# 基于 ElasticSearch 的 IP 活动库的评估

叶忻，龚俭

（东南大学苏州联合研究生院，南京，211189）

**摘　要：**在未来网络 IP 流存储的研究中，海量存储数据库被认为是未来网络存储的基本架构。ElasticSearch 作为基于 Lucene 的搜索服务器，比传统的海量数据库具有更高的搜索能力。本文首先介绍了 IP 活动库的设计背景与 ElasticSearch 的基本性能。然后本文根据对 ElasticSearch 插入，查询和性能的评估，验证 ElasticSearch 是否能满足 IP 活动库的需求。

**关键词：**IP 活动库；海量数据库；ElasticSearch；插入；查询 ；规模

# Evaluation of IP Activity Databases based on ElasticSearch

Ye Xin, Gong Jian

(Suzhou Union Master Academy , Southeast University, Nanjing, 211189)

**Abstract:** In the future IP records storage, the massive database is considered as the future network storage infrastructure. ElasticSearch,as the search server based on Lucene, has better search abilities compared to traditional massive databases. The article introduces background of IP Activity table and basic performance of ElasticSearch. Then,, the article test whether ElasticSearch could meet the need of IP activity table by evaluating ElasticSearch inserting , search and storage perforamance;

**Key words:** IP activity table; Massive database; ElasticSearch; Insert; search; scale

IP 活动库属于“211 工程三期公共服务体系建设项目“、“中国教育和科研计算机网主干网和重点学科信息服务体系升级扩容工程”--CERNET 安全保障系统。CERNET 安全保障系统为网络行为监控和管理系统提供拥有者信息查询，以满足网络服务质量管理和网络有害行为分析追踪的需要。为了对 CERNET 进行网络管理和安全监控，需要以下三个部分的安全保障措施:日常流量监测,网络异常行为的发现，以及异常产生的原因分析和对异常行为的响应。对流记录的异常监测和原因分析以及对异常作出响应是由网络行为监测系统（NBOS）和应急响应协同服务系统（CHAIRS）来提供的。

CERNET 安全保障系统新增的 IP 综合信息系统（IPCIS 系统)负责获取和管理 CERNET 及与 CERNET 相关的 IP 管理归属和使用位置信息以及对应主机的通信特征，为 CERNET 网络管理系统（NBOS 系统）和安全保障系统（Chairs 系统）提供关于 IP 及其对应主机综合信息，包括 IP 地址的管理归属、使用位置、对应主机的服务类型、通信特征和 IP 活动等信息服务。

IP 活动库是集成于 IPCIS 系统中,存储 CERNET 系统在一定时限通信流记录的数据库。在 CERNET 系统中，IP 活动库从 NBOS 驻地系统获取流记录，将这些数据库实时存储并提供实时查询的功能 CERNET 系统中各个模块和外部用户调用。

为存储 CERNET 系统产生的海量流记录，IP 活动库拟设计为网络平台下分布式海量数据库。IP 活动库需存储 CERNET 系统每天产生的流记录,并为用户提供快速查询功能。CERNET 系统中每天产生约 88G 流记录，IP 活动库必须能在小于一天的时间内存储这些流记录。同时，为满足用户对查询的需求，IP 活动库对结果的返回时间尽可能短，最好能小于 100s。因为 IP 活动库所在数据库数据规模有限，应能存储至少 3 个月以上的数据。因此 IP 活动库的实现受到数据规模，插入性能，查询性能的约束。

根据 CAP 理论，即一致性(Consistency)、可用性 (Availability) 和分区容忍性 (Partition tolerance)理论，对于一个分布式系统上述三个条件最多只能同时满足其中两个。传统的关系型数据库保证了强的一致性和高可用性，导致低分区容忍性，因此扩展能力十分有限。非关系型数据库通过牺牲强一致性，通常只需要满足最终一致性，来换取系统可用性和分区容忍性的性能提高。因此，目前海量数据的存储普遍采用 NoSQL 数据库。然而，

NoSql 数据库往往存在数据量过大导致查找效率低的问题。ElasticSearch 的出现很好的解决了这个问题。通过查阅相关资料，RlasticSearch 的查询性能比普通NoSql数据库的存储效率提高了10倍以上。因此拟采用 ElasticSearch 来实现 IP 活动库。

