Netkiller Linux Monitoring 手札

Monitoring, Scanner, Sniffer and Audit...

Mr. Neo Chan, 陈景峰(BG7NYT)

中国广东省深圳市宝安区龙华镇溪山美地
518109
+86 755 29812080
+86 755 29812080
<openunix@163.com>

文档出处: http://netkiller.sourceforge.net/ | http://netkiller.github.com

文档最近一次更新于 Wed Dec 7 08:55:29 UTC 2011

2010-11-18

下面是我多年积累下来的经验总结，整理成文档供大家参考:

Netkiller Architect 手札	Netkiller Linux 手札	Netkiller Developer 手札	Netkiller Database 手札
Netkiller Debian 手札	Netkiller CentOS 手札	Netkiller FreeBSD 手札	Netkiller Shell 手札
Netkiller Web 手札	Netkiller Monitoring 手札	Netkiller Storage 手札	Netkiller Mail System 手札
Netkiller PostgreSQL 手札	Netkiller MySQL 手札	Netkiller LDAP 手札	Netkiller Security 手札
Netkiller Intranet 手札	Netkiller Cisco IOS 手札	Netkiller Writer 手札	Netkiller Version 手札
Netkiller Studio Linux 手札			

目录

下一页
自述

自述

目录

1. 内容简介

当前文档档容比较杂，涉及内容广泛。

慢慢我会将其中章节拆成新文档.

文档内容简介:

1. Network
2. Security
3. Web Application
4. Database
5. Storage And Backup/Restore
6. Cluster
7. Developer

1.1. Audience(读者对象)

This book is intended primarily for Linux system administrators who are familiar with the following activities:

Audience

1. Linux system administration procedures, including kernel configuration
2. Installation and configuration of cluster, such as load balancing, High Availability,
3. Installation and configuration of shared storage networks, such as Fibre Channel SANs
4. Installation and configuration of web server, such as apache, nginx, lighttpd, tomcat/resin ...

本文档的读者对象:

文档面向有所有读者。您可以选读您所需要的章节,无需全篇阅读,因为有些章节不一定对你有用,用得着就翻来看看,暂时用不到的可以不看.

大体分来读者可以分为几类:

1. 架构工程师
2. 系统管理员
3. 系统支持,部署工程师

不管是谁,做什么的,我希望通过阅读这篇文档都能对你有所帮助。

1.2. 写给读者

欢迎提出宝贵的建议,如有问题请到 邮件列表 讨论

为什么写这篇文章

有很多想法,工作中也用不到所以未能实现，所以想写出来,和大家分享.有一点写一点,写得也不好,只要能看懂就行,就当学习笔记了.

开始零零碎碎写过一些文档，也向维基百科供过稿，但维基经常被ZF封锁，后来发现sf.net可以提供主机存放文档，便做了迁移。并开始了我的写作生涯。

这篇文档是作者8年来对工作的总结,是作者一点一滴的积累起来的，有些笔记已经丢失，所以并不完整。

因为工作太忙整理比较缓慢。目前的工作涉及面比较窄所以新文档比较少。

我现在花在技术上的时间越来越少，兴趣转向摄影，无线电。也想写写摄影方面的心得体会。

写作动力:

曾经在网上看到外国开源界对中国的评价，中国人对开源索取无度，但贡献却微乎其微.这句话一直记在我心中，发誓要为中国开源事业做我仅有的一点微薄贡献

另外写文档也是知识积累，还可以增加在圈内的影响力.

人跟动物的不同,就是人类可以把自己学习的经验教给下一代人.下一代在上一代的基础上再创新,不断积累才有今天.

所以我把自己的经验写出来,可以让经验传承

没有内容的章节:

目前我自己一人维护所有文档，写作时间有限，当我发现一个好主题就会加入到文档中，待我有时间再完善章节，所以你会发现很多章节是空无内容的.

文档目前几乎是流水帐试的写作，维护量很大，先将就着看吧.

我想到哪写到哪,你会发现文章没一个中心,今天这里写点,明天跳过本章写其它的.
文中例子绝对多,对喜欢复制然后粘贴朋友很有用,不用动手写,也省时间.
理论的东西,网上大把,我这里就不写了,需要可以去网上查.
我爱写错别字,还有一些是打错的,如果发现请指正.
文中大部分试验是在Debian/Ubuntu/Redhat AS上完成.

