

TTS 10.0 COOKBOOK

(NSD SECURITY DAY01)

版本编号 10.0

2019-06

达内 IT 培训集团

NSD SECURITY DAY01

1. 案例 1：常用系统监控命令

• 问题

本案例要求熟悉查看 Linux 系统状态的常用命令，为进一步执行具体的监控任务做准备：

- 1) 查看内存信息
- 2) 查看交换分区信息
- 3) 查看磁盘信息
- 4) 查看 CPU 信息
- 5) 查看网卡信息
- 6) 查看端口信息
- 7) 查看网络连接信息

• 方案

一般企业做监控的目的：实时报告系统状态，提前发现系统的问题。

监控的资源可以分为：共有数据（HTTP、FTP 等）和私有数据（CPU、内存、进程数等）。

监控软件可以使用：系统自带的命令、Cacti 监控系统、Nagios 监控系统、Zabbix 监控系统。

• 步骤

实现此案例需要按照如下步骤进行。

步骤一：使用命令查看计算机状态数据

1) 查看内存与交换分区信息

```
[root@proxy ~]# free //查看内存信息
              total        used        free      shared  buff/cache   available
Mem:      16166888     8017696     720016        106504        7429176        7731740
Swap:      4194300       218268       3976032

[root@proxy ~]# free | awk '/Mem/{print $4}' //查看剩余内存容量
720928

[root@proxy ~]# swapon -s //查看交换分区信息
文件名          类型      大小    已用    权限
/dev/sda3       partition 4194300 218268 -1
```

步骤二：查看磁盘与 CPU 利用率

1) 查看磁盘信息

```
[root@proxy ~]# df //查看所有磁盘的使用率
文件系统      1K-块      已用      可用      已用% 挂载点
/dev/sda2      476254208 116879624 335159084 26%    /
/dev/sda1      198174     133897    49737     73%    /boot
[root@proxy ~]# df | awk '/\$//{print $5}' //查看根分区的利用率
```

2) 查看 CPU 平均负载

```
[root@proxy ~]# uptime //查看 CPU 负载 (1, 5, 15 分钟)
23:54:12 up 38 days, 14:54, 9 users, load average: 0.00, 0.04, 0.05
[root@proxy ~]# uptime |awk '{print $NF}' //仅查看 CPU 的 15 分钟平均负载
0.05
```

步骤二：查看网卡信息、端口信息、网络连接信息

1) 查看网卡信息

```
[root@proxy ~]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.5 netmask 255.255.255.0 broadcast 172.25.0.255
    inet6 fe80::5054:ff:fe00:b prefixlen 64 scopeid 0x20<link>
    ether 52:54:00:00:00:0b txqueuelen 1000 (Ethernet)
    RX packets 62429 bytes 10612049 (10.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5674 bytes 4121143 (3.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
[root@proxy ~]# ifconfig eth0 |awk '/inet /{print $2}' //查看 IP 地址信息
192.168.4.5
[root@proxy ~]# ifconfig eth0 |awk '/RX p/{print $5}' //网卡接受数据包流量
10625295
[root@proxy ~]# ifconfig eth0 |awk '/TX p/{print $5}' //网卡发送数据包流量
4130821
```

2) 查看端口信息

```
[root@proxy ~]# ss -ntulp //查看本机监听的所有端口
// -n 以数字显示端口号
// -t 显示 tcp 连接
// -u 显示 udp 连接
// -p 显示监听端口对应的程序名称
```

3) 查看网络连接信息

```
[root@proxy ~]# ss -antup //查看所有的网络连接信息
// -a 查看所有连接状态信息
```

2. 案例 2：部署 Zabbix 监控平台

• 问题

本案例要求部署一台 Zabbix 监控服务器，一台被监控主机，为进一步执行具体的监控任务做准备：

- 1) 安装 LNMP 环境
- 2) 源码安装 Zabbix
- 3) 安装监控端主机，修改基本配置
- 4) 初始化 Zabbix 监控 Web 页面
- 5) 修改 PHP 配置文件，满足 Zabbix 需求
- 6) 安装被监控端主机，修改基本配置