基于上述需求，本论文希望通过实验，验证 ElasticSearch 满足 IP 活动库的存储、查询数据规模等需求。因此，文章分为三个部分。第一部分介绍基于 Lucene 的搜索服务器--ElasticSearch。第二部分是通过 IP 活动库的评验证 ElasticSearch 是否满足 IP 活动库的需求。第三部分给出 ElasticSearch 能否满足 IP 活动库需求的结论。

# 1 ElasticSearch 简介

ElasticSearch 是基于 Lucence 的一个搜索服务器。Lucene 是 apache 软件基金会项目组的一个子项目，是一个开放源代码的全文检索引擎工具包，Lucene 的目的是为软件开发人员提供一个简单易用的工具包，以方便的在目标系统中实现全文检索的功能，或者是以此为基础建立起完整的全文检索引擎。

ElasticSearch 由弹性网络演化而来的搜索方法，继承了弹性网络的思想。ES 支持分布式集群（Cluster），集群中有多个节点（Node）。内部来看有一个主节点，可以通过选举产生的。从外部看 ES 集群，无中心节点，在逻辑上是个整体，与任何一个节点的通信和与整个 ES 集群通信是等价的。其基本概念如下表所示：

表 1 ElasticSearch 基本概念

| | |
|---|---|
| Index | 类似于关系数据库的 database |
| shards | es 可以把一个完整的索引分成多个分片，这样的好处是可以把一个大的索引拆分成多个，分布到不同的节点上 |
| Cluster | 代表一个集群 |
| node | 组成 cluster 的各个节点 |
| Replica | 和 replication 通常指的都是一回事，即 index 的冗余备份，可以用于防止数据丢失，或者用来做负载分担 |

ElasticSerch 可以通过三种方式进行访问。第一种方式是在 linux 命令行用 curl 命令进行访问。第二种方式是采用 Marvel 工具对数据库数据和状态进行查询。arvel 是 Elasticsearch 的管理和监控工具，对于开发使用免费的。它配备了一个叫做 Sense 的交互式控制台，方便通过浏览器直接与 Elasticsearch 交互。Marvel 是 Elasticsearch 的管理和监控工具，对于开发使用免费的。它配备了一个叫做 Sense 的交互式控制台，方便通过浏览器直接与 Elasticsearch 交互。第三种方式是在编程工具中调用 ElasticSearch 提供的 java 等 API 进行增删该差等操作。本文的后续评估实验采用第三种方法。

Elasticsearch 相比起传统的海量数据库有更快的搜索速度，且安装简单，可完全自由地搜。其次，ElasticSearch 还可可以简单地通过 HTTP 使用 JSON 索引数据。此外，ElasticSearch 通过创建分布式的搜索集群，能够实时搜索。

# 2 对 ElasticSearch 的性能评估

## 2.1 验证 ElasticSearch 能否满足 IP 活动库的插入需求

该实验的硬件环境为有 8 个物理核，32 个逻辑核的服务器，其硬盘空间为 8T，内存为 132G，且为 64 位。

本实验的测试数据来源于 CERNET 系统中的 NBOS 流记录。保留其中的如下字段：表中数据格式如下，包括原宿地址，下一跳地址，原宿端口，端口号，流结束时间，流开始时间，源地址自治域好，宿地址自治域号，目的网关，源网关，报文数，字节数，Tcp 标志。每张表的大小依据测试条件而定。并根据 CERNET 系统对后续 IP 活动库流活动的分析，增加应用标签，服务类型字段。

表 2 IP 活动库表格式

| 字段 | 说明 | 类型 |
|---|---|---|
| srcaddr | 源 IP 地址 | u_int32 |
| dstaddr | 宿 IP 地址 | u_int32 |
| nexthop | 下一条地址 | u_int32 |
| srcport | 源端口 | u_int16 |
| dstport | 宿端口 | u_int16 |
| prot | IP 协议号，6=tcp，17=udp | u_int8 |
| last | 流结束时间 | u_int32 |
| src_as | 源地址自治域号 | u_int16 |
| dst_as | 宿地址自治域号 | u_int16 |
| src_mask | 源网关 | u_int8 |
| dst_mask | 宿网关 | u_int8 |
| toa | 应用标签 | u_int8 |
| first | 流开始时间 | u_int32 |
| dPkts | 报文数 | u_int32 |
| dOctets | 字节数 | u_int32 |
| tos | 服务类型 | u_int8 |
| Tcp_flags | TCP 标志 | u_int8 |

