身为挨踢达人

ITIL ITSM IT服务管理 IT运维 Prince2 ISO20000 IT规划 BCM ISO27001 CISA PMP ITSS

唯自我增值与免费，不能辜负

扫一扫，从此不再错过

- 每周四晚上8点半
- YY频道89519382
- ITIL先锋论坛网络讲堂
- 与专家们高峰对话！

三人行，必有我师。ITIL先锋论坛，汇聚IT服务管理大师们的力量

如何获取每周专家讲堂信息？告诉你！

关注微信ITILXF_（注意有下划线哦)或者登录www.itilxf.com找社区服务

错过了讲堂怎么办？来这里听录音吧！

http://www.itilxf.com/thread-32695-1-1.html

想学习哪些IT管理知识？告诉我们吧！

http://www.itilxf.com/thread-33143-1-1.html

如何才能上专家讲堂？如何进行合作？

http://www.itilxf.com/thread-33143-1-1.html

专家讲堂由谁主办，来自哪里，看这里！

ITIL先锋论坛是国内最大的IT服务管理专业社区，自2010年底成立以来始终致力于以ITIL为代表的信息技术科学方法论在国内的推广与落地，目前已发展论坛会员已跃20000人，16000多微博粉丝，8000多名QQ群友，60000多条帖子，10000多分可供下载的管理及实践资料。ITIL先锋论坛在各位版主及广大网友的共同努力下，将继续为IT服务管理初学者提供入门的引领，为IT服务管理实践者提供落地的支撑，为IT服务管理业界提供沟通交流的平台

三人行，必有我师。ITIL先锋论坛，汇聚IT服务管理大师们的力量

ITSM-运行日志分析

高郴

13913965008

QQ:377478157

录音地址链接： http://www.itilxf.com/thread-32695-1-1.html

目录

一、ITSM总体介绍

- 1.1、发掘问题
  - 1.1.1、日志分析
  - 1.1.2 、服务台处理
  - 1.1.3 、资产及项目发起
- 1.2、解决问题--工单（服务流程及服务级别）
  - ✓ 服务流程管理；服务SLAs管理；

1.1.1、大数据日志分析

- 日志采集
- 日志分析
  - 【过滤、删重、机器故障等级转换服务等级、行为审核、翻译】
- 问题发布

1.1.2、服务台处理

- 服务台结单；
  - Web、邮件、电话等；
- 服务台自我处理；
  - 知识库和自我能力；
- 无法处理，问题发布

1.1.3、资产及项目发起

- 资产及项目发起
  - 根据预定的服务条款，提前自动发起服务请求【问题发布】

1.2、解决问题–工单产生

* 问题发布之后产生新工单；
* 工单匹配【SLM、SLAs、（UC、OLA）】

1.2、解决问题–工单执行

* 工单执行【变更】
* 工单结单
* 用户对工单客评
* 质监对用户回访
* **质监**关单

二、运行日志分析介绍

2.1、运行日志收集

2.2、收集日志分析

2.3、结果日志发布

2.1-运行日志收集

1、硬件设备运行记录日志

- 服务器（X86服务器、UNIX服务器等）、存储设备(（磁盘柜；光交换设备；虚拟磁带库等）、网络设备（交换机、路由器等）、安全设备（防火墙、网闸、UTM等）、负载均衡设备（应用负载、链路负载等）、环境动力（精密空调；可网管UPS等）；

2、操作系统运行记录日志

- Windows、Linux、Unix；

3、性能日志

- 通讯设备（网络、安全设备等）性能；
- 操作系统性能；

4、应用软件日志

- 中间件
- 数据库
- 行业应用软件

5、安防设备日志

- 摄像机、 DVS、 DVR、 NVR、 可网管光端机 、可网管数字矩阵 、智能设备

6、其它日志

- 工业控制等非常规日志

2.2-收集日志分析

1. 过滤
2. 删重
3. 设备故障级别转换服务级别
4. 风险审核
5. 翻译

2.2、日志分析

* 日志分析收益：
  1. 运行日志的隐患
  2. 运行日志的预警
  3. 行为的违规/违法行为
  4. 运行设备的故障
  5. 设备故障级别转换为服务级别

