**[Top](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/SECURITY/DAY01/CASE/01/index.html" \l "page_top_case)**

# NSD SECURITY DAY01

1. **[案例1：常用系统监控命令](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/SECURITY/DAY01/CASE/01/index.html" \l "case1)**

**监控的目的**

**报告系统运行状况**

**每一部分必须同时监控**

**内容包括吞吐量，反应时间，使用率等**

**提前发现问题**

**进行服务器性能调整前，知道调整什么**

**找出系统的瓶颈在什么地方**

**监控的资源类别**

**公开数据**

**Web,FTP,SSH，数据库等应用服务**

**TCP或UDP端口**

**私有数据**

**CPU,内存，磁盘，网卡流量等使用信息**

**用户，进程等运行信息**

**自动化监控系统**

**Cacti**

**基于SNMP协议的监控软件，强大的绘图能力**

**Nagios**

**基于Agent监控，强大的状态检查与报警机制**

**插件极多，自己写监控脚本潜入到Nagios非常方便**

**Zabbix**

**基于多种监控机制，支持分布式监控**

1. **[案例2：部署Zabbix监控平台](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/SECURITY/DAY01/CASE/01/index.html" \l "case2)**

**Zabbix简绍**

**Zabbix是一个高度集成的监控解决方案**

**可以实现企业级的开源分布式监控**

**Zabbix通过C/S模式采用监控数据**

**Zabbix通过B/S模式实现web管理**

**监控拓扑**

**监控服务器**

**监控服务器开源通过SNMP或Agent采集数据**

**数据可以写入MYSQL，Oracle等数据库中**

**服务器使用LNMP实现web前端管理**

**被监控主机**

**被监控主机需要安装Agent**

**常见的网络设备一般支持SNMP**

**步骤**

**1部署LNMP环境**

**包［yuu -y install gcc pcre-devel zlib-devel openssl-devel php php-mysql php-fpm mariadb mariadb-devel mariadb-server]**

**解包　配置　编译　安装**

**修改nginx配置 inclued fastcgi.conf;**

**启服务nginx mariadb php-fpm**

**2部署Zabbix**

**依赖包**

**［yum -y install net-snmp-devel curl-devel libevent-devel］**

**安装源码**

**]#./configure --enable-server --enable-proxy --enable-agent --with-mysql=/usr/bin/mysql\_config --with-net-snmp --with-libcurl**

