Migrati AWS on Hub。请参阅 CloudTrail 支持的服务和集成。	2017 年 8 月 14 日

更改	描述	发行日期
增加了功能和文档	默认情况下，此版本支持 CloudTrail 为所有 AWS 账户启用。过去七天的账户活动显示在 CloudTrail事件历史记录中，最新事件显示在控制台控制面板上。此功能以前称为 API activity history，现已被 Event history 取代。	2017 年 8 月 14 日
增加了功能和文档	此版本支持从 API 活动历史记录页面上的 CloudTrail 控制台下载事件。您可以下载 JSON 或 CSV 格式的事件。 有关更多信息，请参阅 下载事件。	2017 年 7 月 27 日
新增功能	此版本支持记录两个附加区域 [欧洲地区（伦敦）和加拿大（中部）] 中的 Amazon S3 对象级别 API 操作。 有关更多信息，请参阅 处理 CloudTrail 日志文件。	2017 年 7 月 19 日
增加了服务支持	此版本支持在 API CloudWatch 活动历史记录功能中查找 Amazon Events CloudTrail 的 API。	2017 年 6 月 27 日
增加了功能和文档	此版本支持以下服务的 AP CloudTrail I 活动历史记录功能中的其他 API： • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	2017 年 6 月 27 日
增加了服务支持	此版本支持 AWS CodeStar。请参阅 CloudTrail 支持的服务和集成。	2017 年 6 月 14 日

更改	描述	发行日期

增加了功能和文档	此版本支持对 CloudTrail 处理库的以下更新：
	• 为来自同一 SQS 队列的 SQS 消息添加对不同格式的支持，以识别 CloudTrail 日志文件。支持以下格式：
	  • CloudTrail 发送到 SNS 主题的通知
	  • Simple Storage Service（Amazon S3）发送到 SNS 主题的通知
	  • Simple Storage Service（Amazon S3）直接发送到 SQS 队列的通知
	• 添加对 `deleteMessageUponFailure` 属性的支持，您可以使用该属性来删除无法处理的消息。
	
	有关更多信息，请参阅上使用 CloudTrail 处理库的“CloudTrail 处理库” GitHub。
		2017 年 6 月 1 日

增加了服务支持	此版本支持 Amazon Athena。请参阅 CloudTrail 支持的服务和集成。	2017 年 5 月 19 日
新增功能	此版本支持向 Amazon CloudWatch 日志发送数据事件。 有关配置您的跟踪以记录数据事件的更多信息，请参阅数据事件。 有关向 Logs 发送事件的 CloudWatch 更多信息，请参阅使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。	2017 年 5 月 9 日
增加了服务支持	此版本支持 AWS Marketplace 计量服务。请参阅 CloudTrail 支持的服务和集成。	2017 年 5 月 2 日
增加了服务支持	此版本支持 Amazon QuickSight。请参阅 CloudTrail 支持的服务和集成。	2017 年 4 月 28 日

更改	描述	发行日期
增加了功能和文档	此发布版支持为创建新跟踪记录更新的控制台体验。现在，您可以将新跟踪配置为记录管理和数据事件。有关更多信息，请参阅 创建跟踪。	2017 年 4 月 11 日
添加的文档	如果 CloudTrail 没有将日志传送到您的 S3 存储桶或从您账户中的某些区域发送 SNS 通知，则可能需要更新政策。 要了解有关更新 S3 存储桶策略的更多信息，请参阅 Simple Storage Service（Amazon S3）策略配置常见错误。 要了解有关更新 SNS 主题策略的更多信息，请参阅 CloudTrail 未发送某个地区的通知。	2017 年 3 月 31 日
增加了服务支持	此版本支持 AWS Organizations。请参阅 CloudTrail 支持的服务和集成。	2017 年 2 月 27 日
增加了功能和文档	此版本支持配置用于记录管理事件和数据事件的跟踪记录的更新的控制台体验。有关更多信息，请参阅 处理 CloudTrail 日志文件。	2017 年 2 月 10 日
增加了服务支持	此版本支持 Amazon Cloud Directory。请参阅 CloudTrail 支持的服务和集成。	2017 年 1 月 26 日
增加了功能和文档	此版本支持在 API 活动历史记录中查找 AWS CodeCommit GameLift、Amazon 和 M AWS anaged Services CloudTrail 的 API。	2017 年 1 月 26 日

