Elastic 隐私数据表

云连接中的 AutoOps

产品摘要：云连接中的 AutoOps

分布式搜索架构的演进要求运营管理和诊断能力同步提升。Cloud Connect 中的 Elastic AutoOps 是一款云连接工具，旨在为 Elasticsearch 集群提供实时问题检测、自动化根本原因分析以及可执行的性能建议，帮助企业无需维护完善的本地监控基础设施也能获得专家级见解。

Elastic AutoOps 的架构建立在云连接模型之上，这对于在 Elastic Cloud Enterprise (ECE)、Elastic Cloud on Kubernetes (ECK) 或独立的本地硬件上运行部署的自管理企业用户尤为适用。此模型可确保在 Elastic Cloud 中分析诊断性遥测数据的同时，客户索引中的实际内容绝不离开本地环境。通过严格限制仅处理操作元数据并提供强大的透明度控制，Elastic 可确保组织在优化极其复杂的搜索工作负载时，不损害数据的隐私性。如要在您的 ECE、ECK 或自管理的 Elasticsearch 集群中使用 AutoOps，您首先需要创建一个 Elastic Cloud 账户或登录您的现有账户。随后，安装向导将在所有步骤中引导您安装 Elastic Agent，以将指标从您的集群发送到 Elastic Cloud 中的 AutoOps。

- **产品类型：**软件
- **部署模式：**
    - 云 (SaaS)

在 AutoOps 中处理的数据

Elastic AutoOps 中的数据处理严格分为运行服务所需的管理数据和诊断集群健康所需的操作元数据。值得注意的是，在涉及客户内容时，AutoOps 被设计为只读解决方案；它不访问、获取或存储集群内管理的文档或源客户数据。

访问和使用 Elasticsearch 所需的个人数据类别：

为了管理该服务，需要处理某些类别的个人数据。这些数据对于维护安全访问、管理订阅以及确保系统交互的可审计日志至关重要。

- **管理员和用户标识符：**这包括账户注册、支持互动和事件通知配置时提供的姓名、电子邮件地址和电话号码。
- **凭据与权限：**系统会处理用户名、密码（加密）、会话 cookie 和活动日志，以管理安全访问并实施基于角色的访问控制 (RBAC)。

审计日志：系统会记录管理操作，例如注册集群或修改通知设置，以确保权责明确并满足安全审计的需求。

所处理的其他个人数据类别可能包括但不限于包含在以下内容中的数据：

- 操作元数据和诊断指标
    - 示例：详细的分片信息、全面的节点统计数据、集群范围的配置设置、整体健康状况摘要、索引和可组合模板列表、活跃的集群任务。
        - 收集这些指标可使 AutoOps 执行复杂的分析，例如识别分片不均衡、检测 CPU 使用率过高以及精准定位搜索和索引缓慢的查询请求。虽然其中一些字段（如索引名称或节点主机名）可以间接识别客户配置的内部基础架构，但它们并不包含存储在索引中的实际业务数据或最终用户记录。

处理输入到产品中的客户数据的典型目的：

Elastic AutoOps 对元数据的处理以最大限度地提高 Elasticsearch 平台的运行效率为目标，适用于以下使用场景：

- 实时问题检测和根本原因分析
    - AutoOps 将数百个指标关联起来，提供集群健康状况的统一视图。例如，系统可以识别出，在集群状态变为“红色”之前，磁盘高水位线事件已经持续出现了数日；这使得管理员能够在服务彻底中断之前，提前解决底层的存储问题。这种自动化的根本原因分析 (RCA) 使 DevOps 团队无需对图表和指标进行手动分析，而这在传统上是一个非常耗时的过程。
- 资源和成本优化
    - 处理 CPU 压力、内存利用率和磁盘 I/O 等资源使用指标可使 AutoOps 识别出资源未充分利用的节点或配置低效的索引。通过识别摄取瓶颈或数据结构配置错误，该工具可提供清晰的解析路径，从而提高资源效率并降低硬件成本。例如，“模板优化器”视图会分析映射和设置，并据此提出优化建议，以减少存储开销。
- 支持集成与协作诊断
    - AutoOps 隐私模型中的一个重要特性是“更好的支持”功能。客户可以向 Elastic 支持工程师授予对其 AutoOps 诊断数据的只读访问权限。这种共享的上下文环境使工程师能够准确地看到客户所看到的内容，从而更快、更精确地解决支持工单，无需手动上传诊断包。这种机制有助于实现“最小权限”的支持交付，支持过程对诊断数据的访问是临时的，并且需要客户明确授权。

