



ZABBIX监控模板标准化的意义和价值

何星

Zabbix培训师 宏时数据

ZABBIX



Zabbix监控模板标准化的意义和价值

模板标准化概述

为什么是模板？

- ④ Template: a set of entities (items, triggers, graphs, low-level discovery rules, web scenarios) ready to be applied to one or several hosts.

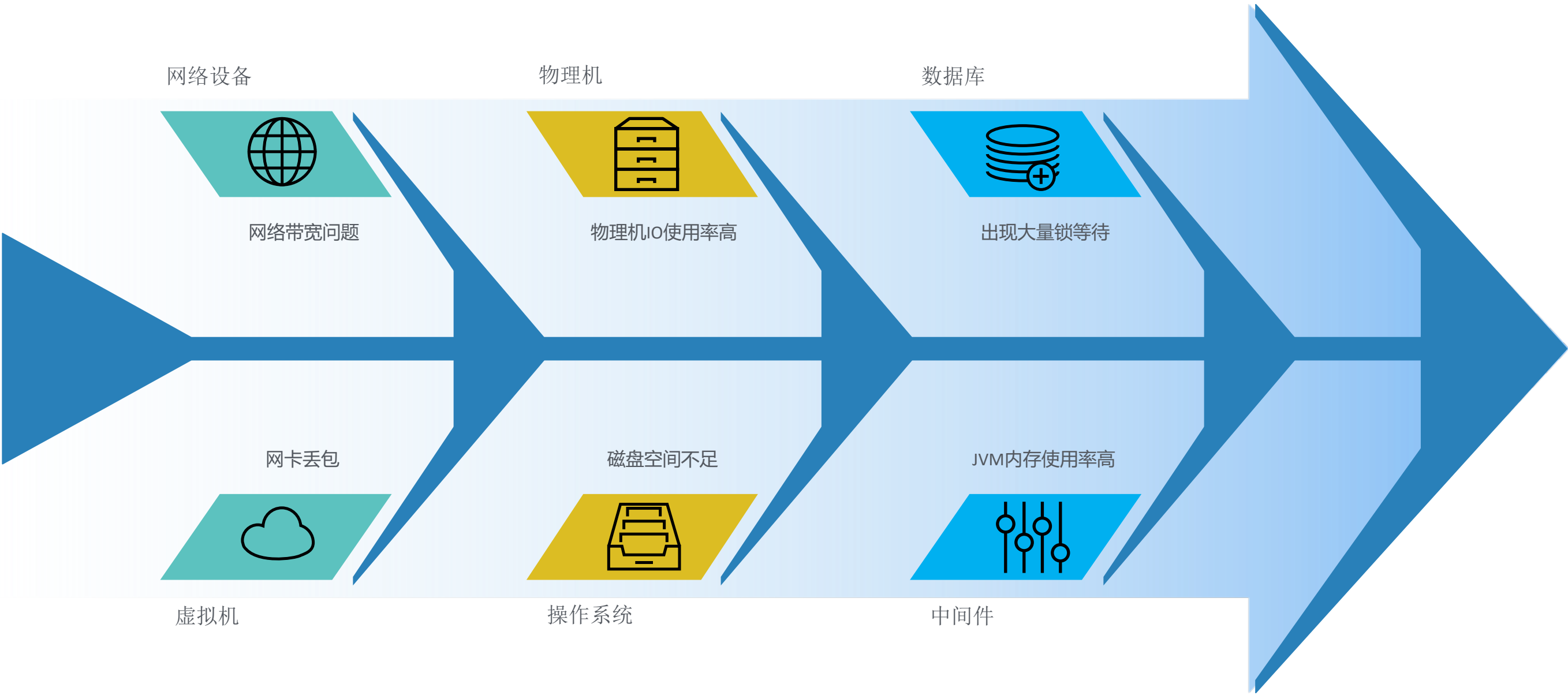


为什么要标准化？

	非标准化	标准化
群组	同类型或者有关联的模板关系不清晰，缺少必要的权限控制	同类型或者有关联的模板可分组放置，且权限控制方便
模板名称	模板名称混乱，遗漏部分关键信息	模板名称清晰，且利于部署
标签	标签定义随意，缺少统一的事件分类方式	可根据标签配置告警策略或者与第三方事件平台集成
正则表达式	部分使用全局正则表达式导致模板迁移出现问题	使用用户宏代替全局正则表达式
值映射	缺少必要的值映射，导致无法知悉获取值的含义	状态类数值使用值映射，数值关系清晰
触发器名称	触发器名称未做到显示问题的定量信息	问题信息全面清晰
触发器表达式	未使用用户宏作为触发器表达式的阈值，修改不方便	使用用户宏作为触发器表达式的阈值，主机层面可修改
用户宏	用户宏多且不清楚其代表的含义	通过用户宏可以了解其关联的指标信息和触发器级别

服务监控和资源监控

- ✓ 服务：对外提供的访问对象
- ✓ 资源：提供服务的组件





Zabbix监控模板标准化的意义和价值

模板标准化指南

优秀模板的特征



模板样式指南

01

避免做过多模板优化

02

避免使用全局宏

03

避免使用全局正则表达式

04

避免模板间的触发器依赖

05

模板语言统一（英语）

06

所有元素都启用

07

模块化

模板名称和模板组

☑ 模板名称：以空格或者下划线分割，包含数据采集方式。

Good	Bad
Nginx by HTTP	Agent 2 template NGINX
MySQL	Template DB MySQL
Brocade switch by SNMPv2	SNMP Brocade switch
Brocade switch SNMPv2	Brocade switch Template
