

基于 Nagios 软件的综合短信联动告警系统 在地震行业中的应用研究*

李刚, 王晓磊, 孙路强, 姚兰予, 周利霞, 齐士超, 姚会琴, 刘文兵

(天津市地震局, 天津 300201)

摘要: 阐述了基于 Nagios 开源网管软件的手机短信联动告警系统的研制思路与初步应用效果, 探索了网络化的地震监测系统中告警信息的分析、处理和多级联动分发技术。

关键词: 短信; 联动告警; Nagios; 触发器

中图分类号: P315 - 39

文献标识码: A

文章编号: 1000 - 0666(2012)01 - 0133 - 06

0 引言

在“十五”项目建设完成后, 地震行业中的网络化监测仪器设备和系统越来越多, 已覆盖信息网络、前兆、测震、强震、GPS、应急指挥、政务办公等业务系统。天津市地震局的网络化地震仪器设备与业务系统就多达 200 项。如何能将众多的仪器与系统的各类告警信息快速、准确地通知到运行管理人员和值班人员, 已成为系统运维管理的重要内容(李刚等, 2009)。

在通常的网络管理系统中, 系统告警一般采用屏幕告警、语音告警、电子邮件告警和手机短信告警 4 种方式。这些手段虽然能在一定程度上缓解告警管理问题, 但随着网络化业务系统的不断扩大与建设发展, 这些告警方式已经不能适应新形势下地震工作的需求, 主要表现如下:

屏幕告警: 只能通过计算机屏幕的显示来展示告警信息, 局限性较大, 只适应于 24 小时人员值守的环境。

语音告警: 把告警信息通过喇叭播放出来, 在屏幕告警视觉提醒的基础上, 加入了语音提示, 增强告警信息的响应模式, 一般和屏幕告警共同使用, 对于远程运维人员起不到良好的告警作用。

电子邮件告警: 将各类告警信息通过电子邮

件的形式发送到指定人员的信箱中, 可以给运维管理人员提供详细的故障消息, 但是对于响应告警信息的时效性无法控制和保障。

手机短信告警: 是近几年各类监控软件提供的新型告警方式, 系统将告警信息通过手机短信的方式发送到运维管理人员手机上, 它比以上三种告警方式能提供更为便捷、高效的告警模式。但是通常的手机短信告警只能把短信发送到固定的手机上, 不能实现与值班工作匹配、按业务系统分类管理的统一告警模式(刘胜国等, 2010)。

要实现手机短信联动告警系统, 就要解决普通手机短信告警机制的不足, 让告警信息可以根据值班情况、设备仪器管理范围等因素, 灵活地将告警消息发送到运维管理和值班人员的手机上, 实现适合地震行业应用的多地、多人对于同一故障的联动响应模式。如某一台站的前兆仪器发生故障, 系统可以将此信息发送给该台站的值班人员, 同时也发送给前兆台网中心值班人员, 而对于该台站的网络仪器故障, 故障信息的发送对象则成了台站和网络中心的值班人员(王秀英等, 2009; 单维峰, 李军, 2010)。

1 系统建设思路

要实现告警信息的联动分发功能, 要具备 3 个

* 收稿日期: 2011 - 04 - 08.

基金项目: 地震科技星火项目“基于开源软件的地震业务系统运行状态监控技术深入研究与应用(XH1002Y)”和天津市地震局“基于 nagios、cacti 的地震信息监控系统推广应用(102004)”联合资助。

条件：(1) 有产生告警信息的监控系统；(2) 有对告警信息进行分类的信息分类系统；(3) 有手机短信的发送系统。因此，笔者选择 Nagios 系统来构建符合要求的告警联合系统，其系统拓扑结构如图 1 所示。

