elastic

适用于 AWS 的 Elastic 可观测性指南

elastic.co/cn →

目录

elastic

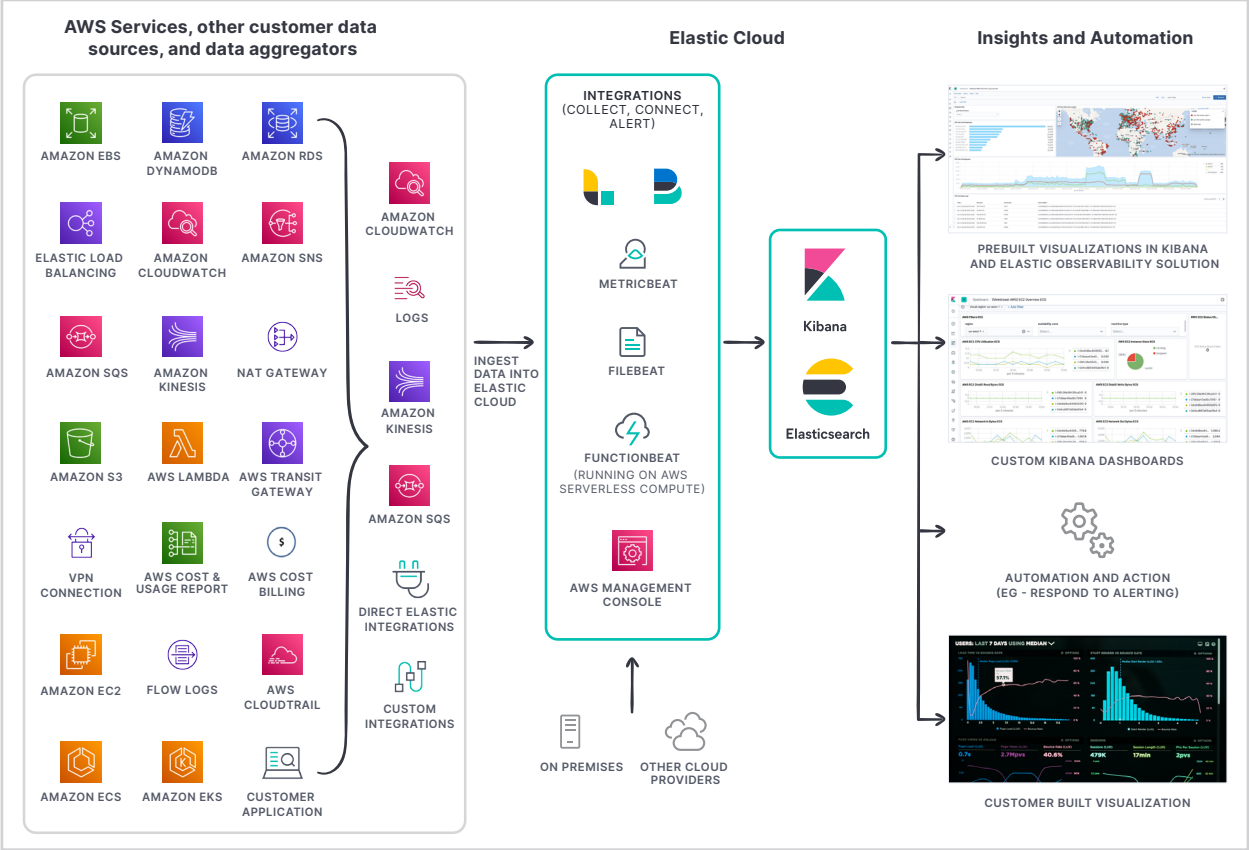
简介

为了充分享用云带来的敏捷性和灵活性，基于数据获得见解并转化为行动的能力至关重要。借助 Elastic 的可观测性解决方案，您可以在整个 AWS 和本地部署环境中实现一体化的可见性，从而更好地了解基础架构、应用程序和业务的可用性、性能和总体运行状况。

AWS 在其云服务中为您提供了一系列范围广泛的日志和指标，让您可以监测云部署并做出更明智的决策。Elastic 可观测性与这些数据源进行了集成，采用统一的方式将您的数据整合在一起，使您能够在 IT、运营和业务方面持续获得可付诸实践的见解。在预构建的仪表板和工具中轻松分析数据，或者构建定制的可视化，以便能够根据您的业务需求快速做出反应。

本指南介绍了如何使用 AWS 服务以最佳方式配置 Elastic 可观测性，以便能够更有效地监测事件并在事件发生时更快地做出反应。请继续阅读本文，进一步了解这些 AWS 服务、使用 Elastic 进行监测的各种益处，以及有助于将这两方面的投资价值实现最大化的最佳实践。

Elastic 可让您利用 AWS 数据成就更多



使用 Elastic 监测和分析 Amazon CloudWatch 日志

使用 Amazon CloudWatch 能够将来自基础架构、应用程序以及您所用 AWS 服务中的日志集中在一个可扩展的服务中。

Amazon CloudWatch 日志使您能够轻松快速地完成以下工作：

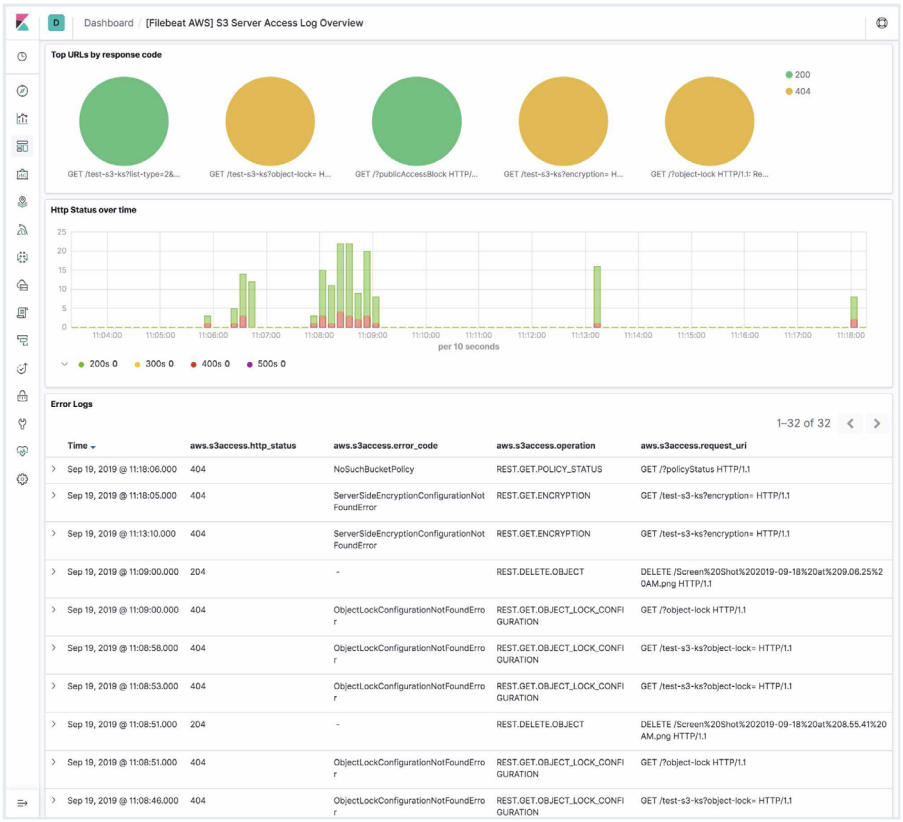
收集、存储和访问不同来源中的日志文件

监测基础架构和应用程序的运行状况和性能

直接从不同的 AWS 日志组观测 Amazon CloudWatch 日志

elastic

如何将 Amazon CloudWatch 日志发送到 Elastic：



首先，您需要收集有关 AWS 环境和 Elastic Cloud 部署的信息。有关这些准备工作的详细信息，请参阅本文后面的**附录 A**。要开始使用 Amazon CloudWatch 日志，请按照本文后面**附录 B** 中的步骤进行演练，其中包括以下方面的详细信息：