2.2.1、服务器运行日志分析

- **A、运行设备的故障隐患**
  - 硬盘坏道；
  - 内存芯片损坏；
  - 服务器自动重启；
  - 设备配置发生变更；
  - 运行服务器是人为关机还是供电问题；
- **B、人为操作的违规/违法行为**
  - 无授权对服务器进行重启；
  - 无授权对服务器进行配置变更；
  - 非本人账户对服务器进行多次尝试登录；
  - 非本人账户对硬件配置发生变更
- **C、运行设备的预警信息**
  - 日志满；
  - CPU超负荷；
  - 机箱内部温度超标；
- **D、运行设备的故障信息**
  - 主板、CPU、硬盘、内存、raid卡、网卡、电源、风扇等物理故障信息；
- **E、日志级别转换为服务级别**
  - 日志级别：日志诊断、信息、提示、警告、错误、致命错误、警报、应急等；
  - 服务级别：结合日志级别、设备使用者、该设备的影响度等综合考虑，排序出1、2、3服务级别；

2.2.2、存储日志分析

- **A、运行设备的故障隐患**
  - 硬盘坏道/损坏；
  - 链路异常；
  - RAID组级别变更；
  - 系统写cache被关闭；
  - 存储自动重启；
  - 主机端口误码过高、传输速率过低；
  - 级联盘柜通讯异常；
  - 运行存储关机是人为关机还是供电问题；
- **B、人为操作的违规/违法行为**
  - 未经审批对存储进行重启；
  - 未经审批对交付的存储进行配置变更；
  - 使用猜密码方式登录存储，接管配置权限；

- **C、运行设备的预警信息**
  - 盘柜机箱温度超标；
  - 存储性能超过阀值；
  - 日志满；
- **D、运行设备的故障信息**
  - 控制器、背板、电源、硬盘、内存、风扇等物理故障信息；
  - 主机端口模块故障，接口故障；
  - RAID组故障信息；
  - LUN故障；
- **E、日志级别转换为服务级别**
  - 日志级别：日志诊断、信息、提示、警告、错误、致命错误、警报、应急等；
  - 服务级别：结合日志级别、设备使用者、该设备的影响度等综合考虑，排序出1、2、3服务级别；

2.2.3、网络安全日志分析

- **A、运行设备的故障隐患**
  - 网络安全设备自动重启；
  - 运行设备关机是人为关机还是供电问题；
  - 设备受到ARP表项欺骗攻击；
  - 某个端口发生源IP和MAC发生攻击事件；
  - IP地址和MAC地址冲突告警；
- **B、人为操作的违规/违法行为**
  - 未经审批对运行中网络安全设备进行重启；
  - 未经审批对交付的网络安全设备进行配置变更；
  - 使用猜密码方式登录网络安全设备，接管配置权限；
  - 恶意对网络进行恶意攻击；
- **C、运行设备的预警信息**
  - 设备运行温度超标；
  - 网络性能超过阀值；
  - 网络丢包；
- **D、运行设备的故障信息**
  - 背板、端口、内存、电源、风扇等物理故障信息；
- **E、日志级别转换为服务级别**
  - 日志级别：日志诊断、信息、提示、警告、错误、致命错误、警报、应急等；
  - 服务级别：结合日志级别、设备使用者、该设备的影响度等综合考虑，排序出1、2、3服务级别；

2.2.4、操作系统日志分析

- **A、运行设备的故障隐患**
  - 网卡丢包；
  - 系统分区容量太小；
  - CPU、内存长时间占用高比率；
  - 系统自动重启；
  - 系统蓝屏；
  - 软硬件不兼容；
  - 系统及驱动补丁升级；
- **B、人为操作的违规/违法行为**
  - 未经审批关闭运行的业务进程；
  - 未经审批重启系统；
  - 未经审批登录系统，并变更配置；
  - 使用猜密码方式登录系统，接管配置权限；
  - 在系统内植入木马等驻留程序；
- **C、运行设备的预警信息**
  - CPU、RAM、内存、网卡超过阀值；
  - 硬盘及存储空间超过阀值；；
  - 业务进程异动超过阀值；
- **D、运行设备的故障信息**
  - 系统无法正常启动；
- **E、日志级别转换为服务级别**
  - 日志级别：日志诊断、信息、提示、警告、错误、致命错误、警报、应急等；
  - 服务级别：结合日志级别、设备使用者、该设备的影响度等综合考虑，排序出1、2、3服务级别；