产品使用数据

对于使用 AutoOps 的 Elastic Cloud 部署，Elastic 会自动收集与产品使用情况相关的某些信息。此类产品使用数据将按照 Elastic 产品隐私声明中所述的方式进行处理。

访问客户数据

- **客户访问：**
    - 客户对所摄入的数据保留完全的控制权和所有权，并可利用集成的基于角色的访问控制 (RBAC) 来定义精细化的权限，从而贯彻最小权限原则。通过统一的云端接口，用户可以访问节点、索引和分片的高层级指标、实时健康事件以及详细的性能可视化视图。
    - 为了让运行自管理集群的客户能够全面了解共享数据，AutoOps Elastic Agent 包含了一个故障排查配置文件。通过使用此配置重启代理，管理员可以在数据发送到 Elastic Cloud 之前，在本地查看从集群收集的数据样本。这样可以对披露的信息进行主动评估，并支持内部合规性审查。
    - 客户可以决定 Elastic 专员能够提取的数据类型——点击此处了解详情。

- **Elastic 的访问：**
    - 对于 Elastic Cloud 产品与服务，仅有极少数 Elastic 员工拥有对生产环境的特权访问权限，且仅用于平台管理、维护及支持目的。此类访问权限严格遵循最小权限原则和按需知晓原则，并定期接受审查，且根据需要进行调整。Elastic 在自管理部署中无法访问数据，只有在客户指示下（例如应客户要求提供支持服务时）才会访问云部署中的客户内容。
    - Elastic AutoOps 中的数据处理严格分为运行服务所需的管理数据和诊断集群健康所需的操作元数据。值得注意的是，在涉及客户内容时，AutoOps 被设计为只读解决方案；它不访问、获取或存储集群内管理的文档或源事件数据。这一设计有助于在共享的上下文中实现更快、更精准的故障排查，同时确保实际业务数据始终留存在客户的本地环境中。
    - Elastic 已实施集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，以记录对客户数据及其所在系统的所有访问。Elastic 的内部团队积极开发和实施针对可疑内部账户活动和未经授权访问的检测，包括文件完整性监控和账户接管指标。
    - Elastic 的原则规定，只有在法律严格强制的情况下，其才会披露客户数据或提供对客户数据的访问权限，这些原则还包括挑战此类请求以及在法律允许的情况下通知相关方的既定规程。

遵守隐私法规

Elastic 按照适用的客户数据处理附录和本隐私数据表中概述的承诺，捕获、处理、存储和保护客户个人数据。我们的信任中心是一个综合性资源平台，提供关于我们隐私实践与合规工作的各类信息。

- **数据所有权：**客户数据仍归客户所有。Elastic 仅为客户协议中指定的目的处理这些数据，并且绝不会将客户数据出售给第三方。
- **GDPR 合规性：**Elastic Cloud 的功能旨在支持遵守《通用数据保护条例》及其他全球数据保护和隐私法律。这包括通过有效的技术和组织措施优先保障个人数据安全，提供符合 GDPR 要求的数据处理附录。Elastic 的专职隐私团队负责 GDPR 合规工作。
- **数据隐私框架 (DPF)：**Elasticsearch, Inc. 已通过由美国商务部制定的《欧盟-美国数据隐私框架》、《欧盟-美国数据隐私框架英国扩展版本》以及《瑞士-美国数据隐私框架》认证。
  跨境数据传输：Elastic 依据现行的标准合同条款及参与数据隐私框架（针对向美国的传输以及从美国发出的后续传输），在开展业务的各司法管辖区之间合法进行个人数据传输。此外，我们还实施强有力的补充措施以保护传输过程中的数据，如传输中加密和静态加密、对公共机构索要数据的请求提出挑战的程序，并为客户提供选择区域服务器的选项以托管数据。

数据可移植性

客户对其摄入至自身集群中的数据保留完全控制权。对于 AutoOps 处理的元数据，用户可以通过“概览”和“节点”视图访问高层级指标。尽管存储在云端的具体遥测数据由 Elastic 负责管理，但原始指标仍保留在客户自管理的集群中，用户可通过标准的 Elasticsearch API 进行提取。

保留和删除

Elastic AutoOps 实施严格的数据保留政策，以遵循数据最小化原则和运营遥测数据的临时性特征。AutoOps 运营指标在 Elastic 的内部云基础设施中保留 10 天。这 10 天保留期既确保了近期性能趋势数据可用于故障诊断，又能自动清除那些在动态环境中通常已丧失运营参考价值的陈旧数据。

