



面向应用感知的网管系统自保障技术

王 飞

(武汉理工大学计算机科学与技术学院 武汉 430070)

摘 要:随着移动通信运营业务的发展,对网管支撑系统集中化和网络监管的要求不断提高。目前,快速有效的监控手段日益缺乏,急需构建面向应用感知的网管自保障系统,在影响用户应用感知之前发现网管支撑系统平台问题并督促处理,从而提升支撑系统自保障管理能力。因此,结合当前移动 4G 快速发展情况,构建以客户体验及系统运行行为视角的网管自监控平台,以进一步提高 IT 系统应急突发响应能力,实现对网管服务水平的持续提升。

关键词:应用感知;自保障;监控体系;智能巡检;拓扑展现

doi: 10.11959/j.issn.1000-0801.2015108

Self-Protection Technology for Application-Aware Network Management System

Wang Fei

(School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070, China)

Abstract: With the development of mobile operational business, there is ever-growing requirement for centralization of NMSS (network management and support system) and network supervision. At present, increasing devoid of fast and effective monitoring means has taken place, especially on construction of application aware-oriented security system for network management, which could find and deal with problems of NMSS platform before repercussions from user application-aware, thus to improve capabilities of self-protection management and support. Therefore, combined with the rapid development of mobile 4G, the customer experience and system operation for the network from the perspective of the monitoring platform was built, the emergency response capacity of the IT system was enhanced, and the service level of network was promoted abidingly.

Key words: application awareness, self-protection, monitoring system, smart patrol, topology show

1 引言

随着维护的不断集中化和网络监管要求的不断提高,各类网管支撑系统已成为运维管理高度依赖的、不可或缺的 IT 手段。网管支撑系统自身的稳定性、重要性日益凸显。目前缺乏快速有效发现网管系统问题的手段,无法在

系统发生故障后及时发现问题,影响了对一线运维的支撑效率。

为了解决上述难题,提出面向应用感知的网管自保障技术,形成设备层、通道层、应用层、数据层四维体系的自保障系统,在影响用户应用感知之前发现网管系统平台问题并督促处理。

收稿日期:2015-03-04;修回日期:2015-04-21

论文引用格式:王飞. 面向应用感知的网管系统自保障技术. 电信科学, 2015108

Wang F. Self-protection technology for application-aware network management system. Telecommunications Science, 2015108



2 系统目标及架构

为实现对 IT 支撑平台从底层硬件到上层数据的全面监控,在影响用户应用感知之前发现平台隐患并督促处理,面向应用感知的网管自保障系统包含 4 个层面,分别是设备层、通道层、应用层及数据层,并从物理、逻辑、应用、业务 4 个维度形成保障体系。

本系统建设目标如下。

- 设备层保障:通过自监控系统可以方便快捷地实现对网管系统的主机、数据库、网络设备等 IT 设备的运行负荷、告警情况的监控,便于及时发现问题和处理故障,避免影响网管自身的业务。
- 通道层保障:随着网管系统接口数的增多,接口的通断情况往往无法及时发现,直接影响运维管理工作。通过自监控系统能够实现对接口通道的通断状态及接口文件的实时监控,出现异常上报告警,以此辅助维护人员及时发现问题或故障。
- 应用层保障:各类网管系统有很多进程,这些进程是保证网管系统运行的核心,往往由于硬件资源或操作系统等某些原因会导致进程僵死或出现异常,

从而影响核心程序的运行,并且这些问题很难及时发现。通过自监控系统可以实现对关键进程运行状态、进程异常情况的监控,从而尽早发现问题或故障并采取解决措施,提高对网管系统正常运行的有效保障。

- 数据层保障:集团考核相关指标在生成和统计过程中是否存在异常情况,同时在出现异常时希望第一时间通知相关人员;监控和发现省内重点报表及指标是否存在异常情况。
- 告警管理:实现自监控系统的告警基本管理功能。
- 拓扑管理:实现自监控系统的拓扑基本管理功能。
- 综合报表分析:系统提供日常监控所需的告警统计分析、报表基础功能以及综合报表等。
- 系统管理:实现自监控系统的系统管理基本功能。

