|  |
| --- |
| 完整告警流程 |
| **作者：付金龙**  **归档：学习笔记**  **2016/6/27** |
| **快捷键：**  Ctrl + 1 标题1  Ctrl + 2 标题2  Ctrl + 3 标题3  Ctrl + 4 实例  Ctrl + 5 程序代码  Ctrl + 6 正文 |
| **格式说明：**  蓝色字体：注释  黄色背景：重要  绿色背景：注意 |

****

**老男孩教育教学核心思想6重：重目标、重思路、重方法、重实践、重习惯、重总结**

**学无止境，老男孩教育成就你人生的起点！**

**联系方式:**

|  |  |
| --- | --- |
| **网站运维QQ交流群：** | |
| Linux 385168604 | 架构师 390642196 |
| Python 29215534 | 大数据 421358633 |
| **官方网站:** | |
| [**http://www.oldboyedu.com**](http://www.oldboyedu.com) |  |

目 录

[完整告警流程： 1](#_Toc470466959)

[1、创建用户组： 1](#_Toc470466960)

[2、添加用户 1](#_Toc470466961)

[Zabbix生产案例实战： 4](#_Toc470466962)

[1、项目规划 4](#_Toc470466963)

[1.1.SNMP监控： 5](#_Toc470466964)

[1.2.IPMI的监控 8](#_Toc470466965)

[1.3.监控Java应用(使用Zabbix Java Gateway代理) 8](#_Toc470466966)

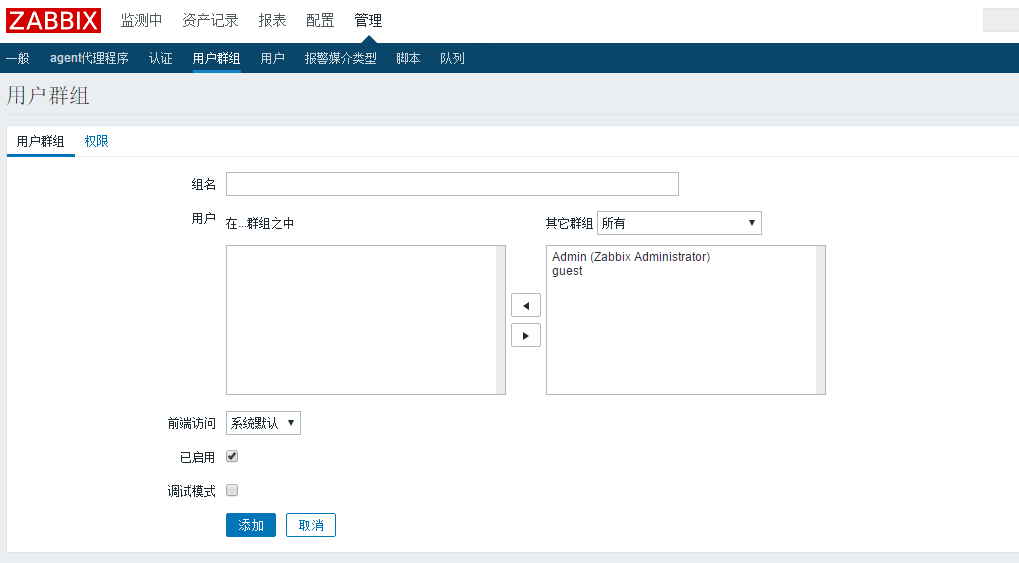
[二、生产角度讲解如何监控nginx 10](#_Toc470466967)

[2.1.、开启nginx 10](#_Toc470466968)

[2.2.编写脚本来进行数据采集 10](#_Toc470466969)