1.3. 获得文档

1.3.1. PDF

Download PDF Document 下载PDF文档1

Download PDF Document 下载PDF文档2

1.3.2. EPUB

http://netkiller.sourceforge.net/technology.html

1.3.3. 获得光盘介质

如有特别需要，请联系我

---

2. 作者简介

主页地址：http://netkiller.sourceforge.net, http://netkiller.github.com/

陈景峰 (ㄔㄣˊ ㄐㄧㄥˇ ㄈㄥ)

Nickname：netkiller | English name: Neo chen | Nippon name: ちんけいほう (音訳) | Korean name: | Thailand name:

IT民工， UNIX like Evangelist, 业余无线电爱好者（呼号：BG7NYT）,户外运动以及摄影爱好者。

《PostgreSQL实用实例参考》，《Postfix 完整解决方案》，《Netkiller Linux 手札》的作者

2001年来深圳进城打工,成为一名外来务工者.

2002年我发现不能埋头苦干,埋头搞技术是不对的,还要学会"做人".

2003年这年最惨,公司拖欠工资16000元,打过两次官司2005才付清.

2004年开始加入分布式计算团队,目前成绩

2004-10月开始玩户外和摄影

2005-6月成为中国无线电运动协会会员

2006年单身生活了这么多年,终于找到归宿.

2007物价上涨,金融危机，休息了4个月（其实是找不到工作）

2008终于找到英文学习方法，， 《Netkiller Developer 手札》，《Netkiller Document 手札》

2008-8-8 08:08:08 结婚,后全家迁居湖南省常德市

2009《Netkiller Database 手札》,年底拿到C1驾照

2010对电子打击乐产生兴趣，计划学习爵士鼓

2011 职业生涯路上继续打怪升级

2.1. 联系作者

Mobile: +86 13113668890

Tel: +86 755 2981-2080

Callsign: BG7NYT QTH: Shenzhen, China

注：请不要问我安装问题!

E-Mail: openunix@163.com
IRC irc.freenode.net #ubuntu / #ubuntu-cn

Yahoo: bg7nyt
ICQ: 101888222
AIM: bg7nyt

TM/QQ: 13721218
MSN: netkiller@msn.com
G Talk: 很少开
网易泡泡：很少开

写给火腿:

欢迎无线电爱好者和我QSO,我的QTH在深圳宝安区龙华镇溪山美地12B7CD,设备YAESU FT-50R,FT-60R,FT-7800 144-430双段机,拉杆天线/GP天线 Nagoya MAG-79EL-3W/Yagi

如果这篇文章对你有所帮助,请寄给我一张QSL卡片,qrz.cn or qrz.com or hamcall.net

Personal Amateur Radiostations of P.R.China

ZONE CQ24 ITU44 ShenZhen, China

Best Regards, VY 73! OP. BG7NYT

---

3. 支持这个项目(Support this project)

Donations

招商银行(China Merchants Bank) 陈景峰 9555500000007459

第 1 章 sys & proc

摘要

目录

1. /sys

1.1. /sys/class/net/

```
$ cat /sys/class/net/eth0/statistics/rx_bytes
$ cat /sys/class/net/eth0/statistics/tx_bytes
```

2. /proc

第 2 章 System Utility

目录

1. User

1.1. last, lastb - show listing of last logged in users

```
[neo@linux ~]$ last reboot
reboot   system boot  2.6.18-164.15.1. Wed Apr 28 23:43         (6+21:31)
reboot   system boot  2.6.18-164.15.1. Fri Apr 16 04:07         (12+19:23)
reboot   system boot  2.6.18-164.15.1. Fri Apr 16 02:19          (01:46)
reboot   system boot  2.6.18-164.el5   Thu Apr 15 18:52          (07:25)

wtmp begins Thu Apr 15 18:52:15 2010
```

2. Memory

2.1. Memory

free - Display amount of free and used memory in the system

```
$ free
             total       used       free     shared    buffers     cached
Mem:       2053440     522028    1531412          0      87076     265952
-/+ buffers/cache:     169000    1884440
Swap:      2441840          0    2441840
```

5秒监控一次

```
neo@neo-OptiPlex-780:~/workspace/Document$ free -s 5
             total       used       free     shared    buffers     cached
Mem:       2054224    1708876     345348          0      58908     696404
-/+ buffers/cache:     953564    1100660
Swap:      2077692      81948    1995744

             total       used       free     shared    buffers     cached
Mem:       2054224    1708876     345348          0      58908     696404
-/+ buffers/cache:     953564    1100660
Swap:      2077692      81948    1995744

             total       used       free     shared    buffers     cached
Mem:       2054224    1709000     345224          0      58908     696404
-/+ buffers/cache:     953688    1100536
Swap:      2077692      81948    1995744
```