1. 设置 Amazon Simple Storage Service (Amazon S3) 存储桶并创建 Amazon Simple Queue Service (Amazon SQS) 队列
2. 下载并安装 Filebeat
3. 连接到 Elastic Stack
4. 配置 Filebeat 以收集 Amazon CloudWatch 日志
5. 启用和配置数据收集模块
6. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
7. 在 Kibana 中分析 Amazon CloudWatch 数据

使用 Elastic 分析 Amazon S3 日志活动并监测访问权限

通过 Amazon S3，您可以存储数据、业务应用程序和托管静态网站。借助 Amazon S3，您可以实施两种类型的工作流程：收集存储在 Amazon S3 中的定制日志，以及监测 Amazon S3 服务的访问权限和指标。

将 Elastic 与 Amazon S3 结合使用，能够实现以下目的：

捕获请求的详细信息，如远程 IP、请求者、存储桶名称等，以便更好地了解针对存储桶的流量性质

在 Kibana 的预定义仪表板中建立基线，分析访问模式并确定趋势

识别安全和合规性问题并在整个组织中进行根本原因分析

分析存储在 Amazon S3 中特定于业务或应用程序的定制日志

如何将 Amazon S3 日志发送到 Elastic：

首先，您需要收集有关 AWS 环境以及 Elastic Cloud 部署的信息。有关这些准备工作的更多详细信息，请参阅附录 A。要开始使用 Amazon S3 日志，请按照附录 B 中的步骤进行演练，其中包括以下方面的详细信息：

1. 设置 Amazon S3 存储桶并创建 Amazon SQS 队列
2. 下载并安装 Filebeat
3. 连接到 Elastic Stack
4. 启用和配置数据收集模块
5. 配置 Filebeat 以收集 Amazon S3 日志
6. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
7. 在 Kibana 中分析 Amazon S3 日志数据

使用 Amazon Kinesis 将数据流式传输到 Elasticsearch

Amazon Kinesis 是一项全托管服务，用于将实时的流数据源交付到 Amazon S3 和 Elastic 等目的地。

使用 Amazon Kinesis，您可以：

实时流式传输日志并使用 Elasticsearch 和 Kibana 对其进行分析，以便您可以快速获得见解并做出更明智的决策

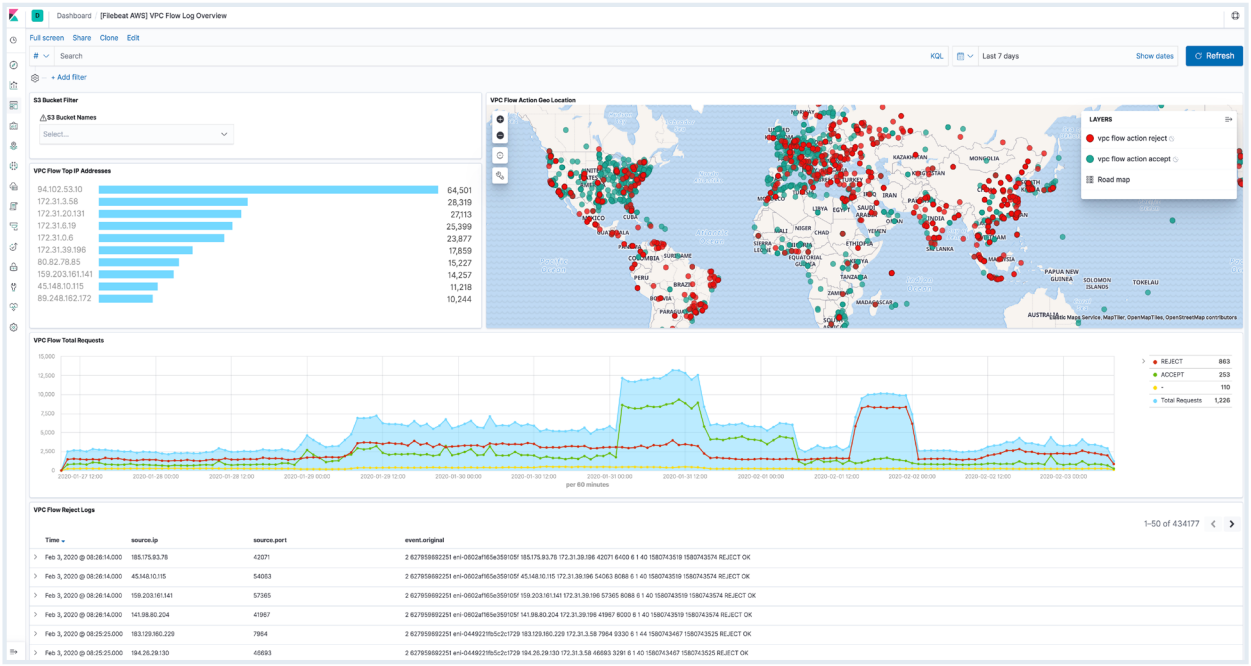
压缩、转换和加密传输中的数据，以减少使用的存储量，同时提高安全性

如何使用 Amazon Kinesis 将数据流式传输到 Elastic：

在开始之前，您需要获得有关 AWS 环境以及 Elastic Cloud 部署的信息。有关这些准备工作的更多详细信息，请参阅**附录 A**。要开始使用 Amazon Kinesis，请按照**附录 C** 中的步骤进行演练，其中包括以下方面的详细信息：

1. 下载并安装 Metricbeat
2. 连接到 Elastic Stack
3. 配置 Metricbeat 以流式传输数据
4. 启用和配置数据收集模块
5. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
6. 在 Kibana 中分析数据

通过结合使用 Amazon VPC 流日志与 Elastic 来监测网络流量



借助 Elastic 可观测性，您可以使用 Kibana 快速搜索、查看和筛选 Amazon Virtual Private Cloud (Amazon VPC) 流日志，以监测 Amazon VPC 内的网络流量。通过这一集成，您可以分析流日志数据并将其与您的安全组配置进行比较，以维护和提高您的云安全性。

