一种分布式实时监控报警系统的研究与实现

张宏海[1,2] 刘亚宁[1,2] 田 丰[1,2] 武学成[1,2] 刘 硕[1,2] 刘中一[1,2]
ZHANG Honghai LIU Yaning TIAN Feng WU Xuecheng LIU Shuo LIU Zhongyi

摘 要 近几年，随着运价系统业务不断增长，服务器节点数量呈现几何式扩张。如何对生产系统近千台服务器及应用进行有效的监控报警，成了企业亟须解决的问题。现有监控系统（如 Nagios、Zabbix、Prometheus 和 Open-Falcon）均无法满足系统对于日志数据深度分析处理并监控报警的能力。基于上述原因，以民航客运运价系统为背景，基于 ELK 体系架构和 Elastalert 日志告警插件，实现了一种分布式实时监控报警系统，不仅能够提供硬件监控、服务器基础监控和应用监控，还拥有强大的日志分析处理能力，可识别出异常的微小波动并及时发出警报，帮助运维人员迅速定位问题，并采取相应的措施，为民航客运运价系统的稳定运行提供了坚实的技术保障，也为处理复杂多变的监控需求提供了有力的工具。

关键词 监控；报警；日志数据；日志分析

doi：10.3969/j.issn.1672-9528.2024.08.006

0 引言

中国航信（TravelSky）作为国内民航业主导的信息服务供应商，运营着国内唯一一套行业级民航客运运价系统。随着互联网和移动互联网的快速发展，在线购买机票的旅客数量出现爆炸式增长，系统每年需要处理千亿级的旅客机票查询请求，导致服务器节点数量呈现几何式增长。如何对生产系统近千台服务器及应用进行有效的监控报警，成了企业亟须解决的问题[1]。

民航客运运价系统由于其业务的复杂性与特殊性，其监控系统在实际生产过程中需要对海量的应用日志进行实时收集与处理，并能够对结果进行快速的统计、分析和可视化展示，满足系统运维和数据分析等需求[2]。传统的监控系统，如 Nagios 和 Zabbix，虽然能够提供硬件监控、服务器基础监控和应用监控等功能，但在处理系统日志方面的能力却显得不足。此外，这些传统的监控系统通常采用单一部署的方式，无法实现横向扩展，不能应用于大规模数据的高并发场景。Prometheus 是一个流行的监控解决方案，虽然支持横向扩展，但需要手动对于监控数据进行拆分，操作复杂并有很大的局限性，而且也缺少对于系统日志分析处理的能力。Open-Falcon 是另一个支持横向扩展的监控工具，但它的安装过程复杂，组件众多，这使得新用户难以快速上手，同时它也不具备对系统日志进行分析处理的功能。

基于上述原因，本文以民航客运运价系统为背景，基于 ELK 体系架构和 Elastalert 日志告警插件，探讨了一种分布式实时监控报警系统的研究与实现。

1 系统设计

如图 1 总体结构图所示，系统主要由五个模块组成，包括数据收集、数据处理、数据存储、数据展示和数据报警。

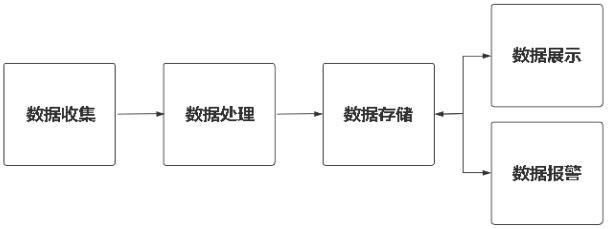

图 1 总体结构图

1.1 数据收集

数据收集主要实现监控数据的收集功能，为了确保数据的准确性和完整性，数据收集模块会部署到每个服务器节点上采集所需的信息。在收集过程中，系统不仅会收集传统的监控数据如硬件数据、服务器基础数据和应用监控数据，还会收集应用处理的请求和结果数据，以及服务器运行的详细信息，比如操作步骤、错误报告和运行时间等，这些信息对于分析系统性能和排除故障至关重要，而服务器的基础监控数据则包括了 CPU 使用率、内存占用、磁盘空间和网络流量等关键指标，这些数据有助于实时监控系统的健康状况和性能表现[3]。

