厦门大学
开源监控系统让运维更高效

厦门大学

文 / 郑海山

监控对于系统运维的重要性不言而喻，监控可以通过一些征兆在问题出现之前得到通知，也可以在故障出现之后比用户更早得到提醒并介入处理，同时监控也是一个很好的资产视图，在网络安全管理中一个最重要的前提是摸清家底，监控项的多寡也反映网络资产梳理的成效。

监控是一个工具手段，本身各个不同系统也会自带，比如网管软件、刀片服务器管理工具、VMWare 自带、现网流量分析工具等等。监控的一个特点是可以多套并行，互相验证，所以在系统自带以外再建立一套统一的基于开源软件的监控也有其必要性。市面上开源监控软件众多，功能存在重合，本文以厦门大学信息与网络中心监控系统的部署实践为例，探讨使用最适合的开源软件，发挥各种不同监控软件的优势，搭建符合高校信息中心业务场景要求的监控系统。最终将选择的开源软件的自动化部署源代码分享在 https://github.com/haishanzheng/CampusMonitor。本文不涉及整合多个监控软件平台数据，也没有对所有业务场景均进行监控，比如针对高性能计算服务器的监控，在服务器增多以后，故障是常规的，这时候只要关注整个集群整体对外提供的计算能力，而无需过多关注单个服务器的故障，在这种情况下 Ganglia 等开源软件是更好的选择。

监控的问题和解决思路

高校信息中心的监控可大致分为两种情况：一种是师生对外访问网络的网速测量。网速是一个非常主观的概念，由于网速与目的地（国内、国外、教育网、运营商）、协议（视频、直播、HTTP、BT）、带宽、时延、抖动、丢包率等均有较大联系，只有这些结合再加上历史基准数据比较才能对网速进行定量分析。另外一种是数据中心对外提供的各种业务服务情况。这两种情况的监控对象存在重合，主要在于交换机、数据中心服务器和不同的链路。

解决思路就是使用 Zabbix 监控内部的所有交换机、数据中心服务器和服务器上的业务状况，使用 SmokePing 监控对外访问状况。

监控级别

监控存在多种级别：

1. 可用性监控。可用性监控是最简单的监控，对系统是非侵入性的。比如监控 Ping，监控 TCP 端口是否正常，监控 HTTP 返回值等等。

2.SNMP 监控。一般交换机均默认自带 SNMP 协议，只需要交换机对监控服务器开放授权即可。

3.Web 业务监控。Web 业务可以从更高层面对 Web 应用进行监控，比如是否可以登录，是否可以成功发送邮件等多个组合操作，这部分需要更多的配置和调试。

4. VMWare 监控。高校一般已经建立了基于 VMWare 的虚拟化集群，对于 VMWare，提供只读的管理账户即可利用 VMWare 自带的 API 对其进行监控，侵入性也较低。

5. 基于 Agent 的监控。需要在被监控服务器上安装 Agent，才可以监控到 CPU、内存、硬盘等信息。

6. 基于应用生成的性能参数或日志的监控。

7. 自定义监控。Zabbix 支持编写自定义监控脚本，本监控手段需要监控管理员和业务共同配合，较为复杂。

如果是从无到有建立监控系统，可以采取逐步完善的过程，监控系统虽然可以在短时间内建立起来，但是对所有资产进行完全监控需要一段较长的时间，初期可以只监控可用性，只需要将服务器或交换机IP地址加入，即可监控是否在线；将网站URL加入，即可监控HTTP服务是否在线；接着对重要的信息系统，在系统上安装Agent进行更多的监控。交换机可以从核心交换机开始，使用SNMP进行监控，再慢慢过渡到全网。有些监控项可以等到故障发生的时候，根据故障的可重现和可测量再针对性的进行监控项添加。

区分处理和观察

高校信息中心除了维护校一级的业务系统外，也需要对二级学院的服务器和网站进行安全管理，然而二级学院的网站或者服务器，有些资产没有收集完整，有些由于二级学院安全设置无法对其进行监控，而且即使监控到问题，也无法立刻处理。然而即使存在这些问题，对于二级学院的网站和服务器也需要监控，但是这部分的监控以观察为主，不设置报警。同时在二级学院内部推广监控系统，督促二级学院自行对服务器进行监控。

Zabbix对于Web URL的监控较为繁琐，对于观察为主的监控，可采用Icinga，只需导入DNS或备案系统内的网站数据，即可快速建立起基于网站的监控。

监控系统的安全

高校内由于安全域划分可能存在包括一卡通、网络层等专网，这些专网需要对监控系统开放访问权限，存在一定的安全隐患。所以可以采用Zabbix的主从监控，在专网内放从监控代理服务器，从监控代理服务器不提供服务，只是收集监控信息并传到主服务器，有效解决了安全问题。