系统功能架构如图 1 所示。

3 系统实现方案

综上所述,本文提出的面向应用感知的网管自保障系统,主要具有以下几个方面的内容。

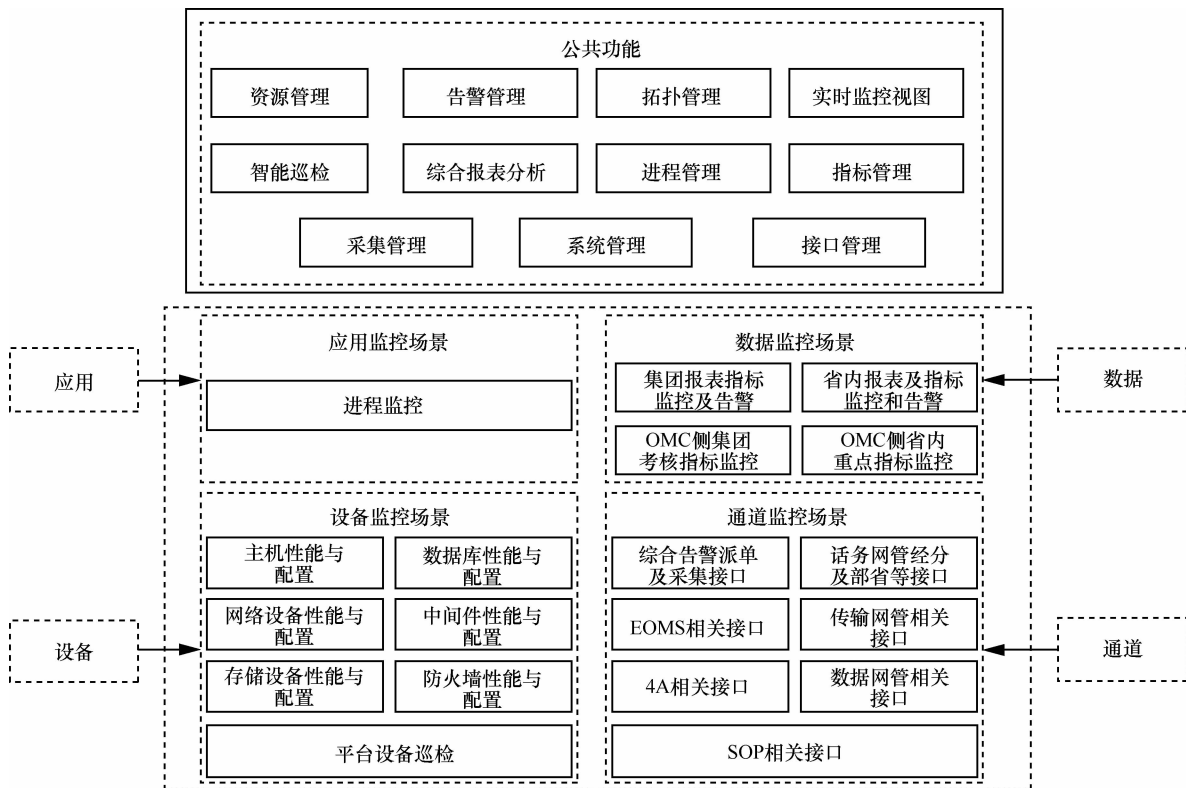


图 1 系统功能架构

3.1 设备层保障技术

3.1.1 设备层监控对象

目前,根据网管自保障系统调研情况,设备层监控对象主要涉及主机(包括 HP-UX、AIX、Linux、Windows、Solaris 等系统类型)、数据库(包括 Oracle、Informix、Sybase、SQL sever、MySQL 等类型)、网络设备(包括负载均衡器、交换机、防火墙、路由器等类型)、中间件(包括 MQ、Weblogic、Tuxedo 等类型)、存储设备(包括 EMC 存储、磁盘阵列等)。

3.1.2 设备层监控内容

监控指标主要包含:主机性能与配置指标(CPU 性能、内存性能、交换区性能、磁盘性能、全局磁盘性能、文件系统性能、CPU 配置、内存配置、交换区配置、物理卷配置、逻辑卷配置、主机磁盘配置等)、数据库性能与配置指标(数据库表空间利用率、数据库工作状态、等待事件、排队列数量、Oracle 共享内存使用情况、Oracle 字典缓冲区参数命中率、Oracle 数据库对象扩展、数据库实例配置、数据库归档日志目录、数据库数据文件配置等)、网络设备性能与配置指标(网络接口性能、网络设备硬件资源(CPU、内存等)、防火墙性能指标(防火墙特有)、系统配置、接口配置、接口 IP 地址配置等)、中间件性能与配置指标、存储设备性能与配置指标等。

3.1.3 设备层监控实现原理

(1)主机设备

主要是自主研发的 agent(代理)程序实现主机相关指标的采集,在被监控主机上部署相应版本 agent 程序后,通过调用系统 API 或命令行方式采集主机相关性能及配置指标,并通过 socket 接口将消息发送至业务采集机,从而实现主机相关数据的采集和入库。

