# 日志系统技术方案

日志系统将在互联网+平台上实现，将各业务系统日志信息集中管理。基本流程包括：日志采集、传输、转发识别、存储、显示、分析及可视化展示。



# 采集系统

## 提供统一的日志读写接口，形成标准化的日志格式；

## 采集接口需要按网络段部署，并且每一段需要支持负载均衡、高并发、高可用；

## 异步通讯、线程安全、高速缓存、可靠性、持久化、安全认证；

## 业务系统调用接口记录日志时应考虑网络中断的情况，中断时要保证日志不丢失，并且当网络恢复时可以自动恢复采集；

## 根据请求数量自动平衡处理能力，削峰填谷；

## 日志消息应包含统一的消息头及消息体，具体见[日志内容规范](#_日志内容规范)；

## 支持网络中断-恢复后自动传输；

## 支持容错及简单的自动修复功能；

## 业务系统调用

1. 日志记录标准：
2. 根据日志标准模型，调用统一的日志接口。

# 传输系统

1. 支持跨网段传输；
2. 支持网段间网络中断后日志不丢，当网络恢复后自动续传；
3. 支持传输确认，保证可靠性；
4. 支持压缩、批量传输，保证传输高效；
5. 以高性能低内存的方式将日志信息转换为流式进行网络传输；
6. 传输大数据时不能对带宽产生影响；

# 转发识别系统

1. 支持路由日志信息，将不同日志分类；
2. 识别告警，当内容匹配到告警正则时，调用监控系统，进行告警；

# 存储系统

1. 日志压缩存储，防篡改，统一保存；
2. 支持本地存储、外部服务器存储、云架构存储等多种存储方式进行备份；
3. 支持高性能分布式存储，对数据进行分片和副本，实现对TB/PB级日志数据的保存，为大数据分析做数据对接；
4. 支持水平扩展，避免快速增长带来的扩容问题；

# 显示系统

1. 支持对日志信息进行秒级查询；
2. 实时显示各网段采集程序的状态信息，当发生异常时报警；
3. 实时按系统，时间，类型等方式查询个业务系统日志；
4. 支持输入任何关键字，对日志信息进行模糊查询；
5. 支持类SQL语法的高级查询；

# 分析系统

1. 在线用户分析：根据用户的登录日志，分析出系统在线人数的峰谷时间段信息；
2. 账号安全分析：根据用户的登录日志，分析出账号是否存在安全隐患，是否被盗用；
3. 认证方式分析：根据用户的登录日志，分析用户登录认证方式的占比情况；
4. 登录认证成功分析：根据用户的登录日志，分析用户平均需要认证几次才能认证成功；
5. 登录认证失败分析：根据用户的登录日志，分析用户登录认证失败的原因，分析是否存在暴力破解攻击的情况；
6. 用户注销分析：根据用户的注销日志，分析哪些用户是主动注销系统，哪些用户是被动超时注销系统，分析是否有延长会话时间的必要；
7. 账号管理分析：根据账号管理日志，分析业务系统管理员是否存在账号管理上的问题，例如频繁的添加、修改、删除；
8. 授权日志分析：根据授权日志，分析用户权限的由来过程，以及哪些权限是公共的，哪些是可配的；
9. 模块分析：根据操作日志，分析出系统中所有模块的使用情况，并得出哪些为热点模块以及该模块的访问时间段信息；
10. 功能分析：根据操作日志，分析出系统中所有功能的使用情况，并分析出哪些为热点功能以及该功能的访问时间段信息；
11. 重点业务环节分析：根据操作日志，分析从此环节到下一环节的平均时长；
12. 重点功能耗时分析：根据操作日志，分析重点功能从点击开始到业务处理结束所需要的平均时长；
13. 系统日志分析，根据历史数据进行异常统计，分析出服务器异常高峰时间、系统的异常轨迹等；
14. 关联分析：通过授权日志+操作日志，分析统计用户常用的权限、日常操作的权限范围等；

# 展示系统

1. 支持对日志分析结果，实时展现业务系统的运行状况；
2. 支持对日志分析结果进行实时告警，并通过搜索、聚类、可视化等方法迅速定位故障；
3. 将分析结果据转化为柱形图、饼图等直观的可视化报表；
4. 将各个账号的管理活动以图形方式展现，包括账号的创建、修改、删除等，以及显示每次活动的详细信息；
5. 应用监控系统调用日志接口，进行日志读取、报警、监控。
6. 互联网+对接

# 日志内容规范

## 日志消息头

业务系统标识、日志级别（INFO/WARN/ERROR）、服务器标识、记录时间、日志类别，安全证书号

## 日志消息体

具体日志信息内容。