

方伟华,周蓝捷,郑韶鹏,等.福建省简易烈度计台网智能监控与实时告警系统[J].地震工程学报,2018,40(增刊):197-204.doi:10.3969/j.issn.1000-0844.2018.Supp.197

FANG Weihua,ZHOU Lanjie,ZHENG Shaopeng,et al.AnIntelligent Monitoring and Real-time Alarm System of Simple Seismic Intensity Meter Network in Fujian Province[J].China Earthquake Engineering Journal,2018,40(Supp):197-204.doi:10.3969/j.issn.1000-0844.2018.Supp.197

福建省简易烈度计台网智能监控与实时告警系统

方伟华,周蓝捷,郑韶鹏,李文惠

(厦门地震勘测研究中心,福建 厦门 361021)

摘要:以福建省简易烈度计数据处理系统为例,介绍福建省简易烈度计台网数据处理的体系流程。引用 Zabbix 开源监控工具,对当前业务系统进行实时监控与自动化处理机制的设计,重点阐述 Earthworm 数据处理系统与 Palert Advance 简易烈度计系统各进程监控的配置,实现台网系统智能监控与自动化处理,有效保障台网业务系统连续性运行。

关键词:简易烈度计台网; Zabbix; 智能监控; 实时告警; 业务连续性

中图分类号: P315.78

文献标志码: A

文章编号: 1000-0844(2018)增刊-0197-08

DOI: 10.3969/j.issn.1000-0844.2018.Supp.197

AnIntelligent Monitoring and Real-time Alarm System of Simple Seismic Intensity Meter Network in Fujian Province

FANG Weihua, ZHOU Lanjie, ZHENG Shaopeng, LI Wenhui

(Xiamen Research Center of Seismic Exploration, Xiamen 361021, Fujian, China)

Abstract: In this paper, the design of the data processing system of a simple seismic intensity meter network in Fujian Province is presented. Through the Zabbix open-source monitoring tool, a real-time monitoring and automatic processing system of current seismic activities is designed and implemented. We utilize the Earthworm platform for the data processing and a simple configuration of Palert seismic intensity meter system. The system can realize an intelligent monitoring and automatic processing of the network and effectively ensure continuous reporting of the seismic activities in the network.

Keywords: simple seismic intensity meter network; Zabbix; intelligent monitoring; real-time alarm; business continuity

0 引言

福建省简易烈度计台网主要采用 Earthworm 框架与台湾研发的 Palert Advance 烈度计进行搭建,拟在全省布设 900 台简易烈度计。当前在简易

烈度计台网运维管理方面的工作较少,基本采用人工交互方式进行检测,无法做到无人值守。

该简易烈度计数据处理系统采用 USGS 开发的 Earthworm 进行搭建,采用 C 语言进行编写,分

收稿日期:2017-11-07

基金项目:中国地震局三结合课题(CEA-JC/3JH-161306)

第一作者简介:方伟华(1982-),男,工程师,主要从事地震业务系统运维工作。E-mail:258279496@qq.com。

成不同的模块进行组建,每个模块完成不同的功能;观测系统采用了台湾的 Palert advance 简易烈度计。该仪器核心是 MEMS 传感器与树莓派的高集成度定制系统,通讯系统采用中国电信提供的 MPLS VPN 进行组网。福建省多区域处于山间丘陵地段,为有效管理好这些子系统,实时了解台网运行的健康状况,熟悉该框架体系中的各个阈值指标,提高台网运行率与工作人员维护响应速度,保障地震预警工程数据的准确性,引用一套高效的智能监控系统显得越来越重要。

该方法采用 Zabbix 开源监控工具进行搭建,通过对基于 Earthworm 框架中各进程模块状态信息与 Palert advance 系统的研究,结合 Earthworm 命令库,定义 Zabbix 用户 key 值,定义通知告警机制,定制故障自动化处理机制,借助福建省地震局微信公众号进行自动告警,在第一时间内将地震仪器故障事件通知给运维人员,目的是使台网运维人员实时了解台网仪器健康状况,提高台网运维智能化监控水平^[1]。

1 架构工具选择

1.1 Zabbix 简介

Zabbix 是一个基于 WEB 界面的提供分布式系统监视以及网络监视功能的企业级的开源解决方案。它能监视各种网络参数,保证服务器系统的安全运营;并提供灵活的通知机制让系统管理员快速定位/解决存在的各种问题。Zabbix 由两部分构成:zabbix server 与可选组件 zabbix agent。zabbix server 可以通过 SNMP、zabbix agent、ping 及端口