更改	描述	发行日期
新增功能	此版本支持与 AWS Health Dashboard集成。 您可以使用 AWS Health Dashboard 来确定您的跟踪是否无法将日志传送到 SNS 主题或 S3 存储桶。当 S3 存储桶或 SNS 主题的策略出现问题时，可能会发生这种情况。 AWS Health Dashboard 会通知您有关受影响的路径并推荐修复策略的方法。 有关更多信息，请参阅《AWS Health 用户指南》。	2017 年 1 月 24 日
增加了功能和文档	此版本支持在 CloudTrail 控制台中按事件源进行筛选。事件源显示向其发出请求的 AWS 服务。 有关更多信息，请参阅 使用控制台查看最近的管理事件。	2017 年 1 月 12 日
增加了服务支持	此版本支持 AWS CodeCommit。请参阅 CloudTrail 支持的服务和集成。	2017 年 1 月 11 日
增加了服务支持	此版本支持 Amazon Lightsail。请参阅 CloudTrail 支持的服务和集成。	2016 年 12 月 23 日
增加了服务支持	此版本支持 Managed S AWS ervices。请参阅 CloudTrail 支持的服务和集成。	2016 年 12 月 21 日
增加了区域支持	此版本支持欧洲（伦敦）区域。请参阅 CloudTrail 支持的区域。	2016 年 12 月 13 日
增加了区域支持	此版本支持加拿大（中部）区域。请参阅 CloudTrail 支持的区域。	2016 年 12 月 8 日
增加了服务支持	此版本支持 S AWS CodeBuild ee CloudTrail 支持的服务和集成。 此版本支持 AWS Health。请参阅 CloudTrail 支持的服务和集成。 此版本支持 AWS Step Functions。请参阅 CloudTrail 支持的服务和集成。	2016 年 12 月 1 日

更改	描述	发行日期
增加了服务支持	此版本支持 Amazon Polly。请参阅 CloudTrail 支持的服务和集成。	2016 年 11 月 30 日
增加了服务支持	此版本支持 AWS OpsWorks for Chef Automate。请参阅 CloudTrail 支持的服务和集成。	2016 年 11 月 23 日
增加了功能和文档	此版本支持将跟踪配置为记录只读事件、只写事件或所有事件。 CloudTrail 支持记录 Amazon S3 对象级别 API 操作`GetObject` ，例如`PutObject` 、和`DeleteObject` 。您可以将跟踪记录配置为记录对象级别 API 操作。 有关更多信息，请参阅 处理 CloudTrail 日志文件。	2016 年 11 月 21 日
增加了功能和文档	此版本支持 `userIdentity` 元素中的 `type` 字段的其他值：`AWSAccount` 和 `AWSService` 。有关更多信息，请参阅字段适用于 `userIdentity` 的 。	2016 年 11 月 16 日
增加了服务支持	此版本支持 Application Auto Scaling。请参阅 CloudTrail 支持的服务和集成。	2016 年 10 月 31 日
增加了区域支持	此版本支持美国东部（俄亥俄）区域。请参阅 CloudTrail 支持的区域。	2016 年 10 月 17 日
增加了功能和文档	此版本支持记录非 API AWS 服务事件。有关更多信息，请参阅 AWS 服务事件。	2016 年 9 月 23 日
增加了功能和文档	此版本支持使用 CloudTrail 控制台查看支持的资源类型 AWS Config。有关更多信息，请参阅 使用 AWS Config查看引用的资源。	2016 年 7 月 7 日
增加了服务支持	此版本支持 AWS Service Catalog。请参阅 CloudTrail 支持的服务和集成。	2016 年 7 月 6 日