Brocade switch_by SNMPv2	Template Brocade Switch

☑ 模板组：所有的模板添加至组-**Templates/<分类名称>**。

Good	Bad
"Cisco by SNMP" 加入 "Templates/Network Devices"	"Cisco by SNMP" 加入 "Datacenter/Network"

监控项名称

- ✓ 监控项名称：简单且描述清晰，可以根据实际添加 *per second* 和 *per hour* 信息。

【监控项原型】 *<metric location>: <metric name> — Interface eth0: Bits in / #0: CPU utilization*

- ✓ 监控项键值：以点作为层级连接符。

namespace.component.metric_name[paras]

- *namespace* (对象名称缩写) : *nginx, pgsql, pgbouncer, docker*等 ;
- *component* (子资源) : *upstream, pool, db, db.table, db.client*等 ;
- *metric_name* (指标名称) : *max_reached*等。

Example:

- ✓ *pgsql.db.connection_time[{#PG_DB},{PG_CONN}]*
- ✓ *pgsql.db.get_connection [...], nginx.get_stub, nginx.get_logs*
- ✓ *nginx.connections.accepted.rate*

警告：\$1 宏不要用在监控项名称中。

监控项属性

- ✓ 单位：B/Bps/s/unixtime/uptime；
- ✓ 值映射：1 – Up, 0 – Down；
- ✓ 数据类型：Numeric (unsigned) / Numeric (float) / Character / Text / Log；
- ✓ 带单位的时间用于时间间隔和可计算表达式中，1m/5m/1d；
- ✓ 选择合适的监控项采集间隔、历史保留时间、趋势保留时间；
- ✓ 预处理：数值转换，重复数据删除等；
- ✓ 应用集：尽量将监控项只加入一个应用集中（Zabbix 5.4没有应用集）；
- ✓ 可计算监控项：添加空格和换行使表达式更易读；
- ✓ SNMP：使用纯数字型OID。