**/usr/local/etc //配置路径**

**/usr/local/bin //使用命令**

**/usr/local/sbin //启动程序**

**3初始化准备**

**创建数据存储的库，允许字符集中文，表及连接用户(授权)**

**拷贝网页页面并修改权限递归修改777**

**修改nginx运行配置，满足zabbix页面的要求**

**Fastcgi\_buffers 8 16k; //缓存php生成的页面内 容８个16k**

**Fastcgi\_buffer\_size 35k; //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**

**启服务**

**安装依赖的软件包**

**Php-gd php-xml php-ldap php-bcmath php-mbstring**

**修改php进程的运行配置**

**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**

**启服务**

**初始化配置**

**Htpp://192.168.2.5/index.php**

**Cat /usr/local/nginx/html/conf/zabbix.conf.php**

**4启动zabbix\_server服务**

**修改服务配置文件(/usr/local/etc/zabbix\_server.conf)**

**DBHost=localhost //数据库主机**

**DBName=zabbix //设置数据库用户**

**DBUser=zabbix //设置数据库账号**

**DBPassword=zabbix //设置数据库密码**

**LogFile=/tmp/zabbix\_server.log //设置日志**

**创建用户zabbix**

**启动zabbix\_server服务查看端口**

**5配置监控服务器**

**监控配置**

**配置被监控客服端**

**依赖包　gcc pcre-deve**

**./configure --enable-agent 客服端服务 make install**

**/usr/local/etc/zabbix\_agent.conf**

**Server=127.0.0.1,192.168.2.5 //允许访问服务地址 列表**

**ServerActive=192.168.2.5:10051//监控服务器ip地 址**

**LogFile=/tmp/zabbix\_ahent.log //日志文件**

**Useradd zabbix**

**运行zabbix\_agent服务 启动服务**

**配置监控服务器**

**Web页面配置**

**添加监控主机**

**选择监控模板**

**查看监控数据**

**自定义监控(在被监控的主机定义命令给监控服务器用)**

**配置客服端**

**/usr/local/etc/zabbix\_zgent.conf**

**UnsafeUserParameters //启用自定义命令设置**

**Lnclude=/usr/local/etc/zabbix\_agent.conf.d/ //加载配置文件目录(指定自定义命令文件路径)**

**创建自定义key**

**vim /usr/local/etc/zabbix\_agent.conf.d/count.line. Passwd.conf(文件名自定义)**

**UserParameter=count.line.passwd(自定义 名),wc -l /etc/passwd | awk ‘{print $1}’**

**重启zabbix\_agent服务**

**配置监控服务器**

**在web页面操作**

**创建的监控模板　Atmp**

**应用集 monuser(建文件夹，文件夹存放不同的监控 资源信息)**

**创建监控项　对应命令　count.line.passwd**

**监控主机时使用新创建的监控模板Atmp**

**查看监控数据**

1. **[案例3：配置及使用Zabbix监控系统](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/SECURITY/DAY01/CASE/01/index.html" \l "case3)**
2. **[案例4：自定义Zabbix监控项目](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201904/SECURITY/DAY01/CASE/01/index.html" \l "case4)**

## **1 案例1：常用系统监控命令**

### **1.1 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：

* 查看内存信息
* 查看交换分区信息
* 查看磁盘信息
* 查看CPU信息
* 查看网卡信息
* 查看端口信息
* 查看网络连接信息

### **1.2 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。

### **1.3 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

1. **[**root@proxy **~]**# free                                     //查看内存信息
2. total used free shared buff**/**cache available
3. Mem**:** **16166888** **8017696** **720016** **106504** **7429176** **7731740**
4. Swap**:** **4194300** **218268** **3976032**
5. **[**root@proxy **~]**# free **|** awk '/Mem/{print $4}'                //查看剩余内存容量
6. **720928**
7. **[**root@proxy **~]**# swapon **-**s                                //查看交换分区信息
8. 文件名                类型            大小        已用        权限
9. /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

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

2）查看CPU平均负载

1. **[**root@proxy **~]**# uptime                             //查看CPU负载（1，5，15分钟）
2. **23:54:12** up **38** days**,** **14:54,** **9** users**,** load average**:** **0.00,** **0.04,** **0.05**
3. **[**root@proxy **~]**# uptime **|**awk '{print $NF}'            //仅查看CPU的15分钟平均负载
4. **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

1. **[**root@proxy **~]**# ifconfig eth0
2. eth0**:** flags**=4163<**UP**,**BROADCAST**,**RUNNING**,**MULTICAST**>** mtu **1500**
3. inet **192.168.4.5** netmask **255.255.255.0** broadcast **172.25.0.255**
4. inet6 fe80**::5054:**ff**:**fe00**:**b prefixlen **64** scopeid **0x20<**link**>**
5. ether **52:54:00:00:00:**0b txqueuelen **1000** **(**Ethernet**)**
6. RX packets **62429** bytes **10612049** **(10.1** MiB**)**
7. RX errors **0** dropped **0** overruns **0** frame **0**
8. TX packets **5674** bytes **4121143** **(3.9** MiB**)**
9. TX errors **0** dropped **0** overruns **0** carrier **0** collisions **0**
10. **[**root@proxy **~]**# ifconfig eth0 **|**awk '/inet /{print $2}'        //查看IP地址信息
11. **192.168.4.5**
12. **[**root@proxy **~]**# ifconfig eth0 **|**awk '/RX p/{print $5}'        //网卡接受数据包流量
13. **10625295**
14. **[**root@proxy **~]**# ifconfig eth0 **|**awk '/TX p/{print $5}'        //网卡发送数据包流量
15. **4130821**

2）查看端口信息

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

3）查看网络连接信息

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

## **2 案例2：部署Zabbix监控平台**

### **2.1 问题**

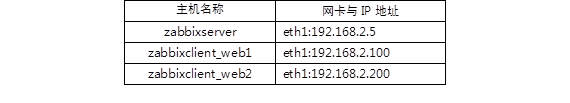
本案例要求部署一台Zabbix监控服务器，一台被监控主机，为进一步执行具体的监控任务做准备：

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

### **2.2 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



### **2.3 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。

1. **[**root@zabbixserver **~]**# yum **-**y install gcc pcre**-**devel openssl**-**devel
2. **[**root@zabbixserver **~]**# tar **-**xf nginx**-1.12.2.**tar**.**gz
3. **[**root@zabbixserver **~]**# cd nginx**-1.12.2**
4. **[**root@zabbixserver nginx**-1.12.2]**# **./**configure **--with-**http\_ssl\_module
5. **[**root@zabbixserver nginx**-1.12.2]**# make **&&** make install
6. **[**root@zabbixserver **~]**# yum **-**y install php php**-**mysql **\**
7. **>** mariadb mariadb**-**devel mariadb**-**server
8. **[**root@zabbixserver **~]**# yum **-**y install php**-**fpm**-5.4.16-42.**el7**.**x86\_64**.**rpm
9. //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。