主机设备采集数据流程如图 2 所示。

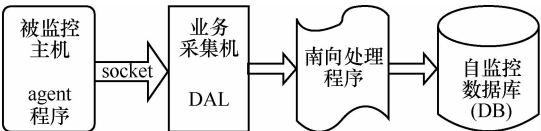


图 2 主机设备采集数据流程

agent 采集原理如图 3 所示。

(2)数据库

主要以 JDBC 方式实现数据库相关指标的采集,采集程序通过 JDBC 方式连接被监控数据库,调用数据库官方 SQL 采集数据库相关性能及配置指标,并通过南向处理程序,将数据库相关数据入库。

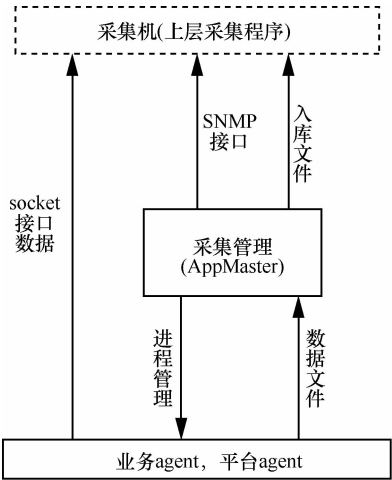


图 3 主机设备 agent 采集原理

数据库采集数据流程如图 4 所示。

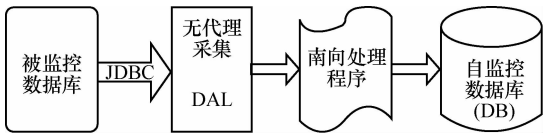


图 4 数据库采集数据流程

数据库采集算法 (以 Oracle 数据库实例配置指标为例)见表 1。

表 1 数据库采集算法

项目	配置指标
数据库类型	Oracle
数据库名	select
数据库实例名	name, instance_name, dbid, host_name, version,
数据库 ID	log_mode, instance_number
数据库实例所在主机名	from v\$database, v\$instance
数据库版本号	
归档方式	
实例的序号	
数据库位数	select banner from v\$version where banner like '%bit%'
数据库支持的字符集	select value from v\$nls_parameters where parameter = 'NLS_CHARACTERSET'
数据库安装选项	select parameter from v\$option where value = 'TRUE'
共享内存大小/MB	select value/1024/1024 FROM V\$PARAMETER WHERE NAME= 'shared_pool_size'
数据库最大进程个数	select value FROM V\$ PARAMETER WHERE NAME = 'processes'

(3)网络设备

主要以 SNMP 方式实现网络设备相关指标的采集,通过 SNMP 从被监控网络设别的 MIB 库中获取相关指标组



的 GroupID,通过无代理采集程序处理后,经过南向程序处理实现性能及配置指标数据的入库。

网络设备采集数据流程如图 5 所示。

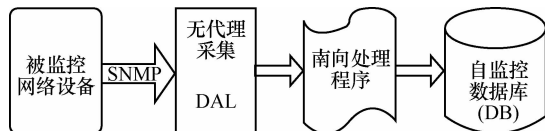


图 5 网络设备采集数据流程

网络设备 MIB 库说明如下。

GroupID:TPM-NETWORK-INTERFACE。

使用 MIB:RFC1213-MIB、IF-MIB。

说明:IF-MIB 是 RFC1213-MIB 的扩展 MIB,IF-MIB 的列是 RFC1213-MIB 的扩展列,通过 Walk 请求方式获取其指示对应 oid,最后一位等于 RFC1213-MIB 的 ifIndex 值,即 1.3.6.1.2.1.2.2.1.1 的值。

(4)中间件

该采集方式与网络设备相同,也是以 SNMP 方式实现网络设备相关指标的采集。

中间件采集数据流流程如图 6 所示(同网络设备采集方式)。

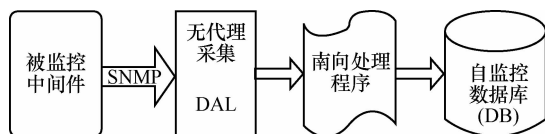


图 6 中间件采集数据流程

网络设备 MIB 库(以 Weblogic 中间件为例)实例说明如下。

MIB 节点实例:

采集的每个 oid 结果都是 oid.实例编号的形式,表示该结果的对应实例。实例编号是“以‘.’间隔的数字”,实例编号中包含多个“.”。

如下的结果中,第 1 行、第 3 行的实例编号相同,那么这两行数据表示的是同一实例的信息,第 2 行表示另外一个实例的信息。

domainName.32.51.57.99.99.55.51.101.50.102.101.52.52.100.97.51.100.97.56.53.54.50.98.55.57.98.99.52.53.56.97.50.51:-->examples

domainObjectName.32.50.56.48.98.56.52.101.100.56.52.52.57.51.57.48.98.101.51.49.48.55.102.56.51.57.52.56.55.101.99.48.98:domain:Weblogic

domainObjectName.32.51.57.99.99.55.51.101.50.102.101.52.52.100.97.51.100.97.56.53.54.50.98.55.57.98.99.52.53.56.97.50.51:domain:examples

(5)存储设备

目前,存储设备监控没有统一的采集方式。根据现有自保障系统存储接入情况,存储设备的监控主要是和厂商根据实际情况来确定接入的方式。如 EMC 存储的监控,EMC 工具软件可以通过 SNMP 方式将告警信息主动推送至自保障系统的业务采集机。

存储设备采集数据流流程如图 7 所示。

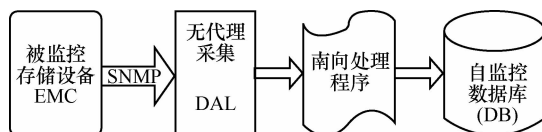


图 7 存储设备采集数据流程

3.2 通道层保障技术

3.2.1 通道层监控对象

实现对综合告警、EOMS 工单系统、传输网管、4A 安全管控、话务网管、数据网管、SOP 等系统的通道监控,实现各系统间的 FTP、Web Services、JDBC、HTTP、socket、TCP 等接口通断状态的实时监控与告警通知;实现对系统内 MQ 队列积压情况、进程状态、TCP 连接数、EOMS 工单压力以及日志检查、数据库联接、数据库检查等情况的实时监控。

3.2.2 通道层监控内容

通道层监控内容见表 2。

3.2.3 通道层监控实现原理

(1)主机通道

主要使用 Linux 下的 ping、FTP、socket、Telnet、SSH 等命令用于探测被监控主机的连通性情况。各命令执行使用各自的协议(如 ping 使用的是 ICMP 传输协议),发出要求回应的信息,若远端主机的网络功能没有问题,就会回应该信息,因而得知该主机是否运作正常。自保障系统将这一功能封装在“统一配置”工具中。

(2)数据库通道

主要是在自监控堡垒机(即自监控服务端,用于监控策略的集中下发)上执行并下发 JDBC 连接串和测试 SQL,向被监控数据库发送连接和访问请求,若反馈测试 SQL 执行结果,则表示数据库连接正常,若连接报错,则表示数据库连接异常。同时,自保障系统已将该功能封装在“统一配置”工具中。

表 2 通道监控内容

设备类型	监控内容	详细说明	实现方式
主机通道	ping 连通性	通过 ping 方式监测主机的网络情况	在统一配置中配置通道连接规则,实现告警、短信通知
	FTP 连通性	通过 FTP 方式监测主机的 FTP 情况	
	socket 连通性	通过 socket 方式监测主机及端口连接情况	
	Telnet 连通性	通过 Telnet 方式监测主机连接情况	
	SSH1 连通性	通过 SSH1 方式监测主机连接情况	
	SSH2 连通性	通过 SSH2 方式监测主机连接情况	
数据库通道	JDBC 连通性	通过 JDBC 方式监测数据库的连接情况	
应用 URL 通道	HTTP 连通性	通过 HTTP 方式监测应用 URL 的连接情况	

JDBC 连接串格式如下:“jdbc:oracle:thin:@10.30.160.21:1521:fwkt2”。

(3)应用 URL 通道

主要通过主动探测方式抓取被检测 URL 地址源代码信息,在源代码中心获取 HTTP 相关信息,若源代码中探测到 HTTP 错误信息,则表示 URL 连接异常,反之,则表示 URL 连接正常。同时,自保障系统将该功能封装在“统一配置”工具中。

通道层监控实现原理如图 8 所示。

统一配置中“协议通断”功能界面如图 9 所示。

3.3 应用层保障技术

3.3.1 应用层监控对象

实现对综合告警、EOMS 工单系统、传输网管、4A 安全管理、话务网管、数据网管、SOP 等重要应用服务进程的性能采集,通过专门应用监控模块,对进程进行周期性检查,

