DBAplus

大数据与安全技术沙龙-长沙站

大数据日志安全审计

讲师名称:谢涛

目录

DBAplus

- 我是谁
- 我来干什么
- 我们怎么干
- 如何证明

我是谁

DBAplus

新炬网络
SNC Net

能力

资质

本地化

艾维力 IVORY
大数据分析系统

日志系统与传统网管的区别

DBAplus

传统网管告警

Gigabit[illegible]状态为Down

网管用来发现问题

现有网管告警，根据设定阈值告警，告警简单、信息单一

日志分析告警

Jun 11 23:59:59 188.9.11.124 VSYS=public; AttackType: Trace route attack[illegible]cpu: 3;
Receive Interface: GigabitEthernet3/0/0 GigabitEthernet1/0/0: f[illegible]97
221.177.225.167 117.142.2.71 223.103.1.39 117.142.7[illegible]177.142.201
221.177.100.214; begin time: 2016-06-11[illegible]

检索字段：

- [illegible]23:59:59
- d[illegible].9.11.124
- attacktype = Trace route attack
- slot: 5;
- cpu: 3;
- Receive Interface: Giga[illegible]
- fromip = [illegible].142.2.71 223.103.1.39
  1[illegible]
- to[illegible]221.177.100.214
- beg[illegible]= 2016-06-11T15:59:29.000Z
- endtime = 2016-06-11T15:59:57.000Z
- appname = /root/netlog/hw.log.bak1
- hostname = shsnc-04

日志用来定位问题

日志用来预测问题

日志可以提供非常丰富的上下文信息，帮助人员快速定位故障

并结合传统网管告警形成更加完整的告警检索体系

运维分析体系建设的四个阶段

DBAplus

PART ONE
0

1

基础管理

基础设备监控
智能告警
ITIL流程

PART TWO
0

2

解决方案与工具

企业资产配置与管理
性能管理
容量管理
故障管理
自动化运维
日志分析

PART THREE
0

3

平台整合

SAAS
PAAS
Cloud化
大数据分析
综合网管
管理制度化

PART FOUR
0

4

以业务维度为核心

业务感知
关联分析
闭环管理
持续改进与优化
人工智能

我来干什么

DBAplus

运维

安全

以前是怎么干的

DBAplus

日志来源	基础设施	软件平台	操作系统	数据库/中间件	业务系统
	• 机柜设备 • 服务器设备 • 网络设备 • 存储设备	• 工作流系统 • 电子表单系统 • 报表软件 • 自动运维系统	• UNIX系统 • Linux系统 • Windows系统	• 关系型数据库 • 消息中间件 • Hadoop • Kafka/JMS	• Log4j • 自定义日志 • 业务数据
	• 组件温度日志 • 风扇异常日志 • 电源模块日志	• 日常运行日志 • 异常告警日志 • 错误故障日志	• 资源使用日志 • 系统事件日志 • 操作运行日志	• 操作运行日志 • 访问监听日志 • 错误故障日志	• 异常诊断日志 • 业务时序日志 • 用户体验日志

日志数据膨胀速度快，最后简单丢弃
分散存放，碎片化难以管理
无法实时告警
缺乏直观的报表，无法挖掘有价值的信息

日志数据分析单一，没有关联
对日志数据的安全分析比较简单
日志数据格式不一，难以分析
无法进行全面的合规审计

现在有些企业是怎么干的

DBAplus

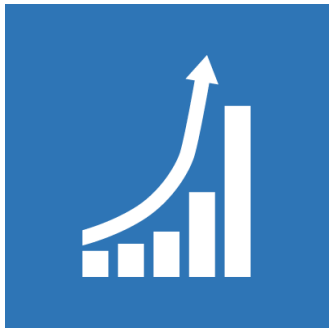
Elasticsearch

- ✓ 实时检索、亿级数据秒级返回结果
- ✓ 分布式系统，对外表现对等，自动均衡
- ✓ 输入/输出 JSON
- ✓ 多租户，不同的用途分索引
- ✓ 可以同时操作多个索引
- ✓ 基于Apache Lucene搜索引擎库

Logstash

- ✓ 分布式集群架构、模块化设计
- ✓ 安装部署方便，支持不同操作系统
- ✓ 扩展性强，支持自定义插件，内置的120多个正则格式
- ✓ output插件，自带90多种插件
- ✓ 性能配置性强，通过配置方式组合各类插件
- ✓ 支持不同的输入源及输出，自带的各类input、filter
- ✓ 数据处理灵活性强