监视等方法提供对远程服务器/网络状态的监视,数据收集等功能,它可以运行在 Linux、Solaris、HP-UX、AIX、Free BSD、Open BSD 及 OS X 等平台上。

1.2 Zabbix 优势

目前国内外公司智能监控解决方案很多,较知名的有 Nagios、Cacti 等,但 Zabbix 整合了 Nagios 与 Cacti 的功能,并且具有 Nagios、Cacti 所不具备的优势。Zabbix 主要优势如下:

- (1) 安装与配置简单,学习成本低;
- (2) 支持多语言(包括中文);
- (3) 完全免费开源;
- (4) 自动发现服务器与网络设备;
- (5) 分布式监视以及 WEB 集中管理功能;
- (6) 可以无 agent 监视;
- (7) 用户安全认证和灵活的授权方式;
- (8) 通过 WEB 界面设置或查看监视结果;
- (9) email、短信、微信等通知功能;
- (10) 监控多达 100 000 台设备;

1.3 基于 Zabbix 开源监控技术架构

Zabbix 监控系统主要分四个部分(图 1):第一部分数据采集,主要采用 zabbix agent 进行,分别对地震数据处理系统与观测系统各进程进行 key 值定义并进行数据采集;第二部分数据存储,对采集完的数据进行数据存储,主要采用 MySQL 数据库架构与实现;第三部分数据展示与分析,主要采用 Nginx 与 php 进行架构与实现;第四部分告警,主要采用应用 Python 语言的调用微信接口实现实时告警。

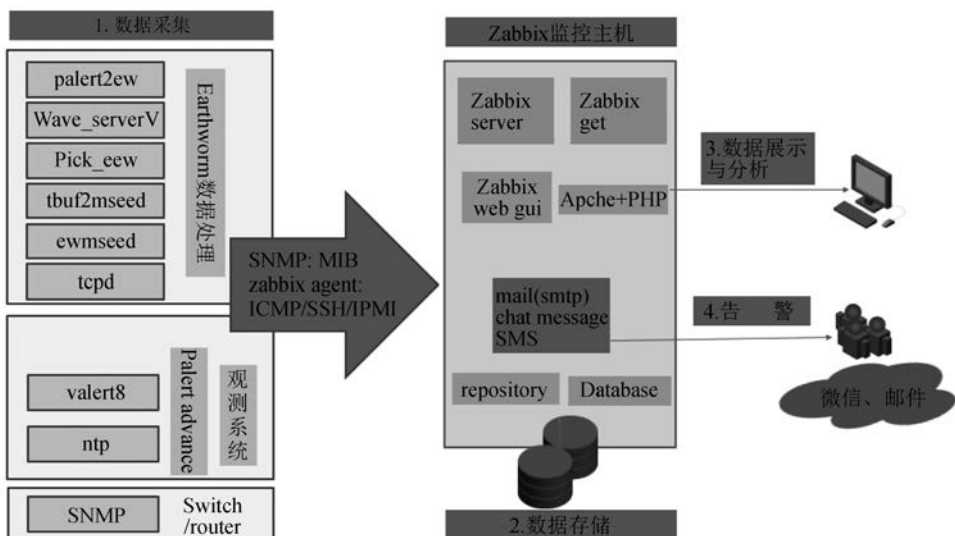


图 1 基于 Zabbix 开源监控的框架体系

2 简易烈度计台网业务流程

2.1 系统总体架构

福建省简易烈度计台网设备一期规模为 300 台左右,通过中国电信的 MPLS VPN 组网方式将数据传输至厦门地震勘测研究中心与福建省地震局(图 2)。每个观测台站提供 2M SDH 链路带宽供烈度计仪数据上报使用,省局与厦门地震勘测研究中心分别采用一条 10 M 光纤汇聚专线接入中国电信 VPN 平台,用于收集各观测台站数据。对于部分未铺设 SDH 链路的区域,采用 3 G 信号进行辅助接入,数据处理中心采用基于 Earthworm 的地震报警软件框架系统。