通过将 Amazon VPC 流日志采集到 Elastic，您能够：

执行更好的分析，以做出更明智的决策

评估安全组规则并发现安全漏洞

设置警报，以在检测到某些流量类型时向您发出告警

识别延迟问题并建立基线，以确保获得一致的性能

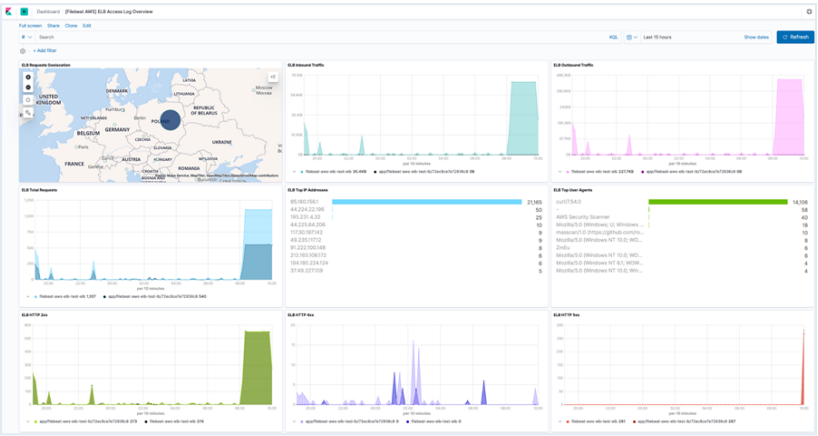
elastic

如何将 Amazon VPC 日志采集到 Elastic：

首先，收集有关 AWS 环境以及 Elastic Cloud 部署的信息。有关这些准备工作的更多详细信息，请参阅**附录 A**。要开始使用 Amazon VPC 流日志，请按照**附录 B** 中的步骤进行演练，其中包括以下方面的详细信息：

1. 设置 Amazon S3 存储桶并创建 Amazon SQS 队列
2. 下载并安装 Filebeat
3. 连接到 Elastic Stack
4. 配置 Filebeat 以收集 Amazon VPC 流日志
5. 启用和配置数据收集模块
6. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
7. 在 Kibana 中分析日志

使用 Amazon ELB 观测 Elastic 中的负载均衡操作



使用 AWS 上的 Elastic Load Balancing (ELB) 服务，您可以自动均衡一组云资源之间的网络流量。

当您在 Elastic 中使用集中式 ELB 日志时，您可以：

观测有关发送到负载均衡器的请求的详细信息

分析流量模式和排查问题，以发现性能问题

深入分析 ELB 日志，以发现服务器响应等。

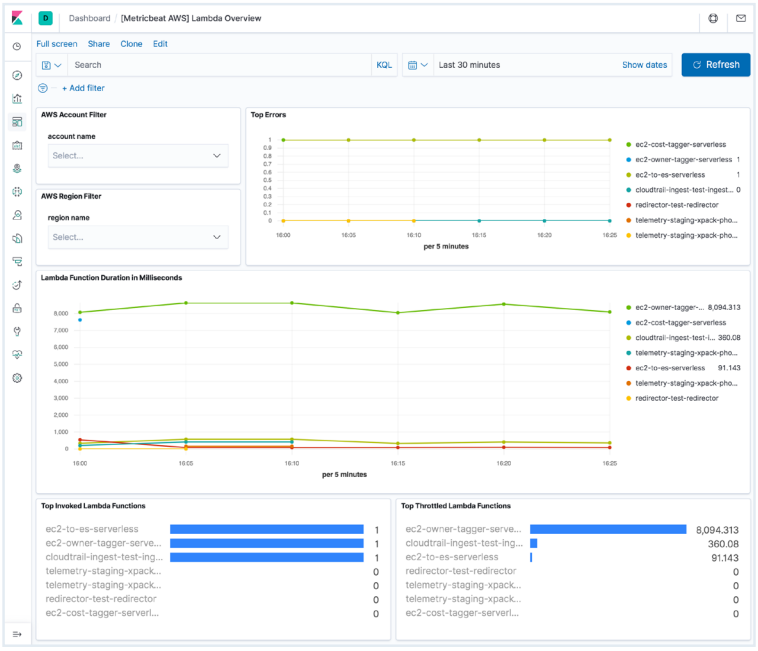
elastic

如何将 Elastic Load Balancing 数据发送到 Elastic：

在开始之前，您需要收集一些有关 AWS 环境以及 Elastic Cloud 部署的信息。
有关这些准备工作的更多详细信息，请参阅**附录 A**。要开始使用 AWS 上的 ELB，
请按照**附录 B** 中的步骤进行演练，其中包括以下方面的详细信息：

1. 设置 Amazon S3 存储桶并创建 Amazon SQS 队列
2. 下载并安装 Filebeat
3. 连接到 Elastic Stack
4. 配置 Filebeat 以收集 AWS 上的 ELB 日志
5. 启用和配置数据收集模块
6. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
7. 在 Kibana 中分析 ELB 日志

在 Elastic 中使用 AWS Lambda 优化运营工作流



借助 AWS Lambda，您可以利用无服务器计算服务来动态运行代码，以响应事件并优化运营工作流。
您还可以执行任何计算任务，使用任何应用程序的代码自动管理您的资源，并且无需执行任何管理任务。

当您在 Elastic 中使用 AWS Lambda 时，您可以：

监测来自不同无服务器应用程序的性能

实时处理日志和指标

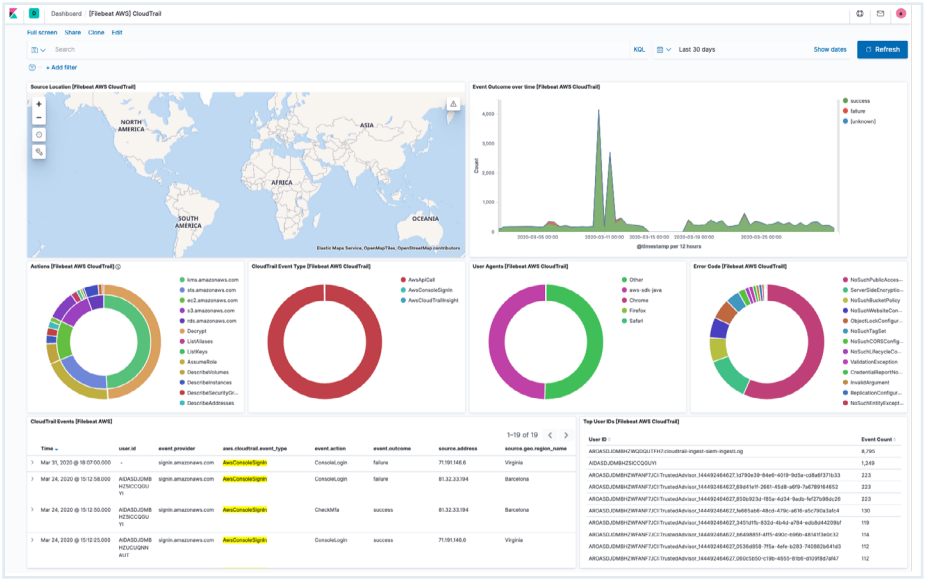
捕获性能数据并将其关联到 Elastic 解决方案

如何在 Elastic 中开始使用 AWS Lambda：

首先，收集有关 AWS 环境以及 Elastic Cloud 部署的信息。有关这些准备工作的更多详细信息，请参阅**附录 A**。要开始使用 AWS Lambda，请按照**附录 D** 中的步骤进行演练，其中包括以下方面的详细信息：

1. 下载并安装 Functionbeat
2. 连接到 Elastic Stack
3. 配置云函数
4. 启用和配置数据收集模块
5. 设置资产和部署 Functionbeat
6. 构建用于分析的 Kibana 仪表板