# 完整告警流程：

## 1、创建用户组：



同时添加权限，对那些主机有权限。

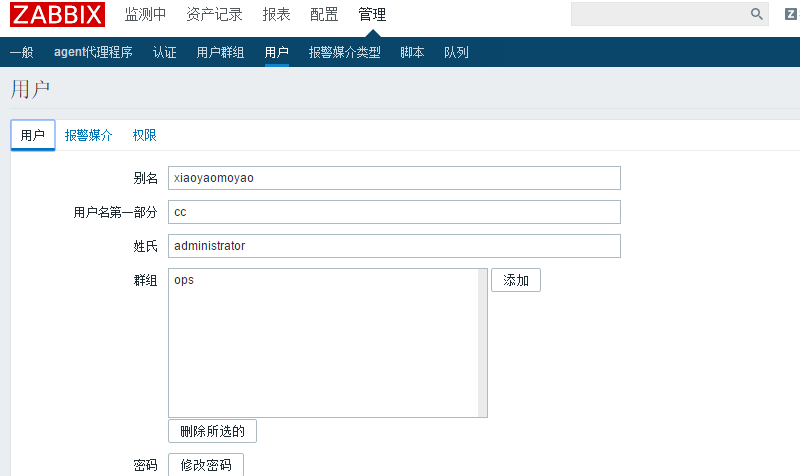
## 2、添加用户

* 用户的基本信息(用户名，所属群组，密码等)
* 报警媒介(mail)[此处后期会讲自定义]

1、报警媒介

2、Action

* 权限(权限那个按照用户组分配、选择用户角色)



报警媒介配置：



Action配置：



全部配置好之后，用户就可以收到报警信息。

注：新加一台，要确认权限分配。

# Zabbix生产案例实战：

## 1、项目规划

主机分组：

交换机

Nginx

Tomcat

MySQL



监控对象识别：

1、使用SNMP监控交换机

2、使用IPMI监控服务器硬件

3、使用Agent监控服务器

4、使用JMX监控Java

5、监控MySQL

6、监控Web状态

7、监控Nginx状态

### 1.1.SNMP监控：

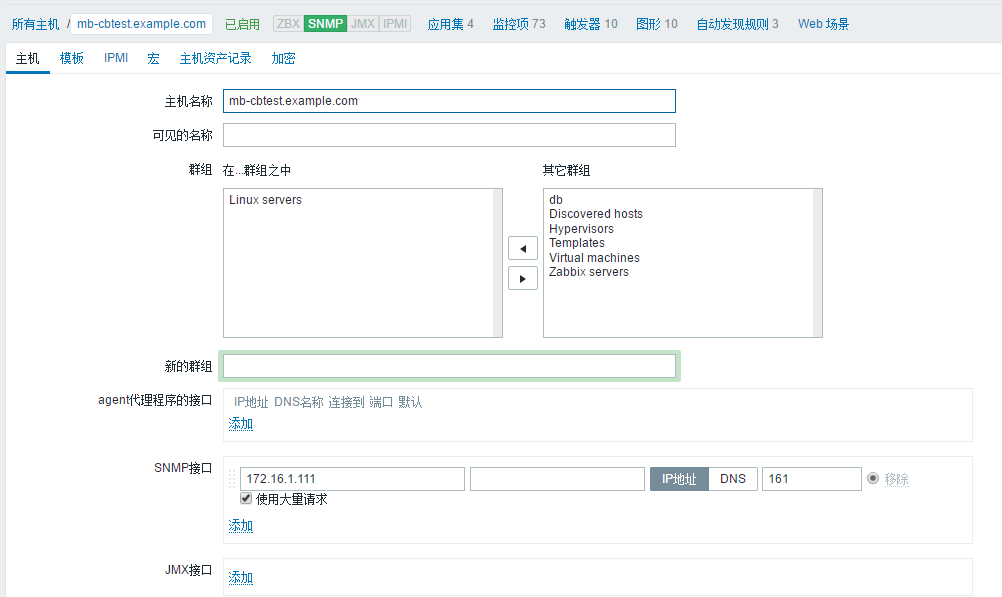
#### 1.1.1、交换机开启SNMP

config t

snmp-server community public ro **#团体名称**

end

#### 1.1.2、在Zabbix上添加监控



设置SNMP Interface

#### 1.1.3、关联监控模版



注意：此处还要设置“宏”内的团体名称(SNMP的团体名称配置)



