张晖，周利霞，姚会琴，孙晶岩，2012．Nagios 监控系统在天津地震应急系统中的综合应用．震灾防御技术，**7**（3）：322—328.

Nagios监控系统在天津地震应急系统中的综合应用 [1]

张 晖 周利霞 姚会琴 孙晶岩

（天津市地震局，天津 300201 ）

摘要 Nagios 等开源监控系统在地震行业中已应用多年，其运行稳定，监控效果良好，可扩展性强，是非常优秀的网络监控软件。本文利用天津市地震局统一建立的全局 Nagios 监控系统，对地震系统“十五”、“十一五”期间建立的地震应急指挥技术系统进行了全面监控管理，包括网络设备、服务器、业务应用系统等，并与值班系统联动，实现故障告警。采用此监控系统后，全面提升了天津市地震局应急指挥系统的运维管理工作效率。同时形成了独立的监控配置文件与脚本，可对行业应急指挥系统进行统一监控。

关键词：地震 应急 Nagios 监控 报警

引言

地震应急指挥技术系统是一个集工程技术、信息技术、空间技术、地震专业模型、决策支持于一体的综合系统（杨天青等，2010）。经过“十五”中国数字地震观测网络项目及“十一五”天津地震安全基础工程项目的建设，天津市地震局已经具备了一套较为完备的地震应急指挥技术系统，其主要包括天津市地震局应急指挥中心系统和滨海地震台应急指挥技术系统（备份中心），系统的基本功能为针对天津周边发生的有感地震进行触发响应、灾害评估与动态跟踪、辅助决策、信息服务、应急指挥等（帅向华等，2009）。随着技术系统的不断建设与完善，其中包括的网络设备、服务器、应用系统等越来越多，如何把应急指挥系统运行维护好，是业务人员在日常工作中面临的一个重要任务。

2012 年初，以天津市地震局建立的全局统一 Nagios 监控与报警系统为平台（李刚等，2011），将应急指挥系统中的各类网络设备、服务器、业务系统进行统一管理，实现了系统监控、运行状态的在线展示、故障报警等功能，全面提升了系统的运行管理能力。

1 天津市地震局 Nagios 监控系统介绍

Nagios 作为一个企业的监控软件，可以对各类主机、设备、服务等进行详细监控，并具

1 基金项目 天津市地震局青年地震科学基金（2200404）
［**收稿日期**］2012-06-15
［**作者简介**］张晖，女，生于 1979 年。工程师。主要从事地震应急工作。E-mail: zhanghui@mail.tjdzj.com

备丰富的扩展功能，目前可用于 Nagios 的扩展插件有上千种。

天津市地震局从 2010 年开始建设全局统一的 Nagios 监控系统，具备了设备、主机到应用系统的综合监控能力，同时与 Cacti、Nagvis、WeatherMap 等开源软件的结合，使系统具备流量统计、运行状态在线展示和流量分析等功能。同时通过二次开发，与全局值班系统相结合，实现了故障消息的全局联动告警服务（李刚等，2012），应用与服务效果良好。