在 Elastic 中使用 AWS CloudTrail 确保符合监管和合规性标准



elastic

AWS CloudTrail 能够帮助您对 AWS 帐户进行监管、合规性检查、操作审计和风险审计。

当您将 AWS CloudTrail 日志集中在 Elastic 中时，您可以轻松地：

在 Kibana 的预构建仪表板中可视化您的 AWS CloudTrail 日志以及帐户和用户活动，以便更快地进行分析

记录有关为跟踪更改和解决故障排除问题而采取的所有操作的信息

保护并监测您的网络连接

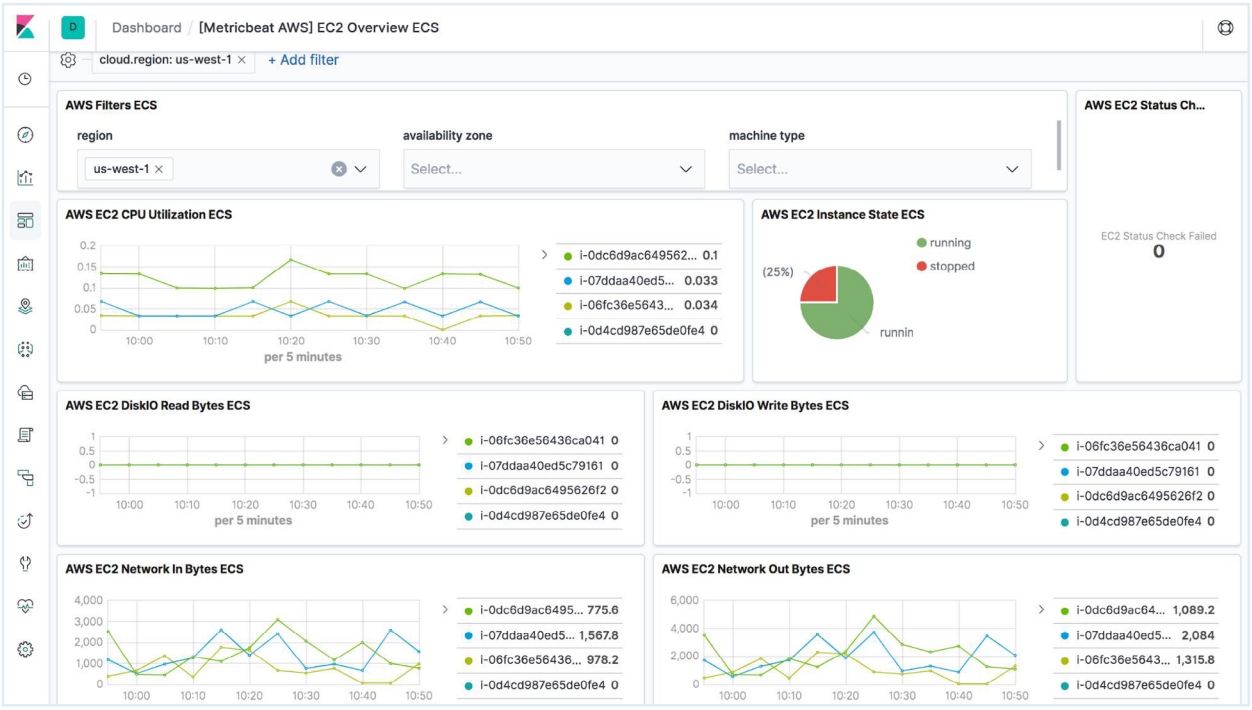
确保符合监管标准及各项政策的要求

如何将 AWS CloudTrail 数据采集到 Elastic：

在开始之前，您需要收集一些有关 AWS 环境以及 Elastic Cloud 部署的信息。有关这些准备工作的更多详细信息，请参阅**附录 A**。要开始使用 AWS CloudTrail，请按照**附录 B** 中的步骤进行演练，其中包括以下方面的详细信息：

1. 设置 Amazon S3 存储桶并创建 Amazon SQS 队列
2. 下载并安装 Filebeat
3. 连接到 Elastic Stack
4. 配置 Filebeat 以收集 AWS CloudTrail 日志
5. 启用和配置数据收集模块
6. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
7. 在 Kibana 中分析 AWS CloudTrail 日志

采集并统一 AWS 环境中的指标以获得全面见解



借助 Elastic 的 AWS 集成和预构建的仪表板，您可以收集使用情况、性能、计费等 AWS 指标，以了解每个信号之间的相关性，从而使您能够做出更明智的业务决策。

通过持续监测和分析您的 AWS 计算、存储、网络和数据指标，您可以快速响应不断变化的业务需求：

- Amazon Relational Database Service (Amazon RDS)
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon VPC Network Address Translation (NAT) Gateway
- Amazon CloudWatch
- Amazon S3
- Amazon DynamoDB
- Amazon Simple Notification Service (SNS)
- Amazon SQS
- AWS 成本和使用情况报告
- AWS 账单和成本管理
- AWS Virtual Private Network (AWS VPN)
- AWS Transit Gateway

AWS 指标可帮助您执行全面分析，从而做出更明智的决策，让您能够：

将计算、存储和数据服务中的指标相互关联，以统一排查问题

评估容量、性能和使用量方面的限制，以做出全面的扩展决策

使用统一的数据集，通过自动化分析和告警，监测和维护优化的云部署

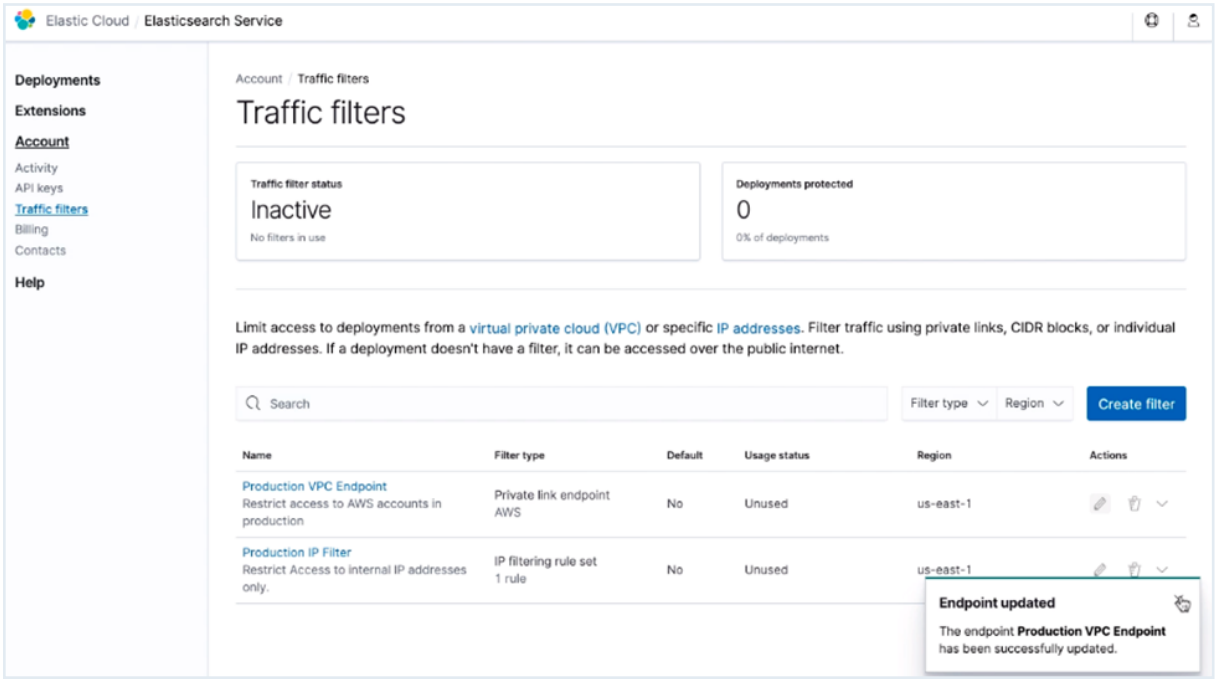
如何开始使用 AWS 指标和定制仪表板：

在开始之前，您需要获得有关 AWS 环境以及 Elastic Cloud 部署的信息。有关这些准备工作的更多详细信息，请参阅**附录 A**。要开始创建仪表板，请按照**附录 C** 中的步骤进行演练，其中包括以下方面的详细信息：

