

Zabbix

企业级分布式监控系统

第2版

吴兆松◎著

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书基于最新稳定版本 Zabbix 4.0, 对 Zabbix 的各项功能进行了详细而深入的讲解, 包括监控系统规划、安装包定制、架构高可用、性能调优、指标数据采集、自动化处理功能、触发器使用与原理、告警配置、Zabbix API、数据可视化、网络拓扑自动发现、内部实现原理以及部分源码分析等内容, 让读者真正通过一本书就能够完全掌握 Zabbix 监控系统的核心技术。

本书第 1 版内容收获了大量读者好评, 是一本实战性很强的工具书, 读者将其称为监控领域的“红宝书”, 书中所写内容均可以在生产环境中直接应用。

而在第 2 版中, 采纳了以往读者的宝贵意见, 增加了作者的最新研究成果, 扩充了大量内容, 但继续保持由浅入深、由易到难的写作风格。通过合理的章节编排, 本书内容分为初级、中级和高级 3 个部分, 从入门的安装与配置, 到复杂的高级使用, 都进行了讲解, 并配有大量的真实监控案例。书中包含作者参与过的真实企业级监控系统构建项目的相关经验, 通过阅读掌握本书的内容, 可以让 Zabbix 监控系统的学习和使用从此不再困难。

本书适合想了解、学习和规划构建监控系统的人员阅读, 可作为学习入门 Zabbix 的工具书, 也适合想更深入理解 Zabbix 监控系统的读者阅读。

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 企业级分布式监控系统 / 吴兆松著. — 2 版. — 北京: 电子工业出版社, 2019.7
ISBN 978-7-121-36877-6

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

中国版本图书馆 CIP 数据核字 (2019) 第 120997 号

责任编辑: 付 睿

印 刷: 三河市双峰印刷装订有限公司

装 订: 三河市双峰印刷装订有限公司

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: 39

字数: 870 千字

版 次: 2014 年 8 月第 1 版

2019 年 7 月第 2 版

印 次: 2019 年 7 月第 1 次印刷

定 价: 139.00 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 zltz@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。

前 言

本书由来

“运筹帷幄之中，决胜千里之外。”在 IT 运维中，监控占据着重要的地位，按比例来算，说占 30%一点也不为过。对 IT 运维工程师来说，构建一个真正可用的监控告警系统是一项艰巨的任务。在监控系统的开源软件中，可供选择的工具众多，然而真正符合需求，能够真正解决业务问题的监控系统软件却凤毛麟角。

笔者在自己的运维从业生涯中用过的监控系统有 Cacti、Nagios 等，以及笔者公司开发的监控告警系统，直到接触了 Zabbix，才发现这个灵活而强大的自动化监控工具正是笔者所寻找的。随着近年来云计算、容器技术的大规模普及，软件架构已经从单体架构走向微服务架构，对监控的灵活性和可靠性的要求越来越高，出现了更多有趣的监控软件，如 Prometheus、Influx 家族，这些监控软件解决了在当前环境中面临的一些问题，提供了非常优秀的监控解决方案，但这并不妨碍 Zabbix 的继续流行。从 2012 年开始，国内 Zabbix 的用户群体在逐步扩大，当前 Zabbix 已经成为运维人员必须掌握的技能之一。究其原因，得益于 Zabbix 灵活的架构设计、极强的扩展能力、丰富的监控能力、易于与外部集成的能力，从硬件监控，到操作系统，再到服务进程，以及网络设备，其无所不能的监控功能令人叹为观止，相信这也是大多数 Zabbix 爱好者选择它的主要原因。

当然，在 Zabbix 的使用过程中，会面临上手容易、精通较难的问题，原因在于 Zabbix 过于灵活，其配置的颗粒度非常细致，这也会让大多数用户刚接触学习它的时候一头雾水，所以查看官方文档和阅读一本相关书籍的学习方式都是明智的选择。