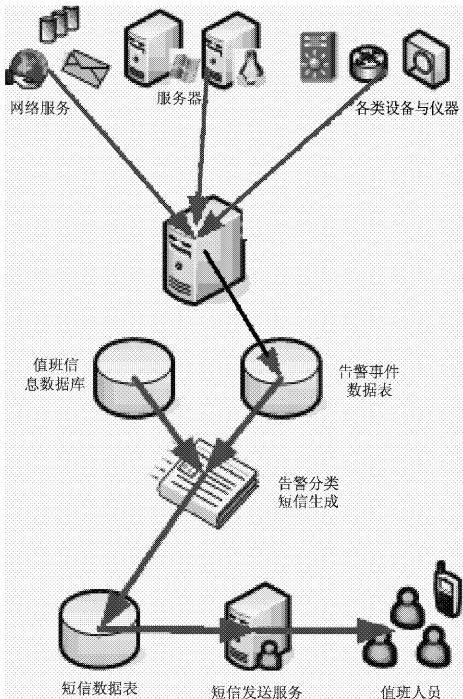


图 1 系统拓扑结构图
Fig. 1 System topological structure

1.1 Nagios 监控系统

2010 年 Nagios 开源网管系统（宋磊，王静文，2009）已经在地震行业中进行了部署，应用该系统能够监控网络化的仪器设备与业务系统，是开源网络管理系统中应用最广的软件之一（吴晓燕

等，2009）。2009 年天津市地震局已经将 Nagios 与 Nagvis、Cacti、WeatherMAP 等软件进行了集成，实现了局内信息网络、强震、前兆、GPS 等系统中的 198 台设备，104 项应用业务与服务的状态监控管理，提供周期为 5 min 的状态轮询机制，即可以最迟在 5 min 内发现各类告警情况，主要包括设备宕机、阈值超限、宕机恢复等。

Nagios 系统本身提供了 3 种告警处理机制，即屏幕告警、语音告警和电子邮件告警，通过相应的 Nagios 插件，还可以实现短信告警。

Nagios 监控的设备或业务产生告警事件后，会根据系统配置情况，将告警信息记录在告警数据表中，本文的联动告警系统就是以告警数据表为依据进行开发建设的。

1.2 运维人员值班管理系统

首先建立被监控设备与系统的运维人员值班管理系统，包括运维人员基本信息、值班时间安排、设备管理区域等内容，目的是能将告警事件和人员信息进行快速比对，找出具备接收告警事件信息的所有人员（王建国等，2009，2010；倪泰山等，2009）。

表 1 中列举了天津前兆台网（王建国等，2009）、GPS 系统和蓟县地震台的管理区域的记录样例。表 2 中列举了前兆台网、GPS 系统，蓟县地震台和综合值班等 9 个人员的值班信息，其中综合值班员要监控 3 个区域（002、003、010）的设备。

1.3 记录详细告警事件

告警系统要能记录分析出详细的告警事件，包括告警设备名称、IP 地址、告警状态，告警产生时间，告警详细情况等。

表 1 管理区域数据示例
Tab. 1 Examples of data in management area

字段名称和区域	前兆台网管理区域	GPS 系统管理区域	蓟县地震台管理区域
mana_dev_area_id	002	003	010
dev_area_name	前兆台网	GPS 系统	蓟县地震台
ip_address_start	010.012.040.000	010.012.052.000	010.012.064.000
ip_address_end	010.012.043.255	010.012.055.255	010.012.067.255
dev_name_keys	qianzhaotw	gps	xx10
管理区域描述	管理范围包括 IP 地址段 10.12.40.0/22，以及名称中包含有“qianzhaotw”字符串的设备和服	管理范围包括 IP 地址段 10.12.52.0/22，以及名称中包含有“gps”字符串的设备和服	管理范围包括 IP 地址段 10.12.64.0/22，以及名称中包含有“xx10”字符串的设备和服

表 2 值班人员信息示例

Tab. 2 Information of people on watch

姓名	值班开始时间		值班结束时间		设备管理范围
	年-月-日	时:分	年-月-日	时:分	
1 号前兆值班员	2011-03-01	08:00	2011-03-05	08:00	002(前兆台网)
2 号前兆值班员	2011-03-05	08:00	2011-03-10	08:00	002(前兆台网)
1 号 GPS 值班员	2011-03-01	08:00	2011-03-05	08:00	003(GPS 系统)
2 号 GPS 值班员	2011-03-05	08:00	2011-03-10	08:00	003(GPS 系统)
蓟县台台长	2011-03-01	08:00	2020-01-01	08:00	010(蓟县地震台)
1 号蓟县台值班员	2011-03-01	08:00	2011-03-05	08:00	010(蓟县地震台)
2 号蓟县台值班员	2011-03-05	08:00	2011-03-10	08:00	010(蓟县地震台)
1 号综合值班员	2011-03-01	08:00	2011-03-05	08:00	002,003,010(前兆、GPS、蓟县台)
2 号综合值班员	2011-03-05	08:00	2011-03-10	08:00	002,003,010(前兆、GPS、蓟县台)