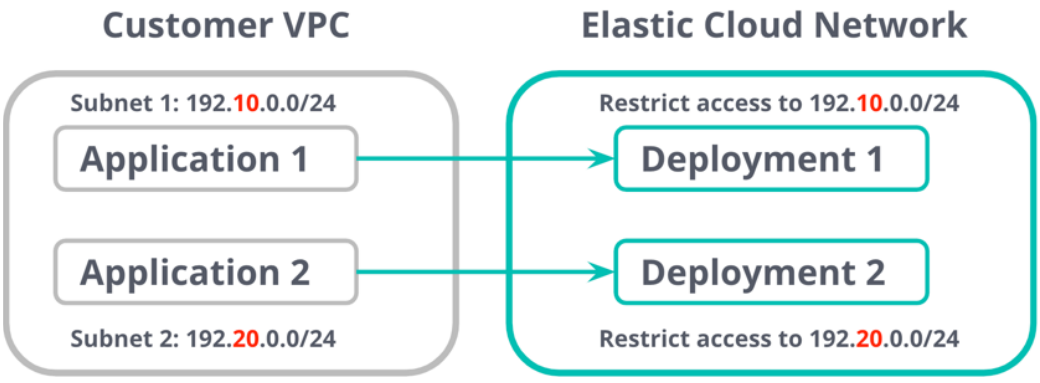
1. 下载并安装 Metricbeat
2. 连接到 Elastic Stack
3. 配置 Metricbeat 以收集指标
4. 启用和配置数据收集模块
5. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
6. 在 Kibana 中分析您的指标

要了解如何构建满足自身需求的定制仪表板，请查看我们的**文档**以及这个简短的**视频教程**。

使用 AWS PrivateLink 从 Elastic 获得更高的安全性和灵活性



AWS PrivateLink 在您的 Amazon VPC、其他 AWS 资源以及本地部署应用程序之间提供了安全的连接。这让您能够轻松确保应用程序和 Elastic 部署之间网络连接的安全性。您的虚拟网络和 Elastic 部署之间的流量通过 AWS 网络（而不是公共网络）传输，从而消除了数据泄露的风险，增加了安全性。



AWS PrivateLink 可让您：

创建具有专用 IP 地址的终端，以便工作负载在您的网络内运行

确保所有流量保持在 Amazon 网络内传输，并且在任何时候都不会离开

得益于简化的网络管理，不再需要维护复杂的基础架构（NAT Gateway、访问控制）

限制从客户虚拟网络到终端的流量（AWS PrivateLink 流量是单向的，而 Amazon VPC 对等中的流量是双向的）

如何开始使用 AWS PrivateLink：

请查看我们的**文档**以获取详细的步骤说明。

elastic

为什么选择 Elastic?

部署 Elastic 可为云带来一组互补功能，有助于您将 AWS 投资价值实现最大化。

Elastic 可观测性及其底层搜索平台功能可与云基础架构创新形成优势互补

自 Elastic 成立以来，提供了源源不断的搜索和数据分析创新，并重新定义了搜索的价值。作为 Elasticsearch 和 Kibana 的开发公司，Elastic 不断为这些产品添加新功能、安全更新和性能增强。Elastic 在软件应用程序层的搜索创新能够与 AWS 在云基础架构层的创新形成优势互补。结合使用后，您可以快速响应业务和运营数据，帮助您成为更加敏捷的数据驱动型组织。

可以灵活选择不同的服务提供商和本地部署方式

Elastic 搜索平台的构建宗旨就是让开发人员和客户能够灵活地在他们选择的位置运行。强大的投资使其能够在平台中构建核心功能，同时在云上构建深度集成。此外，Elastic 搜索平台还在云端和本地部署提供一致的体验。随着您逐渐增加云的使用量，这种混合部署的一致性变得弥足重要，即使是大型企业可能也需要数年时间才能实现这一过程。

如果您选择扩展云的使用范围，以添加来自不同云服务提供商的最佳服务，那么跨多个云的一致性还可以让您更轻松地扩展解决方案。这对于可观测性和安全用例尤其有用，在这些用例中，跨不同位置的一体化视图可以帮助客户加快问题排查速度并降低风险。

即装即用的企业搜索、可观测性和安全解决方案

Elastic 为企业搜索用例（包括 Workplace Search、App Search 和 Site Search）、可观测性用例（包括 Logging 和应用程序性能监测 (APM)）和安全用例（包括 SIEM 和终端保护）提供了即装即用型的预构建应用程序。

支持这些解决方案特定应用程序的所有功能和外部集成均内置在 Elastic 搜索平台中，并提供给选择自己构建定制应用程序来满足自身需求的客户。这包括了将可观测性和安全解决方案所需的数据采集到 AWS 中的广泛集成。

社区和技术人才

Elastic 搜索平台是搜索驱动型解决方案的一个事实标准。Elasticsearch GitHub 社区拥有超过 1,500 名成员。此外，围绕 Elasticsearch 和 Kibana 的技能组合在业界也是公认的。Elasticsearch 还包括为常用的相邻应用程序和数据源提供的现成集成。通过将 Elastic 可观测性与 AWS 结合使用，您便可在发展搜索驱动型解决方案时使用这些资源：人才库、集成和协作式 Elasticsearch 社区。

elastic

积极参与 Elastic 社区活动

论坛

寻求建议或伸出援助之手。在我们的**论坛**（也提供您的母语版本）上询问您亟待解决的关于 Elastic 的所有问题，并与其他用户分享您的智慧。

Slack 和当地社区

加入我们不断发展壮大的 **Elastic Slack**，与其他用户聊天并通过各种渠道寻求建议：#elasticsearch、#kubernetes、#kibana-development 或其他渠道。

此外，全球各地还涌现出了许多**其他在线社区**！请加入您所在地区的一个社区，与当地社区分享您的 Elastic 故事。

学无止境

无论您是刚开始接触 Elastic Stack，还是在寻找详细的深度剖析，都可以通过 **Elastic 示例存储库**获得实操经验，并探索精选数据集和分步说明。另外，还可以通过我们的**社区时事通讯**，了解开发团队的最新动态。