包括进程是否存在、进程是否挂死。通过进程检查、文件检查、日志检查、数据库检查等方式实现对应用进程状态的监控,对发现的异常情况进行告警。

3.3.2 应用层监控内容

应用层监控内容见表 3。

3.3.3 应用层监控实现原理

(1) 应用进程监控

结合各业务系统特点,通过自定义的脚本实现对应用系统关键进程的监控。具体如下:进程是否存在监控,脚本中可调用 UNIX 的 ps 命令来实现;应用进程个数监控,脚本中可调用 UNIX 的 wc 命令来实现;进程状态是否挂死,脚本中可通过监控对应的日志是否刷新进行监控。然后,将调用命令的结果按照一定格式返回,作为告警发送程序(程序名称:SendTrap.pl)的参数将完成告警发送至监控平台,同时通过短信轮询程序(程序名称:SDSM)短信发送至相关责任人。

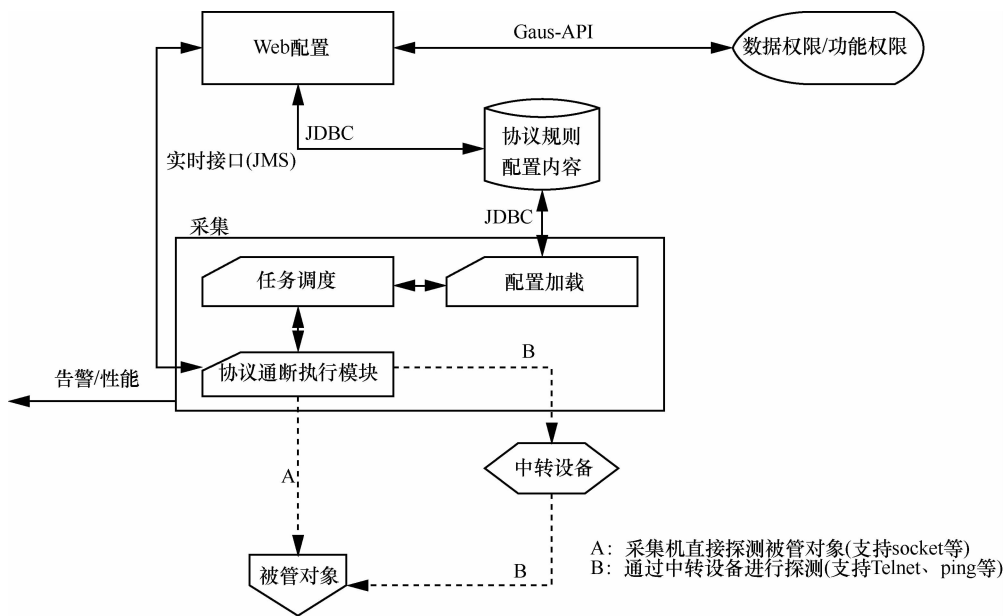


图 8 通道监控实现原理



图9 统一配置中“协议通断”功能界面

表3 应用层监控内容

设备类型	监控内容	详细说明	实现方式
应用进程检查	应用进程状态 _ 是否存在	检查应用进程是否存在	通过应用服务器上配置监控脚本,实现告警、短信通知
	应用进程状态 _ 个数是否正常	检查应用进程个数是否正常	
	应用进程状态 _ 是否挂死	检查应用进程状态是否挂死	
文件检查	文件大小监控	检查文件大小是否符合阈值	
	文件增长率监控	检查文件增长率是否符合阈值	
	文件不刷新监控	检查文件状态是否刷新	
	文件连续性监控	检查文件连续性是否符合阈值	
	文件存在性监控	检查文件是否存在	
	文件关键字监控	检查文件关键字是否符合阈值	

应用进程状态脚本示例如图 10 所示。

SendTrap.pl 和 SDSM 示例如图 11 所示。

(2) 文件检查

结合各业务系统特点,文件检查包含目录检查 filecontiuity 和文件检查 filemon 两部分,通过在被检查文

件所在的服务器上部署 agent 实时获取目录和文件的实时状态,进而根据自定义的阈值数据,完成文件状态检查及告警、短信通知的目的。自监控系统已将该功能封装在“统一配置”工具中。

文件检查 agent 采集原理如图 12 所示。

```
echo "-----检查进程状态开始 ...-----"
echo "当前进程:"
echo "<执行命令:ps -ef|grep -v grep|grep -v gdau.sh|grep -v main-gdau-proc.sh|grep -w gdau>"
ps -ef|grep -v grep|grep -v gdau.sh|grep -v main-gdau-proc.sh|grep -w gdau
ProcID=`ps -ef|grep -v grep|grep -v gdau.sh|grep -v main-gdau-proc.sh|grep -w gdau|awk '{print $2}'`
echo ""
echo "正在检查当前进程是否存在 ..."
echo ""
if [ -z "$ProcID" ]; then
echo "检查结果: 当前进程不存在, 请手工启动该进程 ..."
echo "操作方法:"
echo "启动命令: cd $GDAU_HOME/bin; nohup ./gdau.sh startQ &"
echo "停止命令: cd $GDAU_HOME/bin; gdau.sh stop"
echo ""
```