低级别自动发现-LLD

名称以discovery单词结尾，采集间隔设置为1小时，过滤规则中使用用户宏。

Good	Bad
<pre>{#IFNAME} MATCHES {\$NET.IF.IFNAME.MATCHES} {#IFNAME} NOT_MATCHES {\$NET.IF.IFNAME.NOT_MATCHES} .. {#IFTYPE} MATCHES {\$NET.IF.IFTYPE.MATCHES} {#IFTYPE} NOT_MATCHES {\$NET.IF.IFTYPE.NOT_MATCHES} Where: {\$NET.IF.IFNAME.MATCHES} = ^.*\$ {\$NET.IF.IFNAME.NOT_MATCHES} = (^Software Loopback Interface ^NULL[0-9.]*\$ ^LIo[0-9.]*\$ ^Ss]ystem\$ ^Nu[0-9.]*\$) And {\$NET.IF.IFTYPE.MATCHES} = ^.*\$ {\$NET.IF.IFTYPE.NOT_MATCHES} = CHANGE_IF_NEEDED</pre>	<pre>{#IFNAME} MATCHES "@Network interfaces for discovery"</pre>

触发器

- ✓ 触发器名称：包含触发的原因（ 阈值 ）；
- ✓ 可选名称：使用 {ITEM.LASTVALUE1-9}，而不是添加至触发器名称；
- ✓ 触发器级别：Not classified/Info/Warning/Average/High/Disaster。

Good	Bad
Temperature is too high (over 35 C for 5m) CPU load is too high (over 1.5) MySQL: Refused connections (max_connections limit reached)	Temperature is too high (now: 40) CPU load is too high MySQL: Refused connections

Severity	Examples
未分类	
信息	序列号改变，用户登录
警告	磁盘空闲空间不足但仍可坚持一段时间
一般严重	CPU使用率高，设备温度高，网站访问慢
严重	Ping不通，网站不能访问
灾难	数据中心宕机，核心网络不通

- ✓ 触发器表达式：尽量使用用户宏以及带单位的时间。

Good	Bad
{template:temperature.avg(10m)>{\$TEMP.MAX.WARN}} {template:memory.free.avg(10m)<{\$MEM_FREE.WARN} where {\$MEM_FREE.WARN} = 100M	{template:temperature.avg(600)>{\$TEMP.MAX.WARN}} {template:memory.free.avg(10m)<{\$MEM_FREE.WARN} where {\$MEM_FREE.WARN} = 104857600

用户宏

✔ 用户宏：[A-Z0-9._]，小写字母不支持。

Good	OK	Bad
<code>{ \$MYSQL.HOST }</code> <code>{ \$MYSQL.PORT }</code> <code>{ \$MYSQL.PARAM1 }</code>	<code>{ \$MYSQL_HOST }</code> <code>{ \$MYSQL_PORT }</code> <code>{ \$MYSQL_PARAM1 }</code>	<code>{ \$HOST }</code> <code>{ \$PORT }</code> <code>{ \$PARAM1 }</code>
<code>{ \$IF.ERRORS.WARN:"{ #IFNAME }" }</code> <code>{ \$TEMP.MAX.WARN:"{ #SENSORNAME }" }</code>		<code>{ \$IF.ERRORS.WARN }</code> <code>{ \$TEMP.MAX.WARN }</code>
<code>{ \$MYSQL.REPLICATION_LAG.MAX.WARN }</code> <code>{ \$TEMP.MAX.WARN:"{ #SENSOR }" }</code> <code>{ \$SERVICE.STATUS.CRIT }</code> <code>{ \$IF.ERRORS.MAX.WARN }</code> <code>{ \$DISK.STATUS.OK }</code> <code>{ \$DISK.STATUS.WARN }</code> <code>{ \$DISK.STATUS.CRIT }</code> <code>{ \$MEM_UTIL.MAX.WARN }</code> <code>{ \$MEM_UTIL.MAX.CRIT }</code>		<code>{ \$DISK_OK_STATUS }</code> <code>{ \$MEMORY_UTIL_MAX }</code>