我们非常想听听您的想法

随着技术的进步，Elastic 也在不断发展。我们非常重视听取社区的意见。**请联系我们**以获取帮助或分享您对 Elastic 体验的看法。

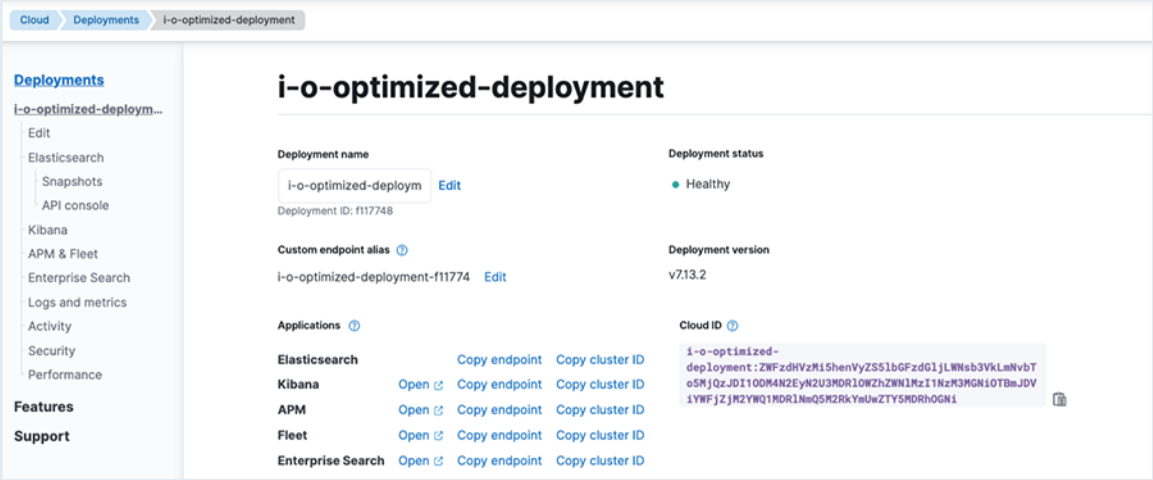
附录 A – 入门前的准备工作

在开始采集 AWS 数据之前，请按照下面的说明获取以下信息：

- 找到云 ID
- 获取登录凭据
- 创建 AWS 访问密钥 ID 和访问密钥

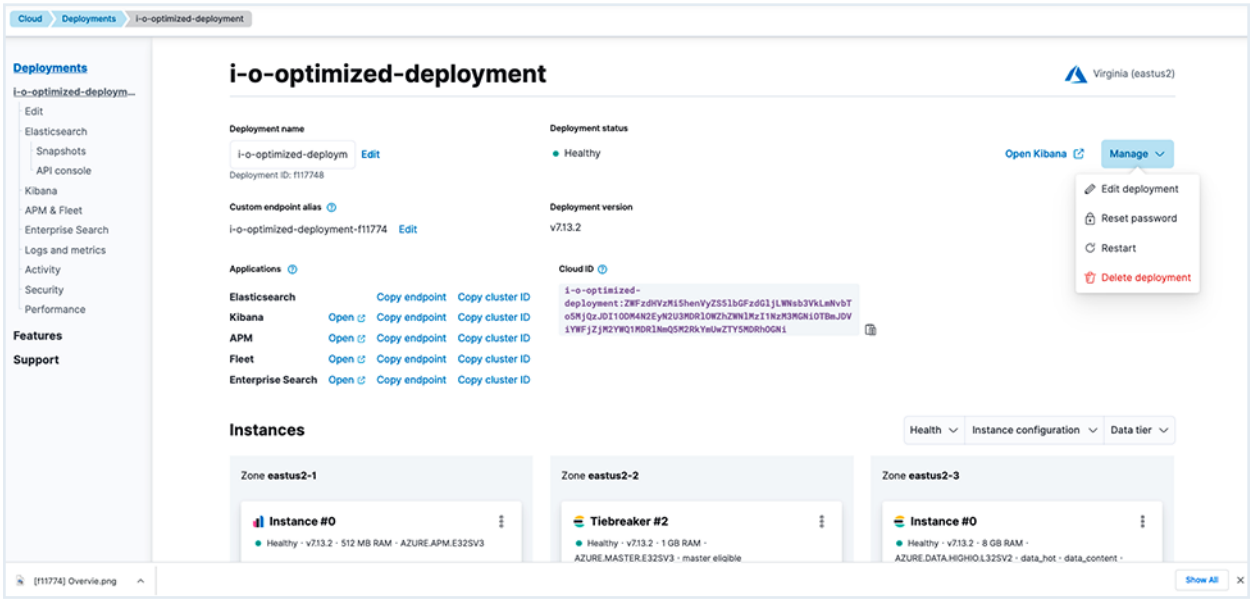
找到云 ID

您可以通过访问 cloud.elastic.co 并选择相关部署来找到您的云 ID。



elastic

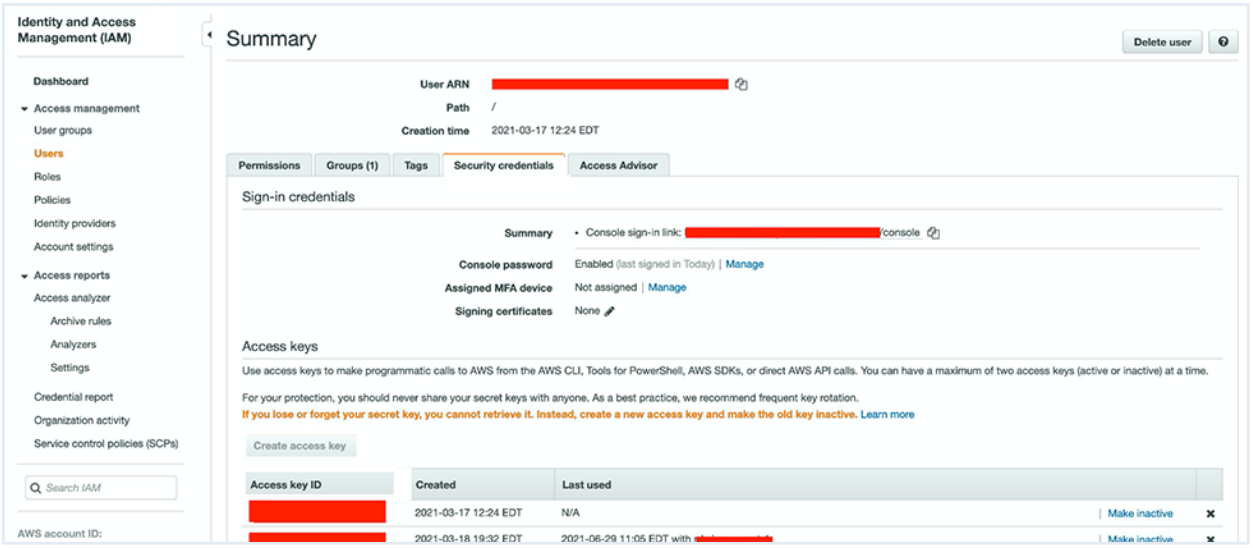
获取登录凭据



将数据发送到 Elasticsearch 时，您可以使用默认的 `Elastic` 用户和创建集群时提供的密码，也可以设置专用的用户和角色，以最少的权限来完成任务。在本例中，我们将使用 `Elastic` 用户和提供的密码。

如果您没有下载或忘记了密码，可以前往 cloud.elastic.co，然后单击来选择“管理”，以重置密码。

创建 AWS 访问密钥 ID 和访问密钥



AWS 访问密钥 ID 和访问密钥用于对您向 AWS 发出的编程请求进行签名。要获得这些信息，只需：

- 通过 https://console.aws.amazon.com/iam/ 登录 AWS Identity and Access Management，并打开 IAM 控制台
- 在左侧导航窗格中选择“用户”。
- 选择用户，然后选择“安全凭据”标签页
- 在“访问密钥”部分中，单击“创建访问密钥”，并选择“显示”来查看访问密钥对，然后复制并保存访问密钥，以用于稍后配置 Filebeat 和 Metricbeat。