在 Nagios 系统中，可以通过对告警事件数据表 (notifications)、监控对象分类表 (objects)、监控设备 (主机) 信息表 (hosts) 和监控业务 (服务) 数据表 (services) 进行关联查询，得到一条包括表 3 所列属性的告警事件详细记录。

1.4 检索接收告警信息的值班人员

通过运维人员值班信息和详细告警事件可以检索接收告警信息的值班人员。检索前要遵循的原则为：(1) 告警信息的接收者必须处于工作时间内；(2) 告警信息接收者必须为产生告警事件的设备或服务的管理者（即运维人员只接收管理区域内的告警信息）。

为了更加清楚地说明告警信息的分类过程，笔者列举了 3 个告警事件（表 4），用表 1、表 2 所

列的管理区域和人员值班情况，推演出故障短信接收人员。

表 3 告警事件详细记录的主要字段

Tab. 3 Primary fields of detailed recording of alarm event

字段名称	字段描述
notification_id	告警编号
notification_type	告警类型,设备或服务告警
object_id	设备或服务编号
start_time	告警时间
state	告警状态(宕机、警告、恢复等)
output	详细告警信息
name1	告警设备名称
name2	告警服务名称
address	告警设备 IP 地址
ailas	告警设备别名

表 4 告警事件详细记录

Tab. 4 Detailed recording of the alarm event

告警信息	告警事件 1	告警事件 2	告警事件 3
编号	001	002	003
告警类型	设备告警	设备告警	服务告警
设备或服务号	100	201	108
告警时间/年-月-日 时:分	2011-03-02 17:03	2011-03-05 08:03	2011-03-06 07:00
告警状态	宕机	宕机	警告
告警详情	无法检测到设备认为宕机	无法检测到设备认为宕机	网络流量超限每秒 50Mb
设备名称	xx10-qianzhaotw-fhd	xx12-gps-ups	xx10-net-switch
服务名称	NULL	NULL	port_up_link
设备 IP 地址	10.12.64.33	10.12.84.9	10.12.64.1
设备别名	FHD_JX_station	UPS_GPS_QC_station	Switch_JX_station

第 1 个告警事件是蓟县地震台的前兆仪器 FHD, 告警时间为 2011 年 3 月 2 日 17 时 03 分。负责接收蓟县地震台设备的人员包括蓟县台台长, 1 号、2 号蓟县台值班员, 1 号、2 号综合值班员; 负责接收前兆类设备的人员包括 1 号、2 号前兆值班员和 1 号、2 号综合值班员。同时根据告警时间, 确定最终接收 001 号告警事件信息的人员为蓟县台台长、1 号蓟县值班员、1 号前兆值班员和 1 号综合值班员, 共 4 人。

第 2 个告警事件是青光地震台 (xx12) 中 GPS 系统中的一台 UPS 设备, 告警时间为 2011 年 3 月 5 日 08 时 03 分。人员表中没有定义接收青光设备告警的人员, 但是 1 号、2 号 GPS 值班员和 1、2 号综合值班员负责接收 GPS 系统告警信息 (名称中包括 “gps” 字符串的仪器设备与系统), 根据告警时间, 002 号告警事件信息发送给 2 号 GPS 值班员和 2 号综合值班员 2 人。

