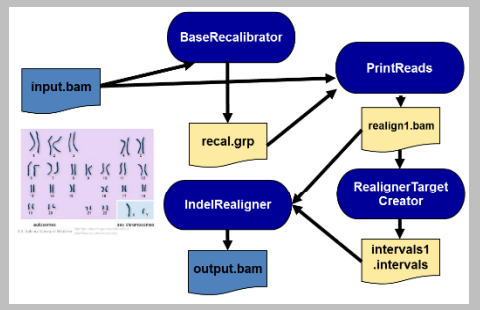
基于Data Thinker技术的大规模实时网络日志分析

瞿庆海* 顾磷† 陈文涛† 马志强† 张欣源†‡

*上海交通大学
†宁波数方信息技术有限公司
‡加大圣地亚哥分校

大数据应用与技术



PRISM

Security

Log analysis

Text mining

GATK

Machine learning

Echelon

Hututa

Palantir

Google

Amazon

MapR

Microsoft

Transwarp

Databricks

Data Thinker

Dryad

Mahout

MLlib

HBase

GraphLab

Spanner

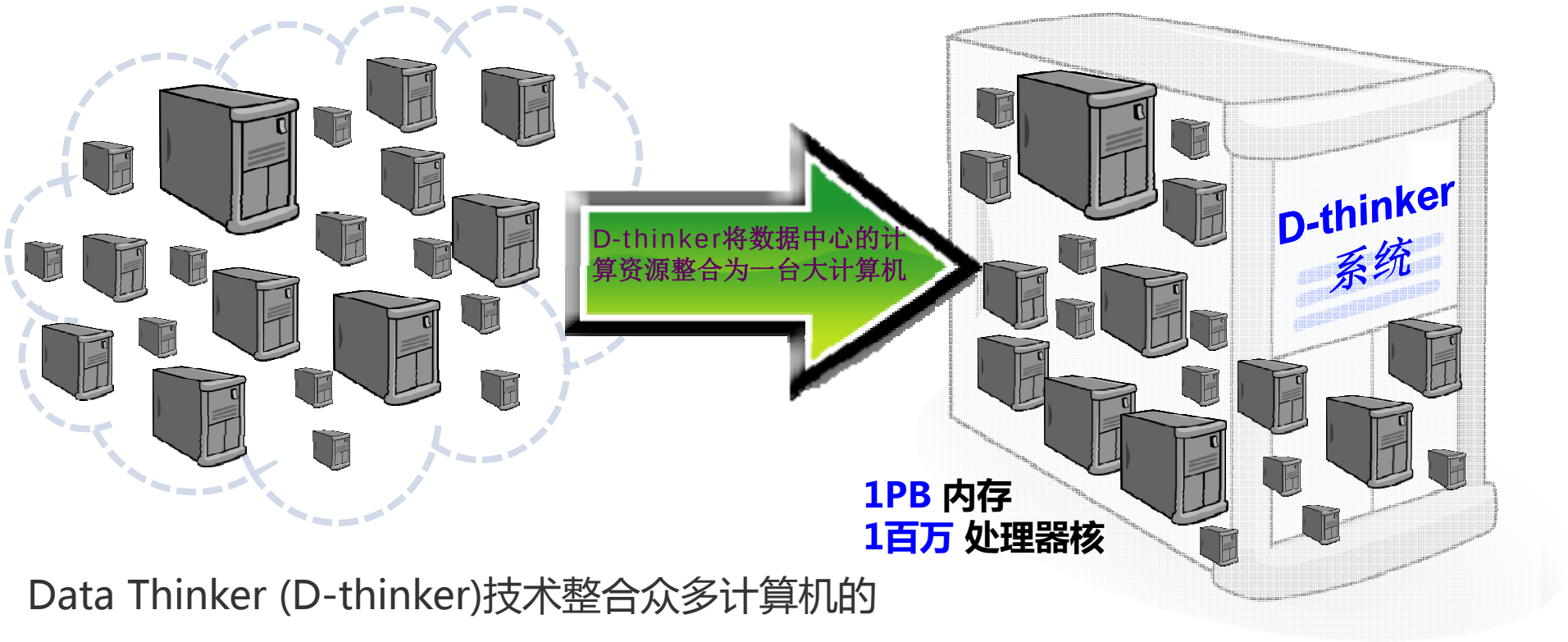
Dynamo

Spark

MPI

Hadoop

Data Thinker (D-thinker)：高性能大数据计算

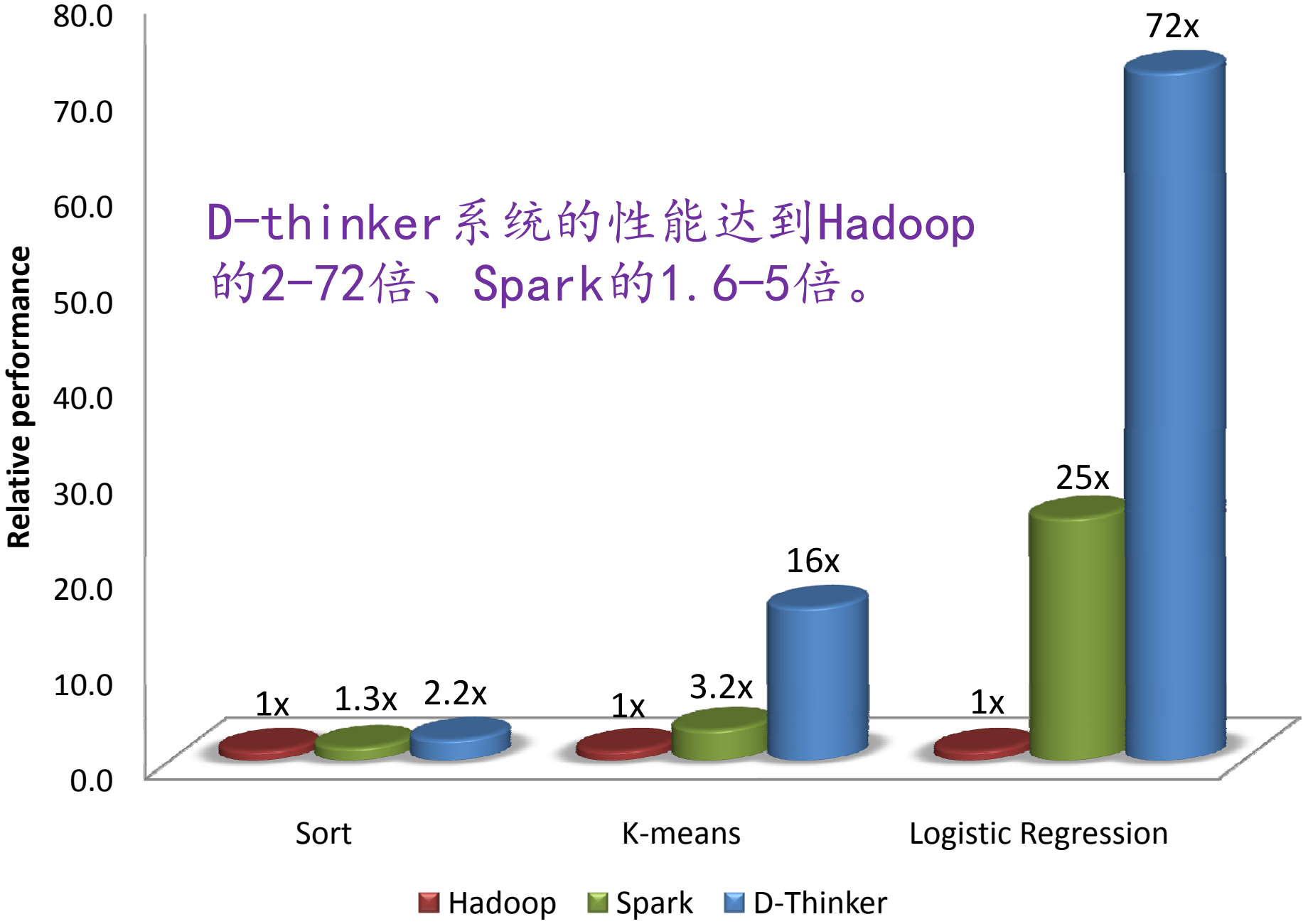


Data Thinker (D-thinker)技术整合众多计算机的CPU、内存及硬盘资源，以经济、高效、可扩展的方式构建高性能、低延时、图灵完备的计算体系，提供对GB-PB量级数据的存储、搜索、挖掘、学习及商业智能处理的能力，其性能较Hadoop高2-70倍、较Spark高1.6-5倍，并且可实现几乎所有大数据算法和应用。

"The datacenter as a computer."