Kibana

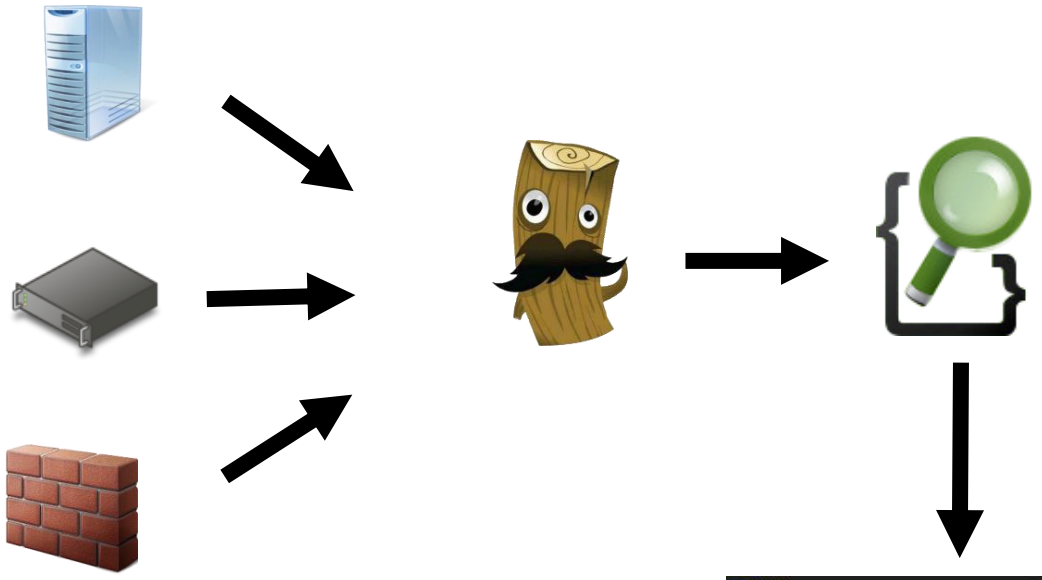


- ✓ 报表配置灵活，易于共享
- ✓ 集成丰富的图表库, 支持复杂的分析报表
- ✓ 自由展示报表大小及位置
- ✓ 数据的实时统计分析
- ✓ 与Elasticsearch的无缝集成

