Holmes日志治理

降低操作风险，提高工作效率

奥英数创（北京）科技有限公司

奥英数创（北京）科技有限公司是一家从事私有云研发与实施的创新型公司，涉足政务、金融、教育、智能制造等领域，为企业提供数字化转型升级服务，在企业业务创新、服务转型、新项目孵化等方面提供强有力的技术支撑。

技术专家团队来自360搜索引擎创始团队，在云计算、大数据方面有着丰富的实践经验，致力于探索利用运维大数据推动业务流程优化，帮助企业更好的使用云计算技术，提升安全生产监管效率。

发展历程

2014 – 2017
360云平台项目

2017.6.17
公司成立
奥英数创 AIBYTE CLOUD

2017.08
东兴证券
实施甲丑容器云平台

2017.11
宇信金服
实施甲丑容器云平台

2018.6
天津银行
私有云一期

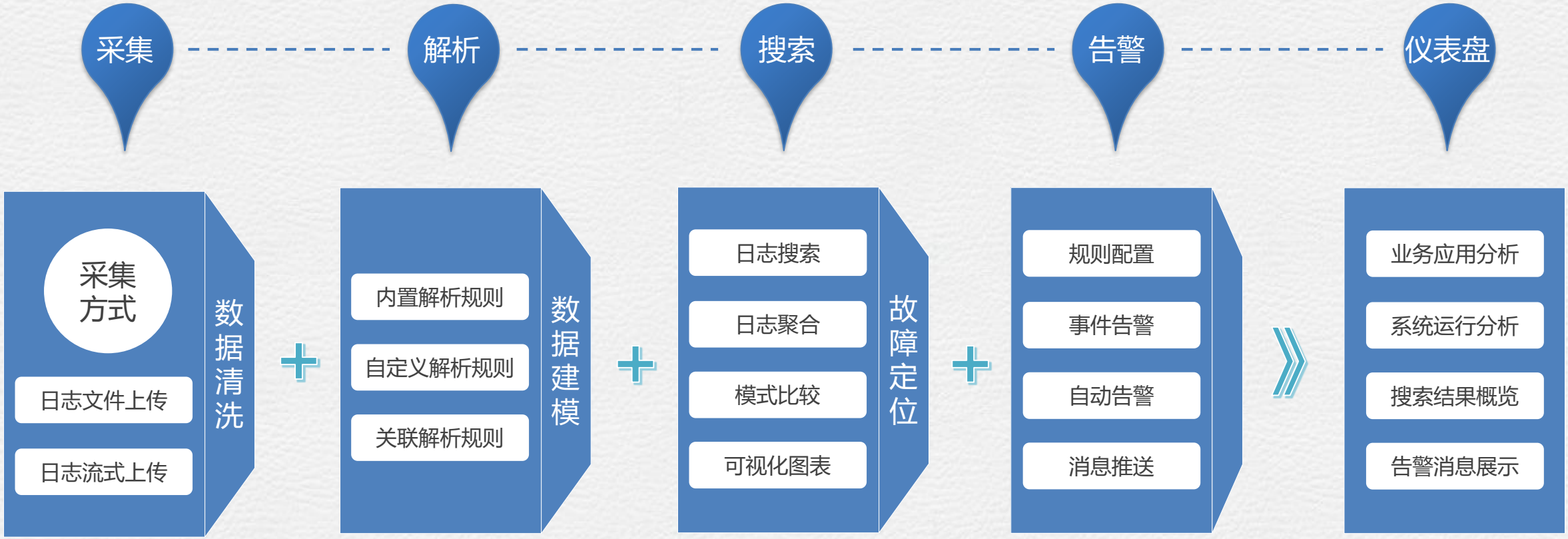
2018.11
四川电信
合作建设金融行业云

第一章 / Part One

产 品 介 绍

日志大数据分析

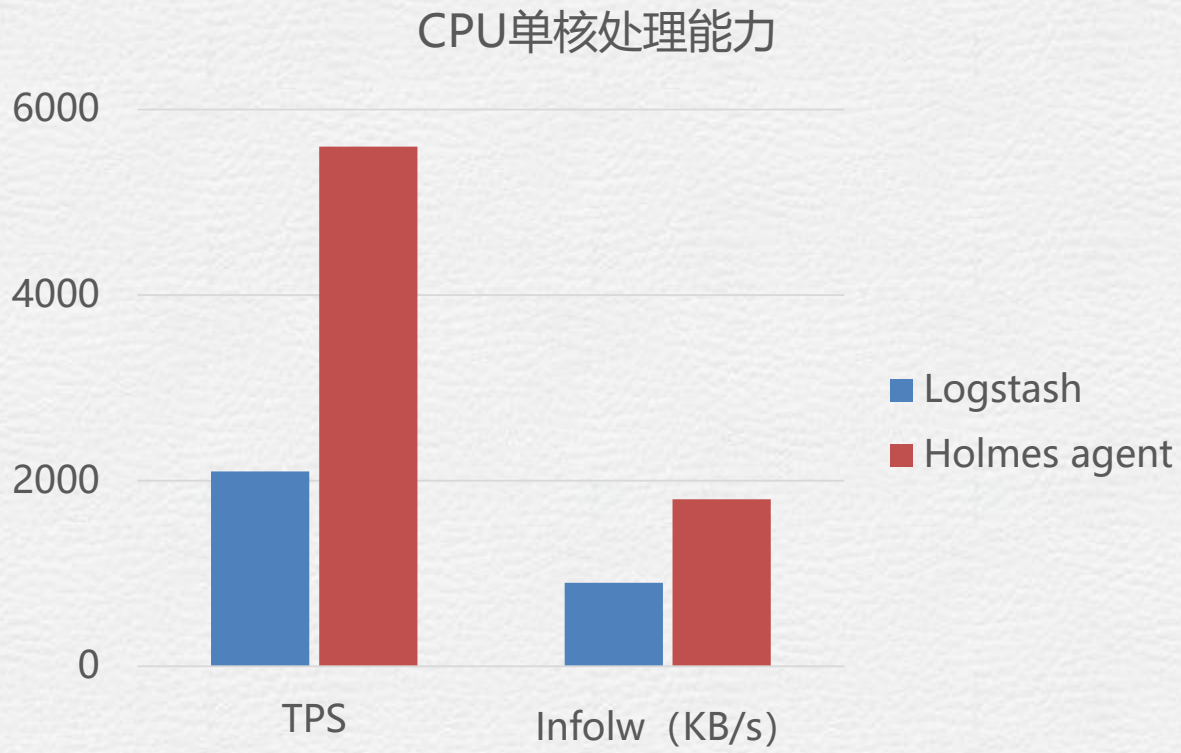
企业级大数据分析产品，对分散在各处的日志进行统一采集和管理，拥有完善的SPL、独有的日志聚合算法、丰富的实用功能应用场景覆盖故障定位、性能分析、安全审计。