图10 应用进程状态脚本示例

```
perl /opt/BOCO/monitor/bin/SendTrap.pl BOMC采集进程监控 BOMC-GDAU critical "BOMC采集机($GDAU_IP)的GDAU进程不存在, 请检查!"
/opt/BOCO/monitor/bin/sdsm -a 10.25.5.34 -t $mobilenum -m "BOMC采集机($GDAU_IP)的GDAU进程不存在, 请检查!"
```

图11 SendTrap.pl 和 SDSM 示例

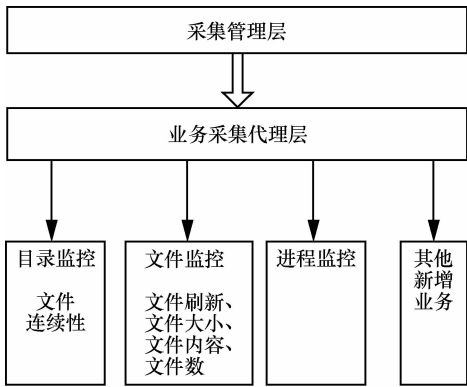


图 12 文件检查 agent 采集原理

统一配置中“文件类采集配置”功能界面如图 13 所示。

3.4 数据层保障技术

3.4.1 数据层监控对象

实现对各类省部接口数据、省内数据、各类报表、OMC 数据、各类网管支持的资源数据及各类输出(告警、工单)等进行检查监控,对发现的异常情况进行告警。

3.4.2 数据层监控内容

数据层(话务网管系统)监控内容见表 4。

3.4.3 数据层监控实现原理

根据被监控业务复杂程度,数据层监控可分为两种方式,即一种为较简单的 SQL 监控逻辑,另外一种为较复杂的 SQL 监控逻辑,其两种情况的实现方式会存在不同。

(1)较简单的 SQL 监控

根据业务 SQL 在统一配置中直接配置规则,并根据业务监控需求设定对应阈值,将业务规则查询出来的数据与阈值数据进行比对,将比对结果转为告警和短信数据发送至监控平台及相应责任人(该方式关键为可通过 1 个 SQL

查询出业务数据进行比较)。

统一配置中“数据库类采集”功能界面如图 14 所示。

(2)较复杂的 SQL 监控

根据业务 SQL 在脚本中实现复杂监控,可根据业务监控需求在脚本中逐一进行规则比对,最终将比对结果通过 SendTrap.pl 和 SDSM 发送告警和短信数据至监控平台及相应责任人(该方式关键为只能通过多个 SQL 查询出业务数据进行比较)。

数据层复杂 SQL 监控脚本示例如图 15 所示。

4 系统应用效果

该系统在中国移动通信集团湖北有限公司网管中已经完成一阶段的功能建设和系统上线,基本涵盖了 EOMS、告警标准化监控系统、传输综合网管、安全管控平台、话务网管报表系统、统一采集平台、无线网优平台等重要专业网管系统监控,实现了“一点监控、全面监控”能力整合,从而形成监控与自监控相结合的安全可靠的专业监控体系。

(1)资源管理

自保障系统将 IT 生产活动中物理资源信息纳入管理范围,打破传统监控系统的资源盲区,对系统自身的物理设备实现精细化管理,保障业务系统的稳定运行。目前,自保障系统纳入资源管理信息包含主机为 486 台、数据库 46 台、网络设备 55 台、安全设备 35 台、业务监控规则 478 个等。

(2)告警监控

告警管理提供告警生成、告警自动处理等灵活的策略控制功能及 IT 基础设施、应用软件及业务运行状态告警数据的统一处理和告警操作功能。同时,该告警管理还支持与综合告警平台告警推送接口、EMOS 工单系统派送功能扩展。

