

国内超大规模Zabbix集群负责人力作

全面讲解Zabbix配置应用，深入剖析Zabbix内部原理

用真实工作需求驱动，以独家实践案例指引，助您监控利器出鞘

Broadview[®]
www.broadview.com.cn




Zabbix

监控系统深度实践

第2版

姚仁捷◎著

 中国工信出版集团

 电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn



Zabbix

监控系统深度实践

第2版

姚仁捷◎著

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书由浅入深，全面讲解Zabbix应用与原理，是作者多年实战经验的总结和浓缩。在概念篇，从一个简单但完整的入门案例讲起，案例中有最基本的概念介绍，通过案例帮助那些只需将服务器加入监控，就能看到监控数据的读者；然后逐步深入，在进阶篇介绍Zabbix的各方面的配置；在设计篇中对Zabbix的内部原理进行深入剖析，包括Zabbix与数据库的交互、Zabbix数据库表的设计等，并分享作者在Zabbix上踩过的坑以及解决问题的思路；最后会在开源部分介绍58同城开源的Zatree和Chrome的插件、手机客户端等工具。

本书从工作中的实际需求出发，以实际案例作为指引，希望对于读者而言，不仅仅是学会某些具体的操作，而是深入了解Zabbix的设计思路，掌握解决问题的方法。

本书适合想使用Zabbix构建监控系统的技术人员阅读，也适合有一定基础、对于Zabbix有更高的要求读者。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

Zabbix监控系统深度实践 / 姚仁捷著. —2版. —北京：电子工业出版社，2016.8
ISBN 978-7-121-29608-6

I. ①Z… II. ①姚… III. ①计算机监控系统 IV. ①TP277

中国版本图书馆CIP数据核字（2016）第181578号

责任编辑：董 英

印 刷：北京嘉恒彩色印刷有限责任公司

装 订：北京嘉恒彩色印刷有限责任公司

出版发行：电子工业出版社

北京市海淀区万寿路173信箱 邮编：100036

开 本：787×980 1/16 印张：23.5 字数：527千字

版 次：2014年8月第1版

2016年8月第2版

印 次：2016年8月第1次印刷

印 数：3000册 定价：79.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlt@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

姚仁捷同学跟我提起,他要写一本关于 Zabbix 的书,其实一开始我是不太鼓励的。在我看来,写书向大众传播知识,是一件很严肃的事情,仁捷作为一名年轻的技术人员,去完成一本书可能还是会有些吃力的。但是我看到他有这个决心,对待书的态度也非常虔诚,每天都会繁忙的工作之余加班写作,书真的写完了,不由得很是佩服,作为他毕业到现在的多年老板,必须顶一下。事实上,从 PPTV 到唯品会,仁捷都基本上是独立承担一个领域的工作,借鉴业界的最佳实践 (Best Practice),从无到有地快速建立起完整的解决方案。的确是,聪明的人,给机会,就能脱颖而出。

Zabbix 是业界近年来较为流行的一个比较完善的开源系统监控解决方案,我们当初也是调研了不少解决方案才选择了它。姚仁捷曾经是 PPTV 的 Zabbix 集群的负责人。PPTV 的 Zabbix 应用,已经是国内较大规模的系统监控了,覆盖了当时 5000 多台主机和上面应用的几十万监控点,近百万的监控点记录,也修改了 Zabbix 多处源码,实现了很多自动化的监控部署和 Proxy-Master 的分布式监控,以及通过 Zabbix Trigger 自动分析等,也就 Zabbix 本身的一些缺点设计了对应的 workaround 的办法和二次开发,可以说是国内较为领先的大规模部署解决实际案例。在 Zabbix 的实践领域,PPTV 的很多方法、思想和技巧都很有价值,仁捷同学在这本书中也都有涉及。