导出模板

☑ 模板导出为XML文件（ Zabbix5.4支持导出为YAML/JSON格式 ），文件以template单词开头。

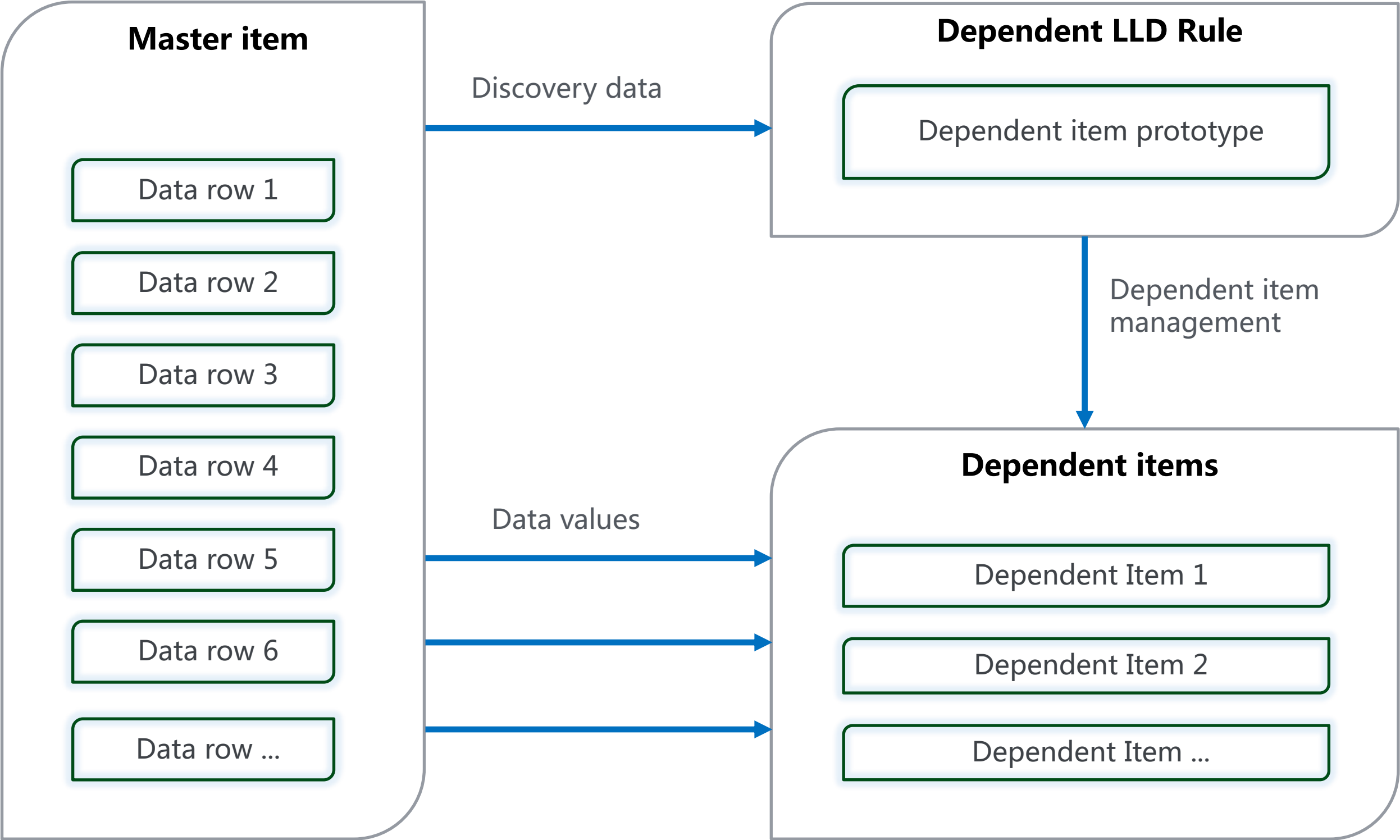
分类长名称	分类短名称	模板名 -- 文件名
Modules	Module	Interfaces SNMPv2 → template_module_interfaces_snmpv2.xml
Network devices	Net	Juniper SNMPv2 → template_net_juniper_snmpv2.xml
Storage devices	Storage	EMC VNX → template_storage_emc_vnx.xml
Server hardware	Server	IBM IMM2 by SNMPv2 → template_server_ibm_imm2_by_snmpv2.xml
Operating systems	OS	Linux → template_os_linux.xml
Databases	DB	Oracle by ODBC → template_db_oracle_by_odbc.xml
Power	Power	APC by SNMPv2 → template_power_apc_by_snmpv2.xml
Telephony	Tel	Asterisk by SNMPv3 → template_tel_asterisk_by_snmpv3.xml
Virtualization	VM	VMWare → template_vm_vmware.xml
Printers	Printer	Printer generic by SNMPv2 → template_printer_generic_by_snmpv2.xml
Applications	App	Apache Tomcat JMX → template_app_apache_tomcat_jmx.xml
Hardware	HW	Skycontrol SNMPv1 → template_hw_skycontrol_snmpv1.xml