在数据收集过程中，为了提高效率和保证数据处理的均衡性，通常会采用负载均衡的方式来分发数据，将数据均匀

1. 中国民航信息网络股份有限公司 北京 101318
2. 北京市民航大数据工程技术研究中心 北京 101318

地分配到数据处理部分的不同处理单元，以避免某一处理单元过载而导致处理延迟或失败。

1.2 数据处理

数据处理主要实现对原始数据进行转换处理的功能，完成对数据的解析和处理[4]。首先，对输入数据的格式进行解析，确保原始数据能够被正确读取；其次，对数据进行分类、筛选、过滤、处理、转换等操作，目的是让数据更加有效，便于后续的统计分析和监控报警。在数据处理的过程中，还涉及对无效或脏数据的处理。无效数据指的是那些不完整、错误或与预期格式不符的数据；脏数据是指包含错误或不一致信息的数据，需要能够识别出这些数据并删除，最后数据将被转换为要存储的格式，发送给数据存储模块。

总之，数据处理的主要目标是通过一系列的转换和处理步骤，确保数据从原始状态转换为可用、有效且可靠的信息。这个过程涉及数据的解析、清洗、处理和转换，每一步都是为了提高数据的质量和使用价值，便于后续的监控报警和数据分析。

1.3 数据存储

数据存储主要是确保数据的持久保存以及为这些数据创建有效的索引机制，是整个系统的核心部分。在处理大规模数据集时，数据存储采用了分片技术，将数据分割成块并分散存储在不同的物理位置。这种分布式存储的方法不仅能够处理和存储海量数据，还能确保系统的高可用性，即使在部分系统组件失效的情况下，也能保证用户能够访问到他们需要的数据[5-6]。为了应对数据量的增长和系统负载的变化，现代数据存储系统设计中包含了横向扩展的能力，这意味着系统可以通过增加更多的节点来扩充其存储和处理能力，而无需进行复杂的系统重构。这种弹性扩展能力使得系统能够灵活地适应不断变化的业务需求和技术挑战。此外，为了提高数据检索的速度和效率，数据存储系统通常会建立倒排索引。倒排索引是一种优化的索引结构，它允许系统快速定位到包含特定关键词的数据项。通过这种方式，即使是在处理大规模的数据集时，系统也能够实现秒级的响应时间，这对于需要快速返回搜索结果的应用场景来说至关重要[7-8]。

综上所述，数据存储系统不仅仅是一个被动地保存数据的仓库，还具备高效管理和检索数据的能力，通过分布式存储、弹性扩展和高效的索引机制，确保系统在处理海量数据时的高性能和高可用性。

1.4 数据展示

数据展示主要功能是对数据存储模块中的数据进行有效的展示，这个过程涉及多个步骤和技术的运用，以确保数据的准确、及时和易于理解的呈现。

首先，数据展示模块发送查询指令给数据存储模块。查询指令是根据用户的需求和查询条件生成的，包含了用户想要获取数据的相关信息，如数据的索引类型、范围、时间等。数据存储模块在接收到查询指令后，会根据指令的内容进行数据检索[9]。

其次，数据展示模块会获取到存储数据不同维度的检索结果。这些结果可能包括原始数据、处理过的数据、统计分析结果等，它们从不同的角度反映了数据的特性和信息，数据展示模块需要对这些结果进行处理和整合，以便于后续的展示。

最后，数据展示模块将处理后的结果以不同的形式展示到前端页面上。这可能包括图表、表格、地图等形式，取决于数据的性质和用户的需求，展示的形式应该直观、易读，能够让用户快速理解和分析数据。

总的来说，数据展示模块通过查询、检索和展示等一系列操作，实现了对数据存储模块中数据的有效展示，帮助用户更好地理解和使用数据。

1.5 数据报警

数据报警的主要职责是对数据存储模块中的数据进行实时监控，并在特定条件下触发报警机制。为了实现这一功能，用户需要提前设定一系列的报警规则，这些规则通常包括了一系列的参数和阈值。在系统运行过程中，数据报警模块会不断地根据用户配置的报警规则，向数据存储模块发送查询指令。这些查询指令的目的是检索与报警规则相关的数据，以便对数据进行实时分析。数据存储模块响应这些查询指令，并返回相应的数据检索结果给数据报警模块。数据报警模块接收到检索结果后，会与预先设定的报警阈值进行比较。当满足或超过了报警阈值时，就会触发报警，例如发送电子邮件或短信等，使得相关人员能够在第一时间得知数据的异常情况，从而采取相应的措施[10]。