笔者从 2012 年开始使用 Zabbix，曾公开自己的使用文档，很高兴文档对不少初学 Zabbix 的朋友有所帮助，但随着向笔者咨询问题的人数增多，其中多数问题是重复的，且笔者解答问题的精力有限，于是萌生出书的想法，在其后的 2014 年，正式出版了《Zabbix 企业级分布式

监控系统》一书，并被广大 Zabbix 爱好者喜爱。时光荏苒，2018 年，Zabbix 4.0 版本正式发布，所以本书也需要升级换代，在此情况下，笔者对书籍内容进行了大幅度的重构，并对书籍的内容和深度进行了扩展，让本书可以真正成为 Zabbix 用户的案头首选参考书。本书得以改版，我们的编辑付睿老师功不可没，在 2016—2017 年的时候，她一直催促笔者更新内容。由于笔者当时是被动更新的，并没有想好新加什么内容，并且笔者基于原有书稿做了一些更新，但内容无法令自己满意，于是就没有继续下去，当时 Zabbix 是 3.0 版本。直到 2018 年，笔者觉得是时候更新内容了。

如何阅读本书

本书共分 3 部分内容，笔者按照从零基础开始学习的路线进行章节编排，从易到难逐步深入，直到读者深入掌握，并且本书对相关的内容和思想进行了拓展，让读者学习到的不仅是 Zabbix，而且是一个监控体系。

第 1 部分为基础部分，包括第 1~6 章。首先介绍监控系统的原理，让初次接触监控的读者了解监控系统的组成部分，从宏观上认识监控系统。接下来讲解了 Zabbix 的架构、Zabbix 的安装、监控配置、自定义监控项、告警配置、告警脚本等功能。这部分内容适合从零基础开始系统地学习 Zabbix 监控系统，对稍有经验的使用者来说，重点掌握 Zabbix 对数据存储的处理（第 3 章），以及第 5 章和第 6 章的内容。

第 2 部分为中级部分，包括第 7~11 章。首先对 Zabbix 的触发器使用以及内部源码实现进行了深入讲解，对 Zabbix 的多种监控方式进行了详述（如 IPMI、SNMP、JMX、ODBC 等）。接着，对自动化功能进行了深入讲解，介绍了分布式监控系统，配有大量自定义脚本的监控案例，并对监控项自动发现（LLD）功能进行了深入讲解，其后对 Zabbix 的数据可视化方案和拓展实现进行了研究，适合对 Zabbix 有一定基础的读者深入学习。通过对这部分内容的学习，读者将会深入理解 Zabbix 的整体功能。

第 3 部分为高级部分，包括第 12~16 章。首先介绍 Zabbix 的性能调优，从底层实现机制讲解，从而理解 Zabbix 在使用过程中遇到性能瓶颈的问题，以及如何解决这些问题，并让读者学会使用 Zabbix API 来扩展 Zabbix，从而为构建运维平台提供了更多的扩展性。同时，这部分也讲解了如何定制 RPM 包，源码构建安装，使用 Elasticsearch 作为后端数据存储，以及如何使用 SaltStack 来自动化部署和配置，通过一个实例来讲解如何构建企业级分布式监控系统。最后一章，探讨了监控系统的整体实现与使用场景，与 DevOps、ITIL 的整合使用，以及告警轮班等深度场景，让读者在更丰富的场景中使用 Zabbix，并理解 IT 运维中的关键思想，

将监控用于更广泛的场景，适合对 Zabbix 非常熟悉的读者进行深入应用。通过对这部分内容的学习，读者能够深入理解 Zabbix，并从更多的角度考虑监控问题。

配套代码

书中包含的相关代码，笔者已将其放到 GitHub 上，地址为 <https://github.com/zabbix-book>，读者可以在生产环境中直接使用相关代码。

读者对象

- Linux 系统管理员
- 系统运维工程师
- 运维开发工程师
- 系统集成商
- 运维监控系统工程
- 监控系统软件开发（设计）人员
- IT 管理人员
- 架构设计人员