目前 Nagios 监控系统已对信息网络、强震、前兆、GNSS 等业务系统实现了统一监控与告警，图 1 为系统结构示意图。

2　天津市地震局应急指挥技术系统监控方案

天津市地震局应急指挥技术系统的 Nagios 监控方案，主要包括以下几个要点：

统一监控：在现有 Nagios 平台上，实现对所有应急指挥系统设备与服务的监控统计，数据统一存储管理；

在线展示：对各类监控要素，要能通过 Nagios、Nagvis、WeatherMap、Cacti 等系统实现统一的在线展示，方便运行人员查看；

故障告警：对各类监控要素设计告警值，能通过全局短信网关将告警信息实时发送给相关人员，提高了故障的处置能力；

可二次利用：在设计与开发上，将监控配置文件与相关脚本编写成独立应用模式，初步形成监控标准模板，方便在行业内扩展应用。

表 1 为天津市地震局应急指挥技术系统被监控的设备与应用清单。

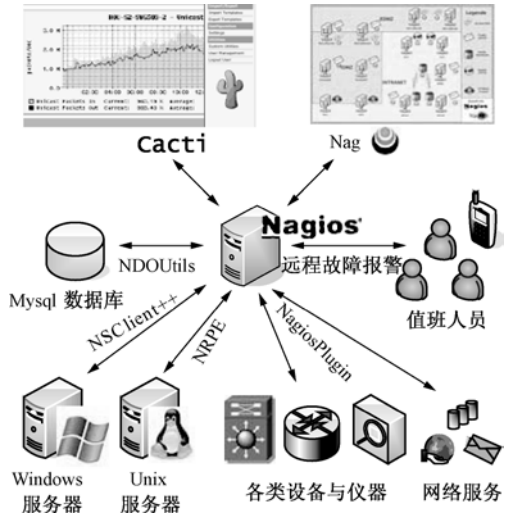

图 1　系统结构示意图

Fig. 1　System structure and set-up

表 1　被监控的设备与应用列表

Table 1　List of equipment and application under the monitoring system

服务器名称	Ip 地址	操作系统	部署应用
数据库服务器	10.12.48.101	Windows 2003	Oracle 10g
总线服务器	10.12.48.7	Windows 2003	ArcIms
			总线系统
			短信触发
认证服务器	10.15.48.5	Windows 2003	吉大认证系统
			指挥终端
			指挥命令与反馈系统
评估服务器	10.12.48.3	Windows 2003	地震快速评估系统
辅助决策服务器	10.12.48.2	Windows 2003	辅助决策支持系统

3 监控系统建设

由于采用全局统一的 Nagios 监控系统，这里不再介绍 Nagios 系统的安装过程。

应急指挥监控系统建设主要从以下几个方面介绍。

3.1 监控对象分组

对象分组是对象定义时必须进行的操作，其主要目的在于方便对象管理，尤其是在大型的网络监控中，分组更为重要。

为了方便管理，从位置属性和设备属性进行了分组，包括局中心应急系统分组、滨海地震台应急系统分组、应急网络设备分组、应急服务器分组和应急业务系统分组。其中应急业务系统分组属于服务监控分组，其他都为设备主机监控分组。我们将应急系统分组建立为 tjyj_group.cfg 文件，存放于 nagios 服务器中的/usr/local/nagios/etc/objects/目录下。

3.2 监控对象命名

对象命名前，要统一命名规则，在实际中采用如下命名方式：

局应急指挥技术系统设备：yingji-设备类型-设备名称-其它可描述设备的信息；

滨海地震台应急指挥技术系统设备：xx19-yingji-设备类型-设备名称-其它可描述设备的信息，其中 xx19 是滨海地震台的系统编号；

局中心各项应用与服务的监控命名：应用与服务名称-yingji-srv-其它可描述信息；

滨海地震台各项应用与服务监控命名：应用与服务名称-xx19-yingji-srv-其它可描述信息。

例如：

局应急指挥中心核心交换机 H3C 6502 的监控名称为：yingji-h3c-6502；

滨海地震台 Oracle 数据库服务器的监控名称为：xx19-yingji-server-75.101-Oracle，其中 75.101 为该服务器的 IP 地址后两位；

局中心数据库服务器上的 Oracle 监控名称为：Oracle-yingji-srv-48.101；

滨海地震台评估服务器上的 Weblogic 服务的监控名称为：Weblogic-xx19-yingji-srv-75.3。

采用这种命名规则时，在管理中可以很清楚地区分各类设备，同时也便于二次开发。

3.3 监控对象定义

有了分组和命名规则后，就可以定义每个对象信息的具体内容。

（1）网络设备的监控定义

局应急指挥技术核心交换机的配置如下，定义中各项内容为所用模板、主机名、别名、IP 地址、主机分组、上层设备名称、主机图片。

```
define host{
use        switchs
host_name   yingji-h3c-6502
alias      yingji-h3c-6502
  address     10.12.254.50
  hostgroups  switches
parents      center-h3c-7510
  statusmap_image multilayer_switch.gd2}
```

（2）Windows 主机及服务的监控配置

Nagios 对于 Windows 主机的监控需要 NSClient++来支持，本文中采用的版本为

win32-0.3.5，首先将 NSClient++安装于所需监控的 Windows 系统中，并将 NSClient++设置为随系统启动的一项常规服务，之后在 NSClient++的安装目录中编辑 nsc.ini 文件，做如下几项修改：

① ［Module］：将 RemoteConfiguration.dll 和 CheckWMI.dll 以外的 DLL 文件注释都去掉。

② ［Setting］：为 password 设定一个密码，并去掉注释。

password=secret-password 改为 password=123456

③ ［Setting］：为 allowed_hosts 选项设定 Nagios 服务器的 IP 或者设定一个 IP 段，并去掉注释。如：allowed_hosts=Nagios 服务器 IP 地址/32。

④ ［NSClient］：确认 port 的端口号是 12489，并去掉注释。

完成修改后，启动 nsclient++服务。

注意：在有些 Windows 主机中，开启了防火墙功能，此时要将 tcp 12489 端口打开，否则将不能正常监控。

在 Windows 主机中安装完成后，在 Nagios 服务器的/usr/local/nagios/etc/objects/command.cfg 文件中，添加一条对于应急指挥系统的监控命令，如下所示：

```
define command{
   command_name    check_nt_yingji
command_line     $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s 123456 -v
$ARG1$ $ARG2$  }
```