附录 B – Filebeat 配置

下面是如何安装 Filebeat 和启用 AWS 模块的演练说明。流程如下：

1. 设置 Amazon S3 存储桶并创建 Amazon SQS 队列
2. 下载并安装 Filebeat
3. 连接到 Elastic Stack
   - 这一步需要提供您用于实施 Elastic 部署的云 ID 和云密码
4. 启用并配置 Filebeat 模块
5. 配置 Filebeat 以收集 AWS 日志
   - 这一步需要提供您的 AWS 模块代码，以及 AWS 访问密钥 ID 和访问密钥
6. 设置您预先配置的 Kibana 仪表板，然后启动 Filebeat
7. 在 Kibana 中查看和分析数据

第 1 步：设置 Amazon S3 存储桶并创建 Amazon SQS 队列

如果对来自每个 Amazon S3 存储桶的日志文件都进行轮询，就会造成重大延迟。为了避免这一延迟，Filebeat 将通知和轮询结合在了一起：在创建新的 Amazon S3 对象时使用 Amazon SQS 来发送 Amazon S3 通知。要了解如何设置 Amazon S3 存储桶和 Amazon SQS 队列，请参阅**使用 Amazon SQS 配置 S3 事件通知**这篇博文。

第 2 步：下载并安装 Filebeat

下载并安装 Filebeat。请根据您的系统使用适当的命令。

- 在这个示例中，我们将使用 Linux 命令。要查找最新版本，请导航到 **Filebeat 文档**，然后选择 “Quick start: installation and configuration”（快速入门：安装和配置）。在这里，您还可以找到适用于其他操作系统的命令。

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/
filebeat-7.13.3-linux-x86_64.tar.gz
tar xzvf filebeat-7.13.3-linux-x86_64.tar.gz
```

第 3 步：连接到 Elastic Stack

要设置 Filebeat，您需要连接到 Elasticsearch 和 Kibana。您将需要修改配置文件，也就是 filebeat.yml 文件。

您会在这一步使用您获得的云 ID 和密码。指定 Elasticsearch Service 的 **cloud.id**，并将 **cloud.auth**（用户名:密码）设置为有权设置 Filebeat 的用户。例如：

```
cloud.id:
"staging:dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4
ODExY jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth: "elastic:<elastic-password>"
```

为了增加安全性，您可以利用 **Filebeat 密钥库**对凭据（用户名、密码、cloud.id 等）进行模糊处理，并创建专用用户和角色，以最少的权限完成任务。对于本例，将使用您在创建部署时收到的默认用户名和密码。此外，作为示例，您将使用默认超级用户。在生产环境中，您可能需要使用完成任务**所需的最少权限**来设置用户和角色。

请务必创建用于已部署函数的定制角色。例如：

```
role: arn:aws:iam::123456789012:role/MyFunction
```

确保定制角色具有运行该函数所需的权限。有关详细信息，请参阅**部署所需的 IAM 权限**。

第 4 步：启用和配置数据收集模块

要启用 aws 模块，请导航到 Filebeat 目录并输入以下命令：

```
./filebeat modules enable aws
```

第 5 步：配置 Filebeat 以收集 AWS 日志

导航到 modules.d 目录下 aws.yml 文件中的 AWS 模块配置。如果缺少所需集成的代码，可以在附录 E 中找到相关代码。

此外，您还需要将从附录 A 的操作中收到的 AWS 凭据添加到顶部的 aws.yml 文件中：

- access_key_id:"YOUR AWS ACCESS KEY ID"
- secret_access_key:"YOUR AWS ACCESS KEY"

如果您习惯使用其他身份验证方法，请参阅 AWS 凭据选项以了解更多详细信息。

请参考以下示例来添加您的 AWS 访问密钥 ID 和访问密钥：

```
module: aws
var.access_key_id:"XyzW4VIA6DCIEKDUNB"
var.secret_access_key: "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

请参考以下示例来添加您的 IAM 角色：

```
module: aws
#AWS IAM Role to assume
var.role_arn: arniam::123456789012:role/test-mb
```

请注意，您还可以使用 Filebeat 密钥库对您的 AWS 访问密钥 ID 和访问密钥进行模糊处理。

第 6 步：设置您预先配置的 Kibana 仪表板，然后启动 Filebeat

Filebeat 附带了用于解析、索引和可视化数据的预定义资产。要加载这些资产：

- 如果您使用的不是 “elastic” 用户（默认用户），请确保在 filebeat.yml 中指定的用户有权设置 Filebeat
- 从安装目录中，运行：

```
./filebeat setup -e
```

在启动 Filebeat 之前，修改 filebeat.yml 中的用户凭据，并指定一个有权发布事件的用户。

要启动 Filebeat，请使用以下命令：

```
sudo chown root filebeat.yml
sudo chown root modules.d/aws.yml
sudo ./filebeat -e -c filebeat.yml &
```

第 7 步：在 Kibana 中查看和分析数据

Filebeat 附带了预构建的 Kibana 仪表板和专用的日志应用程序，可用于可视化、搜索和筛选日志数据，并且非常便于配置异常检测。您之前在运行 setup 命令时已加载了仪表板。

要启动 Kibana，您需要：

- 登录您的 Elastic Cloud 帐户
- 导航到部署中的 Kibana 终端以查看和分析您的数据

附录 C – Metricbeat 配置

下面是如何安装 Metricbeat 和启用 AWS 模块的演练说明。流程如下：

1. 下载并安装 Metricbeat。
2. 连接到 Elastic Stack
   - 这一步需要提供您用于实施 Elastic 部署的云 ID 和云密码
3. 启用和配置数据收集模块
4. 配置 Filebeat 以收集 AWS 指标
   - 这一步需要提供您的 AWS 模块代码，以及 AWS 访问密钥 ID 和访问密钥
5. 设置您预先配置的 Kibana 仪表板，然后启动 Metricbeat
6. 在 Kibana 中查看和分析数据

第 1 步：下载并安装 Metricbeat

下载并安装 Metricbeat。请根据您的系统使用适当的命令。

在这个示例中，我们将使用 Linux 命令。要查找最新版本，请导航到 Metricbeat 文档，然后选择 “Quick start: installation and configuration”（快速入门：安装和配置）。在这里，您还可以找到适用于其他操作系统的命令。

```
curl -L -O https://artifacts.elastic.co/downloads/beats/
metricbeat/metricbeat-7.13.4-linux-x86_64.tar.gz
tar xzvf metricbeat-7.13.4-linux-x86_64.tar.gz
```

第 2 步：连接到 Elastic Stack

配置 Metricbeat 时，您必须编辑配置文件 metricbeat.yml。

您会在这一步使用您获得的云 ID 和密码。指定 Elasticsearch Service 的 **cloud.id**，并将 **cloud.auth**（用户名:密码）设置为有权设置 Metricbeat 的用户。例如：

```
cloud.id:
"staging:dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4
ODExY jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth: "elastic:<elastic-password>"
```

为了增加安全性，您可以利用 **Metricbeat 密钥库**对凭据（用户名、密码、cloud.id 等）进行模糊处理，并创建专用用户和角色，以最少的权限完成任务。对于本例，将使用您在创建部署时收到的默认用户名和密码。此外，作为示例，您将使用默认超级用户。在生产环境中，您可能需要使用完成任务**所需的最少权限**来设置用户和角色。