更改	描述	发行日期
增加了服务支持	此版本支持 Amazon Elastic File System (Amazon EFS)。请参阅 CloudTrail 支持的服务和集成。	2016 年 6 月 28 日
增加了区域支持	此版本支持一个附加区域：ap-south-1，亚太地区（孟买）。请参阅 CloudTrail 支持的区域。	2016 年 6 月 27 日
增加了服务支持	此版本支持 AWS Application Discovery Service。请参阅 CloudTrail 支持的服务和集成。	2016 年 5 月 12 日
增加了服务支持	此版本支持南美洲（圣保罗）区域的 CloudWatch 日志。有关更多信息，请参阅 使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。	2016 年 5 月 6 日
增加了服务支持	此版本支持 AWS WAF。请参阅 CloudTrail 支持的服务和集成。	2016 年 4 月 28 日
增加了服务支持	此版本支持 AWS Support。请参阅 CloudTrail 支持的服务和集成。	2016 年 4 月 21 日
增加了服务支持	此版本支持 Amazon Inspector。请参阅 CloudTrail 支持的服务和集成。	2016 年 4 月 20 日
增加了服务支持	此版本支持 AWS IoT。请参阅 CloudTrail 支持的服务和集成。	2016 年 4 月 11 日
增加了功能和文档	此版本支持使用安全断言标记语言 AWS Security Token Service (SAML AWS STS) 和 Web 联合身份验证进行的 logging () API 调用。有关更多信息，请参阅 具有 SAML 和网络联合身份验证 AWS STS 的 API 的值。	2016 年 3 月 28 日
增加了服务支持	此版本支持 AWS Certificate Manager。请参阅 CloudTrail 支持的服务和集成。	2016 年 3 月 25 日
增加了服务支持	此版本支持 Amazon Data Firehose。请参阅 CloudTrail 支持的服务和集成。	2016 年 3 月 17 日

更改	描述	发行日期
增加了服务支持	此版本支持 Amazon CloudWatch 日志。请参阅 CloudTrail 支持的服务和集成。	2016 年 3 月 10 日
增加了服务支持	此版本支持 Amazon Cognito。请参阅 CloudTrail 支持的服务和集成。	2016 年 2 月 18 日
增加了服务支持	此版本支持 AWS Database Migration Service。请参阅 CloudTrail 支持的服务和集成。	2016 年 2 月 4 日
增加了服务支持	此版本支持亚马逊 GameLift（亚马逊 GameLift）。请参阅 CloudTrail 支持的服务和集成。	2016 年 1 月 27 日
增加了服务支持	此版本支持 Amazon CloudWatch 活动。请参阅 CloudTrail 支持的服务和集成。	2016 年 1 月 16 日
增加了区域支持	此版本支持一个附加区域：ap-northeast-2，亚太地区（首尔）。请参阅 CloudTrail 支持的区域。	2016 年 1 月 6 日
增加了服务支持	此版本支持 Amazon Elastic Container Registry (Amazon ECR)。请参阅 CloudTrail 支持的服务和集成。	2015 年 12 月 21 日
增加了功能和文档	此版本支持在 CloudTrail 所有区域开启，并支持每个区域多条跟踪。有关更多信息，请参阅 处理 CloudTrail 轨迹。	2015 年 12 月 17 日
增加了服务支持	此版本支持 Amazon Machine Learning。请参阅 CloudTrail 支持的服务和集成。	2015 年 12 月 10 日
增加了功能和文档	此版本支持日志文件加密、日志文件完整性验证和标记。有关更多信息，请参阅 使用密 AWS KMS 钥加密 CloudTrail 日志文件 (SSE-KMS)、验证 CloudTrail 日志文件完整性 和 更新跟踪。	2015 年 10 月 1 日
增加了服务支持	此版本支持 Amazon OpenSearch 服务。请参阅 CloudTrail 支持的服务和集成。	2015 年 10 月 1 日