总的来说，数据报警模块的作用是确保数据存储模块中的数据处于一个预期的范围内，一旦数据出现异常，就能够及时通知，以便系维人员能够迅速响应，确保系统稳定运行。

2 系统实现

上述方法已经在中国航信民航运价系统上完成了实践验证，并已经完全应用到生产集群中。该系统每年的访问量达到千亿级别，图 2 为系统的总体架构图。

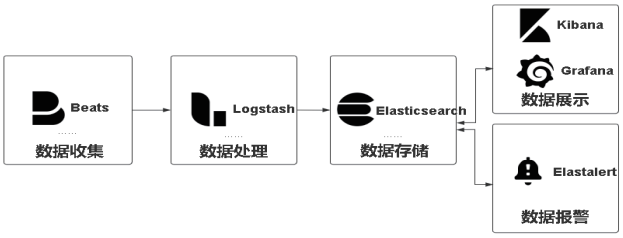

图 2 总体架构图

2.1 数据收集

如图 3 所示，数据收集模块的实现基于一个名为 beats

的技术框架。beats 是一套专为服务器端设计的轻量级数据采集程序，它由多个组件构成，主要包括 filebeat、packetbeat 和 metricbeat 这三个核心组件。

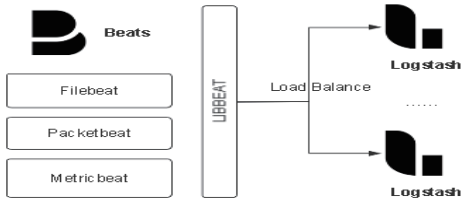

图 3 数据收集实现

首先，filebeat 是一个专门用于收集各种日志数据的组件。它具有强大的文本匹配能力，无论是单行还是多行文本，都能进行有效的匹配。这使得 filebeat 能够精确地记录和采集系统运行过程中的关键信息，为后续的数据分析和报警提供了丰富的数据。

其次，packetbeat 负责采集网络监控数据。通过 packetbeat，系统可以实时了解当前的网络运行状况，包括网络流量、连接状态等关键指标，从而对网络性能进行有效的监控和管理。

最后，metricbeat 是一个用于采集服务器基础监控数据的组件。它能够获取服务器的 CPU 使用情况、内存占用、磁盘空间等关键信息，使得系统管理员能够全面掌控服务器的当前运行状态，及时发现并解决可能出现的问题。

值得一提的是，beats 与 logstash 之间存在一种称为背压协议的机制。这种机制确保了数据在传输过程中的稳定性和可靠性，防止了数据传输过程中的丢失或错误，从而保证了整个数据收集过程的高效和准确。

2.2 数据处理

如图 4 所示，数据处理模块是基于 Logstash 实现。Logstash 能够处理大量的数据流并将其转换为有用的信息。在这个模块中，可以将其内部结构划分为三个主要部分，分别是 inputs、filters 和 outputs。

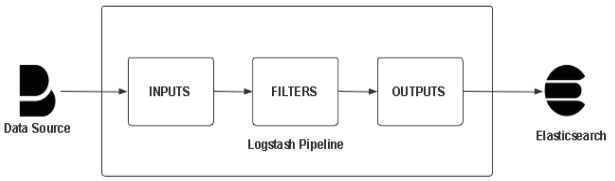

图 4 数据处理实现

首先，inputs 部分负责接收数据。这一部分可以接收来自各种来源的数据，包括文件、网络、系统日志等。这使得 Logstash 能够轻松地从不同的数据源获取数据，为后续的数据处理做好准备。

其次，filters 部分是数据处理的关键所在，也是整个数据处理过程中可能出现性能瓶颈的地方。在这里，通过使用定制的 Ruby 脚本来进行数据的处理，这样不仅可以提升数据处理的性能，还可以使实现更加灵活。