好的经验还是值得分享的,就算还不是完美的。

希望这本书能够给大家带来一手的 Zabbix 实战经验,更加希望大家可以从借鉴作者分享的经验,少走弯路,帮助公司更加多快好省地建设系统监控解决方案。

唯品会高级总监

诸超

序二

Zabbix 作为一款企业级的、开源的、分布式的监控套件，设计理念超前，解决了以往监控软件的短板，可以说是现在最流行的监控解决方案之一。

Zabbix 可以监控网络和服务的健康状况，可以利用模板批量添加服务器，可以自定义监控项，可以利用灵活的报警机制给运维人员发送 E-mail 和短信报警，从而保证了运维人员能快速对问题作出响应。此外，Zabbix 简单易上手，只要稍作学习，就能迅速搭建一套运维监控平台，瞬间高大上。

Zabbix 在分布式方面做了大量的优化工作，这样可以保证在多机房和对海量服务器进行监控时，能快速高效地收集数据，并集中在一个界面内展示。不过目前我所负责项目中，15 万个 Items 和 1000 多个 Hosts 用了一个配置比较高的服务器在抗，毫无压力，等服务器规模再大一些，机房比较多的时候，我会考虑用分布式。

我使用 Zabbix 也快 1 年了，替换了原来的 Nagios+Cacti 方案。Zabbix 兼有 Nagios+Cacti 的特点，所以现在维护一个系统就可以了，极大地方便了运维工作。因为公司大部分都是标准化的服务和服务器，迁移过程也比较顺利，只要事先做好分组，设置几个模板一关联就可以了，迁移的大部分时间花在了寻找合理阈值和设置靠谱 Trigger 上，这个可能需要慢慢积累经验。

作为 Zabbix 插件 Zatree 的开发者之一，我一直比较关注 Zabbix 在国内的发展，这几年来是 Zabbix 发展的快速时期，大量爱好者在 QQ 群、微博和社区参与讨论和分享，极大地丰富了 Zabbix 的中文资料。作为曾经国内最大规模 Zabbix 集群的负责人，姚仁捷在本书中全面讲解了 Zabbix 的安装、配置、使用及技巧，提供了大量的案例和解决问题的心得，其中也介绍了 Zatee 插件的安装和使用，希望大家可以一边看书，一边亲自动手实践，这样效果会更好。

相信人人都能成为监控专家、运维专家。

中国最大开源社区 Chinaunix 创始人之一

窦喆

@ 南非蜘蛛

本书的由来

我从职业生涯开始至今，就一直在和监控系统打交道。

我最早在 eBay 容量规划小组工作，使用监控系统查看服务器状态及网站运营指标；后来到 PPTV 运维部，通过监控系统的数据了解上线发布的结果和网站的健康程度等情况；现在到了唯品会，我们的监控系统能够从业务、技术两个维度考察当前公司网站的运作情况。

在有监控系统之前，工程师需要到服务器上去敲命令来获取系统数据；为了分析问题，可能还需要将数据复制到本地计算机的 Excel 里进行画图；最要命的是，在出现问题的时候无法知道，只有在用户报障后才能察觉。这是多么骇人听闻的场景！

而当我们有了一个好的监控系统后，这些问题就迎刃而解了。我们可以在一个界面中浏览整个机房的服务器状态、可以在 Web 前端方便地查看监控数据、可以回溯寻找事故发生时系统的问题和报警情况。现在，我们的工程师们已经可以一边悠闲地喝着咖啡一边分析问题了。

监控系统是整个运维自动化体系中非常重要的环节。从服务器上架到最后被回收重用，都有监控系统的身影。服务器上架时，它需要添加监控；在服务器工作过程中，监控系统要时刻注意服务器的健康，并且在服务器出现异常时，要发出报警通知对应的人员；在服务器被回收时，监控系统要取消服务器的监控。这些都需要监控系统拥有 API，能够方便地跟外部其他系统一起工作，把自己的工作自动化起来。

国内的互联网巨头们，可以自行开发一套监控系统。而对于绝大多数企业来说，开源的 Zabbix 是非常棒的选择。它能够非常好地实现以上这些需求。可以说，目前 Zabbix 是最热门的开源监控系统。

本书的内容结构

从周围的 QQ 群、论坛等地方，我发现大家对于 Zabbix 的学习都是非常零散的，缺少一个系统的学习过程和解决问题的正确思路。在这本书的前面，我会先向大家介绍一个最简单的入门案例，案例中有最基本的概念介绍，通过案例帮助那些只需将服务器加入监控，并且看到监