勘误支持

尽管笔者和编辑都努力地对书稿进行再三校对，但因笔者水平和时间所限，书中可能存在少许的错误或不妥之处，如读者遇到，还恳请批评、指正。读者若有任何宝贵的意见或建议，可以发送邮件至本书的专题邮箱 zabbix_v2@itnihao.com，笔者将尽快给予反馈解答。本书的勘误也会在随书项目中得到反馈。

内容声明

本书采用的 Zabbix 为 4.0 版本，随着 Zabbix 版本的更新，本书讲解的大部分使用功能与新版本相比会稍有不同。本书采用的操作系统以 Linux（CentOS 7）、Windows 为主，对于其他版本的操作系统并未做过多讲解。本书能保证对 Zabbix 几乎 96% 以上的功能都有细致讲解，但少许笔者认为不重要的内容并未讲解（也许对部分读者来说却非常重要），如涉及加密证书传输数据的内容，关于这部分内容读者可参考学习官方文档。另外，与本书第 1 版相比，第 2 版去掉了 Zabbix 协议的相关章节。本书在编写过程中，参考了大量官方文档和社区的内容，书中都给出了相关链接，如不慎遗漏，重印、改版的时候会进行增补。

本书并不能完全代替 Zabbix 的官方文档, 读者在读完本书后, 建议也阅读 Zabbix 的官方文档, 因为在官方文档中还有更多的细节值得去研究, 如将两者结合, 效果会更好。

示例规范

(1) 在 shell 环境中使用, shell 命令会加粗显示。

```
shell# vim /etc/php.ini
```

(2) 在 MySQL 环境中使用, SQL 命令会加粗显示。

```
mysql> flush privileges;
```

(3) 在本书中, Zabbix-Server 表示 `zabbix_server` 服务或进程, 其他 Zabbix-Agent、Zabbix-Get、Zabbix-Proxy 的情况类似。

联系方式

微博: <http://weibo.com/itnihao>

邮件: zabbix_v2@itnihao.com

目 录

第 1 章 开篇——监控系统简介	1
1.1 监控系统的功能概述	1
1.2 监控系统的实现原理	2
1.2.1 模块组成	2
1.2.2 采集协议	2
1.2.3 采集模式	3
1.2.4 监控指标	3
1.2.5 代理架构	3
1.2.6 数据存储	4
1.2.7 告警功能	5
1.2.8 可扩展性	5
1.2.9 总结归纳	6
1.3 监控系统的开源产品	7
1.3.1 Cacti	7
1.3.2 Nagios	8
1.3.3 InfluxDB 套件	9
1.3.4 Prometheus	10
1.3.5 OpenFalcon	11
1.3.6 Netdata	12
1.3.7 ELK 家族	13
1.3.8 Zabbix	14
第 2 章 Zabbix 简介	16
2.1 Zabbix 的用户群体都有谁	16

2.2	使用 Zabbix 需要具备什么基础	17
2.3	Zabbix 是一个什么样的产品	18
2.4	为何选择 Zabbix 作为监控系统	19
2.5	该选用 Zabbix 的哪个版本	20
2.6	Zabbix 的架构是什么样的	21
2.7	Zabbix 的功能特性都有哪些	22
第 3 章	安装与部署	25
3.1	安装环境概述	25
3.1.1	硬件环境需求	25
3.1.2	软件环境需求	28
3.1.3	网络环境需求	30
3.2	Zabbix-Server 服务器端的安装	30
3.2.1	安装 Zabbix-Server	33
3.2.2	安装 MySQL	33
3.2.3	配置 zabbix_server.conf	36
3.2.4	防火墙、SELinux 和权限的设置	38
3.2.5	配置 Zabbix-Web	40
3.2.6	相关故障的处理	46
3.2.7	zabbix_server 程序的参数	49
3.3	Zabbix-Agent 客户端的安装	51
3.3.1	安装 Zabbix-Agent	51
3.3.2	防火墙的设置	51
3.3.3	配置 zabbix_agentd.conf	52
3.4	SNMP 监控配置	52
3.5	在 Windows 中安装 Zabbix-Agent	53
3.5.1	安装与配置	53
3.5.2	注册服务	53
3.5.3	启动服务	54
3.6	在其他平台安装 Zabbix-Agent	56
3.7	Zabbix-Get 的使用	56
3.8	Zabbix 相关术语 (命令)	57
3.9	Zabbix-Server 对数据的存储	58