对于数据插入效率，我们首先认为是和数据库的规模有关的。我们每隔一小时监测十分钟 ElasticSearch 的数据插入速率。因为统计图太多，现在给出数据库规模为 1GB，6GB，12GB 以及 24GB 的插入时间和插入速率统计图：

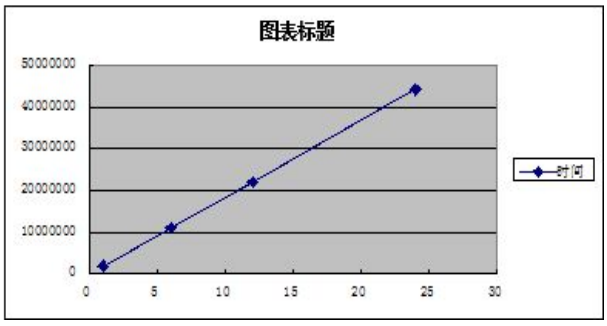


图 1 数量-时间图

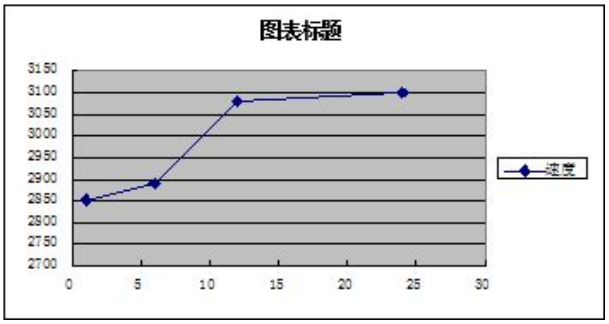


图 2 数量-速度图

查询结果说明，随着插入数量增加，插入所耗时间也增加，但插入速度保持稳定，大约为 3000 条/秒。按这一速度，一小时数据的插入大约需要 40 分钟，这一性能是可以满足 IP 活动库的实时插入需求的。

因此，基于 ElasticSearch 的 IP 活动库可以满足 CERNET 系统中的对于流记录实时存储的需求。

## 2.2 验证 ElasticSearch 能否满足 IP 活动库的查询需求

本实验的实验环境和数据库格式同上一个实验。该实验主要主要针对 IP 活动库单表查询效率。测试数据时用的是 CERNET 系统中处理的过的 NBOS 流。顺序查询大小为 1G, 6G, 12G, 24G 的数据，即 1 小时，6 小时，12 小时，24 小时数据。希望通过查询，发现查询速度和查询数据量的关系。结果如下：

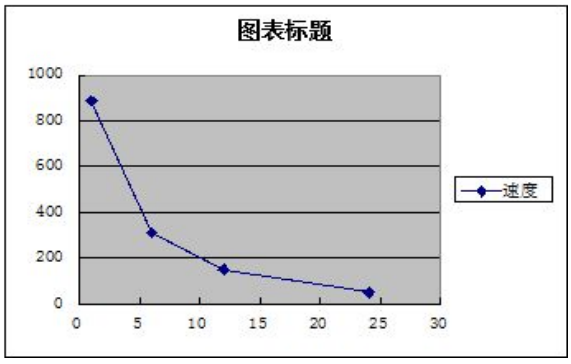


图 3 数量-时间图

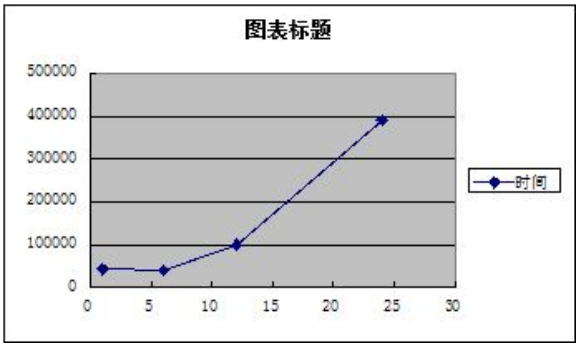


图 4 数量-时间图

该实验结果说明，对于 1G 的数据，查询所用时间最短，约为 50s，返回查询结果速度约为 880 条/秒。而当查询 24G 数据时，所用时间约为 400s，返回查询结果速度为 50 条/秒。