• 方案

使用 1 台 RHEL7 虚拟机，安装部署 LNMP 环境、Zabbix 及相关的依赖包，配置数据库并对 Zabbix 监控平台进行初始化操作。使用 2 台被监控端，源码安装 Zabbix Agent。完成 Zabbix 实验需要我们搭建一个实验环境，拓扑结构如表-1 所示。

表-1 实验拓扑结构

主机名称	网卡与 IP 地址
zabbixserver	eth1:192.168.2.5
zabbixclient_web1	eth1:192.168.2.100
zabbixclient_web2	eth1:192.168.2.200

• 步骤

实现此案例需要按照如下步骤进行。

步骤一：部署监控服务器

- 1) 安装 LNMP 环境

Zabbix 监控管理控制台需要通过 Web 页面展示出来，并且还需要使用 MySQL 来存储数据，因此需要先为 Zabbix 准备基础 LNMP 环境。

```
[root@zabbixserver ~]# yum -y install gcc pcre-devel openssl-devel
[root@zabbixserver ~]# tar -xf nginx-1.12.2.tar.gz
[root@zabbixserver ~]# cd nginx-1.12.2
[root@zabbixserver nginx-1.12.2]# ./configure --with-http_ssl_module
[root@zabbixserver nginx-1.12.2]# make && make install
[root@zabbixserver ~]# yum -y install php php-mysql \
> mariadb mariadb-devel mariadb-server
[root@zabbixserver ~]# yum -y install php-fpm-5.4.16-42.el7.x86_64.rpm
//注意，php-fpm 这个软件包在 lnmp_soft/目录下
```

- 2) 修改 Nginx 配置文件

配置 Nginx 支持 PHP 动态网站，因为有大量 PHP 脚本需要执行，因此还需要开启 Nginx 的各种 fastcgi 缓存，加速 PHP 脚本的执行速度。

```
[root@zabbixserver ~]# vim /usr/local/nginx/conf/nginx.conf
...
http{
...
    fastcgi_buffers 8 16k;                //缓存 php 生成的页面内容，8 个 16k
```

```
fastcgi_buffer_size 32k;           //缓存 php 生产的头部信息
fastcgi_connect_timeout 300;       //连接 PHP 的超时时间
fastcgi_send_timeout 300;         //发送请求的超时时间
fastcgi_read_timeout 300;         //读取请求的超时时间
location ~ \.php$ {
    root            html;
    fastcgi_pass     127.0.0.1:9000;
    fastcgi_index    index.php;
    include          fastcgi.conf;
}
... ..
```

3) 启动服务

启动 Nginx、PHP-FPM、MariaDB 服务，关闭 SELinux 与防火墙。

```
[root@zabbixserver ~]# systemctl start mariadb
[root@zabbixserver ~]# systemctl start php-fpm
[root@zabbixserver ~]# ln -s /usr/local/nginx/sbin/nginx /sbin/nginx
[root@zabbixserver ~]# nginx

[root@zabbixserver ~]# firewall-cmd --set-default-zone=trusted
[root@zabbixserver ~]# setenforce 0
```

4) 客户端测试 LNMP 环境

服务器创建 PHP 测试页面，浏览器访问页面测试网页连通性。

```
[root@zabbixserver ~]# cat /usr/local/nginx/html/test.php
<?php
$i=33;
echo $i;
?>
[root@zabbixserver ~]# curl http://192.168.2.5/test.php
```