– Luiz André Barroso and Urs Hölzle, Google

性能比较： Hadoop, Spark & D-thinker

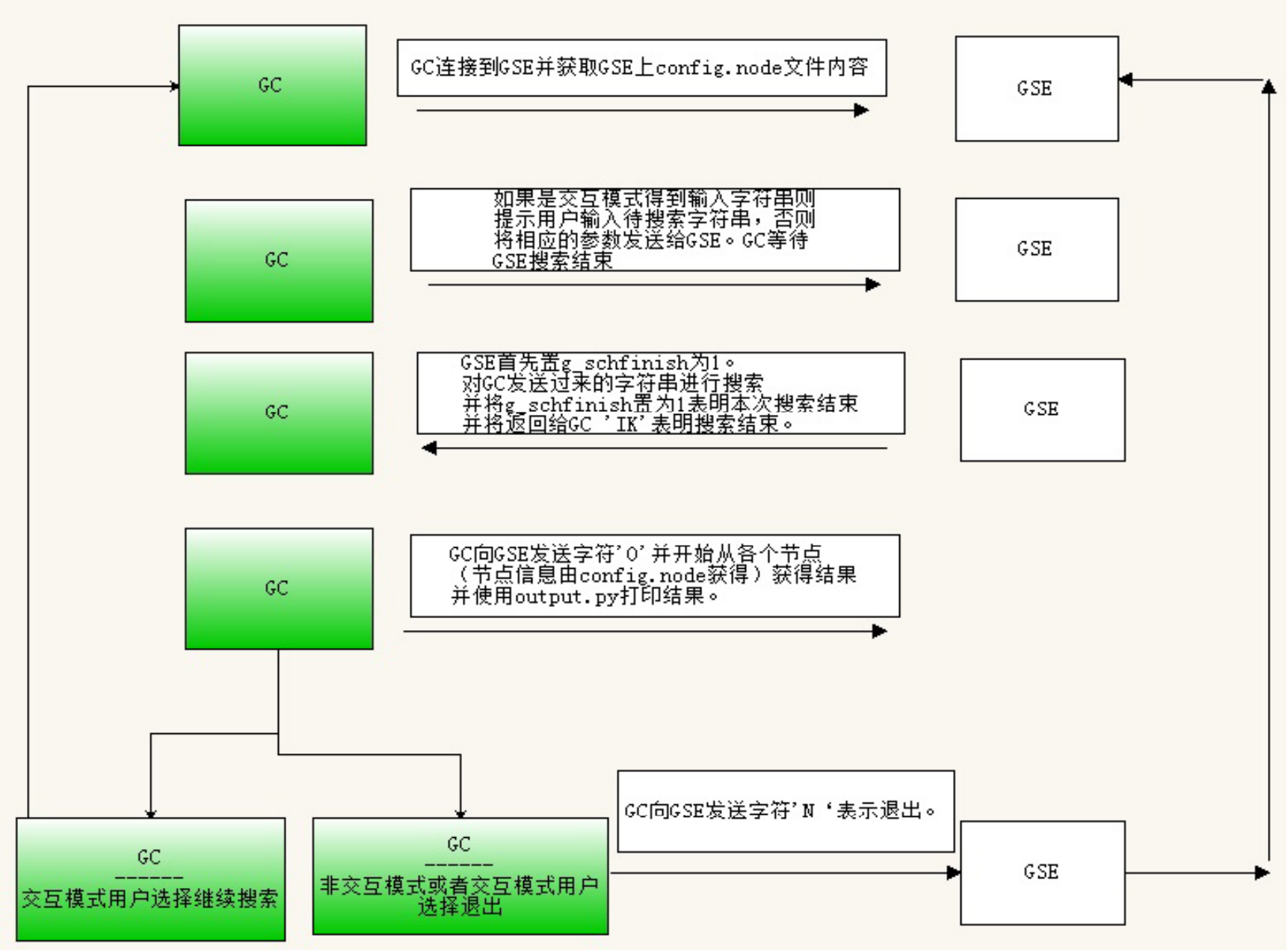


Greppy全文检索引擎

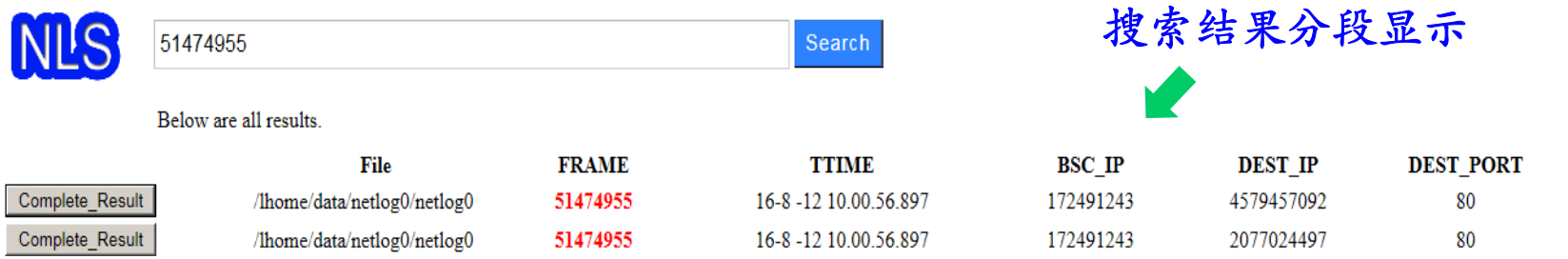
我们基于Data Thinker技术设计和实现Greppy通用全文检索引擎，要求其在秒级时间内完成对TB级数据全文搜索，以支持安全和日志分析应用。系统应达到如下要求：