更改	描述	发行日期
增加了服务支持	此版本支持 Simple Storage Service（Amazon S3）存储桶级别的活动。请参阅 CloudTrail 支持的服务和集成。	2015 年 9 月 1 日
增加了服务支持	此版本支持 AWS Device Farm。请参阅 CloudTrail 支持的服务和集成。	2015 年 7 月 13 日
增加了服务支持	此版本支持 Amazon API Gateway。请参阅 CloudTrail 支持的服务和集成。	2015 年 7 月 9 日
增加了服务支持	此版本支持 CodePipeline。请参阅 CloudTrail 支持的服务和集成。	2015 年 7 月 9 日
增加了服务支持	此版本支持 Amazon DynamoDB。请参阅 CloudTrail 支持的服务和集成。	2015 年 5 月 28 日
增加了服务支持	此版本支持美国西部（加利福尼亚北部）区域的 CloudWatch 日志。有关 CloudTrail 支持 CloudWatch 日志监控的更多信息，请参阅使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。	2015 年 5 月 19 日
增加了服务支持	此版本支持 AWS Directory Service。请参阅 CloudTrail 支持的服务和集成。	2015 年 5 月 14 日
增加了服务支持	此版本支持 Amazon Simple Email Service (Amazon SES)。请参阅 CloudTrail 支持的服务和集成。	2015 年 5 月 7 日
增加了服务支持	此版本支持 Amazon Elastic Container Service，请参阅 CloudTrail 支持的服务和集成。	2015 年 4 月 9 日
增加了服务支持	此版本支持 AWS Lambda。请参阅 CloudTrail 支持的服务和集成。	2015 年 4 月 9 日
增加了服务支持	此版本支持 Amazon WorkSpaces。请参阅 CloudTrail 支持的服务和集成。	2015 年 4 月 9 日

更改	描述	发行日期
	此版本支持查找 CloudTrail（CloudTrail 事件）捕获 AWS 的活动。您可以在账户中查找和筛选与创建、修改或删除有关的事件。要查找这些事件，您可以使用 CloudTrail 控制台、 AWS Command Line Interface (AWS CLI) 或 AWS SDK。有关更多信息，请参阅 处理 CloudTrail 事件历史记录。	2015 年 3 月 12 日
增加了服务支持和新文档	此版本支持亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京）和欧洲（法兰克福）区域的 Amazon CloudWatch 日志。有关更多信息，请参阅向 CloudWatch 日志发送事件。	2015 年 3 月 5 日
新文档	CloudTrail 概念页面中添加了一个描述对 AWS Security Token Service (AWS STS) 区域终端节点 CloudTrail 支持的新部分。	2015 年 2 月 17 日
增加了服务支持	此版本支持 Amazon Route 53。请参阅 CloudTrail 支持的服务和集成。	2015 年 2 月 11 日
增加了服务支持	此版本支持 AWS Config。请参阅 CloudTrail 支持的服务和集成。	2015 年 2 月 10 日
增加了服务支持	此版本支持 AWS CloudHSM。请参阅 CloudTrail 支持的服务和集成。	2015 年 1 月 8 日
增加了服务支持	此版本支持 AWS CodeDeploy。请参阅 CloudTrail 支持的服务和集成。	2014 年 12 月 17 日
增加了服务支持	此版本支持 AWS Storage Gateway。请参阅 CloudTrail 支持的服务和集成。	2014 年 12 月 16 日
增加了区域支持	此版本支持另外一个区域： us-gov-west-1（AWS GovCloud （美国西部））。请参阅 CloudTrail 支持的区域。	2014 年 12 月 16 日
增加了服务支持	此版本支持 Amazon S3 Glacier。请参阅 CloudTrail 支持的服务和集成。	2014 年 12 月 11 日