步骤二：部署监控服务器 Zabbix Server

1) 源码安装 Zabbix Server

多数源码包都是需要依赖包的，zabbix 也一样，源码编译前需要先安装相关依赖包。

```
[root@zabbixserver lnmp_soft]# yum -y install net-snmp-devel \
> curl-devel
//安装相关依赖包
[root@zabbixserver lnmp_soft]# yum -y install \
> libevent-devel-2.0.21-4.el7.x86_64.rpm
//注意 Libevent-devel 这个软件包在 lnmp_soft 目录下有提供
[root@zabbixserver lnmp_soft]# tar -xf zabbix-3.4.4.tar.gz
[root@zabbixserver lnmp_soft]# cd zabbix-3.4.4/
[root@zabbixserver zabbix-3.4.4]# ./configure --enable-server \
> --enable-proxy --enable-agent --with-mysql=/usr/bin/mysql_config \
> --with-net-snmp --with-libcurl
// --enable-server 安装部署 zabbix 服务器端软件
// --enable-agent 安装部署 zabbix 被监控端软件
// --enable-proxy 安装部署 zabbix 代理相关软件
// --with-mysql 配置 mysql_config 路径
// --with-net-snmp 允许 zabbix 通过 snmp 协议监控其他设备
// --with-libcurl 安装相关 curl 库文件，这样 zabbix 就可以通过 curl 连接 http 等服务，测试
被监控主机服务的状态
```

```
[root@zabbixserver zabbix-3.4.4]# make && make install
```

2) 初始化 Zabbix

创建数据库，上线 Zabbix 的 Web 页面

```
[root@zabbixserver ~]# mysql
mysql> create database zabbix character set utf8;
//创建数据库，支持中文字符集
mysql> grant all on zabbix.* to zabbix@'localhost' identified by 'zabbix';
//创建可以访问数据库的账户与密码
[root@zabbixserver ~]# cd lnmp_soft/zabbix-3.4.4/database/mysql/
[root@zabbixserver mysql]# mysql -uzabbix -pzabbix zabbix < schema.sql
[root@zabbixserver mysql]# mysql -uzabbix -pzabbix zabbix < images.sql
[root@zabbixserver mysql]# mysql -uzabbix -pzabbix zabbix < data.sql
//刚刚创建是空数据库，zabbix 源码包目录下，有提前准备好的数据
//使用 mysql 导入这些数据即可（注意导入顺序）
```

上线 Zabbix 的 Web 页面

```
[root@zabbixserver ~]# cd lnmp_soft/zabbix-3.4.4/frontend/php/
[root@zabbixserver php]# cp -r * /usr/local/nginx/html/
[root@zabbixserver php]# chmod -R 777 /usr/local/nginx/html/*
```

修改 Zabbix_server 配置文件，设置数据库相关参数，启动 Zabbix_server 服务

```
[root@zabbixserver ~]# vim /usr/local/etc/zabbix_server.conf
DBHost=localhost
//数据库主机，默认该行被注释
DBName=zabbix
//设置数据库名称
DBUser=zabbix
//设置数据库账户
DBPassword=zabbix
//设置数据库密码，默认该行被注释
LogFile=/tmp/zabbix_server.log
//设置日志，仅查看以下即可
[root@zabbixserver ~]# useradd -s /sbin/nologin zabbix
//不创建用户无法启动服务
[root@zabbixserver ~]# zabbix_server //启动服务

[root@zabbixserver ~]# ss -ntulp |grep zabbix_server //确认连接状态，端口 10051
tcp        LISTEN      0            128          *:10051     *:
users: (("zabbix_server",pid=23275,fd=4),("zabbix_server",pid=23274,fd=4))
```

提示：如果是因为配置文件不对，导致服务无法启动时，不要重复执行 zabbix_server，一定要先使用 killall zabbix_server 关闭服务后，再重新启动一次。