对于监控查看人员进行划分，信息中心内不同部门有不同角色，可能包括网络层、无线、有线、核心交换机、接入交换机、系统层、数据库、业务层、外包人员、值班人员、领导等多个角色，每个角色关注点不同，比如数据库管理员，虽然数据库依托在操作系统上，但是数据库管理员更多关注数据层层面的指标，而操作系统由其他人维护，对于操作系统的运行指标可能需要了解，但是报警可能就无需处理。而外包人员则严格限制只能查看部分监控项，这些可以通过Zabbix自带的强大的监控项分组和人员分组来解决。

监控应当也可对公众提供访问，使得公众可以在某个网站查看高校内某些业务的运行状况，减少在故障发生时信息中心服务台接收到报修请求的数量，并在业务恢复后得到通知。对于对公众提供的展示，为了系统安全需要隐藏系统细节，为了对公众友好需要将多个监控项进行组合并对专业术语进行解读。对于对外访问网速情况，可以直接提供SmokePing界面，对数据中心内业务的情况，可以通过将Zabbix数据传递到Grafana内再进行组合展示。对外提供服务器的Grafana应经常更新安全补丁，访问Zabbix数据库的账户应当是最小权限的只读账户。

系统部署复杂

在分析完以上问题后，监控需要安装包括Zabbix、Grafana、Icinga、SmokePing等多个开源软件，有些为了安全分离需要安装多套，有些需要在重要系统内安装Agent，多个开源软件之间需要整合，比如Zabbix采用主从架构监控，会存在一主多从的多台服务器，Zabbix数据需要传递到Grafana内展示，需要安装插件。SmokePing采用主从架构，从服务器需要放到多个不同二级学院内采集数据，这些需要安装的服务器数量众多，配置繁琐，很难在短时间内建立起来。

解决方法是使用容器或者其他开发者已经建立起来的自动化部署脚本，即可在非常短的时间内建立起监控系统，大大减轻系统部署的难度和工作量。

开源监控系统部署实践

基于以上分析，最终我们整合了多个开源软件，通过编写自动化部署脚本，建立了基于开源软件的信息中心监控体系，图1是监控系统整体框架。

在图1中，黄色服务器为Zabbix主从服务器，从代理服务器部署在靠近被监控区域，并将监控结果传到Zabbix主服务器。主Zabbix数据库将数据分成2份提供给管理员和公众访问的Grafana服务器。绿色服务器为SmokePing主从服务器，从SmokePing服务器从各个区域访问互联网网站，并将链路过程的交换机和最终目的地的监控数据汇总到SmokePing主服务器。

建立监控系统只是整个监控的第一步，接下来需要各色不同人员参与进来添加维护监控项，为避免不规范使用和提高添加效率，应当形成完善的帮助文件。对监控项的添加规则、值班人员需要查看的界面和操作、各个不同人员需要订阅的报警、同一个机器多个不同管理员如何共同处理故障报警的协作方法，制定出最佳实践文档和规范要求，并在内部公开。

Zabbix部署实践

Zabbix支持主从部署，从服务器可以部署到一卡通、网络等专网内，也可以在互联网云平台部署，检测从互联网访问数据中心业务的情况。为了安全，从服务器只允许外传监控数据，同时为了规避Zabbix主服务器被入侵后渗透到内网，应当充分评估是否启用主服务器可以在从服务器发起命令执行功能。

Zabbix的配置项非常灵活，也导致了配置的难度。应当充分利用Zabbix提供的Template机制简化部署。由于Zabbix的权限配置和很多搜索及过滤都会使用“主机群组”，所以“主机群组”应当在前期就