请务必创建用于已部署函数的定制角色。例如：

```
role: arn:aws:iam::123456789012:role/MyFunction
```

确保定制角色具有运行该函数所需的权限。有关详细信息，请参阅**部署所需的 IAM 权限**。

第 3 步：启用和配置数据收集模块

在配置 Metricbeat 时，您需要指定要运行的模块。Metricbeat 使用模块来收集指标。要在 modules.d 目录中启用 AWS Config，请输入以下命令：

```
metricbeat modules enable aws
```

第 4 步：配置 Metricbeat 以收集 AWS 日志

导航到 aws.yml 文件中 modules.d 目录下的 AWS 模块配置。如果缺少所需集成的代码，可以在**附录 E** 中找到相关代码。

此外，您还需要将 AWS 凭据添加到顶部的 aws.yml 文件中：

- access_key_id:"YOUR AWS ACCESS KEY ID"
- secret_access_key:"YOUR AWS ACCESS KEY"

如果您习惯使用其他身份验证方法，请参阅 **AWS 凭据选项**以了解更多详细信息。

请参考以下示例来添加您的 AWS 访问密钥 ID 和访问密钥：

```
module: aws
access_key_id:"XyzW4VIA6DCIEKDUNB"
secret_access_key: "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

请参考以下示例来添加您的 IAM 角色：

```
module: aws
#AWS IAM Role to assume
role_arn: arniam::123456789012:role/test-mb
```

请注意，您还可以使用 **Metricbeat 密钥库**对您的 AWS 访问密钥 ID 和访问密钥进行模糊处理。

第 5 步：设置您预先配置的 Kibana 仪表板，然后启动 Metricbeat

Metricbeat 附带了打包的示例 Kibana 仪表板、可视化和搜索功能，可用于在 Kibana 中可视化 AWS 指标数据，并且非常便于配置告警和异常检测。

- 如果您使用的不是 “elastic” 用户（默认用户），请确保在 metricbeat.yml 中指定的用户**有权设置 Metricbeat**
- 从安装目录中，运行：

```
./metricbeat setup -e
```

要启动 Metricbeat，请使用以下命令：

```
sudo chown root metricbeat.yml
sudo chown root modules.d/aws.yml
sudo ./metricbeat -e -c metricbeat.yml &
```

第 6 步：在 Kibana 中查看和分析数据

Metricbeat 附带了用于可视化指标数据的预构建 Kibana 仪表板和专用应用程序。您之前在运行 setup 命令时已加载了仪表板。

要启动 Kibana，您需要：

- **登录**您的 Elastic Cloud 帐户
- 导航到部署中的 Kibana 终端

附录 D – Functionbeat 配置

下面是如何安装 Functionbeat 和启用 AWS 模块的演练说明。流程如下：

1. 下载并安装 Functionbeat
2. 连接到 Elastic Stack
   - 这一步需要提供您用于实施 Elastic 部署的云 ID 和云密码
3. 配置云函数
   - 这一步需要提供您的 AWS 模块代码，以及 AWS 访问密钥 ID 和访问密钥
4. 设置资产并部署 Functionbeat
5. 构建用于分析的 Kibana 仪表板

第 1 步：下载并安装 Functionbeat

下载并安装 Metricbeat。请根据您的系统使用适当的命令。

- 在这个示例中，我们将使用 Linux 命令。有关适用于其他操作系统的命令，请参阅**文档**。

```
curl -L -O https://artifacts.elastic.co/downloads/beats/
functionbeat/functionbeat-7.13.4-linux-x86_64.tar.gz
tar xzvf functionbeat-7.13.4-linux-x86_64.tar.gz
```

第 2 步：连接到 Elastic Stack

要使用 Filebeat，您需要连接到 Elasticsearch 和 Kibana。您将需要修改配置文件，也就是 functionbeat.yml。

您会在这一步使用您获得的云 ID 和密码。指定 Elasticsearch Service 的 **cloud.id**，并将 **cloud.auth**（密码）设置为有权设置 Functionbeat 的用户。例如：

```
cloud.id:
"staging:dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4
ODExY jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth: "functionbeat_setup:YOUR_PASSWORD"
```

请务必创建用于已部署函数的定制角色。例如：

```
role: arn:aws:iam::123456789012:role/MyFunction
```

确保定制角色具有运行该函数所需的权限。有关详细信息，请参阅**部署所需的 IAM 权限**。

第 3 步：配置云函数

在将 Functionbeat 部署到 AWS 之前，您需要指定有关计划部署的云函数的详细信息，包括函数名称和类型，以及将导致函数执行的触发器。

在 functionbeat.yml 中，配置要部署的函数。配置设置会根据您使用的函数类型和云服务提供商而有所不同。如果缺少所需集成的代码，可以在**附录 E** 中找到相关代码。下面提供了示例配置。

```
functionbeat.provider.aws.endpoint: "s3.amazonaws.com"
functionbeat.provider.aws.deploy_bucket: "functionbeat-deploy"
functionbeat.provider.aws.functions:
  - name: cloudwatch
    enabled: true
    type: cloudwatch_logs
    description: "lambda function for cloudwatch logs"
    triggers:
      - log_group_name: /aws/lambda/my-lambda-function
```

您还需要 AWS 凭据。在 functionbeat.yml 文件的顶部配置您的 AWS 凭据：

- access_key_id:"YOUR AWS ACCESS KEY ID"
- secret_access_key:"YOUR AWS ACCESS KEY"

如果您习惯使用其他身份验证方法，请参阅 **AWS 凭据选项**以了解更多详细信息。

请参考以下示例：

```
module: cloudwatch
enabled: true
access_key_id:"XyzW4VIA6DCIEKDUNB"
secret_access_key: "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

第 4 步：设置资产并部署 Functionbeat

Functionbeat 附带了用于解析、索引和可视化数据的预定义资产。要加载这些资产：

确保 functionbeat.yml 中指定的用户有权设置 Functionbeat。从安装目录中，运行：

```
./functionbeat setup -e
```

要部署云函数，请使用以下命令：

```
./functionbeat -v -e -d "*" deploy cloudwatch
```

现在，该函数已部署到 AWS 并准备好将日志事件发送到配置的输出。

第 5 步：构建用于分析的 Kibana 仪表板

现在，您可以在 Kibana 中构建仪表板。要了解如何查看和探索您的数据，
请参阅 Kibana 用户指南。要启动 Kibana，您需要：

- 登录您的 Elastic Cloud 帐户
- 导航到部署中的 Kibana 终端。

附录 E – 其他资源

有关高级 AWS 配置，请参阅以下文档：

- Filebeat
- Metricbeat
- Functionbeat

elastic

Search. Observe. Protect.

Elastic 能让您在企业搜索、可观测性和安全领域大规模地实时利用数据。Elastic 解决方案基于免费且开放的单一技术栈构建而成，可在任何地方部署，让您从任何类型的数据中都能立即获得可付诸实践的见解 — 从查找文档，到监测基础架构，再到威胁猎捕，无一不能胜任。全球范围内有数以千计的公司/组织使用 Elastic 来为任务关键型系统提供支持，例如，思科、高盛、微软、Mayo 医学中心、美国国家航空航天局 (NASA)、纽约时报、维基百科和 Verizon 等等。Elastic 成立于 2012 年，为 NYSE（纽约证券交易所）上市公司，股票代码为 ESTC。更多详情，请参见 elastic.co/cn。

美洲总部
800 West El Camino Real, Suite 350, Mountain View, California 94040
常规业务 +1 650 458 2620，销售 +1 650 458 2625

info@elastic.co