Agent监控方式

在Agent监控方式下，zabbix-agent会主动收集本机的监控信息并通过TCP协议与zabbix-server传递信息。Agent监控方式分为主动和被动模式。在被动模式下，zabbix-agent监听10050端口，等待zabbix-server的监控信息收集信息请求；在主动模式下，zabbix-agent收集监控信息并通过10050端口主动将数据传给zabbix-server所在服务器的10051端口。

**优点：**

1. 是zabbix最常用的监控方式，监测指标深入细致有针对性。
2. 内置监控功能强大，内置监控项目丰富。
3. TCP方式实现通讯，可靠性也有保证。

**缺点：**

1. 需要在被监控机器上安装zabbix-agent客户端，部署相对麻烦，最初需要逐个机器安装代理软件。
2. zabbix-agent客户端运行在被监控机上，会收集本机信息。

Trapper监控方式

Trapper监控方式使用zabbix-sender程序主动向zabbix-server发送数据。key的名称和发送的数据内容都可以灵活定义。发送的信息采用JSON格式，遵循zabbix-sender协议。可以自定义脚本利用zabbix-sender协议来向zabbix-server发送信息。

**优点：**

1. 不需要在被监控机器安装zabbix-agent
2. 不收集被监控机器的信息
3. 可以自定义发送的信息内容
4. 可以使用自定义脚本发送信息

**缺点：**

1. 需要自定义发送的信息内容
2. 无内置监控项目

SNMP监控方式

SNMP全称Simple Network Management Protocol，即网络管理协议，包括进程管理和被管理设备两部分。作为一种国际通用的网络管理协议被广泛的应用于对各种交换机，路由器等网络设备的管理上，而现在也越来越多被用于对服务器的监控上。

**优点：**

1. 服务器一旦部署SNMPAgent,任何能实现SNMP协议的软件都可对其进行监测。
2. 通过这种手段进行监测不需知道被监测服务器的用户名与密码，比较安全。

**缺点：**

1. 很多服务器并非默认安装SNMPAgent，如果要通过这种方式监测则需要对所有服务器安装部署。
2. 能监测的参数指标比较固定不够深入，无法满足用户的特殊需求。
3. 由于SNMP协议是通过UDP方式实现的，在网络状况不佳的情况下其可靠性难以保证。

JMX监控方式

JMX，全称[**Java**](http://lib.csdn.net/base/java)Management Extensions，即[**Java**](http://lib.csdn.net/base/java)管理拓展，是Java平台为应用程序，设备，系统等植入管理功能的框架。在zabbix中，JMX数据的获取由zabbix-java-gateway代理程序来负责数据的采集。

**优点：**

1. 可以详细地监控各类Java程序的运行状态。

**缺点：**

1. 被监控机上需要安装zabbix-java-gateway

IPMI监控方式

IPMI，全称Intelligent Platform Management Interface，即[**智能**](http://lib.csdn.net/base/aiplanning)平台管理接口，原本是Intel[**架构**](http://lib.csdn.net/base/architecture)中企业系统的周边设备所采用的一种工业标准，后来成为业界通用的标准。用户可以利用IPMI监视服务器的物理特征，如温度，电压，电扇工作状态，电源供应以及机箱入侵等指标。

结论

根据以上对zabbix各主要监控方式的梳理，结论如下：

1. 根据被监控机器的环境和客户要求选用适当的监控方式，可同时配合使用多种监控方式。
2. 有条件在被监控机上部署zabbix-agent客户端时，该方法为第一选择，因为其功能强大且配置相对简便。
3. 需要自定义脚本或者监控信息时，可使用trapper方式，即使用zabbix-sender程序或者自定义脚本遵循zabbix-sender协议，以JSON形式，通过TCP发送自定义信息。