

文章编号:2096 - 5389(2022)05 - 0098 - 04

基于 Zabbix 气象信息业务监控告警方法实现

郭 茜¹, 刘国强¹, 李从英¹, 支亚京¹, 彭宇翔², 金石声¹

(1. 贵州省气象信息中心, 贵州 贵阳 550002; 2. 贵州省人工影响天气办公室, 贵州 贵阳 550081)

摘 要:该文在贵州省气象信息中心搭建的基于 Zabbix 框架气象数据实时监控平台的基础上, 主要介绍了该架构监控流程、企业微信告警服务接入等功能的实现, 利用 Zabbix 开源框架的企业微信告警接口分别对接开发程序模块和睿象云智能告警平台, 实现对气象系统监控到的故障进行企业微信告警推送, 使运维人员及时发现异常故障事件, 并对其进行快速的响应与恢复, 从而为气象大数据云平台资源的自动化运维提供支撑和帮助, 使气象数据故障维护的效率得到大幅提高, 保证气象数据服务应用的及时性和可靠性。

关键词:Zabbix; 监控平台; 告警; 企业微信; 睿象云

中图分类号:TP311.52 **文献标识码:**B

Meteorological Monitoring and Alarming Method Based on Zabbix

GUO Xi¹, LIU Guoqiang¹, LI Congying¹, ZHI Yajing¹, PENG Yuxiang², JIN Shisheng¹

(1. Guizhou Meteorological Information Center, Guiyang 550002, China;

2. Guizhou Weather Modification Office, Guiyang 550081, China)

Abstract: The paper is based on the meteorological Zabbix framework real-time monitoring platform built by Guizhou Meteorological Information Center, mainly introduces the architecture of monitoring process and WeChat Work alarming service access. Using Zabbix open source monitoring alarming interfaces to dock with various social software, this paper realizes multi-channel alarming information pushing and help operation staff obtain alarming information at the first time. WeChat Work alarming improves fault processing effectively in the meteorological big data calculation center, and supports automated operation and maintenance, which makes the efficiency of meteorological data fault maintenance improved greatly, in order to ensure the timeliness and reliability of meteorological data service application.

Key words: Zabbix; monitoring platform; alarming; WeChat Work; CloudAlert

0 引言

近年来, 气象信息化高速发展, 通过大数据、云计算等现代科技信息技术在气象领域的应用与发展, 目前气象行业已进入建设智慧气象的新阶段。贵州省气象信息中心在气象信息化建设基础上, 进一步升级扩展, 形成国家级设计, 升级 CIMISS 分布

式数据存储, 在多中心协同的气象云数据管理能力建设, 气象服务大数据平台、支撑精准预报的众创业务平台, 基础设施资源监控和气象预报预测业务评估信息化系统建设等方面开展工作, 建立了基于混合云结构及标准化体系的气象数据分布式存储系统, 完成 CIMISS 系统的云化升级, 提供高效的数据支撑。并建立国省数据协同、服务协同流程以及

收稿日期: 2021-08-31

第一作者简介: 郭茜 (1989—), 女, 工程师, 硕士, 主要从事气象数据处理工作, E-mail: guoxiguoxi1989@163.com。

通讯作者简介: 刘国强 (1981—), 男, 硕士, 高工, 主要从事气象信息化和人工影响天气技术研究工作, E-mail: 24401052@qq.com。

资助项目: 贵州省科技计划项目 (黔科合基础-ZK[2021]一般 217); 基于风云卫星观测资料的冰雹天气识别研究; 贵州省气象局科研业务项目 (黔气科登[2021]11-23 号); 地面气象月报解析气象要素基于天擎历史分析库存储技术研究。

专有云、公有云同步的数据流程,整体提升了气象数据的服务能力和气象业务服务的能力^[2]。

数十年来,气象信息化基础资源建设得到大力发展,计算资源、数据资源在各行各业广泛应用,大量的数据传输给气象系统运维人员带来了巨大的挑战,为了提高气象数据传输的及时率、缓解系统运维人员监控和维护气象业务数据传输的巨大压力,本文根据省级气象系统维护的实际需要,在前期贵州省气象信息中心搭建的 Zabbix 气象业务系统监控框架的基础之上,通过使用编程语言开发相应的程序模块,使 Zabbix 框架对接企业微信、睿象云等社交软件,便于监控维护人员实时了解当前被监控对象的运行情况,并及时接收告警通知,以实现高效处理故障和缩短维护响应时间。