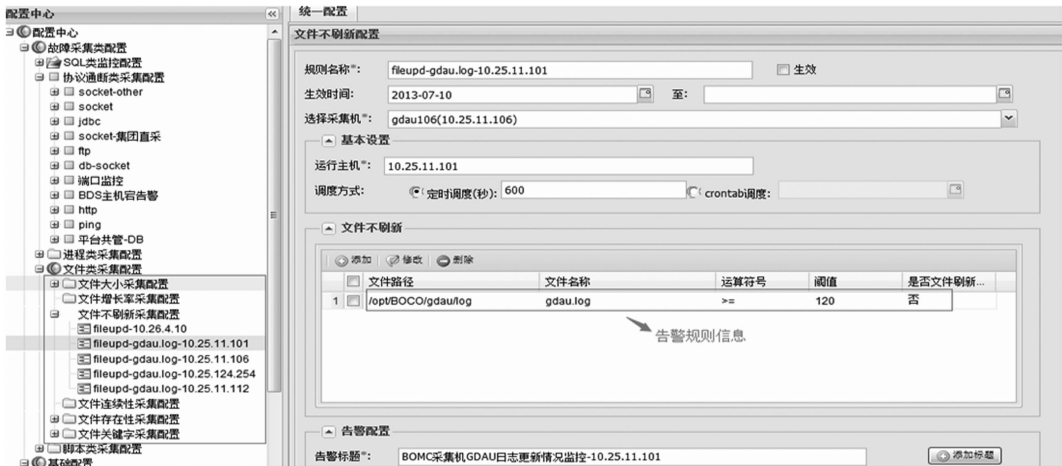


图 13 文件类采集配置



表 4 数据层监控内容

监控类型	监控项	详细说明
省部上报数据	省部上报数据及时性	监控省部接口中相关表数据生成及时性情况。如 tpa_radio_sum_jt12 点的数据应在 14 点 20 分生成,反之告警和短信通知
	省部上报数据完整性	监控省部接口中相关表数据生成完整性情况。如 tpa_radio_sum_jt12 点的数据应为 15 条数据,实际只生成 13 条数据,则告警和短信通知
	上报指标波动情况监控	监控省部接口中相关指标当前数据与历史数据波动情况。如话务量指标当前时间点数据与上周同期时间点相比的波动情况,若超过波动范围,则告警和短信通知
	上报指标门限阈值监控	监控省部接口中相关指标当前数据是否超过门限情况。如话务量指标当前时间,间点数据是否在[50%,100%],若超过波动范围,则告警和短信通知
	集团短信数据集监控	根据集团短信内容,监控相关数据集的完整性情况,包含 MSC、VLR、BSC、RNC、MSCS、SGSN、SMSC、裂化汇总、裂化详情汇总等数据集
	集团短信 LTE 指标监控	根据集团短信内容,监控相关指标的完整性情况,包含 HSS、MME、SGW、PGW、ROAM、eNode B 等指标
省内报表监控	省内报表及时性监控	监控省内报表中相关表数据生成及时性情况。如 tpa_radio_sum12 点的数据应在 14 点 20 分生成,反之告警和短信通知
	省内报表完整性监控	监控省内报表中相关表数据生成完整性情况。如 tpa_radio_sum12 点的数据应为 15 条数据,实际只生成 13 条数据,则告警和短信通知
	省内报表门限阈值监控	监控省内报表中相关指标当前数据是否超过门限情况。如话务量指标当前时间点数据是否在[50%,100%],若超过波动范围,则告警和短信通知
OMC 数据监控	OMC 断连情况监控	监控 OMC 侧或 CORBA 侧连接情况,若出现断连情况,则短信和告警通知
	OMC 数据时长监控	监控 OMC 侧或 CORBA 侧数据未采集时长情况,若延迟阈值外未采集到数据,则短信和告警通知。
	OMC 数据及时性监控	监控 OMC 侧相关主表数据生成及时性情况。如某 OMC 侧 12 点的数据应在 14 点 20 分生成,反之告警和短信通知
	OMC 数据完整性监控	监控 OMC 侧相关主表数据生成完整性情况。如某 OMC 侧 12 点的数据应为 15 条数据,实际只生成 13 条数据,则告警和短信通知
关键指标不同粒度的一致性		监控关键指标不同网元粒度的一致性情况
关键指标省内与集团的一致性		监控关键指标上报集团和省内一致性情况