在宿主机部署轻量级Agent采集数据

支持采集应用日志、系统日志、网络设备日志等多种来源的日志数据，采用插件式架构设计，支持各种不同种类和格式的数据源和数据输出。

同时提供了高可靠和很好的扩展性。采用业界领先的异步并行通信RPC机制，有强大的数据处理能力，同时先进的架构使其对系统资源的占用降到最低。



串联分析

从前端用户行为到后端系统服务之间的各个环节进行日志还原，帮助了解用户真实操作体验。

时序统计

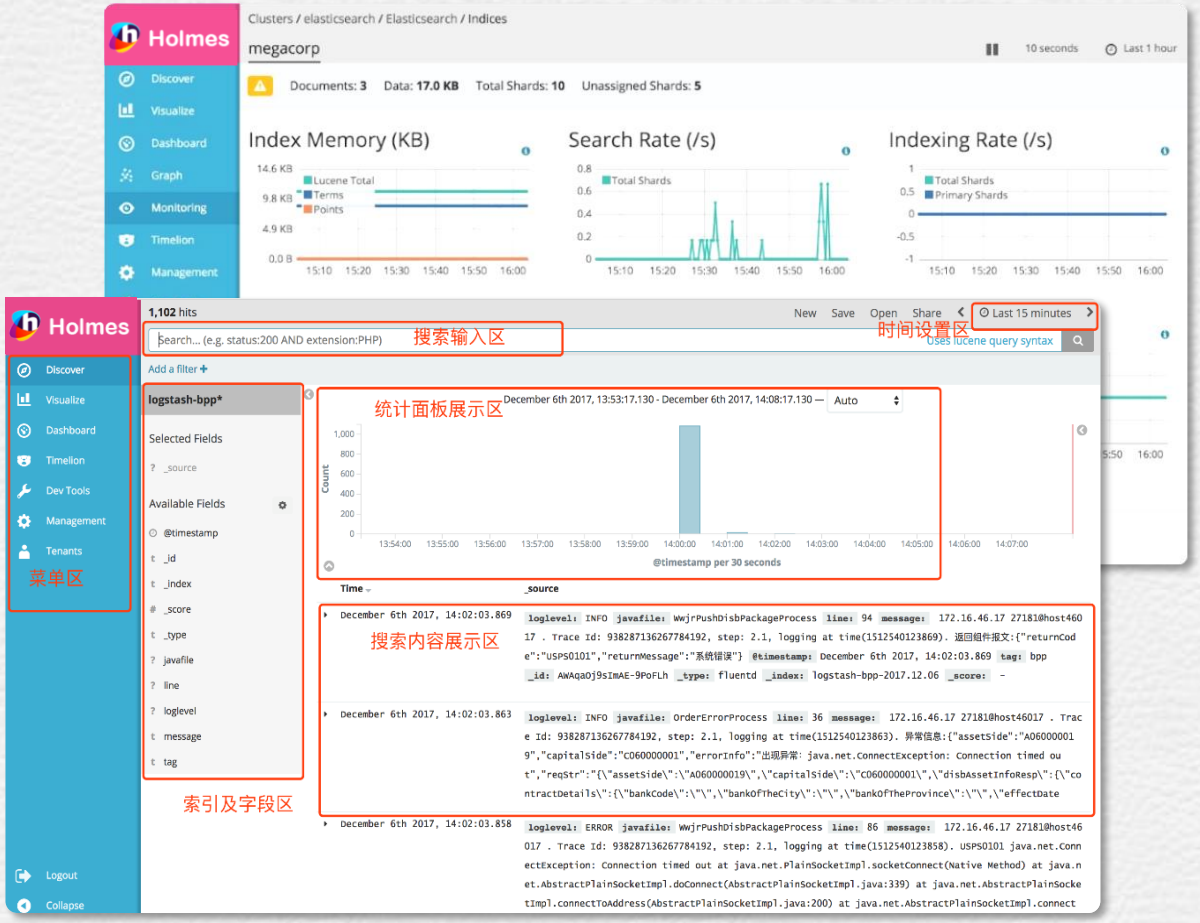