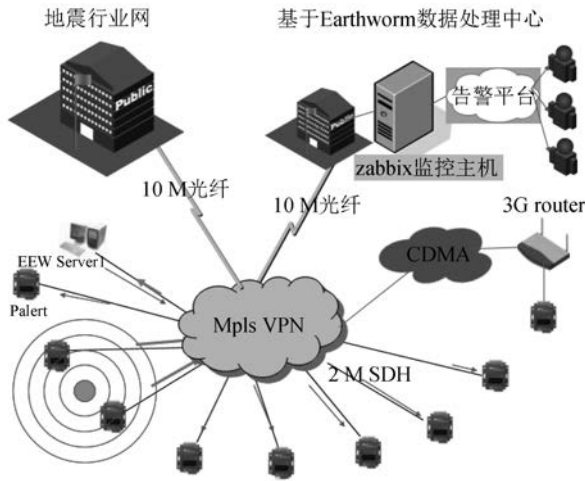


图 2 福建省简易烈度计台网业务系统拓扑图

2.2 数据中心数据处理系统

福建省简易烈度计台网数据处理系统引用了 USGS(美国地质勘探局)开发的 Earthworm 系统。该系统为开源软件,采用 C 语言进行编写,分成不同的模块进行组建。每个模块完成不同的功能,主要包括数据接收模块、P 波拾取模块、地震定位报告产出模块、地震事件图件绘制模块、地震波存储容器等五大功能(图 3)。基于 Earthworm 地震数据处理系统架构采用积木式组合的方式进行搭建,主要包括:

第 1 部分,数据接收部分,它是通过 MPLS VPN 组网方式将各台网观测中的烈度计产生的数据在数据中心进行汇聚,主要采用 Palert2ew 模块进行功能搭建;

第 2 部分,地震波形展示部分,主要采用 wave_server 模块进行功能搭建;

第 3 部分,地震数据处理部分,主要采用 pick_eww、tcpd、ShakeMap 的模块进行功能搭建,pick_eww 模块负责自动震相实取功能,tcpd 模块负责地震定位与震级计算功能,ShakeMap 模块负责烈度图绘制功能;

第 4 部分,地震数据存储部分,主要采用 Tbuf2mseed、Ewmseed Archiver 的模块进行功能搭建,Tbuf2mseed 模块负责进行数据格式转换功能,Ewmseed Archiver 模块负责进行数据文件存档的功能。

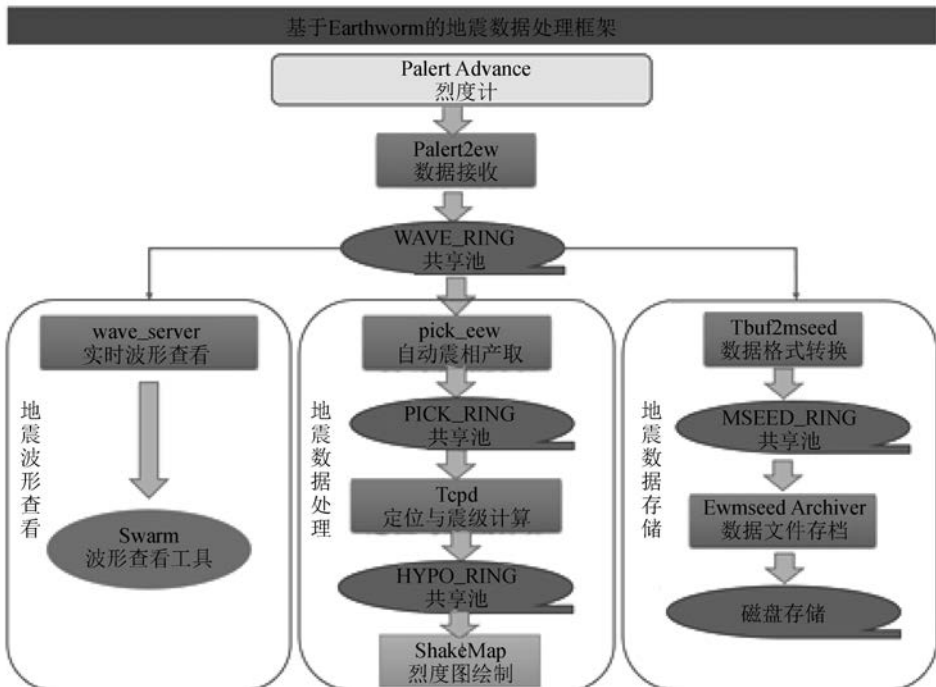


图 3 基于 Earthworm 数据处理系统架构流程图

2.3 地震观测系统

采用台湾生产的 Palert advance 简易烈度计。该烈度计硬件平台采用了树莓派 2B 型进行架构, CPU 采用 ARM Cortex-A7 系统(四核心), 支持运行全系列的 ARM GNU/Linux 发行版操作系统, 内存容量 1 GB LPDDR2 SDRAM, 存储为 16 G 的 Micro SD 存储卡, 操作系统为 Raspbian GNU/