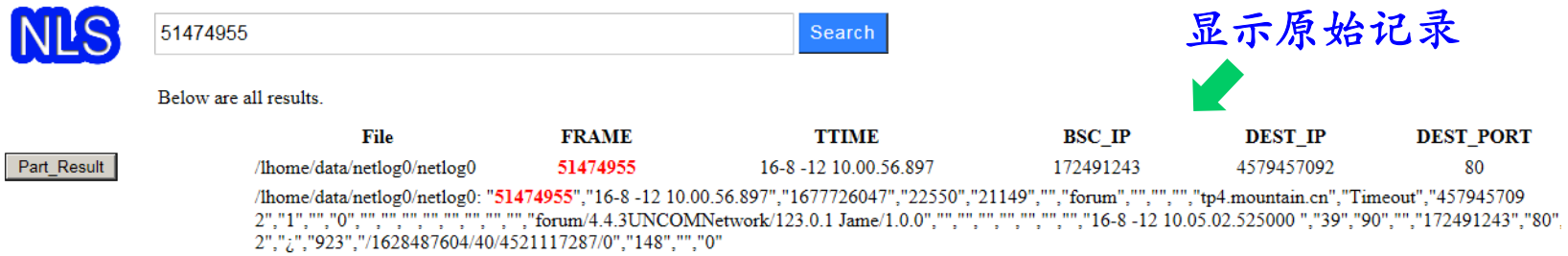
- ✓ 高性能、高性价比：引擎所需硬件平台兼容性广，在PC服务器上即可获得较高性能，性价比高
- ✓ 内存中大数据处理：Greppy系统可将数十TB数据全部载入内存处理，达到极高运算处理速度。
- ✓ 功能强大、定制灵活：既能处理离线检索，也能支持实时查询，既可通过传统字符串匹配搜索，也能支持复杂匹配逻辑运算。整个体系可通过灵活的接口进行深度开发，支持各类应用。
- ✓ 良好的系统扩展性能：系统可自然扩展至上百个节点。