图 14 “数据库类采集”功能界面

```

echo "获取省端当前时间当前指标数据..."
echo "The Current Time is: date '+%Y-%m-%d %H:%M:%S'"
echo "=====
curr_time_pro1= /opt/BOCO.NPM/DB/user/zjk/bin/$pro_shell|grep znm|awk '{print $3}'
curr_time_pro2= /opt/BOCO.NPM/DB/user/zjk/bin/$pro_shell|grep znm|awk '{print $4}'
curr_data_pro= /opt/BOCO.NPM/DB/user/zjk/bin/$pro_shell|grep znm|awk '{print $5}'
curr_time_pro=$curr_time_pro1 $curr_time_pro2
echo "省端当前时间:[$curr_time_pro]指标数据:[$curr_data_pro]"
echo "=====

echo ""
echo "获取集团当前时间当前指标数据..."
echo "The Current Time is: date '+%Y-%m-%d %H:%M:%S'"
echo "=====
curr_time_jt1= /opt/BOCO.NPM/DB/user/zjk/bin/$jt_shell|grep znm|awk '{print $3}'
curr_time_jt2= /opt/BOCO.NPM/DB/user/zjk/bin/$jt_shell|grep znm|awk '{print $4}'
curr_data_jt= /opt/BOCO.NPM/DB/user/zjk/bin/$jt_shell|grep znm|awk '{print $5}'
curr_time_jt=$curr_time_jt1 $curr_time_jt2
echo "集团当前时间:[$curr_time_jt]指标数据:[$curr_data_jt]"
echo "=====

echo ""
echo "判断当前时间当前指标省端数据与集团数据是否一致..."
echo "=====
if [ $curr_data_pro -eq $curr_data_jt ]; then
echo "数据层监控: '$curr_time_pro'的'$name' (网元粒度:$ne_type 时间粒度:$sum_level)指标集团与省端数据一致,为$curr_data_pro."
#alarm_text_all= echo "$curr_time_pro"的'$name' (网元粒度:$ne_type 时间粒度:$sum_level)指标集团与省端数据一致,为$curr_data_pro."
#/opt/BOCO.NPM/DB/user/zjk/bin/SendTrap.sh "数据层监控: '$name'指标集团与省端数据对比" BOMC-DATA Critical "$alarm_text_all"
else
echo "数据层监控: '$curr_time_pro'的'$name' (网元粒度:$ne_type 时间粒度:$sum_level)指标集团与省端数据不一致,省端为$curr_data_pro,集团
为$curr_data_jt."

```

图 15 数据层复杂 SQL 监控脚本示例

(3) 拓扑呈现

拓扑呈现可以分层次地呈现支撑系统所涉及的所有被管理资源的拓扑结构,具有灵活的浏览、监视和编辑的功能,同时在性能、告警、配置等方面动态反映资源环境的变化。在拓扑节点上可以查看相应资源详细配置信息,包括基本数据与汇总数据。

(4) 自动巡检

自动巡检是将日常运维管理中需要手工进行检查的配置文件、运行参数、运行状态、安全设置等巡检项,通过 shell、SQL 等原子操作完成各个巡检项的采集并组合形成巡检任务;通过调度管理进行轮询调度触发或手工触发执行,对巡检项信息进行采集。将返回巡检结果与巡检基线进行比对。最终形成告警、巡检报告,以短信或彩信形式进行推送并以 Excel、PDF 文档形式导出。

5 结束语

随着一阶段自保障系统的建设和完善,设备层、通道层、应用层、数据层四维度的保障体系取得了一定效果,为 IT 网管系统一线运维工作提供了有效支撑,大大提升了面向用户的客户感知度。同时,为适应云计算技术 IT 基础架构更加复杂多变的特点,需进一步强化自保障管理,提升自动化处理及智能处理能力。通过对监控数据处理过程及时性、有效性管理,为自保障系统优化提供数据依据,使得自保障系统能够不断持续优化完善,从而提升保障体系质量。

参考文献

1 吕廷杰.电信运营支撑系统 OSS:理论、策略与实践.北京:人民

邮电出版社,2003

Lv T J. The Telecom Operation Support System OSS: Theory, Policy and Practice. Beijing Posts and Telecom Press, 2003

2 唐宝民,张颖.电信网监控和管理技术.北京:人民邮电出版社,2006

Tang B M, Zhang Y. The Telecommunication Network Monitoring and Management Technology. Beijing: People's Posts and Telecommunications Press, 2006

3 郭健,吴伟明,张爱霞.面向业务的 NGN 综合网管系统的研究.数据通信,2005(3)

Guo J, Wu W M, Zhang A X. Research on NGN integrated network management system of business oriented. Data Communications, 2005(3)

4 电信管理者论坛.增强的电信运营图(eTOM).北京:中信出版社,2003

Telecom Management Forum. Enhanced Telecom Operations Map (eTOM). Beijing: CITIC Publishing House, 2003

5 QB-Y-041-214. 中国移动业务支撑网运营管理系统 BOMC (V5.0)技术规范,2014

QB-Y-041-214. Business Operation Support System BOMC (V5.0) Specification, 2014

[作者简介]



王飞,女,武汉理工大学计算机科学与技术学院软件工程专业,主要研究方向为移动通信综合网管系统日常运维和优化分析。