现在有些企业是怎么干的

DBAplus

与开源ELK对比



无资源控制

没有消息队列缓存

告警功能弱

用户认证及权限管理

不支持关联统计分析

无自身监控能力

无商业化支持

无机器学习

无运维场景

无行业经验积累

难以定制性开发

无数据脱敏

无法即开即用

类似开源软件hadoop，越往后维护的成本越高

我们是怎么干的

DBAplus

展示

大屏视图　安全视角　运维视角　专业报表　鹰眼

场景

实时审计　**网络审计**　配置审计　**数据库审计**　参数审计

分析

海量数据处理　搜索定位　数据结构化　函数搜索语言　权限管理

即开即用　自动化识别　自动化部署　机器学习　端到端服务

接入

Flume　FTP　RestAPI　程序接口　Syslog

设备


主机/操作系统


存储


网络设备


软件平台

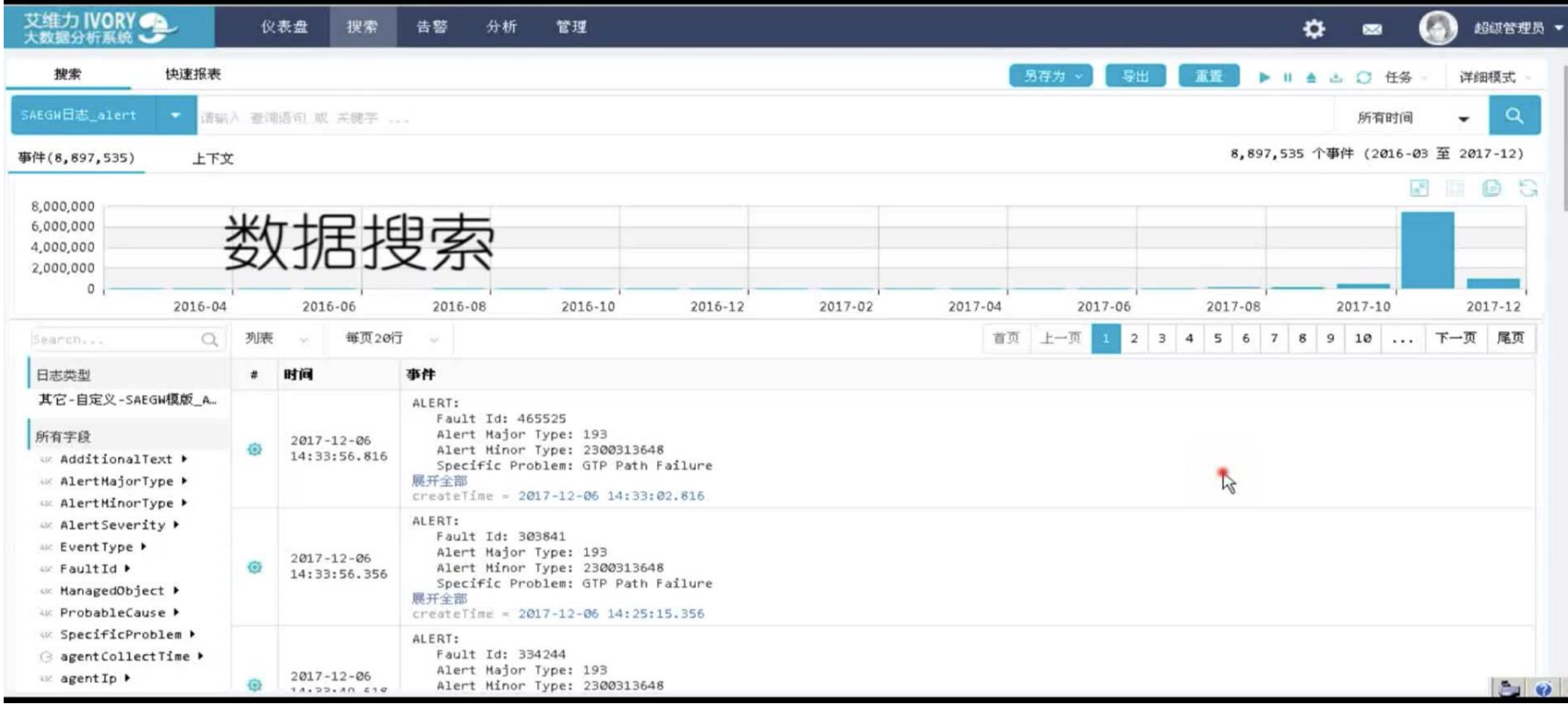

中间件


业务系统

外系统接口

我们是怎么干的

DBAplus



自动识别接入

DBAplus

艾维力 IVORY 大数据分析系统

仪表盘 搜索 告警 分析 管理

超级管理员

提取样本 > Event确认 > 数据切割 > 数据接入

返回 下一步

本地文件

syslog

kafka

数据库

SNMP

OMC

ftp采集

配置1 配置2 配置3 配置4 配置5 配置6 ✖ +

文件匹配: /home/env/apache-tomcat-9 获取

- /home/env/jdk1.8.0_112
- /home/env/data
- /home/env/apache-tomcat-9
  - /home/env/apache-tomcat-9/logs
  - /home/env/apache-tomcat-9/web_ehcache
  - /home/env/apache-tomcat-9/data
  - /home/env/apache-tomcat-9/bin
  - /home/env/apache-tomcat-9/conf
  - /home/env/apache-tomcat-9/temp
  - /home/env/apache-tomcat-9/lib
  - /home/env/apache-tomcat-9/webapps
  - /home/env/apache-tomcat-9/work
  - /home/env/apache-tomcat-9/derby.log