控数据的读者。后面深入一些，会介绍 Zabbix 的方方面面的配置，适合打算使用 Zabbix 高级功能的读者。在接下来的部分，会深入剖析 Zabbix 的内部原理，包括 Zabbix 与数据库的交互、Zabbix 数据库表的设计等我在 Zabbix 上踩过的坑以及解决问题的思路。希望能授之以渔。在本书的最后部分，主要介绍 Zabbix 在开源方面的进展，最主要的就是 58 同城开源的 Zatree，以及 Chrome 的插件和手机客户端。

本书会从我们工作中的实际需求出发，介绍 Zabbix 的使用方法和其配置管理。在这些内容之后，会有深入一些的对于 Zabbix 实现的讲解，希望对于读者而言，不仅仅是学会某些具体的操作，而是深入了解 Zabbix 的设计思路，掌握解决问题的方法。

作者联系方式

由于经验的不足，书中可能会有些不足之处，大家可以通过微博 @ 超大杯摩卡星冰乐，或者邮箱 baniu.yao@gmail.com，与我联系。

声明

在刚开始进行写作时，我考虑到很多读者是用中文版的 Zabbix，所以文中的 Zabbix 的术语都使用中文。但后来我觉得对于 Zabbix 的术语，研究人员是需要了解它的英文说法的，这样在同行之间才能更好地交流，也可以在 Google 上更好地检索信息。基于这个原因，我将之前的中文术语全部又换成了英文。由于这些术语非常多，虽然编辑帮我细致地进行了检查，难免有疏漏，希望大家能够谅解。

致谢

在前言的最后，要感谢很多人。首先感谢的是我的父母，没有你们，就没有我。然后要感谢我的老婆，因为要忙于写书，很多时候不能陪你。最后要感谢的是诸超、陈文春、吴晓刚、周昕毅、朱宁和刘海阳等同事的帮助，在我写书的过程中，给出了很多宝贵的建议。谢谢各位。

第一部分 概念篇

第 1 章 自动化运维和监控系统	2
1.1 互联网公司的运维工作	2
1.2 何谓自动化运维	3
1.3 监控系统在运维自动化中的角色	5
1.4 监控系统的理想化模样	5
第 2 章 Zabbix简介	7
2.1 Zabbix发展现状	7
2.2 选择Zabbix的理由	8
2.3 Zabbix部分名词约定	9
第 3 章 Zabbix安装	11
3.1 获取Zabbix	11
3.2 Zabbix Server安装	12
3.2.1 Zabbix数据库配置	12
3.2.2 安装Zabbix Server	13
3.2.3 安装Zabbix Web前端	16
3.3 Zabbix Agent安装	18
3.3.1 UNIX/Linux上安装Zabbix Agent	18
3.3.2 Windows上安装Zabbix Agent	18
3.4 测试Zabbix Agent和Zabbix Server运行	20
3.5 配置文件详解	20
3.5.1 zabbix_server.conf	20
3.5.2 zabbix_agentd.conf	24

第4章 监控第一台Host	26
4.1 Host在监控系统中的活动	26
4.2 添加一个用户	27
4.3 把服务器加入Zabbix监控	27
4.4 添加Item	28
4.5 添加Trigger	29
4.6 设置Action	31
4.7 收到第一封报警邮件	33
4.8 Zabbix 报警流程	33
4.9 看，Zabbix在工作呢	34
4.9.1 全局搜索框	35
4.9.2 查看监控数据	35
4.9.3 查看报警信息	36
4.10 添加自定义监控点	37

第二部分 配置篇

第5章 增加监控	40
5.1 Host配置	41
5.2 Item属性	45
5.3 Item类型	48
5.3.1 Zabbix Agent类型	48
5.3.2 SNMP类型	51
5.3.3 IPMI类型	52
5.3.4 日志文件监控	53
5.3.5 计算型Item	54
5.3.6 Zabbix内部监控	55
5.3.7 ssh类型Item	58
5.3.8 Telnet类型Item	60
5.3.9 External Check类型Item	60