任意事件范围内的业务数据统计，进行业务性能的指标分析、异常检测和预测。

关联查询

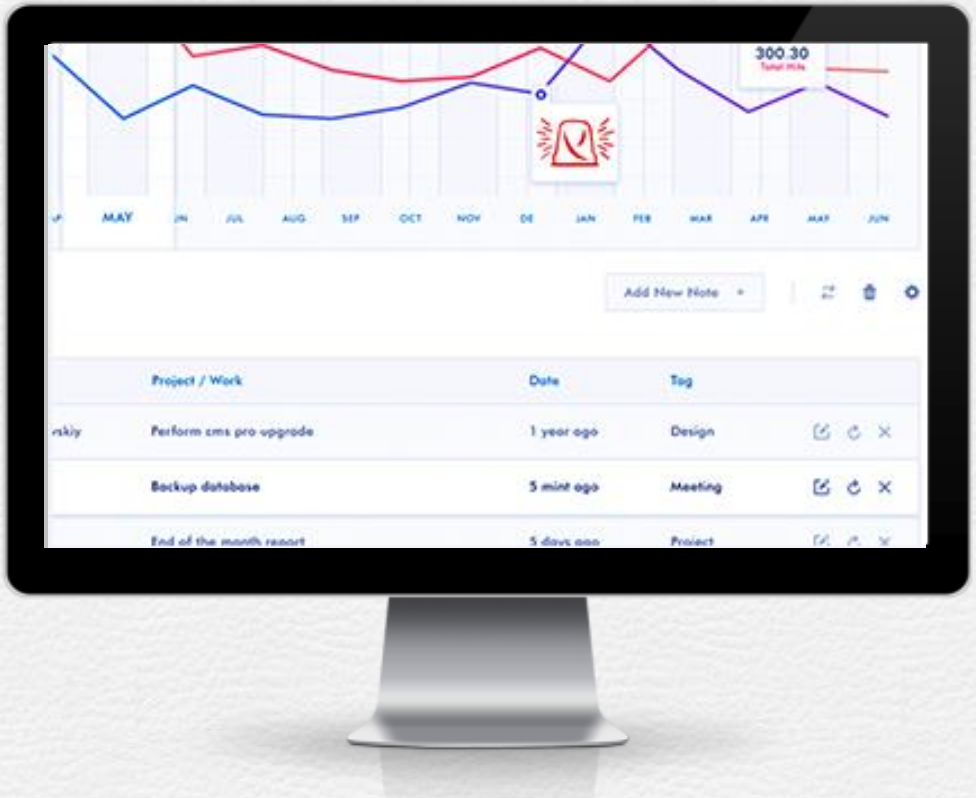
将多个应用、设备的日志进行对照关联分析，从头到尾跟踪业务事务，确保事务完整性。

结果可视化

- 通过 SPL 统计，或快捷统计菜单，创建饼图、柱状图、折线图、地图等各种可视化效果，以支持各种用户场景。
- 将不同纬度的可视化效果汇聚成仪表盘，辅助用户实时查看当前事件变更。
- 关键 KPI 状态高亮显示，突出异常行为的重要性。