Linux 7 发行版, 系统内核版本 3.18.7-v7, 地震传感器为 MEMS 加速度传感器。

3 监控系统设计

福建省简易烈度计台网实现监控主要分为三大部分, 即基于 Earthworm 数据处理系统的监控、基于烈度计 Palert advance 的监控、通信系统的监控^[2](图 4)。

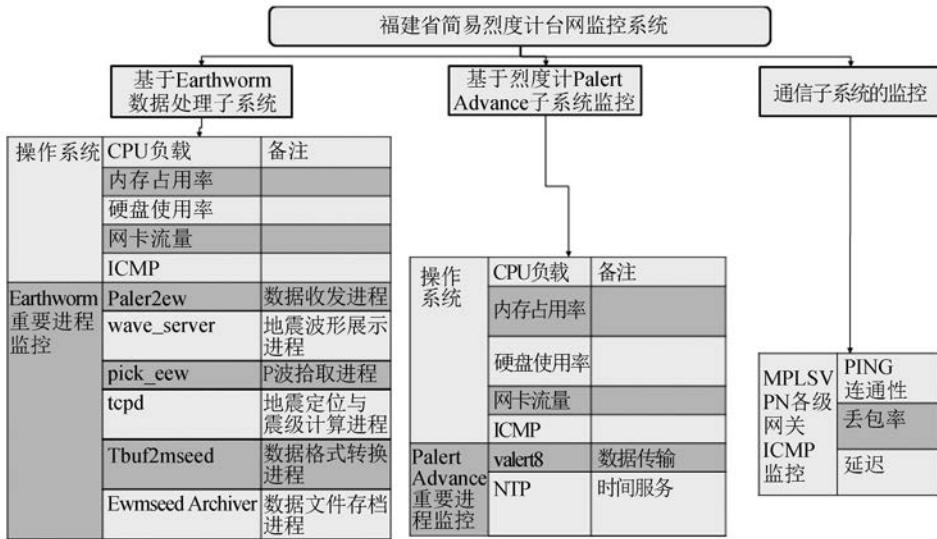


图 4 简易烈度台网监控体系设计

(1) 基于 Earthworm 数据处理系统的监控, 主要包括两部分: 系统部分与重要进程监控部分。系统监控部分包括: CPU 负载、内存使用率、硬盘使用率、网卡流量、ICMP 监控; 重要进程监控包括: 数据收发进程 (Paler2ew)、地震波形展示进程 (wave_server)、P 波拾取进程 (pick_ew)、地震定位与震级计算进程 (tcpd)、数据格式转换进程 (Tbuf2mseed)、数据文件存档进程 (Ewmseed Archiver)。

(2) 基于 Palert 烈度计观测模块的监控主要包括两部分: 系统部分与重要进程监控部分。系统监控部分包括: CPU 负载、内存使用率、硬盘使用率、网卡流量、ICMP 监控; 重要进程监控包括: 数据传输进程 (valert8)、时间服务进程 (NTP)。

(3) 通信系统监控, 主要包括各级网关 ICMP 的监控, 包括 PING 连能性、丢包率、延迟。

(4) 告警阈值设计: 通过对 Earthworm 数据处理子系统、Palert advance 地震观测子系统、通讯子系统各项监控项的观测, 规划出合理的告警阈值, 在出现故障时, 通知值班人员, 进行通知公告(表 1)。

(5) 自动化处理机制: 通过监控系统监控各子系统监控项预定义的阈值指标, 首先由监控系统调

用自动化处理命令进行自动化处理, 如果自动化无法处理再由脚本调用福建省微信公众号接口, 实时将故障信息推送至值班人员。

4 重要进程的监控与配置

Zabbix 工具本身就自带对操作系统的监控模板, 如 CPU 负载、内存、磁盘利用率等监控项, 但有时候监控项目在 zabbix 预定义的 key 中没有定义时, 可以通过编写 zabbix 用户参数的方法来监控我们要求的项目 item。形象一点说 zabbix 代理端配置文件中的 User parameters 就相当于通过脚本获取要监控的值, 把相关的脚本或者命令写入到配置文件中的 User parameter 中, 然后 zabbix server 读取配置文件中的返回值通过处理前端的方式返回给用户^[3]。