2.2.5、应用日志分析

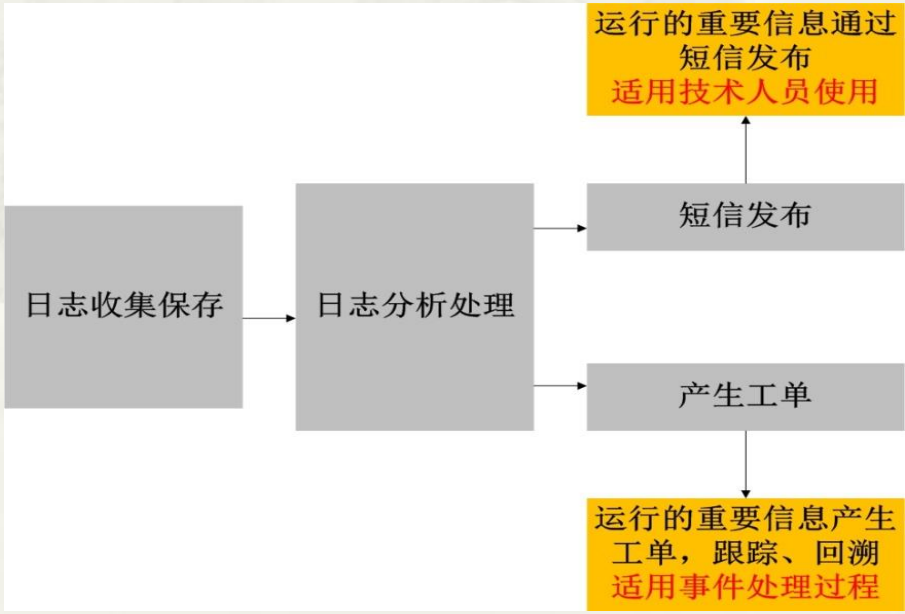
- **A、运行设备的故障隐患**
  - 内存溢出；
  - 中间件进程自动重启；
  - JVM堆栈大小；
  - 活动连接数、等待连接数；
  - JDBC池异常；
- **B、人为操作的违规/违法行为**
  - 未经审批关闭运行的中间件进程；
  - 未经审批手动重启中间件进程；
  - 未经审批对交付的中中间件进行配置变更；
- **C、运行设备的预警信息**
  - 会话数超标；
  - JVM 内存的使用率统计；
- **D、运行设备的故障信息**
  - 中间件停止工作；
- **E、日志级别转换为服务级别**
  - 日志级别：日志诊断、信息、提示、警告、错误、致命错误、警报、应急等；
  - 服务级别：结合日志级别、设备使用者、该设备的影响度等综合考虑，排序出1、2、3服务级别；

5.2.6、应用日志分析

- **A、运行设备的故障隐患**
  - 数据库进程自动重启；
  - 数据库发生坏块；
  - 缓存命中率；
  - 数据库连接数；
  - 活动连接数、等待连接数；
  - JDBC池；
- **B、人为操作的违规/违法行为**
  - 未经审批关闭运行的数据库；
  - 未经审批手动重启数据库；
  - 未经授权查询数据库信息；
  - 未经审批对交付后的数据库进行配置变更；
  - 使用猜密码方式登录数据库，接管配置权限；
- **C、运行设备的预警信息**
  - 表空间超过阀值；
  - 死锁及回滚数
- **D、运行设备的故障信息**
  - 数据库停止工作；
- **E、日志级别转换为服务级别**
  - 日志级别：日志诊断、信息、提示、警告、错误、致命错误、警报、应急等；
  - 服务级别：结合日志级别、设备使用者、该设备的影响度等综合考虑，排序出1、2、3服务级别；