完成上述工作后，可以配置对一台 Windows 主机及其服务的监控，如下：

```
define host{    ‘定义 windows 主机
  use        windows-server   ‘所用监控模板
  host_name   yingji-server-48.3-PingGu   ‘主机名称
  hostgroups  10_YingJi_TianJin,10_YingJi_Server_TianJin  ‘主机所属分组
  alias      yingji-server-48.3-PingGu   ‘主机别名
  address     10.12.48.3    ‘IP 地址
  parents     yingji-h3c-6502  ‘主机上层对象
  statusmap_image win40.gd2   }  ‘主机标识图片

define service{   ‘对 CPU 监控，5 分钟内大于 80%普通告警，大于 90%故障告警
use         generic-port-service  ‘所用监控模板
host_name       yingji-server-48.3-PingGu   ‘服务所属主机
service_description CPU Load yingji-srv-48.3  ‘监控服务描述
check_command       check_nt_yingji!CPULOAD!-l 5,80,90   ‘监控命令
   servicegroups 10_YingJi_Services  ‘所属服务分组
}
```

在服务与业务系统的监控中，可以通过不同的监控命令实现不同监控需求。

对于主机上评估系统的监控：

```
check_command   check_nt_yingji!PROCSTATE!-d SHOWALL -l PGSRV.exe
```

对于主机上有关 TCP 服务端口的监控：

```
check_command          check_my_tcp!10.12.48.3!7005
```

在应急系统中，很多业务系统已采用基于 WebLogic 的 WEB 模式提供服务，不同的应用采用不同端口，通过上面的命令即可实现对其运行状态的监控。

完成监控文件的编写后，上传到 Nagios 服务器，通过如下命令检测配置文件是否正确，在无错误提示的情况下，可通过重新启动 Nagios 进程实现对应急系统的监控。

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

3.4 监控对象的统一展示

在 Nagios 完成系统监控后，通过 NagVis 实现监控系统的统一展示。NagVis 可以将各类 Nagios 监控信息以图形化的方式展示给用户，提高系统的可视化能力。它在用户选择的背景图片上显示主机和服务状态，根据监控对象的状态显示不同图标，红色图标为严重告警，黄色为普通告警，绿色为正常运行，灰色图标为未知状态。详细的 NagVis 使用方法请参考系统手册。

将前面完成的各类监控系统在 NagVis 中进行统一展示，如图 2 所示。图中按机柜与设备的安装部署位置，实时标注出设备与应用服务的运行状态，正方形图标为设备运行状态，圆形图标为应用与服务运行状态。

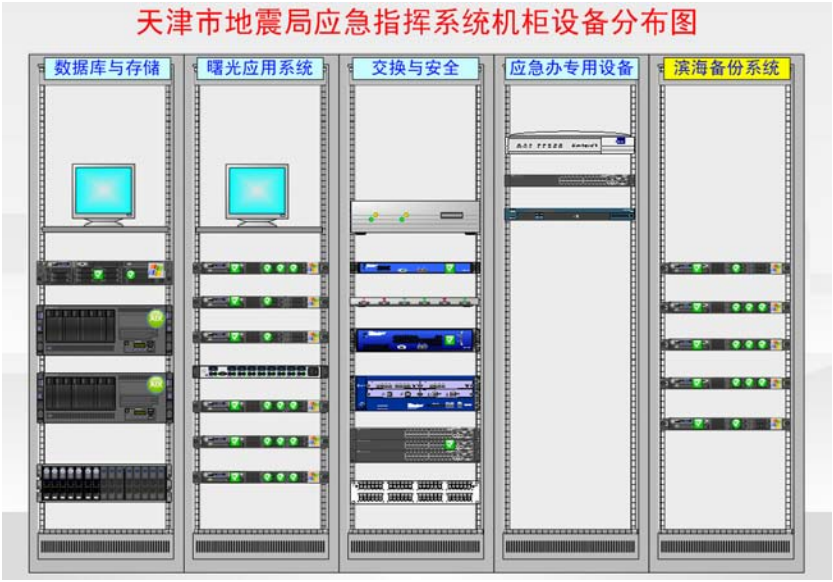

图 2 NagVis 监控图

Fig. 2 Display of NagVis

3.5 故障告警系统应用

在 Nagios 及相应组件中，已经有界面报警、邮件报警和语音报警三个功能，局中心的 Nagios 系统进行了二次开发，实现了与值班系统联动的监控信息故障短信报警功能，可以实现不同业务系统的快速故障通知、通告。系统拓扑图如图 3 所示。