这里以 Earthworm 处理系统中数据收发进程 Palert2ew 模块为例, 我们需要对其监控该进程是否存活及该进程 CPU、内存占用率的监控, 其监控步骤及配置如下(其余重要进程类似):

第一步: 定义需要监控的 key 值(图 5)

在需要监控的系统配置文件 zabbix_agentd.conf 里面配置 UserParameter 项目, 用户参数的语

法 UserParameter=<key>,<command>

其中 UserParameter 为关键字,key 为用户自定义 key 名字可以随便起,<command>为我们运行的命令或者脚本。

定义判断 palert2ew 进程是否存活的 key 值: UserParameter=palert2ew,test \$(ps-aux | grep palert2ew |grep-v grep| wc-l)-gt 0 && echo 1 || echo 0

定义 palert2ew 进程 CUP 开销 key 值:User-

Parameter=palert2ewcup,top-bn1 |grep palert2ew |awk '{print \$9}'

定义 palert2ew 进程内存开销 key 值:UserParameter=palert2ewmem,top-bn1 |grep palert2ew |awk '{print \$10}'

第二步:在 Zabbix 系统中定义 item 项

即在 Zabbix 监控系统中配置需要监控的重要进程,主要是要需要监控的主机上新增监控项,写入第一步中在客户机 zabbix_angentd.conf 中写的

表 1 简易烈度计台网监控项阈值设计

序号	系统	监控项	告警阈值	备注
1		CPU 负载	>5	5 分钟平均负载值
2		内存使用率	<50 M	
3		硬盘使用率	>80%	
4		网卡流量	>6 M	实测 300 台平均 3.17 M
5		ICMP 连通性	=0	1 代表连通,0 代表中断
6		ICMP 丢包率	>20%	
7	Earthworm 数据处理子系统	ICMP 延迟	>0.15 s	
8		数据收发进程 Paler2ew	=0	1 存活,0 无活动
9		地震波形展示进程 Wave_server	=0	1 存活,0 无活动
10		P 波拾取进程 Pick_ew	=0	1 存活,0 无活动
11		地震定位与震级计算进程 tcpd	=0	1 存活,0 无活动
12		数据格式转换进程 Tbuf2mseed	=0	1 存活,0 无活动
13		数据文件存档进程 Ewmseed Archiver	=0	1 存活,0 无活动
14		CPU 负载	>5	
15	Palert advance 地震观测子系统	内存使用率	<50 M	
16		硬盘使用率	>80%	
17		网卡流量	<20 kbps	实测平均 42.3 kbps