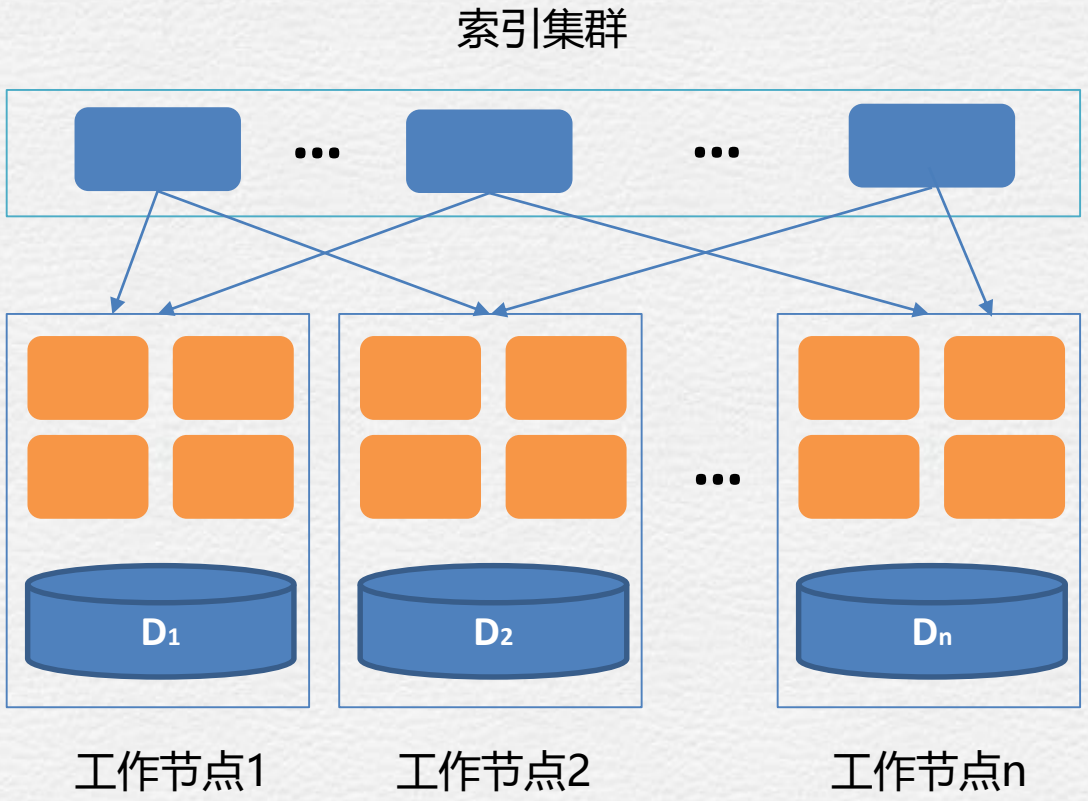


- 对特定事件、固定阈值、动态基线等多种方式的实时、定时监控告警。
- 使用电子邮件、微信、电话、远端接口等各种方式发送自定义告警内容。
- 对长期统计和多维度分析，定时固化为 CVS发送日报、月报，辅助 IT 决策。



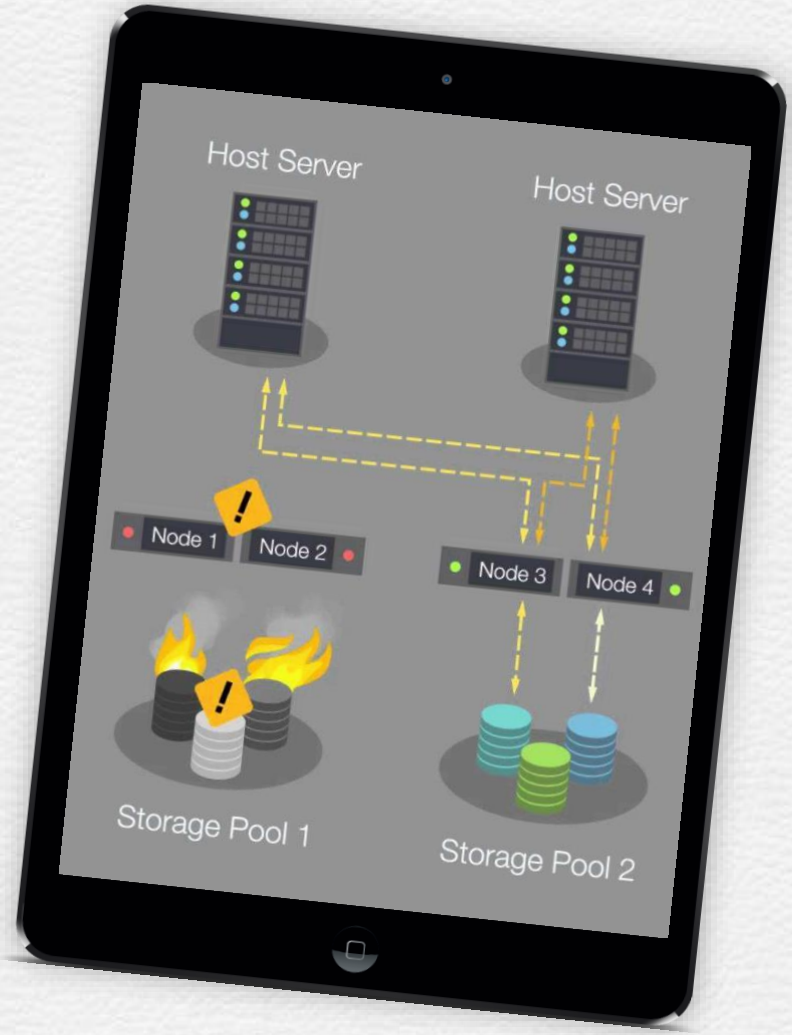
海量数据存储架构

日志存储系统扩展性很好，可以扩展到上百台服务器，处理PB级别的数据。可将索引分拆成多个分片，每个分片可有零个或多个副本，保证数据的高可靠存储。集群中的每个数据节点都可承载一个或多个分片，并且协调和处理各种操作，加快存储与索引数据的速度。