修改 Zabbix_agent 配置文件，启动 Zabbix_agent 服务

```
[root@zabbixserver ~]# vim /usr/local/etc/zabbix_agentd.conf
Server=127.0.0.1,192.168.2.5 //允许哪些主机监控本机
ServerActive=127.0.0.1,192.168.2.5 //允许哪些主机通过主动模式监控本机
Hostname=zabbix_server //设置本机主机名
LogFile=/tmp/zabbix_server.log //设置日志文件
UnsafeUserParameters=1 //是否允许自定义 key
```

```
[root@zabbixserver ~]# zabbix_agentd //启动监控 agent

[root@zabbixserver ~]# ss -ntulp |grep zabbix_agentd //查看端口信息为 10050
tcp        LISTEN      0            128          *:10050      *:10050
users:(("zabbix_agentd",pid=23505,fd=4),("zabbix_agentd",pid=23504,fd=4))
```

提示: 如果是因为配置文件不对, 导致服务无法启动时, 不要重复执行 zabbix_agentd, 一定要先使用 killall zabbix_agentd 关闭服务后, 再重新启动一次。

浏览器访问 Zabbix_server 服务器的 Web 页面

```
[root@zabbixserver ~]# firefox http://192.168.2.5/index.php
//第一次访问, 初始化 PHP 页面会检查计算机环境是否满足要求, 如果不满足会给出修改建议
//默认会提示 PHP 的配置不满足环境要求, 需要修改 PHP 配置文件
```

根据错误提示, 修改 PHP 配置文件, 满足 Zabbix_server 的 Web 环境要求
php-bcmath 和 php-mbstring 都在 lnmp_soft 目录下有提供软件包。

```
[root@zabbixserver ~]# yum -y install php-gd php-xml
[root@zabbixserver ~]# yum install php-bcmath-5.4.16-42.el7.x86_64.rpm
[root@zabbixserver ~]# yum install php-mbstring-5.4.16-42.el7.x86_64.rpm
[root@zabbixserver ~]# vim /etc/php.ini

date.timezone = Asia/Shanghai //设置时区
max_execution_time = 300 //最大执行时间, 秒
post_max_size = 32M //POST 数据最大容量
max_input_time = 300 //服务器接收数据的时间限制
memory_limit = 128M //内存容量限制

[root@zabbixserver ~]# systemctl restart php-fpm
```

修改完 PHP 配置文件后, 再次使用浏览器访问服务器, 则会提示如图-1 和图-2 所示的提示信息。



图-1



ZABBIX

Check of pre-requisites

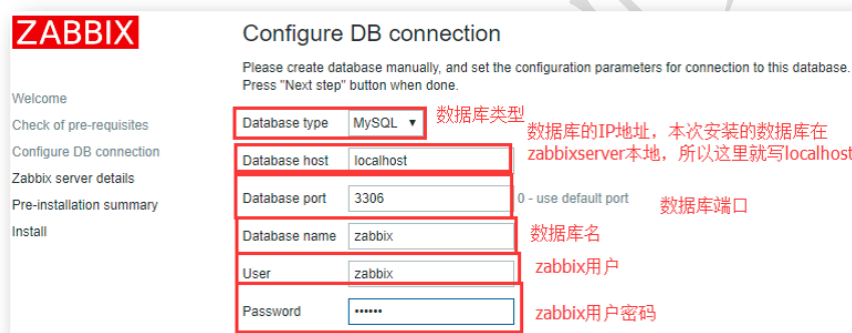
PHP gd PNG support	on	OK	
PHP gd JPEG support	on	OK	
PHP gd FreeType support	on	OK	
PHP libxml	2.9.1	2.6.15	OK
PHP xmlwriter	on	OK	
PHP xmlreader	on	OK	
PHP LDAP	on	确认都是OK的状态	OK
PHP ctype	on	OK	
PHP session	on	OK	
PHP option "session.auto_start"	off	off	OK
PHP gettext	on	OK	
PHP option "arg_separator.output"	&	&	OK

Back Next step

图-2

注意：这里有一个 PHP LDAP 是 warning 状态是没有问题的！

在初始化数据库页面，填写数据库相关参数，如图-3 所示。



ZABBIX

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Database type	MySQL	数据库类型
Database host	localhost	数据库的IP地址，本次安装的数据库在 zabbixserver本地，所以这里就写localhost
Database port	3306	0 - use default port 数据库端口
Database name	zabbix	数据库名
User	zabbix	zabbix用户
Password	*****	zabbix用户密码