Zabbix监控模板标准化的意义和价值

模板标准化最佳实践

依赖项和预处理



健康检查

✔ 定义健康检查触发器：

{TEMPLATE_NAME:METRIC.count(#1,{SERVICE.STATUS.CRIT},eq)}=1

{TEMPLATE_NAME:METRIC.last()}={SERVICE.STATUS.CRIT}

等级	触发器级别	触发器名称	触发器依赖	简单表达式
Not OK	信息	Service X is not OK	depends on warning and critical level triggers	{TEMPLATE_NAME:METRIC.count(#1,{SERVICE.STATUS.OK},ne)}=1
Warning	警告	Service X is in warning	depends on critical level trigger	{TEMPLATE_NAME:METRIC.count(#1,{SERVICE.STATUS.WARN},eq)}=1
Critical	严重/一般严重	Service X is in critical state		{TEMPLATE_NAME:METRIC.count(#1,{SERVICE.STATUS.CRIT},eq)}=1



Zabbix监控模板标准化的意义和价值

模板指南发布

模板指南发布

<https://www.zabbix.com/documentation/guidelines/zh/thosts>

ZABBIX

Zabbix Code Guidelines

guidelines (Development) ▼

中文 ▼

Recent Changes

Log In

Search

Zabbix guidelines

Coding

Naming

Zabbix 指南

Cording

Naming

Development process

sidebar

Webhooks

模版

Development process

Webhooks

Plugins

Templates

模版

Recent Changes

Link

PDF

Table of Contents

Zabbix模版指南

免责声明

此文档的目的不是为了让每个人都严格遵守规则。相反，此文档展示了我们构建模板的方法，文档中描述的任何规则和最佳实践在未来可能被更改或者放弃。

当前文档状态: 草稿 可供预览和反馈。模板定制可联系Zabbix中国——上海宏时数据系统有限公司。

介绍

Zabbix监控方式。 资源与服务

在我们开始讨论什么是最佳的模板之前，让我们来简单讨论一下监控。由于监控是一个很常见且模棱两可的术语，所以没有真正的RFC定义。有人可能会说，监控是指不断地在社交网络上搜索有关你公司地信息，而另一些人可能会说，监控是指收集有关植物土壤营养和水分的传感器数据。Zabbix是通用的监控解决方案，我们为任何类型的监控项目提供一个工具集。但在此文档中，我们会重点讨论对现代分布式系统的监控方法。

一切皆可被视为 服务 或者 资源。

服务 是指你的组织提供给外部的事物。例如在线零售商店，或者公共电子邮件服务。如果你的商店在线并且顾客可以成功的在商店中购买商品 - 那么你的服务是可用的。又或许是你的部门向公司的其他部门提供的服务。比如您根据需要提供给其他部门的计算资源。此类内部服务可能是你的公司在线商店

模版

Zabbix模版指南

免责声明

介绍

制作一个优秀的模板需要哪些东西?

1. 灵活可重用

2. 了解专业知识

3. 模块化和范围

4. 遵循指导原则

结论

样式指南

1.1 总则

1.2 模板

1.3 监控项

1.4 低级别自动发现规则 (LLD)

ZABBIX

FORUM

SHENZHEN 2021

Q&A ?

ZABBIX



THANK YOU!

ZABBIX

ZABBIX

FORUM

SHENZHEN 2021

本次深圳大会照片 <https://live.aiyaopai.com/live/52886185>

往期大会演讲视频 <https://space.bilibili.com/476625813>



微信交流群：17502189550



公众号干货：Zabbix开源社区