而对于海量数据库 MongoDB，查询 1G 数据，查时间则超过 100s,这个性能还是比较优越的。然而，查询 24G 数据时，返回时间已达到 400ms，这个结果是不能接受的。

因此，后续试验应进一步确定如何分表，从而使得查询较大数据量时所用时间是最短的。具体实验如下。

将表分别分为 1G，6G 和 24G 大小来查询 24G 的数据。即把表分为 24 张，4 张和 1 张。希望通过该实验的查询结果，能看出如何分表。下图为多次实验的平均结果：

表 3 IP 活动库分表评测

| | 时间（ms） |
|---|---|
| 1G | 97540 |
| 6G | 18920 |
| 12G | 23415 |
| 24G | 39806 |

表 4 IP 活动库分表评测

| | 时间（ms） |
|---|---|
| 1G | 230380 |
| 6G | 40865 |
| 12G | 56432 |
| 24G | 84356 |

由上图可知，当分表为 6G 时，查询 24、48G 数据消耗时间最少。为知道将表分为 6G 时，查询更多数据是否仍然具有比较高的性能。为判断这一假设是否正确，将表分别分为 1G，6G 和 24G 大小来查询 96G 的数据。

表 5 IP 活动库分表评测

| | 时间（ms） |
|---|---|
| 1G | 543267 |
| 6G | 123120 |
| 12G | 164789 |
| 24G | 215907 |

由上图可知，将表分别分为 1G，6G 和 24G 大小来查询 96G 的数据时，将表分为 6G 大小仍然有最低的查询时间。然而，尽管将表设计为 6G 大小时，IP 活动库拥有最短的查询时间。但是当数据量查询总量为 96G 时，查询时间已经达到 123s,这个是可以接受的，但是还需进一步缩短。

### 2.3 验证 ElasticSearch 能否满足 IP 活动库的数据规模需求

当将表大小设计为 6G 时，对一台可用硬盘容量为 6T 的服务器，建立一个 ElasticSearch 集群，预计会有 1000 张表。当 IP 活动库正式运转时，数据集来自于 CERNET 系统中流经的 Netflow 流，每天的数据将达到 88G。因此，该 IP 活动库预计可以存储 3 个月的数据。

## 3 结论

本文是对 ElasticSearch 的插入，查询和数据规模进行的一个评估。通过实验，ElasticSearch 可以很好满足 IP 活动库的插入、查询需求和数据规模需求。

相信在未来随着 ElasticSearch 技术的普及，必然有越来越多的数据库用到该技术。随着海量数据库存储知识的不断发展，在未来海量数据库必然有更加优秀的架构和性能。

# 参考资料

[1]http://baike.baidu.com/link?url=WhKL5E-z_9YLW1fF7b631KYdCswh-zHJQbqD8YYG4_szC0JrC3_IBZd-LU38uE5rKeHFyXs01j1rd-_9UAOpRa
[2]http://baike.baidu.com/view/1911305.htm?fr=aladdin
[3]http://sh.516878.com/2014/0802/27811.html
[4]http://blog.csdn.net/dinglang_2009/article/details/8180937
[5]http://blog.nosqlfan.com/html/1727.html
[6]http://www.2cto.com/database/201405/301861.html
[7]http://www.oschina.net/question/12_33599
[8]郭匡宇.基于 MongoDB 的传感器数据分布式存储的研究与应用.2013 南京邮电大学
[9]http://www.searchtb.com/2011/01/understanding-hbase.html
[10]硕士论文 姚建.视频网站的Big Data解决之道[J].程序员,2011(08)
[11]http://www.cnblogs.com/lovecindywang/archive/2011/03/02/1969324.html
[12]http://baike.baidu.com/view/1911305.htm?fr=aladdin
[13]http://sh.516878.com/2014/0802/27811.html
[14]http://blog.csdn.net/dinglang_2009/article/details/8180937
[15]http://www.oschina.net/question/12_33599
[16]http://www.open-open.com/news/view/fb4a14
[17] 张华强.关系型数据库与 NoSQL 数据库.电脑知识与技术,2011,07(20)
[18] Brewer E A. Towards robust distributed systems[C]. (Invited Talk PPT) Proceedings of ACM Principles of Distributed Computing, 2000.
[19] 张瑞. 数据库分布式高可用架构[J]. 程序员，2010 (6)：61-63.