图-3

在登陆页面，使用用户(admin)和密码(zabbix)登陆，登陆后设置语言环境为中文，如图-4 和图-5 所示。



ZABBIX

Username

Admin

Password

☒ Remember me for 30 days

Sign in

图-4

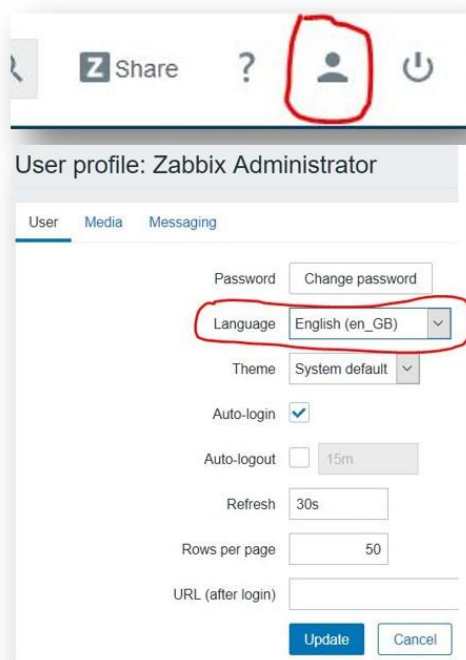


图-5

步骤三：部署被监控主机 Zabbix Agent

1) 源码安装 Zabbix agent 软件

在 2.100 和 2.200 做相同操作 (以 zabbixclient_web1 为例)。

```
[root@zabbixclient_web1 ~]# useradd -s /sbin/nologin zabbix
[root@zabbixclient_web1 ~]# yum -y install gcc pcre-devel
[root@zabbixclient_web1 ~]# tar -xf zabbix-3.4.4.tar.gz
[root@zabbixclient_web1 ~]# cd zabbix-3.4.4/
[root@zabbixclient_web1 zabbix-3.4.4]# ./configure --enable-agent
[root@zabbixclient_web1 zabbix-3.4.4]# make && make install
```

2) 修改 agent 配置文件，启动 Agent

```
[root@zabbixclient_web1 ~]# vim /usr/local/etc/zabbix_agentd.conf
Server=127.0.0.1,192.168.2.5           //谁可以监控本机（被动监控模式）
ServerActive=127.0.0.1,192.168.2.5   //谁可以监控本机（主动监控模式）
Hostname=zabbixclient_web1           //被监控端自己的主机名
EnableRemoteCommands=1
//监控异常后，是否允许服务器远程过来执行命令，如重启某个服务
UnsafeUserParameters=1               //是否允许自定义 key 监控
[root@zabbixclient_web1 ~]# zabbix_agentd //启动 agent 服务
```

3) 拷贝启动脚本 (非必须操作, 可选做), 有启动脚本可以方便管理服务, 启动与关闭服务。启动脚本位于 zabbix 源码目录下。

```
[root@zabbixclient_web1 zabbix-3.4.4]# cd misc/init.d/fedora/core
```

```
[root@zabbixclient_web1 zabbix-3.4.4]# cp zabbix_agentd /etc/init.d/
[root@zabbixclient_web1 zabbix-3.4.4]# /etc/init.d/zabbix_agentd start
[root@zabbixclient_web1 zabbix-3.4.4]# /etc/init.d/zabbix_agentd stop
[root@zabbixclient_web1 zabbix-3.4.4]# /etc/init.d/zabbix_agentd status
[root@zabbixclient_web1 zabbix-3.4.4]# /etc/init.d/zabbix_agentd restart
```