1. **[**root@zabbixserver **~]**# vim **/**usr**/**local**/**nginx**/**conf**/**nginx**.**conf
2. … …
3. http**{**
4. … …
5. fastcgi\_buffers **8** 16k**;**                 //缓存php生成的页面内容，8个16k
6. fastcgi\_buffer\_size 32k**;**                 //缓存php生产的头部信息
7. fastcgi\_connect\_timeout **300;**             //连接PHP的超时时间
8. fastcgi\_send\_timeout **300;**                 //发送请求的超时时间
9. fastcgi\_read\_timeout **300;**                     //读取请求的超时时间
10. location **~** **\.**php$ **{**
11. root html**;**
12. fastcgi\_pass **127.0.0.1:9000;**
13. fastcgi\_index index**.**php**;**
14. include fastcgi**.**conf**;**
15. **}**
16. … …

3）启动服务

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

1. **[**root@zabbixserver **~]**# systemctl start mariadb
2. **[**root@zabbixserver **~]**# systemctl start php**-**fpm
3. **[**root@zabbixserver **~]**# ln **-**s **/**usr**/**local**/**nginx**/**sbin**/**nginx **/**sbin**/**nginx
4. **[**root@zabbixserver **~]**# nginx
5. **[**root@zabbixserver **~]**# firewall**-**cmd **--**set**-default-**zone**=**trusted
6. **[**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。

1. **[**root@zabbixserver **~]**# cat **/**usr**/**local**/**nginx**/**html**/**test**.**php
2. **<?**php
3. $i**=33;**
4. echo $i**;**
5. **?>**
6. **[**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。

1. **[**root@zabbixserver lnmp\_soft**]**# yum **-**y install net**-**snmp**-**devel **\**
2. **>** curl**-**devel
3. //安装相关依赖包
4. **[**root@zabbixserver lnmp\_soft**]**# yum **-**y install **\**
5. **>** libevent**-**devel**-2.0.21-4.**el7**.**x86\_64**.**rpm
6. //注意libevent-devel这个软件包在lnmp\_soft目录下有提供
7. **[**root@zabbixserver lnmp\_soft**]**# tar **-**xf zabbix**-3.4.4.**tar**.**gz
8. **[**root@zabbixserver lnmp\_soft**]**# cd zabbix**-3.4.4/**
9. **[**root@zabbixserver zabbix**-3.4.4]**# **./**configure **--**enable**-**server **\**
10. **>** **--**enable**-**proxy **--**enable**-**agent **--with-**mysql**=**/usr/bin**/**mysql\_config **\**
11. **>** **--with-**net**-**snmp **--with-**libcurl
12. // --enable-server安装部署zabbix服务器端软件
13. // --enable-agent安装部署zabbix被监控端软件
14. // --enable-proxy安装部署zabbix代理相关软件
15. // --with-mysql配置mysql\_config路径
16. // --with-net-snmp允许zabbix通过snmp协议监控其他设备
17. // --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
18. **[**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

1. **[**root@zabbixserver **~]**# mysql
2. mysql**>** create database zabbix character set utf8**;**
3. //创建数据库，支持中文字符集
4. mysql**>** grant all on zabbix**.\*** to zabbix@'localhost' identified by 'zabbix'**;**
5. //创建可以访问数据库的账户与密码
6. **[**root@zabbixserver **~]**# cd lnmp\_soft**/**zabbix**-3.4.4/**database**/**mysql**/**
7. **[**root@zabbixserver mysql**]**# mysql **-**uzabbix **-**pzabbix zabbix **<** schema**.**sql
8. **[**root@zabbixserver mysql**]**# mysql **-**uzabbix **-**pzabbix zabbix **<** images**.**sql
9. **[**root@zabbixserver mysql**]**# mysql **-**uzabbix **-**pzabbix zabbix **<** data**.**sql
10. //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
11. //使用mysql导入这些数据即可（注意导入顺序）

上线Zabbix的Web页面

1. **[**root@zabbixserver **~]**# cd lnmp\_soft**/**zabbix**-3.4.4/**frontends**/**php**/**
2. **[**root@zabbixserver php**]**# cp **-**r **\*** /usr/local**/**nginx**/**html**/**
3. **[**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