自动化识别

自动安装部署

DBAplus

管理视角数据可视化

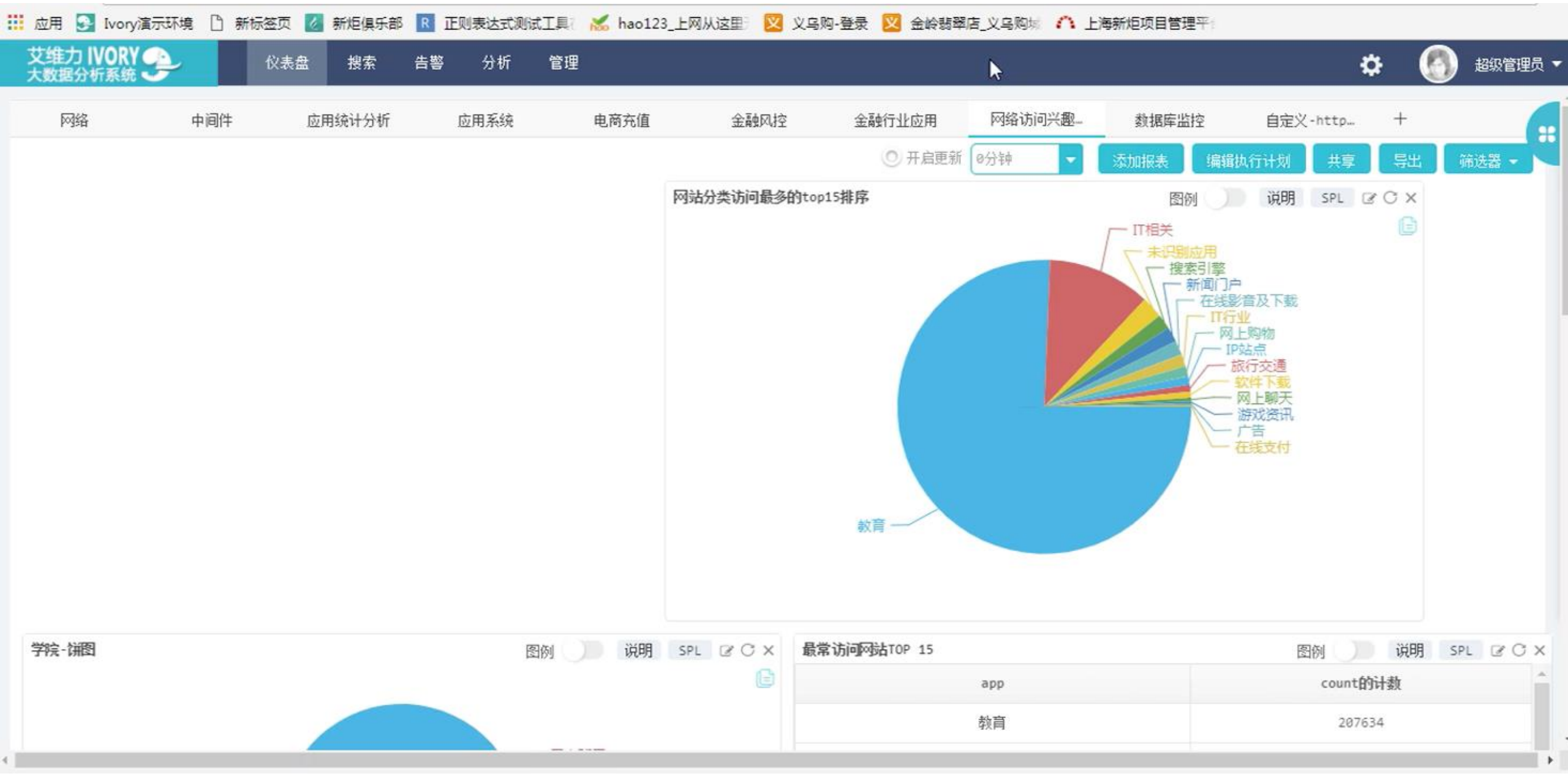
DBAplus

运维视角时间轴分析

DBAplus

自监控可视化大屏

DBAplus

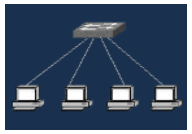


兼顾非结构化和数据库格式

机器对文本的读写性能远胜于传统数据库，但是数据库格式化的数据才能真正实现商务智能分析

大数据日志分析体系建设步骤

DBAplus



01 日志分析平台

集中化日志分析平台

- 分布式采集
- 统一存储
- 实时检索
- 报表分析
- 告警推送
- 大屏展示

02 大数据运维分析平台

提供其他平台数据接入，对系统和业务异构数据进行整合和分析，提供更多的场景：

- 调度管理系统
- 关联分析
- 元数据管理
- 数据安全系统
- 可视化分析系统

03 智能运营平台

基于机器学习算法构建智能分析系统，基于业务为企业提供预测和决策支持

- 个性化推荐系统
- 舆情洞察系统
- 用户标签管理系统
- 问题预测

怎么证明-案例分享

中国移动 China Mobile

广东　浙江

山东　四川

中国电信 CHINA TELECOM

湖北　湖南

博时基金

景顺长城 Invesco Great Wall

安吉汽车物流有限公司 ANJI AUTOMOTIVE LOGISTICS CO.,LTD

服务平台的广泛应用

IVORY日志大数据分析平台，已在多家大型企业使用，主要涉及电信、金融、交通、政府等领域，典型客户包括博时基金、景顺长城基金管理有限公司、湖南电信、山东移动、广东移动等。客户每天采集处理入库的日志量最高达3.8T，实现T级别日志数据查找秒级响应的速度，并为客户提供第三方日志分析专家顾问服务

等级保护合规参考

DBAplus

第二级要求（G2）

网络安全

- 运行状态
- 网络流量
- 用户行为

主机安全（服务器）

- 重要用户操作
- 重要系统命令
- 系统资源异常

应用安全

- 用户操作日志
- 应用重要事件

记录、保存周期不少于1个月
定期检查报告应保证无法删除、
修改和覆盖

第三级要求（G3）

网络安全

- 运行状态
- 网络流量
- 用户行为

主机安全（服务器和重要客户端*）

- 重要用户操作
- 重要系统命令
- 系统资源异常

应用安全

- 用户操作日志
- 应用重要事件