3. 案例 3：配置及使用 Zabbix 监控系统

• 问题

沿用练习一，使用 Zabbix 监控平台监控 Linux 服务器，实现以下目标：

- 1) 监控 CPU
- 2) 监控内存
- 3) 监控进程
- 4) 监控网络流量
- 5) 监控硬盘

• 方案

通过 Zabbix 监控平台，添加被监控 zabbixclient_web1 主机（192.168.2.100）并链接监控模板即可，Zabbix 默认模板就可以监控 CPU、内存、进程、网络、磁盘等项目。

• 步骤

实现此案例需要按照如下步骤进行。

步骤一：添加监控主机

主机是 Zabbix 监控的基础，Zabbix 所有监控都是基于 Host 主机。

使用火狐浏览器登录 <http://192.168.2.5>，通过 Configuration（配置）-->Hosts（主机）-->Create Host（创建主机）添加被监控 Linux 主机，如图-7 所示。



图-7

添加被监控主机时，需要根据提示输入被监控 Linux 主机的主机名称（最好与电脑的主机名一致，但也允许不一致）、主机组、IP 地址等参数，具体参考图-8 所示。

主机 模板 IPMI 宏 主机资产记录 加密

主机名称 zabbix_client_web1

可见的名称 zabbix_client_web1

群组 在 群组之中

Linux servers

新的群组

agent代理程序的接口 IP地址 DNS名称

192.168.2.100

添加

图-8

步骤二：为被监控主机添加监控模板

Zabbix 通过监控模板来对监控对象实施具体的监控功能，根据模板来定义需要监控哪些数据，对于 Linux 服务器的监控，Zabbix 已经内置了相关的模板(Template OS Linux)，选择模板并链接到主机即可，如图-9 所示。

主机 模板 IPMI 宏 主机资产记录 加密

链接的模板 名称 动作

Template OS Linux 取消链接 取消链接并清理

链接指示器 在此输入搜索 选择

添加

更新 克隆 全克隆 删除 取消

图-9

步骤三：查看监控数据

查看监控数据，登录 Zabbix Web 控制台，点击 Monitoring(监控中)-> Latest data(最新数据)，正过滤器中填写过滤条件，根据监控组和监控主机选择需要查看哪些监控数据，如图-10 所示。



图-10

找到需要监控的数据后，可以点击后面的 Graph 查看监控图形，如图-11 所示。



图-11

4. 案例 4：自定义 Zabbix 监控项目

• 问题

沿用练习二，使用 Zabbix 实现自定义监控，实现以下目标：监控 Linux 服务器系统账户的数量。

• 方案

需要使用 Zabbix 自定义 key 的方式实现自定义监控，参考如下操作步骤：

- 1) 创建自定义 key
- 2) 创建监控项目
- 3) 创建监控图形
- 4) 将监控模板关联到主机

• 步骤

实现此案例需要按照如下步骤进行。

步骤一：被监控主机创建自定义 key (在 192.168.2.100 操作)

1) 创建自定义 key

自定义 key 语法格式为：UserParameter=自定义 key 名称, 命令。

自定义的 key 文件一般存储在 /usr/local/etc/zabbix_agentd.conf.d/ 目录, 这里还需要修改 zabbix_agentd.conf 文件, 允许自定义监控 key, 来读取该目录下的所有文件。

```
[root@zabbixclient_web1 ~]# vim /usr/local/etc/zabbix_agentd.conf
Include=/usr/local/etc/zabbix_agentd.conf.d/           //加载配置文件目录
[root@zabbixclient_web1 ~]# cd /usr/local/etc/zabbix_agentd.conf.d/
[root@zabbixclient_web1 zabbix_agentd.conf.d]# vim count.line.passwd
UserParameter=count.line.passwd,wc -l /etc/passwd | awk ' {print $1} '
////自定义 key 语法格式:
//UserParameter=自定义 key 名称,命令
```

2) 测试自定义 key 是否正常工作

```
[root@zabbixclient_web1 ~]# killall zabbix_agentd
[root@zabbixclient_web1 ~]# zabbix_agentd                // 重启
agent 服务
[root@zabbixclient_web1 ~]# zabbix_get -s 127.0.0.1 -k count.line.passwd
21
```