Greppy系统架构


GC
GC连接到GSE并获取GSE上config.node文件内容
GSE
GC
如果是交互模式得到输入字符串则
提示用户输入待搜索字符串，否则
将相应的参数发送给GSE。GC等待
GSE搜索结束
GSE
GC
GSE首先置g_schfinish为1。
对GC发送过来的字符串进行搜索
并将g_schfinish置为1表明本次搜索结束
并将返回给GC 'IK'表明搜索结束。
GSE
GC
GC向GSE发送字符'O'并开始从各个节点
（节点信息由config.node获得）获得结果
并使用output.py打印结果。
GC向GSE发送字符'N'表示退出。
GC
交互模式用户选择继续搜索
GC
非交互模式或者交互模式用户
选择退出
GSE

使用Greppy系统分析网络流量



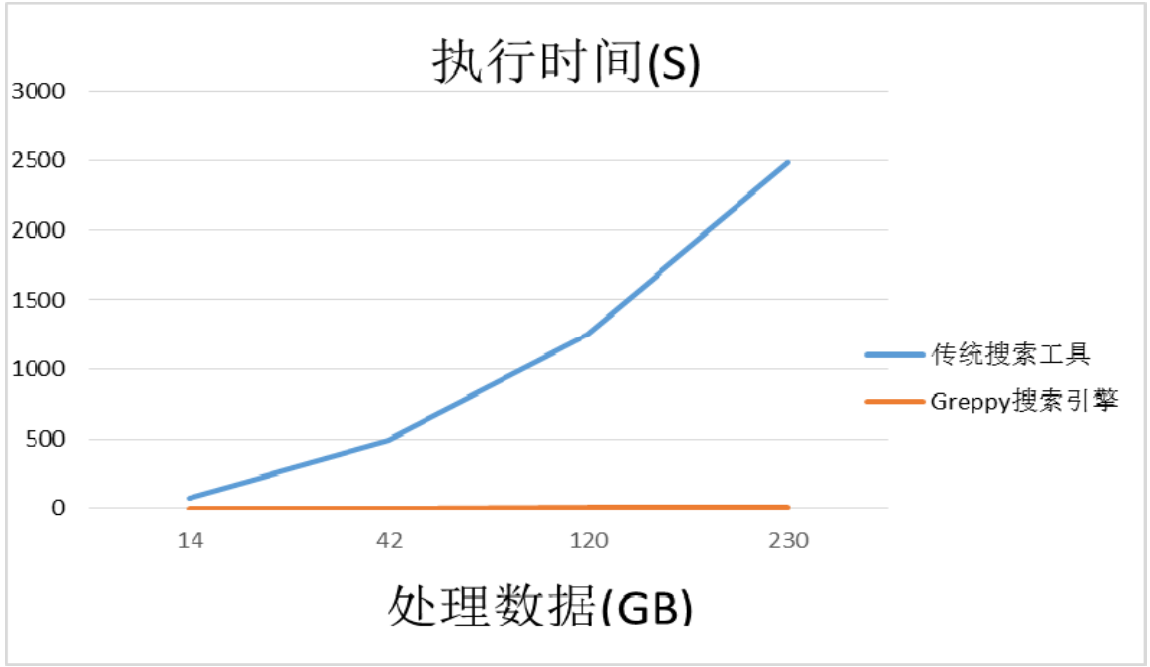


Greppy系统网页客户端在搜索完毕后会将搜索结果以行为单位进行输出，并且对每一行的各个字段进行注解。对于较长的结果可通过按钮控制，灵活度大。

性能分析：搜索时间