第 3 个告警事件是蓟县地震台网络交换机中的一个端口流量过大产生的警告事件, 告警时间为 2011 年 3 月 6 日 07 时 00 分。负责接收蓟县地震台设备的人员包括蓟县台台长, 1 号、2 号蓟县台值班员, 1 号、2 号综合值班员, 值班人员信息表中没有定义负责接收网络设备告警信息的人员, 因此 003 号告警事件最终为蓟县台台长、2 号蓟县台值班员和 2 号综合值班员 3 人生成告警信息。

1.5 发送信息实现联动告警

我们在 Nagios 数据库中建立了一个短信数据库表, 用于存储生成的告警信息。表中每 1 行记录为 1 条告警信息, 主要内容包括: 告警时间、设备或服务名称、告警状态, 信息接收者姓名、手机号、信息存入表格时间、信息发送时间、信息是否发送标志等。检索出接收告警信息的值班人员后, 要为每位人员在此表中生成一条待发送的手机短信记录行。

最后通过开发的手机短信息发送程序, 对表中未发送的短信进行轮询式发送, 实现对于同一事件的联动告警。

2 软件开发

根据建设思路, 我们着手进行了 3 方面的系统开发建设, 包括值班管理系统、告警信息触发器

和短信发送程序。

2.1 值班管理系统

值班管理系统采用 B/S 架构模式, 开发语言为 PHP, 系统具备部门管理、人员信息管理、监控区域管理、值班管理、权限管理、短信状态查询等功能, 系统界面如图 2 所示。



图 2 值班管理系统界面

Fig. 2 Interface of duty management system

2.2 告警信息触发器

如何快速地将告警事件转换成告警信息是程序设计过程中的一个重点和难点, 我们设计了多种方案, 在通过分析告警事件产生频率和 Nagios 服务器运行压力等综合因素后, 最终决定采用 MySQL 的触发器 (单德华等, 2010) 机制建立告警信息生成模块。

MySQL 在 5.0 版本后就具备了触发器的功能, 触发器功能就是当数据表中数据发生变化时, 可以人为设置执行一些预先编写好的程序模式。根据这一功能, 我们在 Nagios 产生告警事件并将其写入 notifications 数据表后, 自动执行 “告警信息生成触发器” 模块, 实现从告警产生→分析数据→查找人员→写入发送数据库的所有功能。采用触发器的好处在于, 其稳定性非常好, 同时它有良好的并发处理能力。

2.3 短信发送系统

短信发送系统采用 VB6.0 语言编写, 实现基于串口或 USB 接口的 GSM Modem 短信发送功能,

发送方式为轮询抢占式发送（郑黎辉等，2009）。图 3 为短信系统的查询界面。

<div><div>TJSEI</div><div>天津市地震局短消息中心</div><div>http://sms.tjdj.com</div></div>					
2011年3月24日 星期四 14:00:00 用户登录 退出 帮助 系统公告 短信接收 短信发送 短信接收 短信发送					
天津市地震局信息中心-短信接收					
请输入接收号码					
所有消息记录 消息方式 短信 手机号码 接收者 发送状态 信息内容					
所有记录(100/4)条 前页 后页 100条 短信发送于: 11:21:21(41/91)					
记录序号	信息接收者	发送状态	发送时间	信息内容	系统接收消息时间
213886	黄冠江	发送成功	2011-03-23 10:42:27	Nagios:2011-03-23 10:42:10[0.12.92.92] pass	2011-03-23 10:42:30
213887	黄冠江	发送成功	2011-03-23 10:42:28	Nagios:2011-03-23 10:37:59[0.12.92.92] pass	2011-03-23 10:37:59
213888	周利霞	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16
213889	李国	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16
213890	周利霞	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16
213891	李国	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16
213892	周利霞	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16
213893	李国	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16
213894	周利霞	发送成功	2011-03-23 17:21:16	Nagios:2011-03-23 17:21:16 [0.12.2.61] 10.12.2.81-mss:Passy Usage: [WARNING]	2011-03-23 17:21:16

图 3 短信查询界面

Fig. 3 Interface of short message query

3 系统应用效果与总结

综合短信联动告警系统通过对 Nagios 监控、值班管理、短信自动发动 3 部分的集成，实现了对行业中基于网络的业务系统的综合故障告警。此系统在天津市地震局使用以来，已为信息网络、前兆、强震、GPS 等系统发送告警信息 7 200 余条，较好地解决了局内业务系统联动告警问题，特别是告警和值班系统的结合，实现了多地、多人对于同一事件的联动处置，大大提高了业务系统对于各类告警事件的处置能力。