Zabbix 监控框架支持的插件多、组件多,集成了多种告警推送的方式,但是邮件告警信息常因没有专门的邮件应用分类,容易被运维人员忽略未及时查看,错过解决问题的最佳时机;短信告警的内容不仅不全面还容易被忽略,且通信资费高昂^[3]。微信目前是国内最受欢迎的即时通讯软件,因其体积小、速度快、功能多的特点、用户超十亿人,涵盖社会各类人群。企业微信在微信的用户群基础上建立,保留了用户对微信的使用习惯,在服务、功能和使用目的上区别于微信,使工作团体间能便利地沟通与应用,使企业和组织能够提高整体运营效率。大量的企业通过使用企业微信丰富、免费、多样化的第三方接口对接监控应用软件来推送告警信息,这样可以方便系统和数据运维人员及时查看告警信息,得以高效处理故障^[4]。

因此,本文在贵州省气象信息中心初步搭建的 Zabbix 监控气象数据传输框架的基础上进行企业微信告警推送功能的探索和研究^[5]。

1 Zabbix 监控告警流程

贵州省气象信息中心搭建的 Zabbix 采用的是分布式的分层架构:客户端采集数据在服务器端进行处理后通过 Web 前端交互界面以图表等方式展示给用户,代理服务器做代理,图 1 展示了 Zabbix 监控报警流程。告警触发是 Zabbix 监控报警流程中的关键环节,监控平台能够根据告警级别区分发送对象和范围^[6]。Zabbix 可以通过 Zabbix 服务器到客户端主动采集数据,也可以通过安装 Zabbix 监控代理后将数据由代理推送至 Zabbix - Server 的方式获取。通过配置监控项 Item 周期性地从主机里采集数据,并存到其对应的数据库中,同时将所采集到的数据信息通知到框架触发器 Trigger,由 Trigger 进行采集值与告警阈值的比较判断。若采集到的监控项数据超过触发器阈值,达到触发条件则产生告警事件 Event,Zabbix 将按照该告警事件所对应的 Action(动作)来进行处理。Action 会根据预设流程,利用 Zabbix 框架通过告警状态体形成相应告警信息,将告警推送给数据系统维护人员。产生的该事件可以通过多种方式,例如:企业微信告警、短信、邮件等方式通知触发器所属的主机组负责人;若监控项数据未超过触发器阈值,则不产生告警事件,监控项 Item 将继续进行该主机监控数据采集工作^[7]。

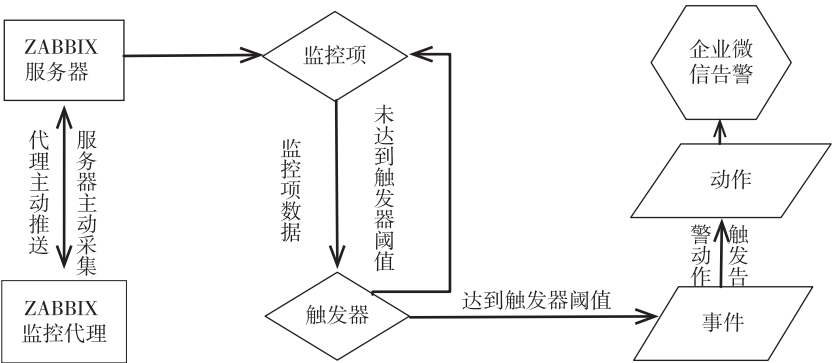


图 1 Zabbix 监控报警流程
Fig. 1 Zabbix alarming process

2 程序模块设计

2.1 Zabbix 实现企业微信告警

企业微信区别于个人微信的优势在于它支持

一键群发、标签群发,并且客户资源属于企业,以便员工利用社交账号专门处理企业工作内容。同时企业微信的后台开放 API 接口,可以通过专门的企业微信 ID 号对接各开源告警平台,将公众号、小程序

序等流量池数据打通,实现精细化的运营管理。大多数故障是通过监控系统发现、推送告警信息给系统维护人员,由运维人员及时处理以避免造成重大损失。因此,及时、准确地分析和处理各类告警成为系统运维重中之重的内容。在系统监控运维工作中,传统告警方式是邮件和短信,但邮件告警的及时性比较差,告警邮件容易被忽略;短信告警及时性比较强,但告警内容单一,维护人员不能够及时精确地判断故障的具体情况。另一种告警方式就是通过企业微信进行监控告警,保证运维人员日常使用社交软件的同时,也能够关注到监控系统的告警信息,并及时进行维护和处理^[8]。本文基于 Zabbix 监控框架与企业微信进行关联,利用 Python 语言开发相应的功能模块实现企业微信应用推送运维告警信息。