最后，outputs 部分负责将处理后的数据输出到指定的目标。这一部分也有着丰富的插件，可以将数据输出到各种不同的存储系统中，如 Elasticsearch、MySQL、Kafka 等。

2.3 数据存储

如图 5 所示，数据存储模块是基于 Elasticsearch 集群实现。在 Elasticsearch 集群中，使用了两种不同类型的节点，分别是 master 节点和 data 节点。这两种节点在集群中扮演着不同的角色，共同确保了整个集群的稳定运行和数据的高效管理。master 节点的主要职责是存储和管理 Elasticsearch 集群中所有的索引和分片的信息，对整个集群的状态进行监控，并对数据分片进行管理，确保数据的正确分布和有效存储。master 节点的存在，使得集群能够有一个中心化的管理点，从而更好地协调各个节点之间的工作。而 data 节点则是负责存储具体的数据分片，它们实现了数据的写入和查找功能。当需要存储或检索数据时，data 节点会执行相应的操作，这种设计使得 data 节点可以专注于数据处理，提高了整个集群的处理效率。

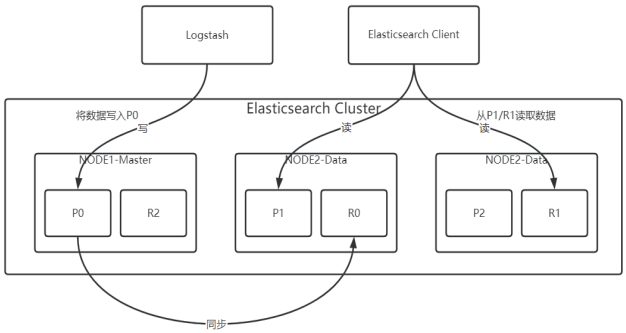

图 5 数据存储实现

在数据存储的过程中，当 Logstash 将数据输出到 Elasticsearch 集群时，master 节点首先会接收到这些数据，然后根据数据的特点和集群的当前状态，将数据分配到具体的索引分片上；接着 master 节点会将这些数据发送给对应的 data 节点，data 节点在接收到数据后，会对数据进行存储，并构建相应的索引；构建完成后，data 节点还会将数据同步到对应的副本分片中，这样便完成了数据的持久化存储。

为了提高数据的可用性和容错性，采用了增加分片的副本的方法。例如，如图 5 所示，当 Logstash 要写入数据到 P0 分片时，写完后会自动同步到 R0 分片上。这样，即使某个分片出现了问题，也可以从其副本中恢复数据，确保了数据的完整性和一致性。

2.4 数据展示

如图 6 所示，数据展示模块基于 Kibana 和 Grafana 实现，通过与 Elasticsearch 建立连接，该模块能够支持实时查询和展示 Elasticsearch 中存储的数据。

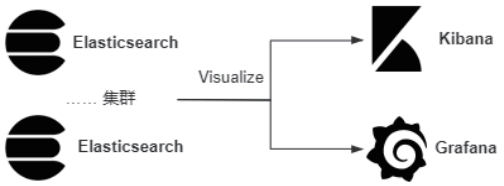

图 6 数据展示实现

Kibana 是 ELK 系统中的一个关键组件，它是专门为 Elasticsearch 设计的数据展示工具。在 Kibana 的 Discover 功能中，用户可以根据不同的条件来查找 Elasticsearch 中存储的数据，这使得数据的检索和分析变得非常灵活和方便。

Kibana 还提供了强大的可视化功能，允许用户根据自身需求生成各种不同风格的 Dashboard 报表。这些报表可以包含各种图表、表格和其他可视化元素，以便更直观地展示数据分析结果，用户还可以设置报表的刷新时间，以便实时更新数据和报表内容。而 Grafana 则是一个更为通用的数据可视化工具，它支持与 Elasticsearch 进行连接。Grafana 提供了丰富的仪表盘和图表选项，使用户能够根据需要创建各种定制的数据展示界面。