3.9.1	监控数据的存储	58
3.9.2	MySQL 表分区实例	62
3.10	高可用和安全	70
3.10.1	高可用	70
3.10.2	通信安全	70
3.10.3	禁用 Zabbix 的 guest 用户	70
3.11	Zabbix 数据库备份	70
3.12	升级 Zabbix	73
3.12.1	同版本升级的方法	73
3.12.2	跨版本升级的方法	74
3.12.3	数据库自动升级的原理	74
3.12.4	升级失败的处理案例	75
第 4 章	快速配置和使用	77
4.1	配置流程	77
4.2	添加主机组	78
4.2.1	如何划分主机组	78
4.2.2	如何添加主机组	78
4.2.3	层级主机分组	80
4.3	添加模板	81
4.4	添加主机	82
4.5	配置图形	86
4.6	配置大屏	92
4.7	配置幻灯片	94
4.8	配置地图	96
4.8.1	添加背景图	96
4.8.2	添加地图	96
4.9	使用 IT 服务	102
4.10	使用报表	105
4.11	资产管理	108
4.12	图形共享	109
4.13	全局搜索	110
4.14	最新数据	111

4.15	故障	112
4.16	数据的导入/导出	112
4.17	用户权限	113
4.17.1	用户组	113
4.17.2	用户组权限	114
4.17.3	用户	116
4.17.4	匿名用户	117
4.18	调试模式	117
4.19	与 LDAP 对接	118
4.20	维护模式	119
4.21	故障确认	121
4.22	批量更新	123
第 5 章	处理监控指标数据	124
5.1	添加新的监控项	124
5.1.1	监控项的含义	124
5.1.2	如何添加监控项	124
5.2	监控指标的自定义	130
5.2.1	key 的格式	130
5.2.2	key 名称的定义范围	130
5.2.3	key 的参数数组应用实例	131
5.2.4	用户自定义参数	131
5.3	Zabbix 内置的监控方式	133
5.3.1	Zabbix-Agent 监控方式	134
5.3.2	Simple check 监控方式	140
5.3.3	日志监控方式	144
5.3.4	计算型监控方式	152
5.3.5	聚合型监控方式	156
5.3.6	内部检测监控方式	163
5.3.7	SSH 监控方式	163
5.3.8	Telnet 监控方式	167
5.3.9	扩展检测监控方式	169
5.4	监控项指标数据的预处理	171

5.4.1	预处理概述.....	171
5.4.2	预处理的运行流程.....	172
5.4.3	预处理的数据类型.....	173
5.5	配置宏.....	177
5.5.1	全局宏.....	177
5.5.2	模板宏.....	178
5.5.3	主机宏.....	178
5.5.4	监控项宏.....	179
5.5.5	宏的函数运算.....	180
5.5.6	宏使用总结.....	181
5.5.7	宏的上下文.....	182
5.6	配置值映射.....	183
第 6 章	精通告警配置.....	185
6.1	告警流程.....	185
6.2	告警触发器的配置.....	186
6.2.1	Trigger 的作用.....	186
6.2.2	Trigger 的故障等级定义.....	187
6.2.3	Trigger 的配置步骤.....	187
6.2.4	Trigger 告警依赖.....	191
6.2.5	Trigger 中的数值单位.....	192
6.2.6	Trigger 表达式.....	192
6.3	告警处理的配置.....	200
6.3.1	如何发送告警.....	200
6.3.2	Action 功能概述.....	200
6.3.3	Action 配置步骤.....	201
6.3.4	告警处理措施.....	203
6.3.5	在告警消息中使用宏.....	207
6.3.6	告警恢复措施.....	208
6.3.7	告警更新措施.....	209
6.3.8	发送告警消息的步骤总结.....	210
6.3.9	查看告警消息的发送记录.....	211
6.3.10	执行远程命令.....	211