- 运行状态

外部人员访问管理*

- 操作对象与操作内容

安全管理中心

- 所有安全事件

记录、保存周期不少于3个月定期分析和
审计报表应保护审计进程不中断应保证
无法删除、修改和覆盖

第四级要求（G3）

网络安全

- 运行状态
- 网络流量
- 用户行为

主机安全（服务器和重要客户端*）

- 重要用户操作
- 重要系统命令
- 系统资源异常

应用安全

- 用户操作日志
- 应用重要事件
- 运行状态

外部人员访问管理*

- 操作对象与操作内容

安全管理中心

- 所有安全事件

记录、保存周期不少于3个月实时分析和审计报
表应保护审计进程不中断应保证无法删除、修改
和覆盖定义审计存储空间阈值统一安全策略，集
中审计时钟保持与时钟服务器同步

银监会《商业银行信息科技风险管理指引》

DBAplus

第二十七条

◆商业银行应制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。日志可以在软件的不同层次、不同的计算机和网络设备上完成，日志划分为两大类：网络流量

交易日志

◆交易日志由应用软件和数据库管理系统产生，内容包括用户登录尝试、数据修改、错误信息等。交易日志应按照国家会计准则要求予以保存、搜索。

系统日志

◆系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等生成，内容包括管理登录尝试、系统事件、网络事件、错误信息等。系统日志保存期限按系统的风险等级确定，但不能少于一年。

各行业内控与合规审计管理标准规范

DBAplus

随着国家对信息安全越来越重视，法律法规、相关政策制度要求各行业去开展等级保护工作。

法律法规	相关条款	与日志审计相关的主要内容
《信息系统安全等级化保护基本要求》	对于网络安全、主机安全和应用安全部分	从二级开始，到四级都明确要求进行日志审计。
ISO27001:2013	A12.4 日志和监视	系统管理员和系统操作员活动应记入日志，并对日志进行保护和定期评审
《企业内部控制基本规范》	第四十一条	企业应当加强对信息系统的开发与维护、访问与变更、数据输入与输出、文件存储与保管、网络安全等方面的控制，保证信息系统安全稳定运行。（注：间接要求安全审计）
《商业银行内部控制指引》	第一百二十六条	商业银行的网络设备、操作系统、数据库系统、应用程序等均当设置必要的日志。日志应当能够满足各类内部和外部审计的需要。