配置完成之后，Zabbix会搜索出设备的所有端口以及VLAN的配置（如果有），并会绘制出流量图(出、入)。

如果SNMP是服务器：SNMP的配置文件内容：

[root@mb-cbtest ~]# egrep -v "^($|#| )" /etc/snmp/snmpd.conf

com2sec notConfigUser default public

com2sec notConfigUser 172.16.1.81 public

com2sec notConfigUser 172.16.1.51 public

group notConfigGroup v1 notConfigUser

group notConfigGroup v2c notConfigUser

view systemview included .1

view systemview included .1.3.6.1.2.1.1

view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none

access notConfigGroup "" any noauth exact all none none

group MyRWGroup any local

group MyROGroup any mynetwork

group MyRWGroup any otherv3user

syslocation Unknown (edit /etc/snmp/snmpd.conf)

syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf)

proc mountd

proc ntalkd 4

proc sendmail 10 1

exec echotest /bin/echo hello world

disk / 10000

load 12 14 14

pass .1.3.6.1.4.1.4413.4.1 /usr/bin/ucd5820stat

mibs +MY-MIB

### 1.2.IPMI的监控

监控硬件的，但是性能有问题，经常容易超时。推荐使用自定义脚本，服务器本地使用ipmitool命令来获取数据。

### 1.3.监控Java应用(使用Zabbix Java Gateway代理)



注：此处也可以参考Tomcat章节内容。

#### 1.3.1.YUM安装的zabbix需要安装：

yum install -y java java-devel zabbix-java-gateway

源码安装：

--enable-java

#### 1.3.2.本机配置文件：（需要注意的地方）

[root@zb01 ~]# vim /etc/zabbix/zabbix\_java\_gateway.conf

# LISTEN\_IP="0.0.0.0"

# LISTEN\_PORT=10052

# START\_POLLERS=5 #跟Java应用数量有关，一般或者想等

TIMEOUT=3 #一般设置30（目前默认即可）

#### 1.3.3.启动服务

systemctl start zabbix-java-gateway.service

#### 小技巧：CentOS7支持命令补全

#安装这个包即可

[root@mb-cbtest ~]# yum install bash-completion

#### 1.3.4.检查端口、服务是否存在

#### 1.3.5.配置Zabbix\_Server配置

#需要注意的点

JavaGateway=172.16.1.81

# JavaGatewayPort=10052

StartJavaPollers=5 #Server端去问gateway的

#### 1.3.6.重启Zabbix\_Server进程

systemctl restart zabbix\_server.service

#### 1.3.7.配置tomcat（在主机10.0.0.8上）

#101行之后

CATALINA\_OPTS="$CATALINA\_OPTS

-Dcom.sun.management.jmxremote

-Dcom.sun.management.jmxremote.port=12345

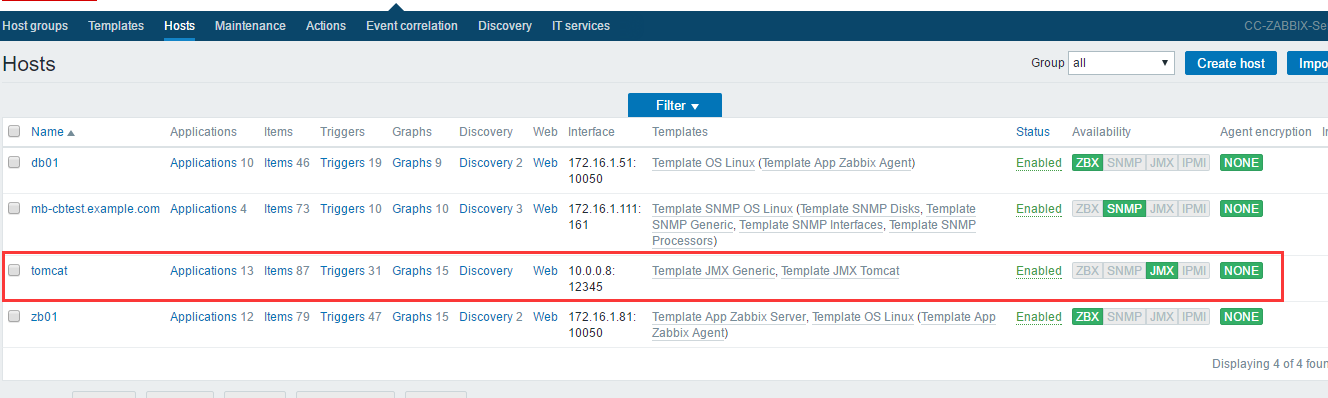
-Dcom.sun.management.jmxremote.authenticate=false