6.3.11	不支持的 Item 发送告警	215
6.4	邮件告警配置	215
6.4.1	创建 Media 类型	215
6.4.2	创建用户	216
6.4.3	创建 Action	217
6.5	自定义脚本告警	218
6.5.1	自定义脚本告警的原理	218
6.5.2	电话告警	220
6.5.3	短信接口告警	221
6.5.4	微信告警	221
6.6	邮件告警脚本的配置	222
6.6.1	Zabbix-Server 自定义告警脚本	222
6.6.2	Zabbix-Server 重启服务	224
6.6.3	Zabbix-Web 配置自定义脚本	225
6.6.4	告警接收邮件的配置	226
6.6.5	查看邮件发送状态	227
6.7	告警升级机制	227
6.7.1	告警升级的作用	227
6.7.2	告警升级的配置	228
6.8	触发器标签配置	230
6.8.1	标签设置	230
6.8.2	标签的复杂匹配	231
6.9	手动关闭告警	233
6.10	如何取消告警发送	235
6.11	如何删除故障信息	235
6.12	告警聚合	236
6.12.1	告警聚合的原理	236
6.12.2	基于触发器的告警聚合	236
6.12.3	基于全局的告警聚合	239
6.13	告警配置故障排查	242
6.13.1	告警消息未发送示例	242
6.13.2	邮件服务器连接失败示例	243

第 7 章 探究告警触发器	244
7.1 Trigger 函数的意义	244
7.2 Trigger 函数的分类	244
7.3 Trigger 函数——比较与查找	245
7.3.1 求最近两值差的绝对值——abschange	245
7.3.2 求最大值与最小值的差——delta	248
7.3.3 判断最近两值是否相同——diff	251
7.3.4 求最近两值的变化量——change	254
7.3.5 数值的位与运算——band	256
7.3.6 数据失联——nodata	261
7.3.7 获取最新数据——last	264
7.3.8 求前一个值——prev	266
7.4 Trigger 函数——计算	268
7.4.1 求最大值——max	268
7.4.2 求最小值——min	271
7.4.3 求平均值——avg	273
7.4.4 值求和——sum	276
7.4.5 统计个数——count	278
7.5 Trigger 函数——时间	286
7.5.1 返回当前时间（年月日时分秒）——now	286
7.5.2 返回当前日期（年月日）——date	288
7.5.3 返回当前时间（时分秒）——time	289
7.5.4 本月第几天——dayofmonth	291
7.5.5 本周第几天——dayofweek	292
7.5.6 时间对比——fuzzytime	293
7.6 Trigger 函数——日志	295
7.6.1 日志 ID——logeventid	295
7.6.2 获取日志等级——logseverity	296
7.6.3 获取日志来源——logsource	297
7.7 Trigger 函数——字符串匹配	299
7.7.1 正则表达式不区分大小写——iregexp	299
7.7.2 正则表达式区分大小写——regexp	301
7.7.3 字符串匹配——str	302

7.7.4	字符串长度——strlen.....	304
7.8	Trigger 函数——趋势预测.....	305
7.8.1	百分线——percentile.....	305
7.8.2	趋势预测——forecast.....	307
7.8.3	剩余时间——timeleft.....	311
7.8.4	趋势预测计算型监控方式.....	314
7.9	参考资料.....	318
第 8 章	剖析监控方式.....	319
8.1	Zabbix 支持的监控方式.....	319
8.2	Zabbix 监控方式的逻辑.....	320
8.3	Zabbix-Agent 的工作模式.....	321
8.3.1	工作模式概述.....	321
8.3.2	被动模式的配置.....	323
8.3.3	主动模式的配置.....	324
8.4	Zabbix-Trapper (zabbix_sender) 监控方式.....	326
8.4.1	Zabbix-Trapper 的配置步骤.....	326
8.4.2	Zabbix-Trapper 的配置示例.....	326
8.4.3	使用 zabbix_sender 程序发送数据.....	328
8.4.4	使用 zabbix_sender 程序批量读取文件.....	329
8.5	SNMP 监控方式.....	330
8.5.1	SNMP 协议概述.....	330
8.5.2	SNMP 协议的工作方式.....	331
8.5.3	SNMP 协议的工作原理.....	331
8.5.4	SNMP MIB 简介.....	334
8.5.5	SNMP 相关术语.....	336
8.5.6	配置 Zabbix-Server 的 SNMP 监控.....	337
8.5.7	SNMP 监控中的 LLD 原理.....	340
8.6	SNMPTraps 监控方式.....	343
8.6.1	SNMPTraps 的概念.....	343
8.6.2	SNMPTraps 的工作原理.....	343
8.6.3	SNMPTraps 的安装与配置.....	343
8.6.4	SNMPTraps 的测试.....	346