法律法规	相关条款	与日志审计相关的主要内容
《银行业信息科技风险管理指引》	第二十五条	对于所有计算机操作系统和系统软件的安全，在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项，手动或自动监控系统出现的任何异常事件，定期汇报监控情况。
	第二十六条	对于所有信息系统的安全，以书面或者电子格式保存审计痕迹；要求用户管理员监控和审查未成功的登录和用户账户的修改。
	第二十七条	银行业应制定相关策略和流程，管理所有生产系统的日志，以支持有效的审核、安全取证分析和预防欺诈。
《证券公司内部控制指引》	第一百一十七条	证券公司应保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志应至少保存 15 年。
《互联网安全保护技术措施规定》（公安部 82 号令）	第八条	记录、跟踪网络运行状态，监测、记录用户各种信息、网络安全事件等安全审计功能。
萨班斯（SOX）法案	第 404 款	公司管理层建立和维护内部控制系统及相应控制程序充分有效的责任；发行人管理层最近财政年度末对内部控制体系及控制程序有效性的评价。（注：在 SOX 中，信息系统日志审计系统及其审计结果是评判内控评价有效性的一个重要工具和佐证）

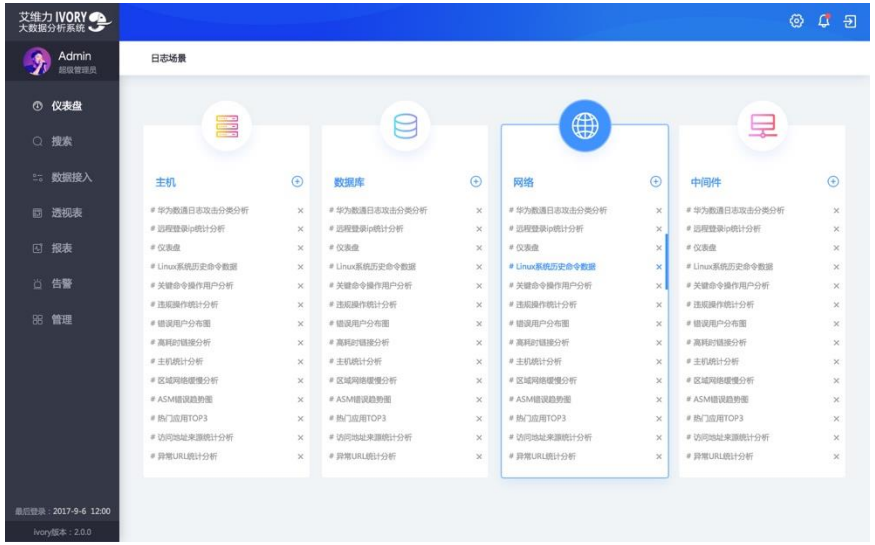
产品定位-基础版日志审计一体机

DBAplus

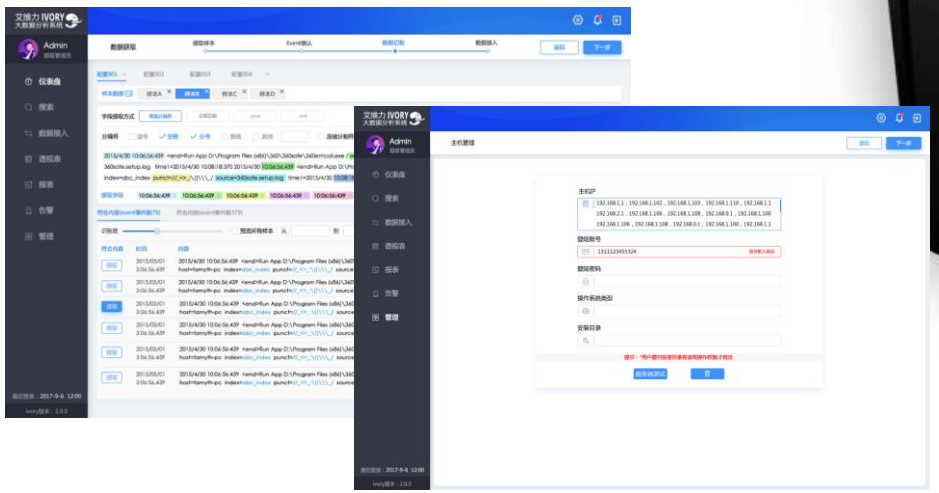
匹配银监会日志规范，满足三级等保要求，告别服务器复杂搭建

整体页面简洁直观，易于上手，日志数据管理傻瓜化

内载标准化安全场景，一步完成银监会日志规范，实现三级等保需求



部署批量可视化，面对茫茫待接入的数据不再让人头疼



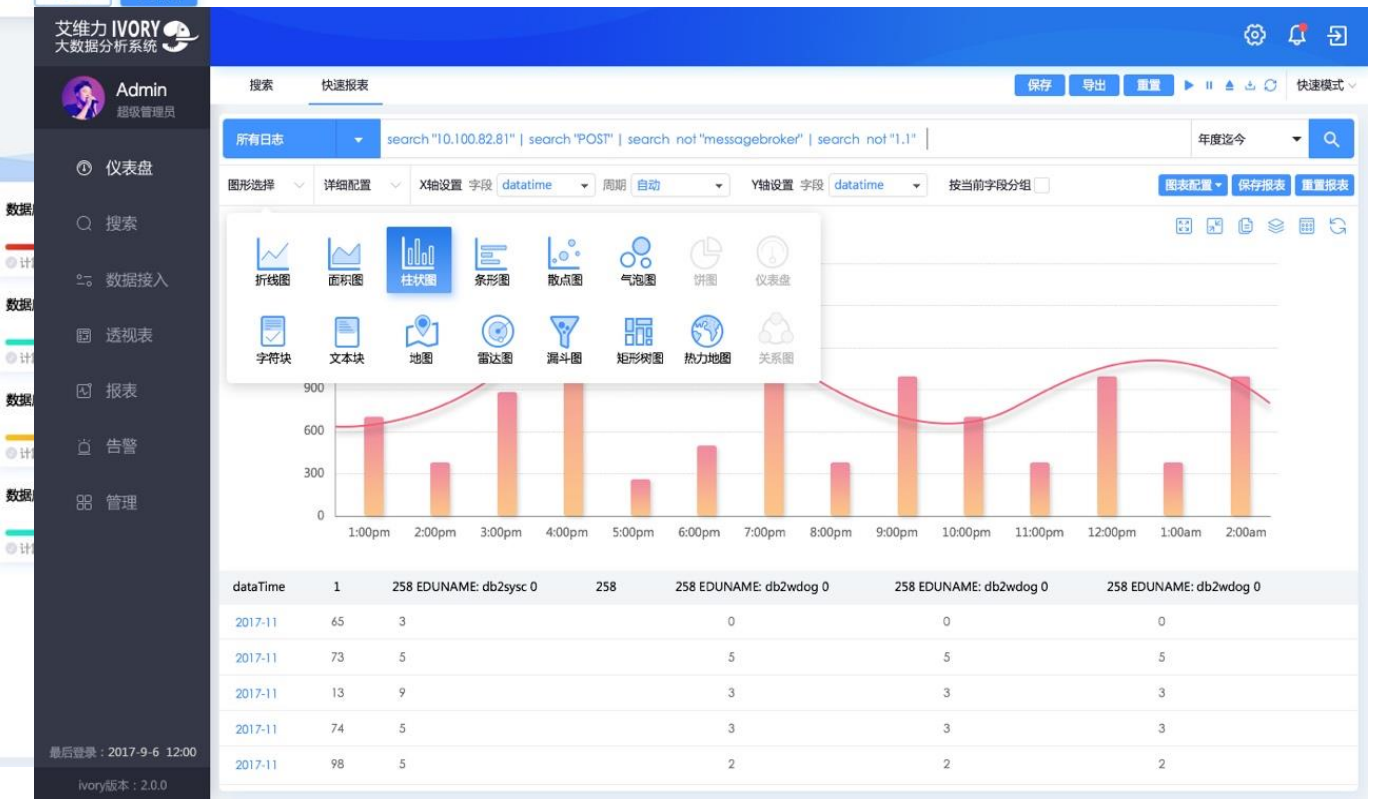
产品定位-高级定制版

DBAplus

定制化提供大量应用场景，搭建定制化的数据安全管理中心

自动化切割识别，自动生成通用场景，数据标签化

量身定制超过30个应用场景，覆盖日常95%应用需求



产品定位-智能旗舰版

DBAplus

结合机器学习分析算法，全面构造智能数据运营平台

通过机器学习算法，深度挖掘数据价值，实现未雨绸缪，为决策提供支持

联系我们

DBAplus

艾维力 IVORY
大数据分析系统

入群请告知自己公司名称

微信讨论组

DBAplus

www.dbaplus.cn

THANK YOU !