在系统中，首先由 Nagios 监控系统生成故障告警信息，故障分类系统根据设定的分类原则并与值班数据库进行匹配检测，生成告警短消息，写入短信发送系统，实现故障信息短信通知。

此系统设计的非常灵活，如我部门 5 位值班员，滨海地震台 3 位值班员，部门管理员可以为所有人员根据值班时间设定值班数据信息，实现故障消息只发送给在班人员。同时，如果是局中心的应急系统出现故障，则信息只发送给局中心值班人员；如果是滨海地震台应急

系统出现故障，则故障消息通过消息分类原则，分别为局中心应急系统值班员和滨海地震台应急系统值班员同时发送故障信息，实现故障响应联动，提高故障响应能力。有关故障告警功能的详细内容，请参考李刚编写的《基于Nagios软件的手机短信联动告警系统在地震行业中的初步研究应用》[1]，其中有详细表述。

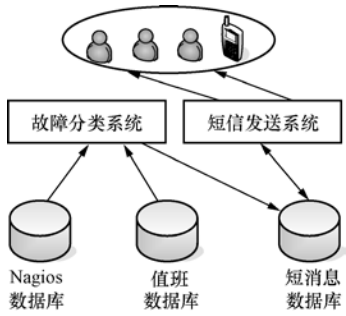

图 3　故障信息系统示意图

Fig. 3　Frame of failure reporting system

4　应用效果

通过应急指挥监控系统的实施与应用，天津市地震局应急指挥技术的运行监控能力得到了很大的提高，具体如表 2 所示。

表 2　应用效果对比

Table 2　Comparison of application effect with and without the system

分　类	使用前	使　用　后
设备与应用系统在线监控	较为简单	通过全局 Nagios 系统统一监控
设备运行状态展示	人工检查	通过浏览器可查看设定好的各类设备与系统服务的实时运行状态
故障告警与响应	人工检查	通过 NagVis 实现界面告警、语音告警，通过与值班系统和短消息系统联动，实现故障信息分类联动告警，可实现与滨海地震台应急指挥系统的故障联动响应与处置
综合管理与运行维护能力	一般	通过 Nagios、NagVis 可以在有网络接入的环境中，实时查看到系统运行状态，具备了一定的综合管理服务能力

系统运行后，大大提高了天津市地震局应急指挥系统的运行维护管理能力，使技术系统的设备和业务系统得到全面监控、实时了解与掌握系统状态，从而提升了系统的服务水平。

5　结语

Nagios 开源网管系统在 2010 年已经在地震行业中进行了部署应用，Nagios 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。通过上述工作，将天津市地震应急指挥技术系统的业务加入到天津市地震局综合监控系统当中，实现了基于 B/S 结构的网络管理方式，为应急指挥技术系统的各类 IP 设备、仪器与服务运行监控管理工作提供了帮助，实现了故障联动报警功能，大大提高了业务系统的故障响应与处置能力。

致谢：本项工作的实施得到了天津市地震局信息中心李刚的大力支持和帮助，在此表示衷心的感谢！

参考文献

李刚，周利霞，王晓磊等，2011. 开源网管系统在地震监测网络中的应用. 西北地震学报，**33**（4）：380—385.

李刚，王晓磊，孙路强等，2012. 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. 地震研究，**35**（1）：133—138.

1　李刚，2012. 基于 Nagios 软件的手机短信联动告警系统在地震行业中的初步研究应用. 天津市地震局.

帅向华，姜立新，王栋梁，2009. 国家地震应急指挥软件系统研究. 自然灾害学报，**18**（3）：99—105.
杨天青，帅向华，2010. 国家地震应急指挥技术系统建设中的关键技术及应用. 震灾防御技术，**5**（2）：208—214.

Comprehensive Application of Nagios Monitoring System in Tianjin Earthquake Emergency System

Zhang Hui, Zhou Lixia, Yao Huiqin and Sun Jingyan

（Earthquake Administration of Tianjin Municipality, Tianjin 300201, China）

Abstract Based on the Open Source Systems of Nagios, Cacti, NagVis, an Operation Monitoring System was developed in the Industry Network of Tianjin Seismological Bureau. This system is capable of monitoring various types of network equipment, instruments and services. Moreover, the system failure alarm system with the duty system linkage was realized to improve ability of the overall operation Monitoring Failure correspondence. It has been shown that the operation of the Open Source Systems in the Seismic Industry Network made it more efficient for the emergency responding system of Tianjin Seismological Bureau.

Key words: Earthquake; Emergency; Nagios; Monitoring; Alarm