2.5 数据报警

如图 7 所示，数据报警模块是基于 Elastalert 实现的。Elastalert 是 Yelp 公司基于 Python 开发的一款开源的 ELK 日志报警插件，通过查询 Elasticsearch 中的数据与预定的告警规则进行对比，判断是否满足报警条件。当发生匹配时，将触发一个或多个报警动作，报警规则由 Elastalert 的 rules 定义，每个规则定义一个查询。

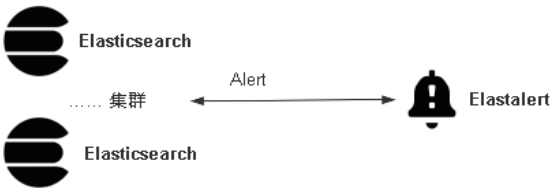

图 7 数据报警实现

具体来说，Elastalert 的工作流程如下。

（1）配置报警规则：用户根据实际需要，通过配置文件，设定一系列的报警规则。这些规则定义了什么样的数据状态会触发报警，例如数据超出预设的阈值、数据趋势异常等。

（2）规则查询：在用户配置好报警规则后，数据报警模块会根据这些规则，定期向 Elasticsearch 发送查询指令，检索当前数据状态，以便与报警规则进行比对。

（3）获取检索结果：Elasticsearch 在接收到查询指令后，会返回相应的数据检索结果。这些结果包含了数据的最新状态，如数值、变化趋势等关键信息。

（4）触发报警阈值：Elastalert 将获取到的数据检索结果与用户配置的报警规则进行比对，如果发现数据状态满足报警条件，即触发了报警阈值，包括向用户发送警报通知、记录日志、执行自动响应脚本等。

3 结论

综上所述，本文设计的分布式实时报警监控系统不仅为民航客运运价系统的稳定运行提供了坚实的技术保障，也为处理复杂多变的监控需求提供了有力的工具，为民航行业的信息安全与系统维护工作贡献了一套高效、可靠的解决方案。

参考文献：

[1] 张宏海，刘亚宁 . 一种分布式日志采集与分析系统 [J]. 信息技术与信息化 ,2022(6):87-90.

[2] 张宏海，刘亚宁 . 一种基于 Logstash 的高效数据处理方法 [J]. 信息技术与信息化 ,2022(7):84-87.

[3] 张宏海，刘亚宁，武学成，等 . 一种云上日志采集与分析系统的研究与实现 [J]. 信息技术与信息化 ,2023,(11):16-19.

[4] 郑逸凡 . 大型网站的架构模式研究 [J]. 山东农业工程学院学报 ,2016,33(12):151-152.

[5] 陈乐，余粟，王盟 . 基于分布式集群的高可用日志分析系统的设计 [J]. 中国电子科学研究院学报 ,2020,15(5):420-426.

[6] 付生 . 基于网络日志挖掘技术数据信息分析的研究 [J]. 科技与创新 ,2015(6):68-69.

[7] 李大洲 . 基于大数据的用户行为日志系统设计与实现 [D]. 南京 : 南京邮电大学 ,2020.

[8] 陈飞，艾中良，基于 Flume 的分布式日志采集分析系统设计与实现 [J]. 软件 ,2016,37(12):82-88.

[9] 张川，邓珍荣，邓星，等 . 基于 Chukwa 的大规模日志智能监测收集方法 [J]. 计算机工程与设计 ,2014,35(9):3263-3269.

[10] 尤勇，汪浩，任天，等 . 一种监控系统的链路跟踪型日志数据的存储设计 [J]. 软件学报 ,2021,32(5):1302-1321.

【作者简介】

张宏海（1978—），男，黑龙江哈尔滨人，硕士，高级工程师，研究方向：民航信息化技术。

刘亚宁（1987—），男，河北张家口人，学士，工程师，研究方向：民航信息化技术。

田丰（1980—），男，北京人，硕士，高级工程师，研究方向：中间件、云计算架构。

武学成（1986—），男，山东潍坊人，硕士，工程师，研究方向：民航信息化技术。

刘硕（1978—），女，辽宁葫芦岛人，硕士，高级工程师，研究方向：民航信息化技术。

刘中一（1987—），男，山西天镇人，硕士，高级工程师，研究方向：民航客票运价系统、密集计算系统。

（收稿日期：2024-05-27）