2.2. vmstat - Report virtual memory statistics

vmstat

```
# vmstat
procs -----------memory---------- ---swap-- -----io---- --system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in    cs us sy id wa
 0  0      0 203668  53352 2878928    0    0     0     2    4     6  0  0 100  0
```

```
procs:
r               ;在运行队列中等待的进程数
b               ;在等待io的进程数
w               ;可以进入运行队列但被替换的进程

memoy
swap    ;现时可用的交换内存（k表示）
free    ;空闲的内存（k表示）

pages
re          回收的页面
mf          非严重错误的页面
pi          进入页面数（k表示）
po          出页面数（k表示）
fr          空余的页面数（k表示）
de          提前读入的页面中的未命中数
sr          通过时钟算法扫描的页面

disk 显示每秒的磁盘操作。 s表示scsi盘，0表示盘号

fault 显示每秒的中断数
in          设备中断
```

```
sy         系统中断
cy         cpu交换

cpu 表示cpu的使用状态
cs         用户进程使用的时间
sy         系统进程使用的时间
id         cpu空闲的时间
```

```
$ vmstat 1
procs -----------memory---------- ---swap-- -----io---- -system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa
 2  0      0 2692472 347884 442576    0    0     0    54   11    7 99  1  0  0
 2  0      0 2692420 347884 442600    0    0     0     0    6   87 100  0  0  0
 2  1      0 2692320 347884 442600    0    0     0  2568   26  121 100  0  0  0
 2  0      0 2687872 347884 442600    0    0     0    72   28  129 100  1  0  0
 2  0      0 2684716 347884 442600    0    0     0     0   16   91 100  0  0  0
 2  0      0 2680528 347884 442600    0    0     0     0   12   88 100  1  0  0

vmstat 参数详解

procs:
r-->在运行队列中等待的进程数
b-->在等待io的进程数
w-->可以进入运行队列但被替换的进程

memoy
swap-->现时可用的交换内存（k表示）
free-->空闲的内存（k表示）

pages
re——》回收的页面
mf——》非严重错误的页面
pi——》进入页面数（k表示）
po——》出页面数（k表示）
fr——》空余的页面数（k表示）
de——》提前读入的页面中的未命中数
sr——》通过时钟算法扫描的页面

disk 显示每秒的磁盘操作。 s表示scsi盘, 0表示盘号

fault 显示每秒的中断数
in——》设备中断
sy——》系统中断
cy——》cpu交换

cpu 表示cpu的使用状态
cs——》用户进程使用的时间
sy——》系统进程使用的时间
id——》cpu空闲的时间
```

2.3. mpstat

```
# mpstat -P ALL
Linux 2.6.18-194.el5 (cms)      08/30/2010

07:30:56 PM  CPU   %user   %nice    %sys %iowait    %irq   %soft  %steal   %idle
intr/s
07:30:56 PM  all    0.73    0.00    3.91    0.61    0.02    0.11    0.00   94.62
1380.14
07:30:56 PM    0    1.62    0.00    5.40    1.82    0.08    0.42    0.00   90.65
1375.30
07:30:56 PM    1    0.35    0.00    3.78    0.21    0.00    0.00    0.00   95.66
0.00
07:30:56 PM    2    0.44    0.00    2.74    0.22    0.00    0.00    0.00   96.59
0.00
07:30:56 PM    3    0.50    0.00    3.72    0.20    0.00    0.00    0.00   95.59
0.00
```