注意：如 zabbix_get 命令执行错误, 提示 Check access restrictions in Zabbix agent configuration, 则需要检查 agent 配置文件是否正确：

```
[root@zabbixclient_web1 ~]# vim /usr/local/etc/zabbix_agentd.conf
Server=127.0.0.1,192.168.2.5
ServerActive=127.0.0.1,192.168.2.5
```

步骤二：创建监控模板

模板、应用集与监控项目的关系图, 参考图-12 所示

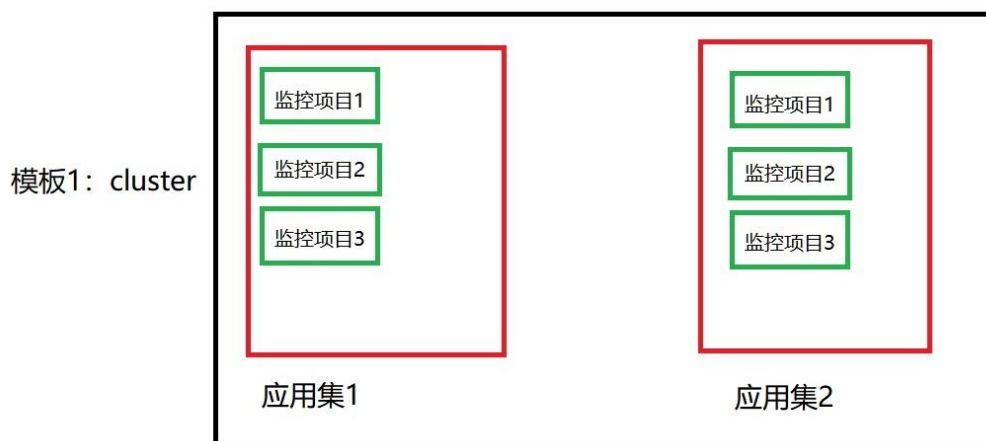


图-12

1) 添加监控模板

登录 Zabbix Web 监控控制台，通过 Configuration(配置)-->Template(模板)->Create template(创建模板)，填写模板名称，新建模板群组，如图-13 所示。

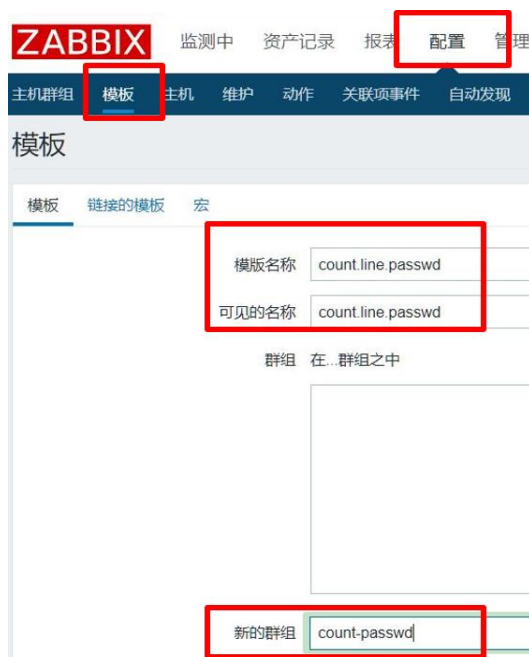


图-13

创建模板后，默认模板中没有任何应用、项目、触发器、图形等，如图-14 所示。

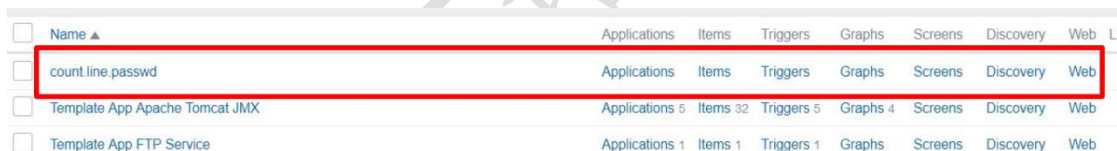


图-14

2) 创建应用

创建完成模板后，默认模板中没有任何应用、项目、触发器、图形等资源。这里需要点击模板后面的 Application（应用集）链接打开创建应用的页面，如图-15 所示。