在相同配置的服务器上对不同规模数据进行文本搜索，比较Greppy与传统grep搜索执行时间

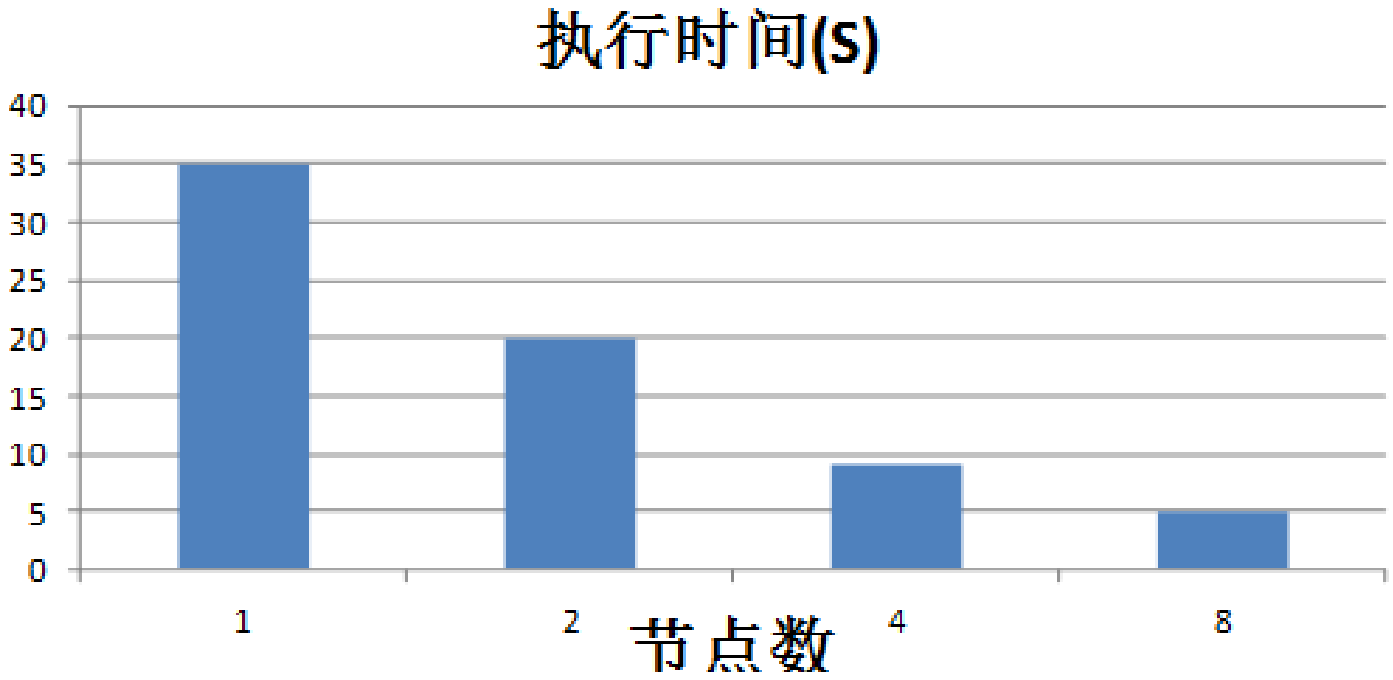
- 使用传统搜索工具grep随着数据的集的增长其所需时间呈超线性增长，从230GB数据中得到搜索结果需要2500s。
- Greppy搜索230GB数据只需5s左右。
- Greppy/Data Thinker使得单次查询时间缩短并保持在10秒以内，使得网络管理员能够在合理时间内根据情况进行多次查询，从而分析网络事件情况，支持实时、交互式应用。



性能分析：可扩展性

依次增加节点数，测量Greppy数据检索时间

- 每个网络日志查询需处理200GB数据，并且对每个字段进行分析和精确匹配。
- 随着节点数增多，Greppy检索时间从35秒下降到5秒，引擎处理能力随着节点数的增加大致呈线性增长。
- Data Thinker支持总量为16EB的存储能力，使得该系统可近乎无限地扩展存储能力，而扩展可以以渐进的方式进行。



不同节点数检索200GB数据所需时间