2.4. pmap - report memory map of a process

```
# pmap -d PID
```

```
[root@development ~]# pmap -d 3817
3817:   /sbin/mingetty tty3
```

```
Address           Kbytes Mode  Offset           Device    Mapping
0000000000400000      12 r-x-- 0000000000000000 008:00002 mingetty
0000000000602000       8 rw--- 0000000000002000 008:00002 mingetty
000000001b9f8000     132 rw--- 000000001b9f8000 000:00000   [ anon ]
0000003fd8200000     112 r-x-- 0000000000000000 008:00002 ld-2.5.so
0000003fd841b000       4 r---- 000000000001b000 008:00002 ld-2.5.so
0000003fd841c000       4 rw--- 000000000001c000 008:00002 ld-2.5.so
0000003fd9200000    1332 r-x-- 0000000000000000 008:00002 libc-2.5.so
0000003fd934d000    2048 ----- 000000000014d000 008:00002 libc-2.5.so
0000003fd954d000      16 r---- 000000000014d000 008:00002 libc-2.5.so
0000003fd9551000       4 rw--- 0000000000151000 008:00002 libc-2.5.so
0000003fd9552000      20 rw--- 0000003fd9552000 000:00000   [ anon ]
00002ba6fbb68000       8 rw--- 00002ba6fbb68000 000:00000   [ anon ]
00002ba6fbb7d000       8 rw--- 00002ba6fbb7d000 000:00000   [ anon ]
00007fff2ba17000      84 rw--- 00007ffffffea000 000:00000   [ stack ]
ffffffffff600000    8192 ----- 0000000000000000 000:00000   [ anon ]
mapped: 11984K    writeable/private: 268K    shared: 0K
```

---

3. CPU

3.1. uptime - Tell how long the system has been running.

uptime

```
# uptime
 21:26:06 up 15 days, 58 min,  1 user,  load average: 0.85, 1.16, 2.21
```

3.2. top - display Linux tasks

5 秒监控一次

```
top -d 5
```

4. Processes

4.1. strace - trace system calls and signals

```
$ strace -f -F lighttpd
```

4.2. lsof - list open files

```
$ sudo lsof -c lighttpd
```

4.2.1. 谁打开了该文件

显示打开文件filename的进程

```
lsof filename
```

4.2.2. 谁在占用端口

什么程序运行在22端口上

```
lsof -i :22
```

4.2.3. 该进程打开了那些文件

显示httpd进程现在打开的文件

```
lsof -c httpd
```

-p 进程ID

```
pgrep httpd
lsof -p 1782
```

5. IO

5.1. input/output statistics

```
$ sudo apt-get install sysstat
```

iostat

```
$ iostat
Linux 2.6.24-21-generic (netkiller)     Thursday, December 04, 2008

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.57    0.03    0.14    0.41    0.00   98.85

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               6.45       132.69        68.33     595116     306456
sda1              0.00         0.00         0.00       1606         58
sda2              0.00         0.00         0.00        820          0
sda3              2.20         1.16        17.27    1502618   22448752
```

sudo iostat -x 2

```
# iostat -x 1
avg-cpu: %user %nice %sys %idle
2.04 0.00 97.96 0.00
Device: rrqm/s wrqm/s r/s w/s rsec/s wsec/s rkB/s wkB/s avgrq-sz avgqu-sz await
svctm %util
/dev/sda 0.00 633.67 3.06 102.31 24.49 5281.63 12.24 2640.82 288.89 73.67 113.89
27.22 50.00

从输出我们看到w/s=102,wKB/s=2640.所以2640/102=23KB per I/O.

因此对于连续I/O系统来说我们要关注系统读取大量数据的能力即KB per request.对于随机I/O系统我们注
重IOPS值.
```

5.1.1. 5 秒监控一次

```
iostat -d 5
```

5.2. iotop

```
# yum install iotop
```

```

```

6. Network

6.1. netstat

netstat 监控TCP状态

```
#netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'
```

```
状态:                描述
CLOSED:            无连接是活动的或正在进行
LISTEN:            服务器在等待进入呼叫
SYN_RECV:          一个连接请求已经到达，等待确认
SYN_SENT:          应用已经开始，打开一个连接
ESTABLISHED: 正常数据传输状态
FIN_WAIT1:         应用说它已经完成
FIN_WAIT2:         另一边已同意释放
ITMED_WAIT: 等待所有分组死掉
CLOSING:           两边同时尝试关闭
TIME_WAIT:         另一边已初始化一个释放
LAST_ACK:          等待所有分组死掉
```