图 5 定义监控项

UserParameter 关键字^[4]。

第四步:定义触发值

第三步:绘制可视化图形

根据对该进程 CUP 开销值的长期观测,得出

根据定义好的监控项绘制可视化图形(图 6)。

均值,定义触发值(图 7)。



图 6 重要进程可视化图形配置

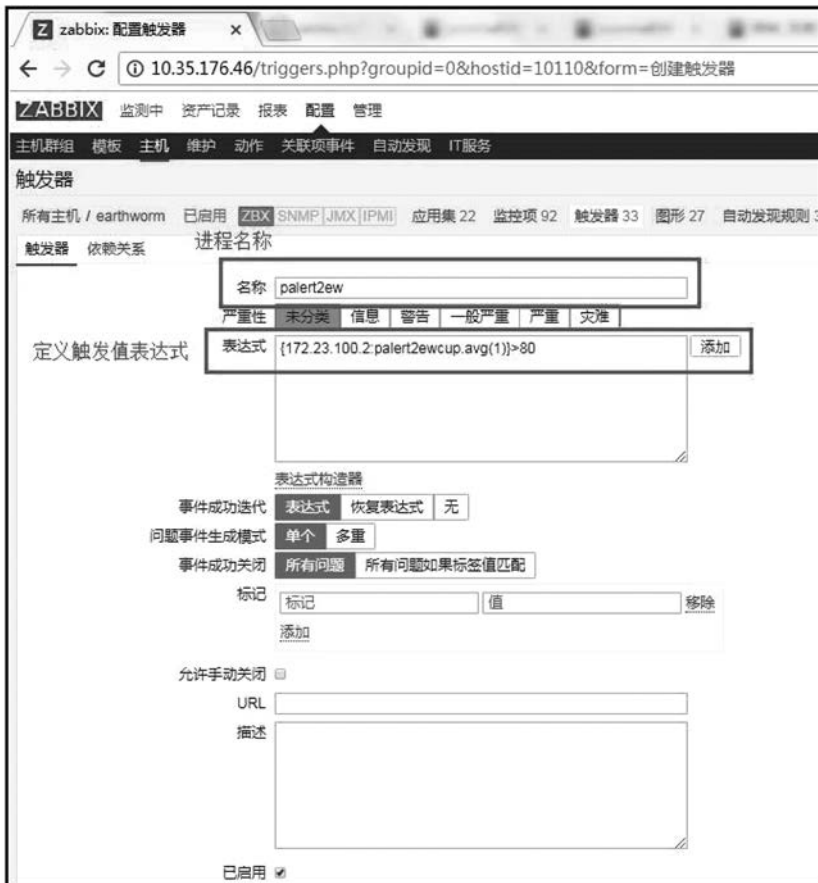


图 7 告警触发值设定

5 系统运行情况

5.1 状态汇总仪表盘

通过该系统状态栏,值班人员可以方便地查看台网目前所要处理的所有台站(图 8)。

5.2 数据处理系统重要进程监控可视化效果

Earthworm 地震数据处理系统各重要进程监控可视化见图 9。

5.3 基于福建省地震微信企业号的告警

实时将台网的故障信息在第一时间报送至值班人员(图 10)。

6 结束语

本文通过对 Earthworm 框架中各进程模块与 Palert advance 简易烈度计系统的研究,提取各子系统重要进程,结合开源告警软件平台,对其进行实时监控。通过该系统的试部署,发现 Earthworm 数据处理系统的主要特点是各项进程资源开销相当低,一般各个监控项资源使用率都不会超过 10%,且系统稳定性较好。台湾生厂的这套简易烈度计的主要告警有以下几类情况:第 1 系统频繁重启现象,通过固件更新此现象已明显修复;第 2 内存使用率周期