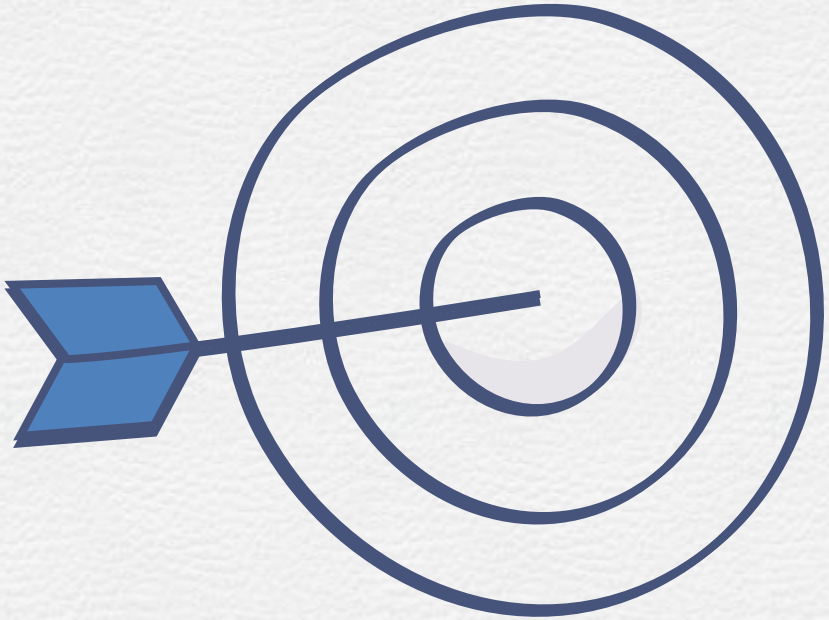
高可靠容灾部署方案

- 将日志分区到不同的容器或者分片中，这些分片可以存在于一个或多个节点中。
- 将分片均匀的分配到各个节点，对索引和搜索做负载均衡。
- 可以做到冗余每一个分片，防止硬件故障造成的数据丢失。
- 将集群中任意一个节点上的请求路由到相应数据所在的节点。
- 无论是增加节点，还是移除节点，分片都可以做到无缝的扩展和迁移。



核心竞争优势

- 提供了统一的部署、管理、监控告警等功能，非常方便运维管理
- 使用简单的查询语法，通过用户图形界面实现各种统计分析功能，简单易用，用户上手快
- 日志进入系统后，就抽取关键字段并做索引，检索时直接查询这些关键字段，速度非常快
- 在日志来源多样、日志量大、延时要求短、功能要求多、希望拿来就用（不需要二次开发）的情况下，Holmes日志治理系统是您的最好选择。