6.2. ss

```
# ss
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
CLOSE-WAIT 1      0           192.168.3.124:19644       130.75.116.209:http
CLOSE-WAIT 1      0           192.168.3.124:31289       170.224.194.69:https
CLOSE-WAIT 1      0           192.168.3.124:64903         198.20.8.241:https
CLOSE-WAIT 1      0           192.168.3.124:64902         198.20.8.241:https
CLOSE-WAIT 1      0           192.168.3.124:27528      170.224.160.205:https
CLOSE-WAIT 1      0           192.168.3.124:10152         198.20.8.241:https
CLOSE-WAIT 1      0           192.168.3.124:18263       170.224.194.69:http
CLOSE-WAIT 1      0           192.168.3.124:18262       170.224.194.69:http
CLOSE-WAIT 1      0           192.168.3.124:27792         129.89.61.70:http
CLOSE-WAIT 1      0           192.168.3.124:27595         129.89.61.70:http
CLOSE-WAIT 1      0           192.168.3.124:28970         129.89.61.70:http
CLOSE-WAIT 1      0           192.168.3.124:28158       130.75.116.210:http
CLOSE-WAIT 1      0           192.168.3.124:26186       130.75.116.210:http
CLOSE-WAIT 1      0           192.168.3.124:26185       130.75.116.210:http
CLOSE-WAIT 1      0           192.168.3.124:42563         74.125.71.99:http
CLOSE-WAIT 1      0           192.168.3.124:42564         74.125.71.99:http
CLOSE-WAIT 1      0           192.168.3.124:63459       130.75.116.202:http
CLOSE-WAIT 1      0           192.168.3.124:63458       130.75.116.202:http
ESTAB      0      0           192.168.3.124:30829         192.168.3.17:3260
ESTAB      0      0           192.168.3.124:13234         192.168.3.15:3260
ESTAB      0      0        ::ffff:192.168.3.124:ssh        ::ffff:192.168.80.5:5
2682
ESTAB      0      1960     ::ffff:192.168.3.124:ssh        ::ffff:192.168.80.5:5
2957


$ ss
State      Recv-Q Send-Q                Local Address:Port
Peer Address:Port
ESTAB      0      0                      192.168.80.1:38281
64.4.61.72:1863
ESTAB      0      0                      192.168.80.1:54504
112.95.240.77:8000
ESTAB      0      0                      192.168.80.1:14698
74.125.71.125:5222
ESTAB      0      0                      192.168.80.1:14697
74.125.71.125:5222
ESTAB      0      0                      192.168.80.1:54123
64.12.28.171:https
ESTAB      0      0                      192.168.80.1:4225
```

```
64.4.61.171:1863
ESTAB      0      0                       192.168.80.1:ssh
192.168.80.5:51291
ESTAB      0      0                ::ffff:192.168.80.1:microsoft-ds
::ffff:192.168.80.5:51094
ESTAB      0      0                       192.168.80.1:22074
205.188.1.241:https
ESTAB      0      0                       192.168.80.1:59340
64.4.34.213:1863
ESTAB      0      0                       192.168.80.1:9766
91.189.89.114:https
ESTAB      0      0                       192.168.80.1:3300
64.4.44.78:1863
```

6.3. iftop - display bandwidth usage on an interface by host

```
# yum install -y iftop
```

6.4. iptraf - Interactive Colorful IP LAN Monitor

```
[root@development ~]# yum -y install iptraf
```

6.5. nload: Console application which monitors network traffic and bandwidth

CentOS

```
# yum install nload -y
```

Ubuntu

```
# sudo apt-get install nload
```

运行监控命令

```
# nload
```

```
Device eth0 [172.16.3.90] (1/5):
================================================================================
Incoming:

                                                  Curr: 10.00 kBit/s
                                                  Avg: 103.95 kBit/s
                                                  Min: 0.00 Bit/s
             ||                                   Max: 3.23 MBit/s
             ##                                   Ttl: 1090.93 GByte
Outgoing:

                                                  Curr: 12.84 kBit/s
                                                  Avg: 15.29 kBit/s
                                                  Min: 0.00 Bit/s
                                                  Max: 206.63 kBit/s
                                                  Ttl: 48.57 GByte
```

7. Hardware

7.1. temperature/voltage/fan

lm-sensors - utilities to read temperature/voltage/fan sensors

```
$ sudo apt-get install lm-sensors
$ sudo sensors-detect
$ sensors
```

8. log

8.1. logwatch

logwatch - log analyser with nice output written in Perl

http://www.logwatch.org/

过程 2.1. logwatch 安装步骤:

1. Install

   Ubuntu 7.10

```
netkiller@shenzhen:/etc/webmin$ apt-cache search logwatch
fwlogwatch - Firewall log analyzer
logwatch - log analyser with nice output written in Perl
```

   apt-get install

```
# apt-get install logwatch
```

   the logwatch has been installed, it should create a file in '/etc/cron.daily/00logwatch'.