1. **[**root@zabbixserver **~]**# vim **/**usr**/**local**/**etc**/**zabbix\_server**.**conf
2. DBHost**=**localhost
3. //数据库主机，默认该行被注释
4. DBName**=**zabbix
5. //设置数据库名称
6. DBUser**=**zabbix
7. //设置数据库账户
8. DBPassword**=**zabbix
9. //设置数据库密码，默认该行被注释
10. LogFile**=**/tmp/zabbix\_server**.**log
11. //设置日志，仅查看以下即可
12. **[**root@zabbixserver **~]**# useradd **-**s **/**sbin**/**nologin zabbix
13. //不创建用户无法启动服务
14. **[**root@zabbixserver **~]**# zabbix\_server                 //启动服务
15. **[**root@zabbixserver **~]**# ss **-**ntulp **|**grep zabbix\_server //确认连接状态，端口10051
16. 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

1. **[**root@zabbixserver **~]**# vim **/**usr**/**local**/**etc**/**zabbix\_agentd**.**conf
2. Server**=127.0.0.1,192.168.2.5**                    //允许哪些主机监控本机
3. 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
4. Hostname**=**zabbix\_server                        //设置本机主机名
5. LogFile**=**/tmp/zabbix\_server**.**log                    //设置日志文件
6. UnsafeUserParameters**=1**                        //是否允许自定义key
7. **[**root@zabbixserver **~]**# zabbix\_agentd            //启动监控agent
8. **[**root@zabbixserver **~]**# ss **-**ntulp **|**grep zabbix\_agentd //查看端口信息为10050
9. tcp LISTEN **0** **128** **\*: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

1. **[**root@zabbixserver **~]**# firefox http**:**//192.168.2.5/index.php
2. //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
3. //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。

1. **[**root@zabbixserver **~]**# yum **-**y install php**-**gd php**-**xml
2. **[**root@zabbixserver **~]**# yum install php**-**bcmath**-5.4.16-42.**el7**.**x86\_64**.**rpm
3. **[**root@zabbixserver **~]**# yum install php**-**mbstring**-5.4.16-42.**el7**.**x86\_64**.**rpm
4. **[**root@zabbixserver **~]**# vim **/**etc**/**php**.**ini
5. date**.**timezone **=** Asia**/**Shanghai                //设置时区
6. max\_execution\_time **=** **300**                    //最大执行时间，秒
7. post\_max\_size **=** 32M                        //POST数据最大容量
8. max\_input\_time **=** **300**                        //服务器接收数据的时间限制
9. memory\_limit **=** 128M                        //内存容量限制
10. **[**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

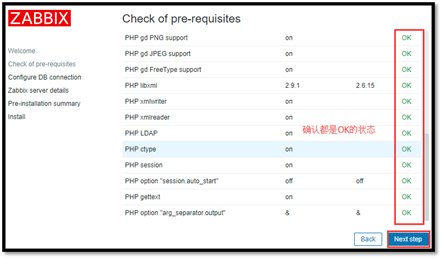


图-2

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。

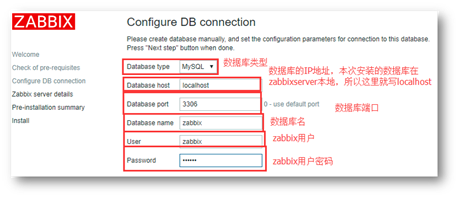


图-3

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。

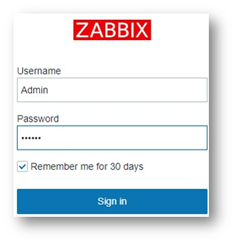


图-4

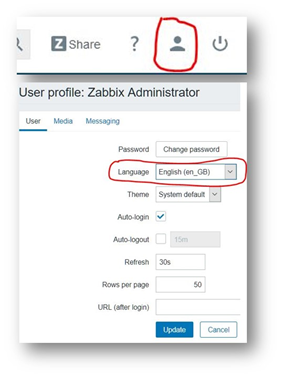


图-5

**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）。

1. **[**root@zabbixclient\_web1 **~]**# useradd **-**s **/**sbin**/**nologin zabbix
2. **[**root@zabbixclient\_web1 **~]**# yum **-**y install gcc pcre**-**devel
3. **[**root@zabbixclient\_web1 **~]**# tar **-**xf zabbix**-3.4.4.**tar**.**gz
4. **[**root@zabbixclient\_web1 **~]**# cd zabbix**-3.4.4/**
5. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# **./**configure **--**enable**-**agent
6. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# make **&&** make install

2）修改agent配置文件，启动Agent

1. **[**root@zabbixclient\_web1 **~]**# vim **/**usr**/**local**/**etc**/**zabbix\_agentd**.**conf
2. Server**=127.0.0.1,192.168.2.5**                //谁可以监控本机（被动监控模式）
3. ServerActive**=127.0.0.1,192.168.2.5**            //谁可以监控本机（主动监控模式）
4. Hostname**=**zabbixclient\_web1                 //被监控端自己的主机名
5. EnableRemoteCommands**=1**
6. //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
7. UnsafeUserParameters**=1**                     //是否允许自定义key监控
8. **[**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。

1. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# cd misc**/**init**.**d**/**fedora**/**core
2. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# cp zabbix\_agentd **/**etc**/**init**.**d**/**
3. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# /etc/init**.**d**/**zabbix\_agentd start
4. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# /etc/init**.**d**/**zabbix\_agentd stop
5. **[**root@zabbixclient\_web1 zabbix**-3.4.4]**# /etc/init**.**d**/**zabbix\_agentd status
6. **[**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**

### **3.1 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

### **3.2 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。

### **3.3 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。

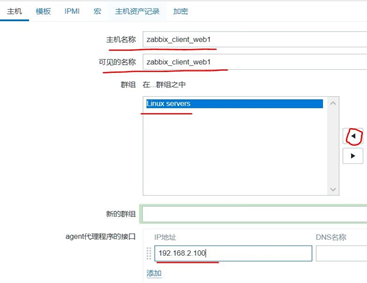


图-8

**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。



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。

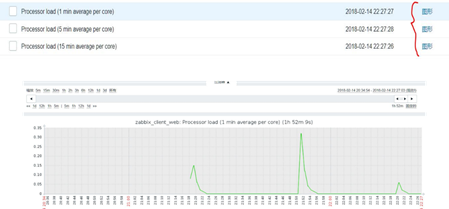


图-11

## **4 案例4：自定义Zabbix监控项目**

### **4.1 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。

### **4.2 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

### **4.3 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 。

1. **[**root@zabbixclient\_web1 **~]**# vim **/**usr**/**local**/**etc**/**zabbix\_agentd**.**conf
2. Include**=**/usr/local**/**etc**/**zabbix\_agentd**.**conf**.**d**/**                //加载配置文件目录
3. **[**root@zabbixclient\_web1 **~]**# cd **/**usr**/**local**/**etc**/**zabbix\_agentd**.**conf**.**d**/**
4. **[**root@zabbixclient\_web1 zabbix\_agentd**.**conf**.**d**]**# vim count**.**line**.**passwd
5. UserParameter**=**count**.**line**.**passwd**,**wc **-**l **/**etc**/**passwd **|** awk ' {print $1} '
6. ////自定义key语法格式:
7. //UserParameter=自定义key名称,命令

2）测试自定义key是否正常工作

1. **[**root@zabbixclient\_web1 **~]**# killall zabbix\_agentd
2. **[**root@zabbixclient\_web1 **~]**# zabbix\_agentd                                //重启agent服务
3. **[**root@zabbixclient\_web1 **~]**# zabbix\_get **-**s **127.0.0.1** **-**k count**.**line**.**passwd
4. **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：

1. **[**root@zabbixclient\_web1 **~]**# vim **/**usr**/**local**/**etc**/**zabbix\_agentd**.**conf
2. Server**=127.0.0.1,192.168.2.5**
3. 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

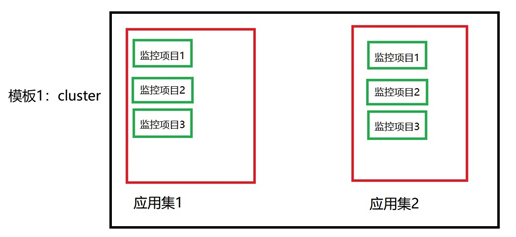


图-12

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。

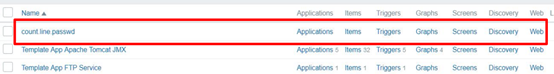


图-14

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。

IMG_270

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。

IMG_271

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。



图-18

IMG_274

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。

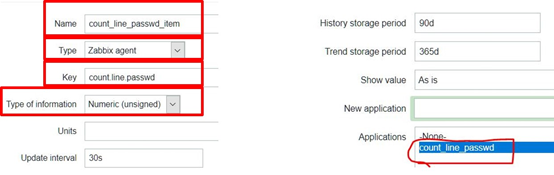


图-20

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。



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。

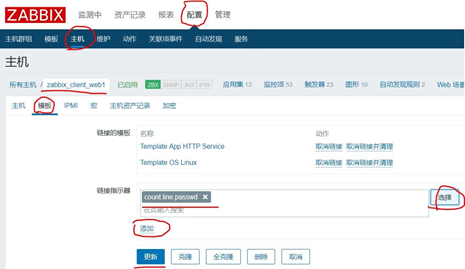


图-23

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-25