-Dcom.sun.management.jmxremote.ssl=false

-Djava.rmi.server.hostname=10.0.0.8"

参考：http://tomcat.apache.org/tomcat-8.0-doc/monitoring.html#Enabling\_JMX\_Remote

#### 1.3.8.配置完成之后



说明：配置更改完之后，可以使用windows的jdk下的jconsole.exe进行验证。

#### 1.3.9.JMX的监控类型

三种类型：

1、无密码认证

2、用户名密码认证

3、ssl

#### 1.3.10.手动监测监控数据

zabbix\_get -s 172.16.1.8 -k ${you-key}

#### 1.3.11.命令行方式获取jmx值

参考文档：

<http://blog.csdn.net/reblue520/article/details/52623604>

# 二、生产角度讲解如何监控nginx

## 2.1.、开启nginx

## 2.2.编写脚本来进行数据采集

1）确认zabbix\_agent.conf配置文件

Include=/application/zabbix/etc/zabbix\_agentd.conf.d/\*.conf

2）将脚本上传到

/application/zabbix/etc/zabbix\_agentd.conf.d/

[root@zb01 zabbix\_agentd.conf.d]# chmod +x zabbix\_linux\_plugin.sh

[root@zb01 zabbix\_agentd.conf.d]# ./zabbix\_linux\_plugin.sh

Usage: ./zabbix\_linux\_plugin.sh {tcp\_status key|memcached\_status key|redis\_status key|nginx\_status key}

3）修改nginx的status配置，确认跟脚本中的参数一样

server {

listen \*:80 default\_server;

server\_name \_;

location /nginx\_status {

stub\_status on;

access\_log off;

allow 127.0.0.1;

deny all;

}

4）重载nginx

5）手动脚本尝试

./zabbix\_linux\_plugin.sh nginx\_status 80 active

6）添加自定义监控项

[root@zb01 zabbix\_agentd.conf.d]# cat nginx1.conf

UserParameter=linux\_status[\*],/application/zabbix/etc/zabbix\_agentd.conf.d/zabbix\_linux\_plugin.sh "$1" "$2" "$3"

说明：[\*]理解为数组，可以传参，具体的参数就是$1，$2，$3

7）重启zabbix-agent服务

systemctl restart zabbix-agent

8）手动获取测试

[root@zb01 zabbix\_agentd.conf.d]# zabbix\_get -s 172.16.1.81 -k linux\_status[nginx\_status,80,active]

2

9）通过界面添加模版

注：注意监控颗粒度，过小容易给服务器造成压力，过大可能会有些监控不到。

2.3.设置用户自定义参数

2.4.重启zabbix-agent

2.5.添加item

2.6.创建图形

2.7.创建触发器

2.8.创建模版



## 自定义告警脚本：

1、放在zabbix/share/zabbix/alertscripts下

2、要支持三个参数：1)收件人2)主题3)内容

3、执行权限

4、Web界面添加

5、修改Actions

## 通过precona监控插件监控MySQL：

1、安装precona模版

yum install http://www.percona.com/downloads/percona-release/redhat/0.1-3/percona-release-0.1-3.noarch.rpm

相关说明文档：https://www.percona.com/doc/percona-server/5.6/installation/yum\_repo.html#standalone-rpm

https://www.percona.com/doc/percona-monitoring-plugins/LATEST/zabbix/index.html

2、yum install percona-zabbix-templates php php-mysql

1、php脚本用来数据采集

2、shell 调用php脚本

3、zabbix的配置文件

4、zabbix的模版文件