2. config

```
$ sudo cp /usr/share/logwatch/default.conf/logwatch.conf
/etc/logwatch/conf/logwatch.conf
$ sudo mkdir /var/cache/logwatch
$ sudo vim /etc/logwatch/conf/logwatch.conf
```

   mail to

```
# Default person to mail reports to.  Can be a local account or a
# complete email address.
MailTo = root, openunix@163.com, other@example.com
```

   To change detail level for the report

```
# The default detail level for the report.
# This can either be Low, Med, High or a number.
# Low = 0
# Med = 5
# High = 10
Detail = High
```

   Crontab

```
netkiller@shenzhen:~$ cat /etc/cron.daily/00logwatch
#!/bin/bash

#Check if removed-but-not-purged
test -x /usr/share/logwatch/scripts/logwatch.pl || exit 0
```

```
#execute
/usr/sbin/logwatch
```

3. The logwatch is command, you can run it.

logwatch --print

单独查看某个服务，比如 SSH 登录信息

logwatch --service sshd --print

8.2. nulog

例 2.1. config.php

9. Service

9.1. nfswatch

```
yum install -y nfswatch
```

```
J13-85-www                  Mon Sep 19 18:33:54 2011   Elapsed time:   00:00:30
Interval packets:    125711 (network)      61695 (to host)          0 (dropped)
Total packets:       140549 (network)      68996 (to host)          0 (dropped)
                     Monitoring packets from interface eth0
                     int   pct    total                        int   pct    total
NFS3 Read              0    0%        0 TCP Packets          61688  100%    68973
NFS3 Write             0    0%        0 UDP Packets              0    0%        1
NFS Read               0    0%        0 ICMP Packets             0    0%        0
NFS Write              0    0%        0 Routing Control          0    0%        0
NFS Mount              0    0%        0 Addr Resolution          0    0%        3
Port Mapper            0    0%        0 Rev Addr Resol           0    0%        0
RPC Authorization  59257   96%    66197 Ether/FDDI Bdcst         0    0%        3
Other RPC Packets      1    0%        5 Other Packets            7    0%       19
                                  0 file systems
     File Sys        int   pct    total      File Sys        int   pct    total
```

9.2. apachetop

```
# yum install apachetop -y
```

```
# apachetop
last hit: 00:00:00          atop runtime:  0 days, 00:00:00              09:42:54
All:            0 reqs (   0.0/sec)          0.0B (    0.0B/sec)        0.0B/req
2xx:       0 ( 0.0%) 3xx:       0 ( 0.0%) 4xx:      0 ( 0.0%) 5xx:      0 ( 0.0%)
R (  1s):       0 reqs (   0.0/sec)          0.0B (    0.0B/sec)        0.0B/req
2xx:       0 ( 0.0%) 3xx:       0 ( 0.0%) 4xx:      0 ( 0.0%) 5xx:      0 ( 0.0%)
```

10. watchdog

11. nmon

http://nmon.sourceforge.net/

例 2.2. nmon

```
$ apt-cache search nmon
libtime-modules-perl - Various Perl modules for time/date manipulation
nmon - performance monitoring tool for Linux
xfce4-genmon-plugin - Generic Monitor for the Xfce4 panel
xfce4-goodies - enhancements for the Xfce4 Desktop Environment

neo@monitor:~$ sudo apt-get install nmon

neo@monitor:~$ nmon
```

nmon -f -s 360 -c 86400 -m /home/user/nmon

第 3 章 Scanner & Sniffer

目录

1. nmap - Network exploration tool and security / port scanner

nmap

```
$ nmap localhost

Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-19 05:20 EST
Interesting ports on localhost (127.0.0.1):
Not shown: 1689 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
```

1.1. 扫描一个网段

```
$ nmap  -v -sP 172.16.0.0/24

Starting Nmap 4.62 ( http://nmap.org ) at 2010-11-27 10:00 CST
Initiating Ping Scan at 10:00
Scanning 256 hosts [1 port/host]
Completed Ping Scan at 10:00, 0.80s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 10:00
Completed Parallel DNS resolution of 256 hosts. at 10:00, 2.77s elapsed
Host 172.16.0.0 appears to be down.
Host 172.16.0.1 appears to be up.
```

```
Host 172.16.0.2 appears to be up.
Host 172.16.0.3 appears to be down.
Host 172.16.0.4 appears to be down.
Host 172.16.0.5 appears to be up.
Host 172.16.0.6 appears to be down.
Host 172.16.0.7 appears to be down.
Host 172.16.0.8 appears to be down.
Host 172.16.0.9 appears to be up.
...
...
Host 172.16.0.253 appears to be down.
Host 172.16.0.254 appears to be down.
Host 172.16.0.255 appears to be down.
Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.596 seconds
```