第二章 / Part Two

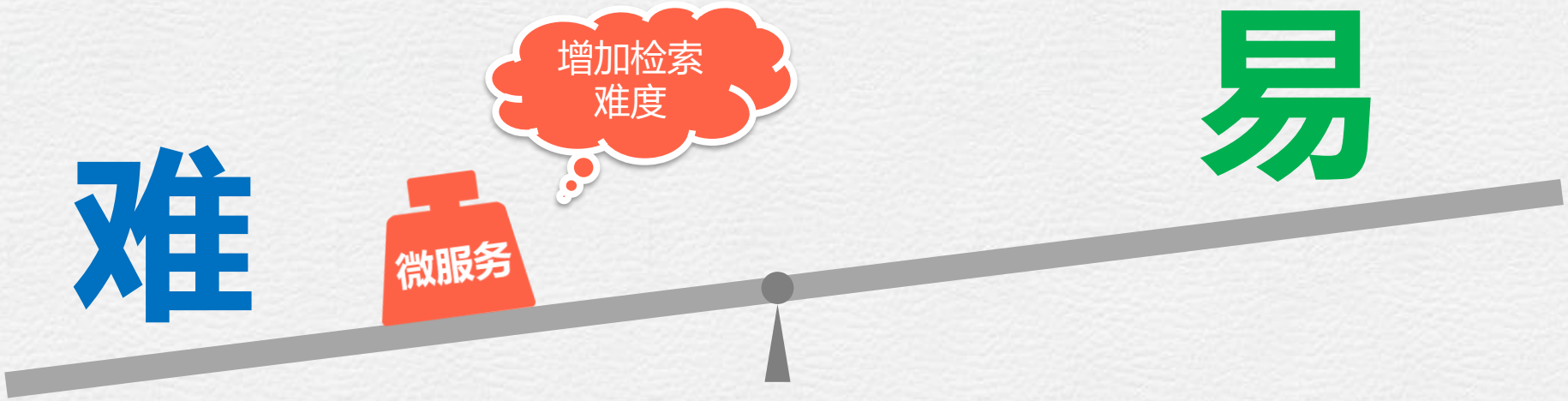
客 户 案 例

Linux 脚本工具

在系统发生异常或安全风险后，登录各台服务器，使用grep/sed/awk等Linux脚本工具去日志里查找故障原因，排障时间长，未必能及时找到异常根源。

Holmes日志治理

快速接收原始日志，统一管理并建立索引，能在几秒内返回搜索分析结果，帮助及时定位异常，提供智能预测与根因分析。

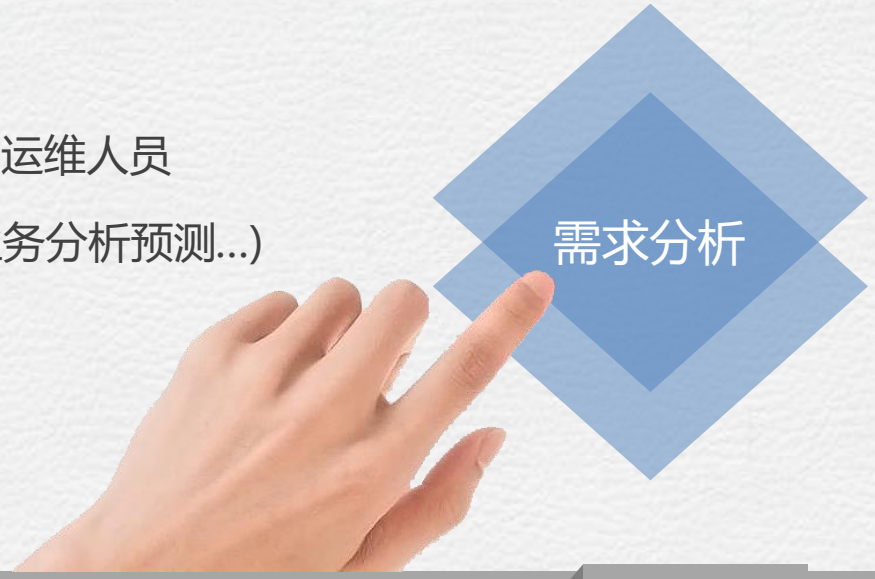


现状分析：

业务应用是由第三方公司开发，当遇到问题开发人员需要查日志时，为了保障业务数据安全，会安排运维人员或业务负责人的陪同下，登录到生产服务器上，找到对应的日志并通过各种脚本工具进行查询。

问题定位：

- 存在监管风险，特别是今年《网络安全法》实施以后，监管更严。
- 故障定位困难，效率低，问题定位时间长
- 成本高，开发运维只能同一地点办公，当业务增多时，只能对应增加运维人员
- 日志作为宝贵的数据，没有得到有效的利用（告警、审计、风控、业务分析预测...）



天津银行网贷业务是开放型互联网金融信贷平台，2018年6月上线以来累计放款金额已过千亿，日均交易量200多万笔。Holmes日志治理为日志运维提供了安全管理和快速定位的能力。

- 业务日志统一采集和管理，3年以上日志存储和秒级查询能力，基于业务事件的准实时内容监控和风险检测。
- 开发人员各自持有不同权限的账号，可自行检索权限内的业务日志，无需运维人员支持。准实时的日志收集检索能力，帮助工程师快速定位问题。

东兴证券

中航信托

天津银行

厦门农商行

青海银行

湖北消费金融

Thanks For Listening !

谢谢聆听！

奥英数创（北京）科技有限公司

奥英数创（北京）科技有限公司
联系人：董国安
电话：139-1134-1217　（微信同号）
地址：北京市朝阳区望京SOHO –T3-A座1009