5.3.10	Aggregate类型Item	60
5.3.11	Trapper类型Item	62
5.3.12	JMX类型Item	62
5.3.13	ODBC类型Item	64
5.4	Item历史数据History和Trends	66
5.5	使用Application对Item分组	67
5.6	Item Key详解	68
5.7	Template模板	69
5.7.1	新建和配置一个Template	69
5.7.2	建立/取消Host和Template的关联	71
5.7.3	修改Template	73
5.7.4	Template和Host	73
5.7.5	Template之间的父子关系	74
5.8	Clone、Full Clone和Mass Update	75
5.9	Windows监控	76
5.10	VMware监控	82
5.11	Zabbix监控性能	84
第6章	报警配置	86
6.1	Triggers	86
6.1.1	配置Triggers	86
6.1.2	Trigger expression	87
6.1.3	Function详解	89
6.1.4	Trigger依赖	92
6.1.5	Trigger等级	94
6.1.6	单位	95
6.2	Events	95
6.3	Actions	96
6.3.1	Action	97
6.3.2	Operation	99

6.3.3	Condition	104
6.3.4	Escalations	107
6.3.5	Unsupported状态的Items的报警	110
6.4	Media类型	111
6.5	Maintenance状态	116
第7章	数据可视化	118
7.1	Graph	118
7.2	Network Maps	123
7.2.1	新建Maps	123
7.2.2	创建元素	124
7.2.3	选择元素	126
7.2.4	关联元素	126
7.2.5	关联指示器	126
7.3	Screens	127
7.4	Slide shows	131
第8章	Users和Macros	133
8.1	User和User group	133
8.1.1	配置User	133
8.1.2	User group	135
8.2	Macros	136
8.2.1	自带宏	136
8.2.2	用户自定义宏	137
8.2.3	自定义宏的适用范围	139
第9章	IT services服务监控与Web monitoring网络监控	140
9.1	Services服务监控	140
9.2	服务配置	141
9.3	Web monitoring网络监控配置	145
9.4	监控百度示例	148

第 10 章 Zabbix前端界面	151
10.1 Monitoring板块	151
10.1.1 Dashboard栏目	151
10.1.2 Overview栏目	157
10.1.3 Web栏目	158
10.1.4 Latest data栏目	159
10.1.5 Triggers栏目	159
10.1.6 Events栏目	160
10.1.7 Graphs&Screens&Maps栏目	161
10.2 Inventory板块	161
10.3 Reports板块	161
10.4 Configuration板块	166
10.4.1 Host groups栏目	166
10.4.2 Template栏目	167
10.4.3 Hosts栏目	168
10.4.4 Maintenance栏目	170
10.4.5 其他	170
10.5 Administration板块	171
10.5.1 General栏目	171
10.5.2 DM栏目	177
10.5.3 Authentication栏目	178
10.5.4 Users栏目	179
10.5.5 Media types栏目	181
10.5.6 Scripts栏目	181
10.5.7 Audit栏目	185
10.5.8 Queue栏目	186
10.5.9 Notification栏目	186
10.5.10 Installation栏目	187
10.6 前端配置	187

10.6.1	全局配置参数	187
10.6.2	前端维护状态显示	189
10.6.3	Profile设置	190
10.7	全局搜索框	192
第 11 章	Discovery	193
11.1	基于网络的Discovery	193
11.2	Discovery的一个例子	195
11.3	Discovery Rule和Discovery Action的配置	196
11.4	存活Agent自动加入监控	199
11.5	low-level discovery	200

第三部分 进阶篇

第 12 章	Zabbix API	206
12.1	Zabbix API POST参数	206
12.2	Item支持的Zabbix API方法	207
12.2.1	Item object	208
12.2.2	item.create	209
12.2.3	item.delete	210
12.2.4	item.exists	210
12.2.5	item.get	211
12.2.6	item.getobjects	214
12.2.7	item.isreadable/item.iswritable	215
12.2.8	item.update	215
12.3	如何阅读Zabbix API文档	216
第 13 章	Zabbix分布式监控	217
13.1	两种分布式架构对比	217
13.2	Proxy单级分布式架构	218
13.3	Proxy配置	219