通过企业微信创建 Zabbix 应用,并添加气象业务系统的运维成员账户,所有与 Zabbix 相关的告警信息将通过该应用进行推送。

创建成功后,企业微信会分配出每个成员的账号,AgentID(应用 ID)、CorpID(企业 ID)和 CorpSecret(秘钥),Zabbix 框架在调用 API 接口时用以上信息作为身份 ID 识别码。企业微信告警模块是基于 Python 环境开发的,该 Python 程序主要是用于对接 Zabbix 框架与企业微信中建立的 Zabbix 应用,以实现通过 Zabbix 监控目标主机数据触发告警,并通过企业微信应用推送到系统运维人员。将编写好的模块.py 放入 Zabbix 服务器端/etc/Zabbix/alertscripts 目录下,并赋予权限,使 Zabbix 用户能够执行该程序。测试该模块是否能够正常与企业微信对接时,可以在 Zabbix 服务端 bin 目录下进行,通过命令行对已编译的 WXAlert.py 进行测试,若能够在企业微信中收到消息,证明该程序运行正常,测试命令如下:

```
[root@localhost alertscripts]# ./WXAlert.py
username test 1615helloZabbixTest https://qyapi.
weixin.qq.com/cgi-bin/- gettoken? corpid=ww1
* * * cd&corpsecret=1wV5 * * * ZywVEW2dIac。
```

2.2 程序模块核心代码

在企业微信告警核心代码程序中,主要创建 2 个函数:Gettoken 函数与 Senddata 函数。Gettoken 函数用于创建令牌。从已注册的企业微信中获取 CorpID(企业号标识)、CorpSecret(企业号秘钥)并对 2 个参数进行编码后一并存入 Token 中。创建 Token 令牌主要是用于企业微信客户端访问服务端时的身份验证,当客户端第一次访问服务端时,服务

端生成 Token 后返回给客户端,之后客户端无需重复输入用户名和密码,只需携带身份令牌 Token 便可频繁地访问企业微信服务端。否则每次发送告警信息时客户端都需输入账户密码,造成服务端访问压力过大,客户端发送告警通知的流程变复杂,同时账户和密码泄漏风险增大,增加了黑客截取账户的机会。因此,在核心程序中,使用 Token 令牌进行身份验证,而非将账户密码存储于 Session 中。Gettoken 函数如下:

```
def gettoken(corpid,corpsecret):
    gettoken_url =
        'https://qyapi.weixin.qq.com/cgi-bin/
gettoken? corpid='+corpid+'&corpsecret='+corpsecret

    print gettoken_url
    try:
        token_file = urllib2.urlopen(gettoken_url)
    except urllib2.HTTPError as e:
        print e.code
        print e.read().decode("utf8")
        sys.exit()
    token_data = token_file.read().decode('utf
-8')

    token_json = json.loads(token_data)
    token_json.keys()
    token = token_json['access_token']
    return token
```

函数 Senddata 用于传送企业微信告警接收用户(企业微信用户账号 touser:aa、bb、cc、dd)、Toparty 是企业微信中的部门 ID:8、agentid 是企业微信中的应用 ID:100003、告警主题 Subject 以及告警内容 Content。

```
def senddata(access_token, user, subject, content):
    send_url =
        'https://qyapi.weixin.qq.com/cgi-bin/mes-
sage/send? access_token='+access_token

    send_values = {
        "touser": "aa|bb|cc|dd",
        "toparty": "8"
        "msgtype": "text"
        "agentid": "1000003"
        "text": {
        "content": subject + '\n'+ content
    }
```

```
"safe": "0"
}
```

主程序接收以上程序传递过来的 3 个数组:企业微信接收用户、企业微信告警主题、企业微信告警内容。

```
if_name_ == '_main_': user = str(sys.argv[1])
    subject = str(sys.argv[2])
    content = str(sys.argv[3])
```

从企业微信号中找到企业号标识 `ww1***cd`、企业号密钥 `1wV5***ZywVEW2dIac`,并在程序中分别赋值给 `CorpID`、`CorpSecret` 参数,将 `Get-token` 令牌函数获取到的参数赋值给 `Access token` 参数,并将以上形成的实际参数全部赋予 `Senddata` 函数进行处理。