在此套系统的支持下，天津市地震局前兆台网在行业评比中取得 2009 年度系统运行第 1 名、产出与应用第 2 名，2010 年度系统运行第 1 名、产出与应用第 1 名、技术管理优秀第 1 名的好成绩。信息网络系统 2009 年度骨干网运行率达到 99.995%，区域网络（26 节点）运行率达到 99.877%，2010 年度骨干网运行率达到 100%，区域网络运行率达到 99.858%。

此套系统现已在新疆、安徽、甘肃等地震网络中心使用。另外，系统还设置有短信息写入接

口，各业务系统可以根据接口要求，通过二次开发使用短信息发送系统，实现各类定制短信息的发送。

虽然此套系统已经具备了一定的联动告警处理能力，但是还有很多有待完善和优化的地方，我们会在今后逐渐加以解决。

系统在研究、开发和测试过程中，得到了中国地震局监测预报司信息网络处王飞、唐毅、赵广平，中国地震台网中心李卫东、赵军，天津市地震局王建国，山东省地震局王方建、河北省地震局李永庆、宁夏回族自治区地震局吴晓燕、新疆维吾尔自治区地震局陈述新、安徽省地震局孙静，甘肃省地震局郝怪、高永国等领导 and 同事的大力支持和帮助，在此表示衷心的感谢。

参考文献：

李刚,周利霞,王晓磊,等.2009. 高速区域网络环境中的网站负载均衡系统[J]. 西北地震学报,31(3):296-301.

刘胜国,蒋春花,高景春,等.2010. 地震应急快速触发与短信息发送软件的核心技术和实现方法[J]. 西北地震学报,32(2):196-200.

倪泰山,阙云彩,李祥,等.2009. 基于 B/S 结构的地震台站综合信息管理系统的设计与实现[J]. 地震研究,32(1):89-93.

宋磊,王静文.2009. OpenBSD 下基于 Nagios 的网络服务监控报警系统研究[J]. 电脑编程技巧与维护,(14):112-113.

单德华,杨红艳,孙鸿延,等.2010. 大型数据平台搭建技术在地震行业中的应用与研究[J]. 地震研究,33(2):234-237.

单维峰,李军.2010. 地震前兆观测设备模拟通信软件关键技术研究[J]. 地震研究,33(4):365-370.

王建国,栗连弟,崔晓峰,等.2009. 数字化地震前兆台网日常工作管理软件[J]. 地震研究,32(1):79-83.

王建国,王伟,贺同江,等.2009. 汶川地震期间天津地震前兆台网运行与管理[J]. 防灾科技学院学报,11(3):96-100.

王建国,姚会琴,高逊,等.2010. 天津市地震前兆台网的运行监控与维护管理[J]. 大地测量与地球动力学,30(x1):111-115.

王秀英,周振安,刘爱春.2009. 地震前兆设备动态监控报警功能设计与实现[J]. 地震研究,32(4):431-435.

吴晓燕,周海生,吉祥.2009. Nagios 在网络管理工作中的应用与探讨[J]. 高原地震,22(3):58-60.

郑黎辉,黄宏生,王启东,等.2009. 网络故障短信报警在地震信息网络中的实现与应用[J]. 华南地震,29(2):124-129.

Application of the Integrated Short Message Warning System Based on Nagios Software to the Earthquake Profession

LI Gang, WANG Xiao-lei, SUN Lu-qiang, YAO Lan-yu, ZHOU Li-xia,
QI Shi-chao, YAO Hui-qin, LIU Wen-bing
(*Earthquake Administration of Tianjin Municipality, Tianjin 300201, China*)

Abstract

Based on the open source network management software Nagios, we expound the development approach and primary application effect of short message warning system. We also discuss the analysis, processing and multiple-level interactive distribution technology of network alert information in the seismic monitoring system.

Key words: short message; linkage warning; Nagios; trigger