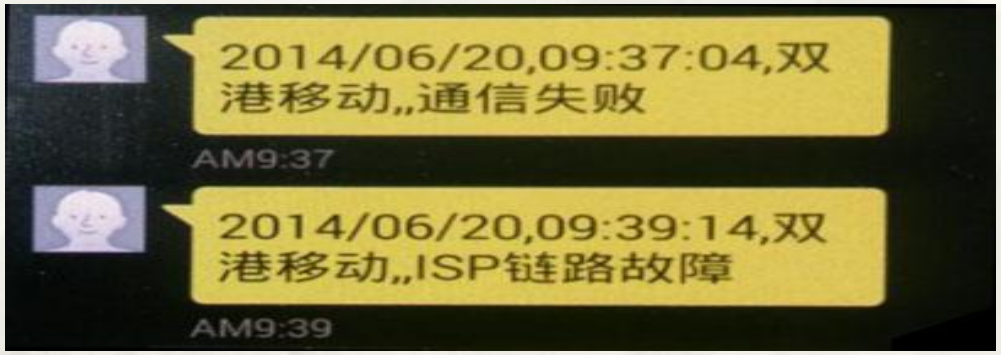
2.3、结果发布

- 2.3.1、直接对外发布（SMS、电话、邮件及移动APP）
- 2.3.2、自动生成工单
- PS:工单介绍



2.3.1、短信发布

- 把日志分析的结果通过短信直接发布；



- 缺点：
  - 短信发送出去，是否接收到不清楚；
  - 短信发送出去，是否处理不清楚；
  - 短信发送之后，发送信息无法回溯；
  - 无法统计分析结果及处理结果的质量

2.3.2、工单生成

- 把分析出来的重要信息直接生成工单

- 优点：
  - 分析结果转换成工单，对工单的处理就是对分析结果的处理
  - 工单系统有完善的PDCA流程机制，确保信息准确无误的送到服务团队手中
  - 根据工单预置SLM、SLAs及流程进行服务处理
  - 支持工单事后查询、处理流程回溯
  - 查询处理工单工程师的服务质量以及服务过程记录
  - 支持统计分析结果，并且可以查询各服务单服务质量

PS：工单介绍

* 1、工单生成
* 2、工单执行
* 3、工单查询

PS：工单介绍

- 1、工单产生
  - 大数据日志分析的结果发送到工单系统，工单系统自动产生一个新工单；
- 2、工单执行
  - 工程师根据产生的新工单提供服务，此工单附带服务目录及对应的服务级别；
  - 根据约定的时长进行服务，过程中根据需求可以进行变更；
  - 工程服务结束后，此单属于结单，等待用户客评；
  - 用户根据工程师服务态度、响应事件及服务水平进行综合考评；考评结束后，此单转为关单；

PS：工单介绍

- 三、工单查询统计
  - 统计当日产生多少新单，分别配备给哪些工程师，当日完成多少工单，遗留多少工单，投诉多少工单；
  - 查询每位工程接到的工单总数，完成数量，剩余数量，投诉数量，超时数量，其中有多少变更数量；
  - 查询已经关闭的工单，回溯此工单服务详细过程以及服务质量；

三、运行日志分析案例分享

- 3.1、网络
- 3.2、主机
- 3.3、应用

3.1、网络

- 一、隐患
  - A、IP地址冲突
    - 使用IP地址越来越多，有使用DHCP来管理，有使用IP地址规划，但是实际过程还是存在IP地址乱使用现象；
  - B、链路故障
    - 网络重要性导致冗余建设，如果其中一个出现问题，另外一个是无法及时发现，冗余的付作用就出现了；
- 二、行为
  - A、配置变更
    - 拥有网络的变更权限，缺少监管；
  - B、帐号盗用
    - 盗用别人帐号进行操作，变更；

3.2、主机

- 一、隐患
  - A、硬件隐患
    - 硬盘出现磁道，内存出现芯片损坏
    - 主机网卡产生丢包
  - B、虚拟机
    - 虚拟机漂移，无法及时发现
    - 虚拟资源不够无法及时发现
    - 虚拟服务器增减设备，加密狗等
- 二、行为
  - A、配置变更
    - 拥有主机的变更权限，缺少监管；【虚机随意开】
  - B、帐号盗用
    - 盗用别人帐号进行操作，变更；

3.3、应用

- 一、隐患
  - A、数据库容错
    - 已经切换，没有及时对故障主机进行服务
  - B、数据库
    - 表空间达到阀值
    - 数据库坏块
- 二、行为
  - A、配置变更
    - 对数据库进行越权操作
  - B、帐号盗用
    - 盗用他人帐号进行数据库操作

谢谢观看，欢迎电询！

高郴
QQ：377478157
13913965008