13.4	Node多级分布式架构	220
第 14 章	Zabbix系统优化	227
14.1	Zabbix内部运行机制	227
14.2	Items过多造成性能下降	228
14.3	数据库及其他调优	232
第 15 章	轻量级日志监控应用	233
15.1	准备工作	233
15.2	添加 Item	234
15.3	测试	234
15.4	配置报警	236
15.5	轮转的日志文件	237
15.6	获取关键字	238

第四部分 设计篇

第 16 章	Zabbix数据库表结构解析	240
16.1	表结构概述	240
16.2	Hosts表	241
16.3	Items表	244
16.4	Trigger在数据库中的结构	248
16.5	Events表	253
16.6	Triggers和Events生成的规则	255
第 17 章	History和Trends	256
17.1	sync字段的含义	257
17.2	history和trends的区别	261
17.3	housekeeper和trends表	262
17.4	Graph对于history和trends的选择	263
第 18 章	Zabbix和数据库交互详解	268
18.1	include/zbxdb.h	268

18.2	zbxdb/db.c	270
18.3	zbxdbhgh	271
第 19 章	Zabbix 2.2新功能介绍	274
19.1	数据库自动升级	274
19.1.1	检查数据库版本	274
19.1.2	mandatory和optional字段	275
19.1.3	数据库升级过程	277
19.1.4	前端提示	278
19.2	Web监控	279
19.2.1	Web监控Template化	279
19.2.2	Web监控重试机制	279
19.2.3	使用HTTP代理	280
19.2.4	URL监控中使用页面内容作为变量	281
19.3	数据映射	282
19.4	history和trends存储的代码分析	282
19.4.1	DCsync_history	283
19.4.2	DCsync_trends	285
19.4.3	整个流程	285
19.5	网页字符串匹配	286
19.6	日志文件监控	287
19.7	Latest Data局部刷新	288
19.8	动态载入模块	288
19.9	SNMP监控改进	292
19.9.1	SNMPv3相关的增强	292
19.8.2	SNMP重试和超时机制改进	293
19.9.3	lld的复杂OIDs	293
第 20 章	Zabbix内置监控项实现	294
20.1	system.hostname	294
20.2	system.cpu.load	295

第五部分 社区和开源

第 21 章 典型案例分析	300
21.1 前端显示Zabbix server停止工作问题	300
21.2 Item设置了但没有数据	306
21.2.1 看页面是否有报错	306
21.2.2 Zabbix Server和Zabbix Agent的网络是否互通	307
21.2.3 zabbix_get是否能够获取到数据	308
21.2.4 总结	308
21.3 一个扫描history全表的SQL问题	309
21.4 解决问题的思路	319
第 22 章 Zabbix代码问题和解决	320
22.1 Duplicated Host问题	320
22.2 拼接大SQL问题	322
22.3 nextid问题	323
22.4 在Zabbix中打印日志	325
第 23 章 PPTV的Zabbix监控体系	326
23.1 Python Zabbix API	326
23.2 Spider——服务器添加Zabbix监控	328
23.3 Event Console	330
23.4 Rule Engine	330
23.5 报警系统架构	331
第 24 章 Zatree	332
24.1 使用Zatree	332
24.2 Zabbix二次开发和重新开发监控系统的选择	334
第 25 章 Zabbix第三方插件	337
25.1 Chromix	337
25.2 Zabbix Notifier	338

25.3 手机端Zabbix App	339
25.3.1 ZBX Mobile	339
25.3.2 Zabbkit	341
第 26 章 微信公众平台报警	344
26.1 申请微信公众平台账号	344
26.2 配置微信公众平台账号	345
26.2.1 使用SAE进行测试开发	347
26.2.2 申请测试账号	348
26.2.3 获取access_token	348
26.2.4 获取用户的openid	349
26.2.5 发送第一条文字消息	349
26.3 微信接口请求次数限制	350
第 27 章 社区论坛	351
附录 Zabbix自带宏	353
后记	355
程序员职业生涯的一些感悟	356