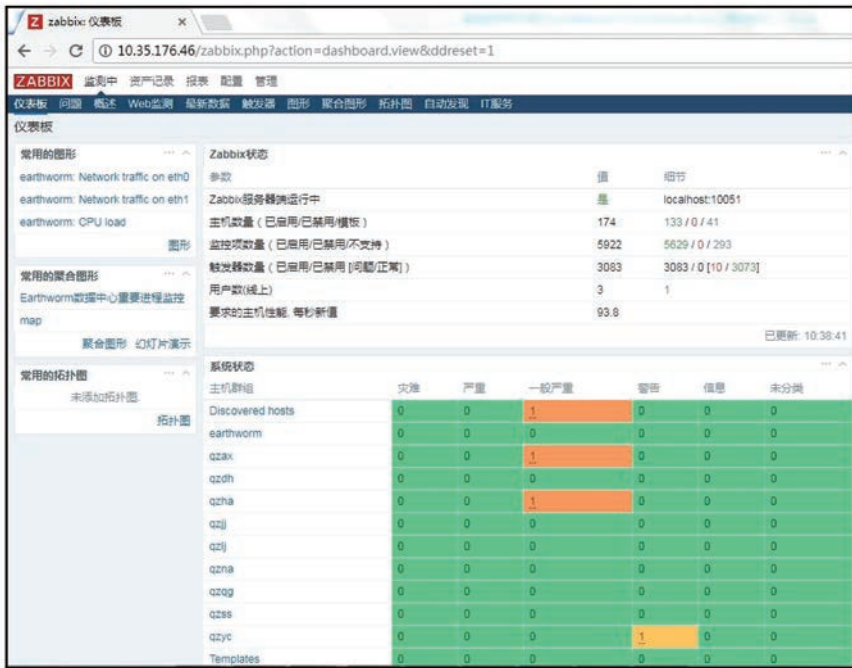


图 8 监控系统故障汇总仪表盘

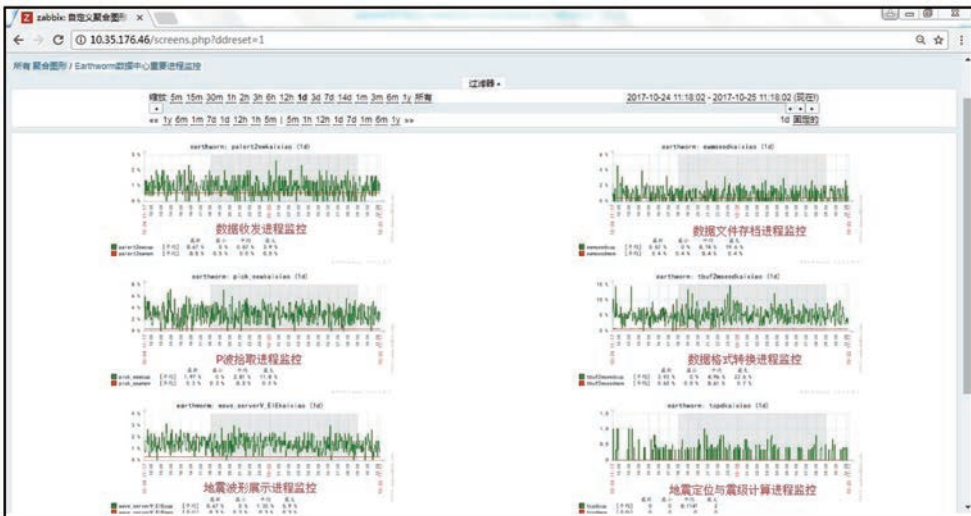


图 9 Earthworm 地震数据处理系统各重要进程监控可视化图示

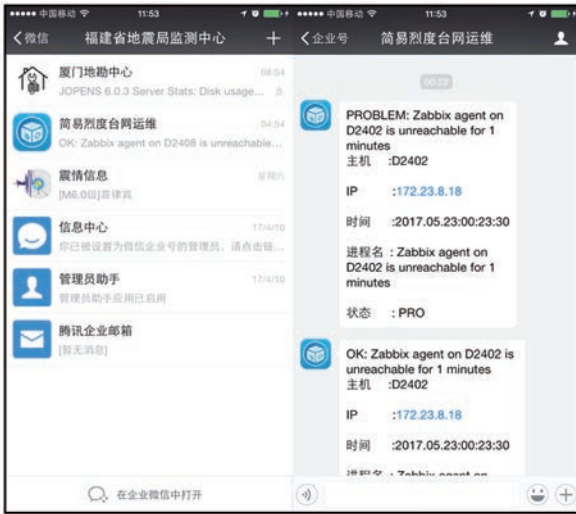


图 10 调用福建省地震局微信公众号进行故障实时告警

性超过 80%，主要原因是数传程序与系统兼容性差导致，目前已与厂家沟通协调，需对数传程序进行优化；第 3 硬盘使用率周期性超过 80% 的现象，主要原因是电流超限出错，导致 log 暴涨占用磁盘空间。

通过该系统的部署，笔者认为借助 Zabbix 这套开源监控系统可以在第一时间将烈度计台网故障事件通知给运维工作人员。以往地震行业内应用 Nagios 监控系统存在监控超过 200 台站点均会出现故

障告警延迟的现象，且存在可视化效果差，配置繁琐，而简易烈度计台网运维的主要特点是台站数量众多（福建区域未来是 1 000 台次左右），其通过 Zabbix 的分布式、可视化效果好、自动发现等功能，可有效解决传统监控系统存在的这些问题，使台网运维工作人员实时了解台网仪器健康状况，提高台网运维智能化监控水平。笔者认为随着国家经济的不断进步，地震行业的台网规模会不断扩大，像简易烈度计这种大规模台网运维，监控系统首先需要具备分布式的特点，才能更好地实时了解台网仪器的健康状况，保障台网的连续性观测质量。通过该方法的试部署，笔者建议将此方法在地震行业中推广应用。

参考文献

- [1] 李刚,周利霞,王晓磊,等.开源网管系统在地震监测网络中的应用[J].西北地震学报,2011,33(4):380-385.
- [2] 李刚,王晓磊,孙路强,等.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[J].地震研究,2012,35(1):133-138.
- [3] 郭晓慧,李润知,张茜,等.基于 Zabbix 的分布式服务器监控应用研究[J].通信学报,2013,34(增刊 2):94-98.
- [4] 李朝阳.利用 Zabbix 进行系统和网络管理[J].计算机时代,2008(10):19-22.