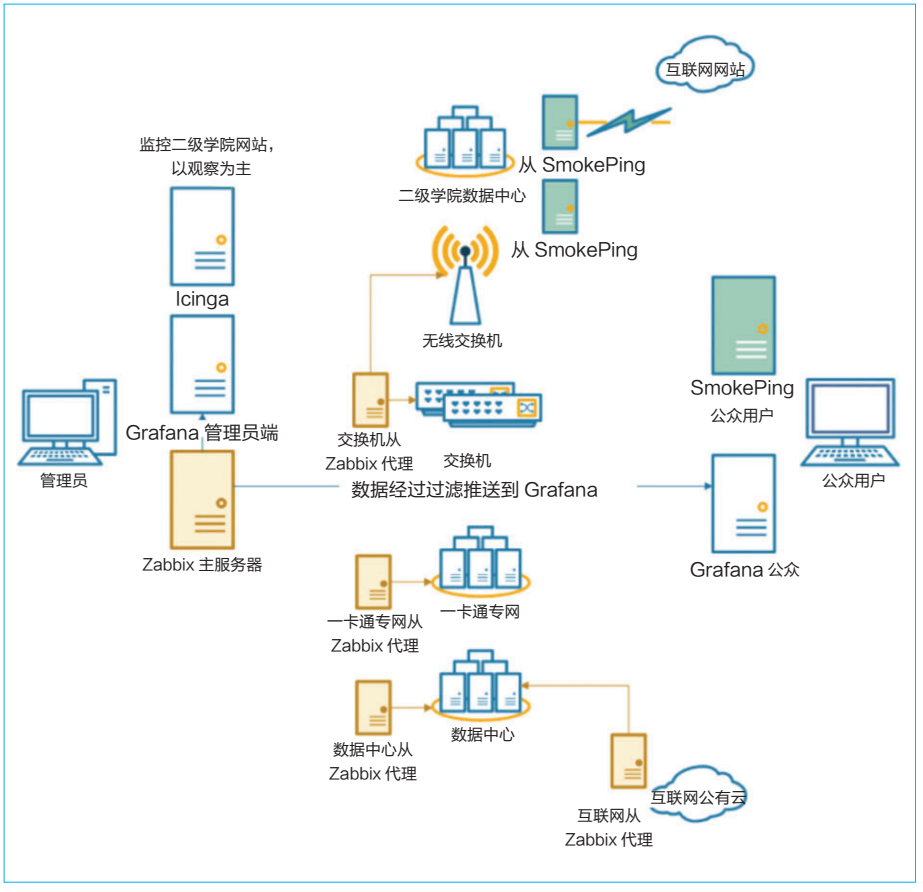

图 1 监控系统整体部署框架

做好规划，“主机群组”本质上类似标签，也支持树形关系，以“/”区分子主机群组，第一级“主机群组”应当是信息中心部门，业务名称和区域等等。比如办公自动化主机，可以分配包括“服务器”、“业务 / 办公自动化”、“系统部”、“新机房”等多个主机群组，方便对其进行权限过滤和监控配置。

Zabbix 可以使用 GUI、API 和导入导出配置主机，GUI 配置稍显麻烦，对于大量的交换机，可以考虑使用 Excel 管理，然后再使用类似 Python 脚本解析 Excel 生成导出文件导入到 Zabbix。对于一般 Ping 的监控可以使用模板“Template Module ICMP Ping”，而对于交换机的 SNMP 监控可以使用模板“Template Net Network Generic Device SNMPv2”。

Grafana 部署实践

Grafana 的引入是基于安全和可视化考虑。Zabbix 的仪表盘功能非常强大，但配置较为麻烦，Grafana 的仪表盘效果更为酷炫，技术上更先进，通过引入 Grafana，可以将 Zabbix 作为一个数据源，很快配置起仪表盘，也可以将多个图表指标整合在一起生成新的图。同时为了隔离对公众提供的 Grafana 的安全性，应当单独部署一套 Grafana，设置严格的安全策略，并对历史数据查看进行限制。

Grafana 有对自动化部署作优化，所有的数据库连接和仪表盘均可以使用自动化部署配置。

Icinga 部署实践

Icinga 的所有功能 Zabbix 也都支持，然而 Icinga 配置更为灵活，可以使用纯文本配置，通过跟 Python 脚本对接，可以快速建立起对网站的监控，通过剥离 Zabbix 和 Icinga，使用 Icinga 来监控二级学院的网站，只做观察不做处理，减少对 Zabbix 的干扰。Icinga 使用的 IP 地址应当告知二级学院管理员以免被安全软件拦截。

SmokePing 部署实践

SmokePing 跟 Icinga 引入的作用类似，功能上 Zabbix 都支持。SmokePing 使用 Perl 编写，使用 RRD 画图，技术较为古老，但是 SmokePing 由于功能较为单一，更为聚焦，配置使用纯文本，更加灵活，而且 SmokePing 对公众提供服务，独立后安全性更高。

SmokePing 支持主从模式部署，通过将从服务器部署到各个不同区域，可以监控主从服务器对不同互联网出口链路上的交换机、互联网服务器和网站的时延。SmokePing 也支持将多个图在一个图集中展示比较。对于从服务器，从成本考虑可以使用价格更对低廉的树莓派大量部署。

SmokePing 配置文件内的移动、电信、联通、教育网等多个运营商，各省，各大网站数据可以多个高校共享，CampusMonitor 项目在配置里对共享和自定义的内容进行了剥离，有效解决了数据共享问题。

通过对高校信息中心监控目标的分析，通过编写自动化部署工具一键部署起包括 Zabbix、Grafana、Icinga、SmokePing 等多个适合高校信息中心的开源监控系统，实现了信息中心对访问互联网网速的测量和对数据中心业务的监控，提高了信息中心的运维水平。通过将监控结果进行友好性解读后展现给公众，让信息中心对外提供的服务更加透明。对信息中心全资产监控的建立不是一朝一夕可以完成的，需要对资产引入全生命周期管理理念，在资产产生时就需要纳入监控管理，在日常工作中增加单个资产更多的监控项，将监控做广做深，并让公众参与监督，才可以真正提升信息中心的运维和服务水平。CEN

（责编：付涵）

（作者单位为厦门大学信息与网络中心）