8.7	IPMI 监控方式	348
8.7.1	IPMI 的概念	348
8.7.2	IPMI 的特性	349
8.7.3	配置 Zabbix-Server 监控 IPMI	349
8.7.4	Zabbix 自带的 IPMI 模板	350
8.7.5	在 Linux 系统中使用 OpenIPMI	350
8.7.6	创建 IPMI 模板	352
8.7.7	IPMI 监控主机	353
8.8	JMX 监控方式	354
8.8.1	JMX 在 Zabbix 中的运行流程	354
8.8.2	JMX 监控的安装和配置	355
8.8.3	安装 Zabbix-Java-Gateway	355
8.8.4	配置 Zabbix-Java-Gateway	356
8.8.5	查看 Zabbix-Java-Gateway 日志	357
8.8.6	监控 Java 应用程序的方法	357
8.8.7	开启 Tomcat 的 JMX	358
8.8.8	获取 JMX 数据	359
8.8.9	JMX 数据的 LLD	363
8.8.10	JMX 监控的核心技术实现	367
8.9	HTTP agent 监控方式	369
8.9.1	HTTP agent 监控概述	369
8.9.2	HTTP agent 监控实例	369
8.9.3	HTTP agent 监控配置	370
8.9.4	转换 HTTP agent 获取的数据结果	371
8.10	Web 监控方式	372
8.10.1	Web 监控的原理	372
8.10.2	Web 监控指标	372
8.10.3	Web 监控的配置步骤	373
8.10.4	Web 监控用户认证支持	376
8.10.5	Web 监控触发器的配置	379
8.10.6	Web 监控排错	381
8.11	Dependent item 监控方式	381
8.12	ODBC 监控方式	381

8.12.1	安装 ODBC 软件包.....	381
8.12.2	查看 ODBC 配置.....	381
8.12.3	安装 MySQL ODBC 驱动.....	382
8.12.4	使用 ODBC 驱动连接 MySQL.....	382
8.12.5	配置 Item.....	383
8.12.6	ODBC 错误处理.....	385
8.12.7	安装 Oracle ODBC 驱动.....	385
8.12.8	安装 PostgreSQL ODBC 驱动.....	387
8.12.9	ODBC 的监控项自动发现.....	388
8.13	其他监控方式.....	391
8.14	命令执行的监控方式.....	391
8.14.1	system.run.....	391
8.14.2	远程命令.....	391
第 9 章	分布式监控与自动化.....	392
9.1	Zabbix-Proxy 分布式监控.....	392
9.1.1	安装 Zabbix-Proxy.....	395
9.1.2	导入 Zabbix-Proxy 的数据库.....	396
9.1.3	配置 zabbix_proxy.conf.....	397
9.1.4	启动 Zabbix-Proxy 服务.....	397
9.1.5	查看 Zabbix-Proxy 日志.....	397
9.1.6	添加 Proxy.....	398
9.1.7	添加 Proxy 的主机监控.....	398
9.2	监控的自动化功能.....	399
9.3	网络自动发现.....	400
9.4	主动方式的自动注册功能.....	403
9.4.1	功能概述.....	403
9.4.2	配置过程.....	404
9.5	监控项自动发现功能.....	406
9.5.1	功能概述.....	406
9.5.2	LLD 的原理.....	406
9.5.3	LLD 的数据格式.....	407
9.5.4	LLD 应用案例.....	411