图-15

点击 Application（应用集）后，会刷新出图-16 所示页面，在该页面中点击 Create application（创建应用集）按钮。



图-16

设置应用名称如图-17 所示。

图-17

3) 创建监控项目 item (监控项)

与创建应用一样，在模板中还需要创建监控项目，如图-18 所示，并在刷新出的新页面中选择 Create items (创建监控项) 创建项目，如图-19 所示。

Name ▲	Applications	Items	Triggers	Graphs
count.line.passwd	Applications 1	Items	Triggers	Graphs
Template App Apache Tomcat JMX	Applications 5	Items 32	Triggers 5	Graphs 4

图-18



图-19

接下来，还需要给项目设置名称及对应的自定义 key，如图-20 所示。

图-20

4) 创建图形

为了后期可以通过图形的方式展示监控数据，还需要在模板中创建图形，设置方法与前面的步骤一致，在监控模板后面点击 Graph (图形) 即可创建图形，设置监控图形基于什么监控数据，如图-21 所示。

名称: count_line_passwd_graph

宽: 900

高: 200

图形类别: 正常

查看图例: ☒

查看工作时间: ☒

查看触发器: ☒

监控项名称: 1: count.line.passwd: count_line_passwd_item

添加

取消

图-21

5) 将模板链接到被监控主机

将完整的监控模板制作完成后, 就可以将模板链接到主机实现监控功能了。首先找到被监控主机 Configuration (配置) --> Hosts (主机), 如图-22 所示。



图-22

点击需要的被监控主机链接, 打开监控主机设置页面, 在 Template (模板) 页面中选择需要链接到该主机的模板, 在此选择刚刚创建的模板 count_line_passwd 添加即可, 如图-23 所示。

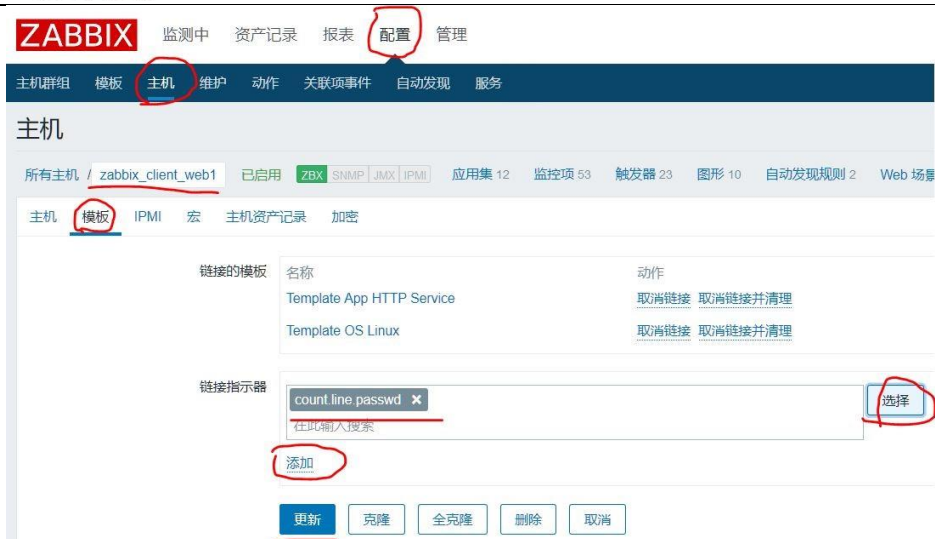


图-23

6) 查看监控数据图形

点击 Monitoring (监控中) --> Craphs (图形), 根据需要选择条件, 查看监控图形, 如图-24 和图-25 所示。



图-24



图-25