安全性

Elastic 实施了一套深度防御安全模型，致力于在整个生命周期内保护客户数据。访问处理 AutoOps 数据的系统受严格的组织和技术措施的管控。您的 Elastic Cloud 数据的安全性取决于您是否对您的 Elasticsearch 集群进行了安全配置，并妥善保管了您的 Elastic Cloud 登录凭据（如需了解更多信息，请参阅我们的安全性常见问题解答）。

- **AutoOps 架构：**Elastic AutoOps 的架构对于在 Elastic Cloud Enterprise (ECE)、Elastic Cloud on Kubernetes (ECK) 或独立本地硬件上运行部署的自管理企业用户而言尤为适用。此模型可确保在云端分析诊断性遥测数据的同时，底层业务数据（即客户索引中的实际内容）绝不离开本地环境。
- **通信协议：**Elastic AutoOps 利用两种主要通信协议，确保安全的遥测数据摄取。两个通道均通过标准端口 443 运行，确保与常见防火墙配置的兼容性，同时维护高加密标准。
  - 注册通道(HTTP/HTTPS)：此通道用于将本地集群注册到 Elastic Cloud。它使用一个受严格限制的 Elastic Cloud API 密钥，该密钥仅限在 Cloud 连接框架内使用。

    - 遥测通道（基于 HTTP 的 OTLP）：OpenTelemetry 协议 (OTLP) 用于收集运营数据。该通道使用 AutoOps 令牌进行身份验证，该令牌在功能上等同于 API 密钥，可确保只有授权专员才能将数据流式传输到特定的客户组织。
- **加密：**客户数据在静态下使用 AES-256 加密，在传输中通过 TLS 1.2 或更高版本进行加密。Elastic 实施严格的加密密钥管理程序，确保只有经授权的流程和用户才能访问加密数据。对于托管云部署，客户数据还通过集成到云服务提供商 (CSP) 基础架构中的强大密钥管理加以保护。
- **访问控制：**Elastic 实施技术、逻辑和管理控制措施，使数据访问权限限制在授权用户范围内。这些控制措施包括多因素身份验证、严格的密码强度标准以及使用虚拟专用网络 (VPN) 进行管理访问等。此外，基于角色的访问控制 (RBAC) 已集成到 Elastic 部署和 Elastic Cloud 管理平台中，允许对用户权限进行精细控制。
- **日志记录和监控：**Elastic 已实施集中式日志记录，包括代理日志、访问日志、Elasticsearch 日志和 Auditbeat 日志，以记录对客户数据及其所在系统的所有访问。Elastic 的威胁检测和响应团队利用自动化工作流程来检测和调查可疑的内部账户活动和未经授权的访问，包括文件完整性监控和账户接管指标。
- **系统更新和补丁：**Elasticsearch 实例会定期根据最新的操作系统内核进行更新和部署。每当在任何组件软件中识别出常见漏洞与披露 (CVE) 时，我们都会及时应用相应的补丁。
- **事件检测与响应：**Elastic 已实施并持续更新针对可疑活动和未经授权访问的检测规则。这些检测是自动化工作流的一部分，可以向威胁检测与响应团队发出警报，并触发分析调查。Elastic 在内部使用 Elastic Security，该解决方案包括终端检测和响应功能，并集成了威胁情报源以支持入侵检测。它通过与第三方 SOAR 平台集成支持自动响应，从而降低了数据泄露的可能性并缩短了响应时间。
- **安全软件开发框架 (SSDF)：**Elastic 维护着一套基于 NIST 800-218 标准的安全软件开发框架。该框架指导着所有 Elastic 软件的安全设计、开发、部署、跟踪和维护过程，确保落实“设计即安全”和“默认安全”的原则。
- **第三方供应商审核：**Elastic 与主要 IaaS 提供商（AWS、GCP、Azure）开展合作，并按第三方风险管理计划对他们的安全与合规标准进行严格审核，包括审核其 SOC 2 审计报告和 ISO 27001 及 27701 认证情况。
- **渗透测试：**Elastic Cloud 至少每年由独立的第三方机构进行应用程序和网络渗透测试。Elastic 还设有公开的漏洞赏金计划，供研究人员进行持续测试。
- **员工培训：**所有 Elastic 员工在入职时及之后至少每年都必须完成全面的信息安全和数据保护/隐私培训。