扫描正在使用的IP地址

```
$ nmap  -v -sP 172.16.0.0/24 | grep up
Host 172.16.0.1 appears to be up.
Host 172.16.0.2 appears to be up.
Host 172.16.0.5 appears to be up.
Host 172.16.0.9 appears to be up.
Host 172.16.0.19 appears to be up.
Host 172.16.0.40 appears to be up.
Host 172.16.0.188 appears to be up.
Host 172.16.0.252 appears to be up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 6.574 seconds
```

```
nmap -sP -PI -PT -oN ipandmaclist.txt 192.168.80.0/24
```

1.2. UDP 扫描

扫描DNS端口

```
$ sudo nmap -sU -p 53 120.132.144.20
```

2. tcpdump - A powerful tool for network monitoring and data acquisition

tcpdump

2.1. 监控网络适配器接口

```
$ sudo tcpdump -n -i eth1
```

2.2. 监控主机

tcpdump host 172.16.5.51

```
# tcpdump host 172.16.5.51
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
17:49:26.202556 IP 172.16.1.3 > 172.16.5.51: ICMP echo request, id 4, seq 22397,
length 40
17:49:26.203002 IP 172.16.5.51 > 172.16.1.3: ICMP echo reply, id 4, seq 22397,
length 40
```

2.3. 监控TCP端口

显示所有到的FTP会话

```
# tcpdump -i eth1 'dst 202.40.100.5 and (port 21 or 20)'
```

```
$ tcpdump -n -i eth0 port 80
```

监控网络但排除 SSH 22 端口

```
$ sudo tcpdump -n not dst port 22 and not src port 22
```

显示所有到192.168.0.5的HTTP会话

```
# tcpdump -ni eth0 'dst 192.168.0.5 and tcp and port http'
```

监控DNS的网络流量

```
# tcpdump -i eth0 'udp port 53'
```

2.4. 监控协议

```
$ tcpdump -n -i eth0 icmp or arp
```

2.5. 输出到文件

```
# tcpdump -n -i eth1 -s 0 -w output.txt src or dst port 80
```

使用wireshark分析输出文件，下面地址下载

http://www.wireshark.org/

2.6. Cisco Discovery Protocol (CDP)

```
$ sudo tcpdump -nn -v -i eth0 -s 1500 -c 1 'ether[20:2] == 0x2000'
[sudo] password for neo:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
13:51:31.825893 CDPv2, ttl: 180s, checksum: 692 (unverified), length 375
        Device-ID (0x01), length: 7 bytes: '4A3750G'
        Version String (0x05), length: 182 bytes:
          Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version
12.2(35)SE5, RELEASE SOFTWARE (fc1)
          Copyright (c) 1986-2007 by Cisco Systems, Inc.
          Compiled Thu 19-Jul-07 19:15 by nachen
        Platform (0x06), length: 23 bytes: 'cisco WS-C3750G-24TS-1U'
        Address (0x02), length: 13 bytes: IPv4 (1) 193.168.0.254
        Port-ID (0x03), length: 21 bytes: 'GigabitEthernet1/0/15'
        Capability (0x04), length: 4 bytes: (0x00000029): Router, L2 Switch, IGMP
snooping
        Protocol-Hello option (0x08), length: 32 bytes:
        VTP Management Domain (0x09), length: 3 bytes: 'xiu'
        Native VLAN ID (0x0a), length: 2 bytes: 11
        Duplex (0x0b), length: 1 byte: full
        AVVID trust bitmap (0x12), length: 1 byte: 0x00
        AVVID untrusted ports CoS (0x13), length: 1 byte: 0x00
        Management Addresses (0x16), length: 13 bytes: IPv4 (1) 193.168.0.254
        unknown field type (0x1a), length: 12 bytes:
          0x0000:  0000 0001 0000 0000 ffff ffff
1 packets captured
1 packets received by filter
0 packets dropped by kernel
```

```
$ sudo tcpdump -nn -v -i eth0 -s 1500 -c 1 'ether[20:2] == 0x2000'
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
13:52:03.451238 CDPv2, ttl: 180s, checksum: 692 (unverified), length 420
        Device-ID (0x01), length: 9 bytes: 'O9-Switch'
        Version String (0x05), length: 248 bytes:
          Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version
12.2(55)SE3, RELEASE SOFTWARE (fc1)
          Technical Support: http://www.cisco.com/techsupport
          Copyright (c) 1986-2011 by Cisco Systems, Inc.
          Compiled Thu 05-May-11 16:56 by prod_rel_team
        Platform (0x06), length: 22 bytes: 'cisco WS-C2960S-48TD-L'
        Address (0x02), length: 4 bytes:
        Port-ID (0x03), length: 20 bytes: 'GigabitEthernet1/0/8'
        Capability (0x04), length: 4 bytes: (0x00000028): L2 Switch, IGMP
snooping
        Protocol-Hello option (0x08), length: 32 bytes:
        VTP Management Domain (0x09), length: 0 byte: ''
1 packets captured
3 packets received by filter
0 packets dropped by kernel
```

```
$ sudo tcpdump -nn -v -i eth0 -s 1500 -c 1 'ether[20:2] == 0x2000' | grep
GigabitEthernet
[sudo] password for neo:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1500 bytes
        Port-ID (0x03), length: 21 bytes: 'GigabitEthernet1/0/15'
1 packets captured
1 packets received by filter
0 packets dropped by kernel
```