更改	描述	发行日期
增加了服务支持	此版本支持 AWS Data Pipeline。请参阅 CloudTrail 支持的服务和集成。	2014 年 12 月 2 日
增加了服务支持	此版本支持 AWS Key Management Service。请参阅 CloudTrail 支持的服务和集成。	2014 年 11 月 12 日
新文档	指南中增加了一个新的部分：使用 Amazon CloudTrail 日志监控 CloudWatch 日志文件。它描述了如何使用 Amazon CloudWatch 日志来监控 CloudTrail 日志事件。	2014 年 11 月 10 日
新文档	指南中增加了一个新的部分：使用 CloudTrail 处理库。它提供了有关如何使用处理库用 Java 编写 CloudTrail 日志 AWS CloudTrail 处理器的信息。	2014 年 11 月 5 日
增加了服务支持	此版本支持 Amazon Elastic Transcoder。请参阅 CloudTrail 支持的服务和集成。	2014 年 10 月 27 日
增加了区域支持	此版本支持一个附加区域：eu-central-1（欧洲（法兰克福））。请参阅 CloudTrail 支持的区域。	2014 年 10 月 23 日
增加了服务支持	此版本支持 Amazon CloudSearch。请参阅 CloudTrail 支持的服务和集成。	2014 年 10 月 16 日
增加了服务支持	此版本支持 Amazon Simple Notification Service。请参阅 CloudTrail 支持的服务和集成。	2014 年 10 月 09 日
增加了服务支持	此版本支持 Amazon ElastiCache。请参阅 CloudTrail 支持的服务和集成。	2014 年 9 月 15 日
增加了服务支持	此版本支持 Amazon WorkDocs。请参阅 CloudTrail 支持的服务和集成。	2014 年 8 月 27 日
新增内容	此版本包括讨论日志记录登录事件的主题。请参阅 AWS Management Console 登录事件。	2014 年 7 月 24 日

更改	描述	发行日期
新增内容	此版本的 eventVersion 元素已升级到版本 1.02，并且添加了三个新字段。请参阅 CloudTrail 录制内容。	2014 年 7 月 18 日
增加了服务支持	此版本支持 Auto Scaling（请参阅 CloudTrail 支持的服务和集成)。	2014 年 7 月 17 日
增加了区域支持	此版本支持三个附加区域：ap-southeast-1，亚太地区（新加坡）；ap-northeast-1，亚太地区（东京）；sa-east-1，南美洲（圣保罗）。请参阅 CloudTrail 支持的区域。	2014 年 6 月 30 日
附加服务支持	此版本支持 Amazon Redshift。请参阅 CloudTrail 支持的服务和集成。	2014 年 6 月 10 日
增加了服务支持	此版本支持 AWS OpsWorks。请参阅 CloudTrail 支持的服务和集成。	2014 年 6 月 5 日
增加了服务支持	此版本支持 Amazon CloudFront。请参阅 CloudTrail 支持的服务和集成。	2014 年 5 月 28 日
增加了区域支持	此版本支持三个附加区域：us-west-1，美国西部（北加利福尼亚）；eu-west-1，欧洲地区（爱尔兰）；ap-southeast-2，亚太地区（悉尼）。请参阅 CloudTrail 支持的区域。	2014 年 5 月 13 日
增加了服务支持	此版本支持 Amazon Simple Workflow Service。请参阅 CloudTrail 支持的服务和集成。	2014 年 5 月 9 日
新增内容	此版本包括讨论在账户之间共享日志文件的主题。请参阅 在 AWS 账户之间共享 CloudTrail 日志文件。	2014 年 5 月 2 日
增加了服务支持	此版本支持 Amazon CloudWatch。请参阅 CloudTrail 支持的服务和集成。	2014 年 4 月 28 日
增加了服务支持	此版本支持 Amazon Kinesis。请参阅 CloudTrail 支持的服务和集成。	2014 年 4 月 22 日

更改	描述	发行日期
增加了服务支持	此版本支持 AWS Direct Connect。请参阅 CloudTrail 支持的服务和集成。	2014 年 4 月 11 日
增加了服务支持	此版本支持 Amazon EMR。请参阅 CloudTrail 支持的服务和集成。	2014 年 4 月 4 日
增加了服务支持	此版本支持 Elastic Beanstalk。请参阅 CloudTrail 支持的服务和集成。	2014 年 4 月 2 日
附加服务支持	此版本支持 AWS CloudFormation。请参阅 CloudTrail 支持的服务和集成。	2014 年 3 月 7 日
新指南	此版本引入了 AWS CloudTrail。	2013 年 11 月 13 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。