在 Zabbix 网页显示端,对报警媒介和触发报警动作进行配置,使得 Zabbix 框架网页显示端与 `WX-Alert.py` 程序关联起来。Web 端配置报警媒介:点击管理→报警媒介→创建报警媒介→设置用户。

Web 端配置触发报警动作:点击配置→动作→创建动作→编辑告警信息状态体,动作的事件源为触发器,可以设置发送告警的时间间隔等。

本文以设置某主机 CPU 负载率超过 1% 作为触发告警事件项测试企业微信告警。当该主机 CPU 负载率超过 1% 时,在企业微信 Zabbix 应用中产生了准确的告警信息。至此,Zabbix 框架对接企业微信告警模块的开发和部署已完成,运维人员可在 Zabbix 创建的企业微信 Zabbix 应用信息对话框中看到 Zabbix 框架监控到的测试主机项目告警信息:当该主机 CPU 负载 > 1% 时告警,并且当该故障及时得到恢复的时候,Zabbix 同样也将已恢复的告警信息发送至该企业微信应用。

2.3 睿象云规则压缩告警至企业微信

Zabbix 虽然能够直接推送告警至企业微信平台,但如遇到网络中断、闪断,监控内容多、设备多的情况下,会产生海量的告警信息,从而导致告警风暴,运维人员很难从海量告警中筛选出重要告警信息。Zabbix 框架推送的告警信息经过睿象云智能告警平台可以实现告警压缩与降噪,在不遗漏重要告警的前提下,通过聚类算法快速智能合并重复信息,减少告警。本文利用睿象云智能告警平台 `CloudAlert` 对接 Zabbix 框架进行企业微信的告警推送。首先,通过睿象云平台集成 Zabbix 框架,并在 Zabbix

-Server 服务端安装睿象云采集告警的代理 AGENT,并得到代理安装密钥: `ec1ec423***ce050cc`。

在睿象云平台集成企业微信应用,获取企业微信机器人 `webhook url`: `https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=7a493fld-***1d1e2` 在企业微信 Zabbix 应用中点击添加群机器人→添加机器人→输入机器人名字→填写 `webhook url`。睿象云智能告警平台通过告警机器人集成推送告警信息至企业微信。

3 结论

本文利用 Zabbix 开源监控框架监测气象核心业务系统的运行状况,并开发框架内相应程序模块,通过企业微信成功实现告警推送,同时通过搭建睿象云智能告警平台对 Zabbix 框架内告警信息进行降噪、压缩后再推送告警至企业微信。在 Zabbix 框架内配置各个监控项对应采集值的触发策略以及告警动作,根据对告警信息的不同等级的综合分级及判定,利用程序模块对接企业微信开源 API 接口高效、及时推送告警信息以便运维人员及时处理,实现对气象核心系统进程的自动化运维。利用企业微信推送基于 Zabbix 框架的告警信息,既有效地控制运维的成本,又能保障气象 IT 系统业务正常、安全、有效运行。

参考文献

- [1] 杨立苑,胡佳军,邓卫华,等.基于 Zabbix 的省级气象云监控运维系统[J].计算机系统应用,2021,30(8):73-80.
- [2] 刘远超,李树彬.基于 Zabbix 和微信企业号实现网络监控的研究[J].山东科学,2017,30(4):124-130.
- [3] 支亚京,汤宁,吴兴洋,等.贵州省常规站海平面气压疑似信息分析[J].中低纬山地气象,2021,45(2):91-93.
- [4] 陆慧妍.企业信息系统监控平台的设计与实现[D].华南理工大学,2015.
- [5] 周昊.利用 Zabbix 和企业微信实现公安监控[J].中国有线电视,2017,11(26):1324-1325.
- [6] 白铁男,彭宇翔,郭茜.Zabbix 系统在气象业务监控中的研究与实践[J].福建电脑,2020,36(10):101-103.
- [7] 李从英,金石声,郭茜.使用 SymmetricDS 软件同步 CIMISS 核心库数据[J].中低纬山地气象,2020,44(1):71-75.
- [8] 廖婷婷,王彪,肖卫青,等.Storm 流式技术在地面气象数据处理中的应用[J].中低纬山地气象,2019,43(5):78-81.
- [9] 朱君,王浩,蒲晓虎,等.重庆气象可视化监控平台的设计与实现[J].气象水文海洋仪器,2021,38(3):82-82.