Z-LOG 日志管理系统

产品概述

Product Summary

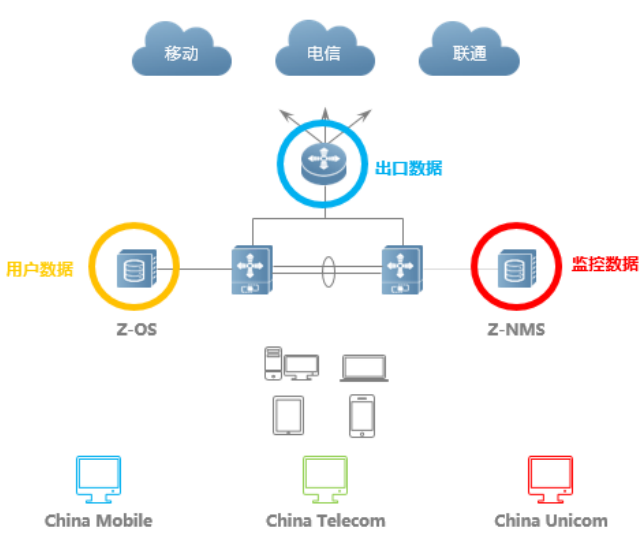
Z-LOG 是卓智自主开发的数据分析系统，该产品不但可以接收网关、流控设备同步的 NAT 日志和用户访问互联网络的 URL，还可以接收运营管理系统同步的用户账号信息、用户访问网络资源时的上下线明细、用户认证时的错误信息，网路管理系统同步的设备 SYSLOG 等。软件平台通过 HBase 的方式进行数据存储，引入 elasticSearch 作为二级索引，提升数据查询的效率。

Z-LOG 通过将用户账号信息与采集数据进行关联，实现实名数据记录，完全满足公安部 82 号令《互联网安全保护技术措施规定》信息留存及监督的要求，以及无线新网《公共场所无线上网安全管理系统》相关规定的管理要求。数据的分析采集为管理者的管理提供数据方面的支撑；

产品特性

Product Features

① 相关数据集中管理



✧ **接收出口设备日志**

✓ 接收出口设备的 NAT 日志、用户访问互联的 URL 信息，出口设备流量信息等；

✓ 标准日志数据接收接口，支持大部分常见网关设备；

✧ **接收运营管理系统数据**

✓ 运营管理系统保存大量用户账号信息、用户访问网络资源的上下线信息、用户接入网络时认证信息；

✓ 通过系统联动实现运营管理系统数据异地保存；

✧ **接收网络管理系统数据**

✓ 监控平台主要用于网络实时监控，在监控过程中会收集大量的设备日志信息；

✓ 通过系统联动实现网络状态数据异地存储、分析，为周期性网络健康分析提供支撑；

② 网络海量数据存储

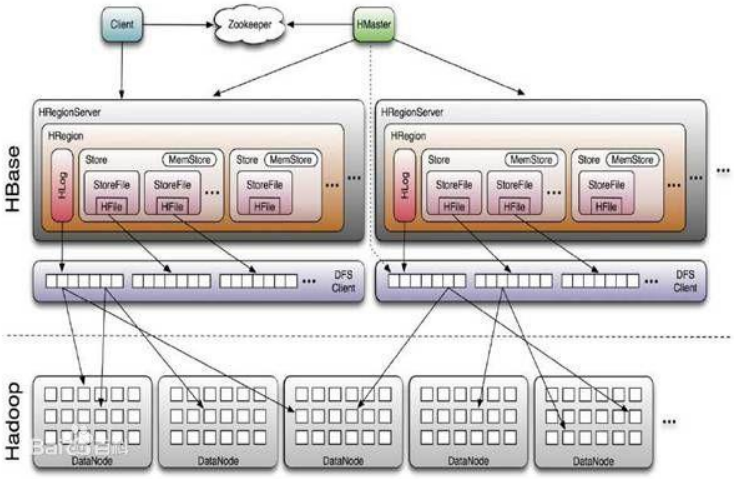
✧ **数据存储**

✓ Z-LOG 使用主流框架 hadoop-hbase 作为数据仓库，存储性能较高，单节点测试性能 20000 条/秒；HBase 不同于一般的关系数据库，它是一个适合于非结构化数据

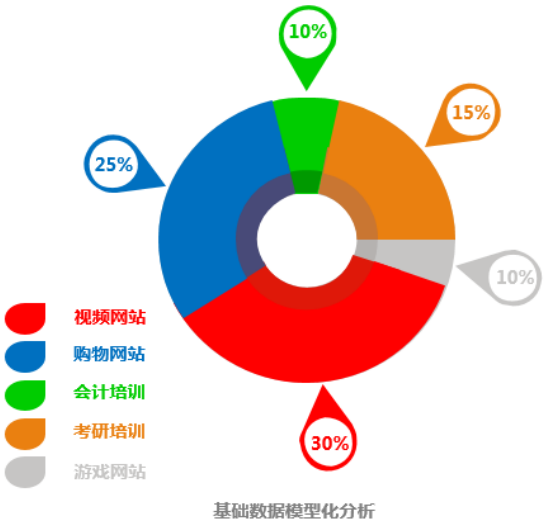
存储的数据库。另一个不同的是 HBase 基于列的而不是基于行的模式；HBase 是一个高可靠性、高性能、面向列、可伸缩的分布式存储系统，利用 HBase 技术可在 Server 上搭建起大规模结构化存储集群。

✧ **数据检索**

✓ 引入 elasticSearch 作为二级索引，大幅提高查询效率，单节点测试性能 2000 条/秒，满足实时分页查询需求。



③ 基础数据模型化分析



基础数据模型化分析

✧ **用户画像**

✓ 通过收集的 NAT 日志\URL 信息反向解析，分析出学生喜欢访问网站的类型；

✓ 通过爬虫技术收集用户经常浏览的数据内容，并分类整理；

✧ **用户体验**

- ✓ 通过 Z-OS 系统同步的用户上网明细，分析用户上网轨迹；
- ✓ 分析校园网热点区域的位置、上网高峰时间、网络中接入主要终端类型等

✧ **网络健康度**

- ✓ 通过 Z-NMS 系统同步的网络设备实时监控数据，基于网络模型分析网络健康度，影响健康的主要因素；
- ✓ 网络设备运行历史数据分析，为网络优化提供数据支撑；

④ 82 号令实名日志记录

第八条 提供互联网接入服务的单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：

(一) 记录并留存用户注册信息；

(二) 使用内部网络地址与互联网网络地址转换方式为用户提供接入服务的，能够记录并留存用户使用的互联网网络地址和内部网络地址对应关系；

(三) 记录、跟踪网络运行状态，监测、记录网络安全事件等安全审计功能；

第十三条 互联网服务提供者和联网使用单位依照本规定落实的记录留存技术措施，应当具有至少保存六十天记录备份的功能；

如上图所示，Z-LOG 系统独特的 HBase 数据存储技术，数据保存的时间只和服务器的硬盘大小有关，数据库存储能力不再是瓶颈。通过与 Z-OS 系统联动实现数据的实名保存，

同时高效的数据检索方式为日志查询提供支撑。

订购信息

Order information

型号	描述	备注
Z-LOG 日志管理平台	接收出口网关设备数据，Z-OS 用户数据、Z-NMS 监控数据，提供实名 NAT/URL 记录及查询，满足公安部 82 号令要求；	
Z-LOG 数据分析组件	Z-LOG 功能组件，实现数据建模分析，并提供对外图形化展示和结果查询功能；	