2.7. 案例

2.7.1. 监控80端口与icmp,arp

```
$ tcpdump -n -i eth0 port 80 or icmp or arp
```

2.7.2. monitor mysql tcp package

```
#!/bin/bash

tcpdump -i eth0 -s 0 -l -w - dst port 3306 | strings | perl -e '
while(<>) { chomp; next if /^[^ ]+[ ]*$/;
  if(/^(SELECT|UPDATE|DELETE|INSERT|SET|COMMIT|ROLLBACK|CREATE|DROP|ALTER)/i) {
    if (defined $q) { print "$q\n"; }
    $q=$_;
  } else {
    $_ =~ s/^[ \t]+//; $q.=" $_";
  }
}'
```

2.7.3. HTTP 包

```
tcpdump -i eth0 -s 0 -l -w - dst port 80 | strings
```

2.7.4. 显示SYN、FIN和ACK-only包

显示所有进出80端口IPv4 HTTP包，也就是只打印包含数据的包。例如：SYN、FIN包和ACK-only包输入：

```
# tcpdump 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2))
!= 0)'
```

3. nc - TCP/IP swiss army knife

上一页 上一级 下一页
2. tcpdump - A powerful tool for network monitoring and data acquisition 起始页 4. Unicornscan，Zenmap，nast

4. Unicornscan，Zenmap，nast

5. netstat-nat - Show the natted connections on a linux iptable firewall

```
neo@monitor:~$ sudo netstat-nat
Proto NATed Address                 Destination Address           State
tcp   10.8.0.14:1355                172.16.1.25:ssh               ESTABLISHED
tcp   10.8.0.14:1345                172.16.1.63:ssh               ESTABLISHED
tcp   10.8.0.14:1340                172.16.1.46:ssh               ESTABLISHED
tcp   10.8.0.14:1346                172.16.1.25:ssh               ESTABLISHED
tcp   10.8.0.14:1344                172.16.1.62:ssh               ESTABLISHED
tcp   10.8.0.14:1343                172.16.1.48:ssh               ESTABLISHED
```

你也同时可以使用下面命令查看

```
$ cat /proc/net/ip_conntrack
$ cat /proc/net/nf_conntrack
```

6. Wireshark

Wireshark is a network protocol analyzer for Unix and Windows.

http://www.wireshark.org/

第 4 章 Vulnerability Scanner

目录

1. Nessus

http://www.nessus.org/

```
[root@centos6 src]# rpm -ivh Nessus-4.4.1-es6.x86_64.rpm
Preparing...                ########################################### [100%]
   1:Nessus                 ########################################### [100%]
nessusd (Nessus) 4.4.1 [build M15078] for Linux
(C) 1998 - 2011 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
 - Please run /opt/nessus//sbin/nessus-adduser to add a user
 - Register your Nessus scanner at http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /sbin/service nessusd start
```

```
[root@centos6 src]# /opt/nessus/sbin/nessus-adduser
Login : admin
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
(y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that admin has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)



Login             : admin
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y]
User added
```

申请一个验证吗http://www.nessus.org/products/nessus/nessus-plugins/obtain-an-activation-code会发送到你的邮箱中。

```
[root@centos6 src]# /opt/nessus/bin/nessus-fetch --register 433E-3B47-94AF-5CF8-
7E8E
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

```
[root@centos6 src]# /sbin/service nessusd start
Starting Nessus services:
[root@centos6 src]# Missing plugins. Attempting a plugin update...
Your installation is missing plugins. Please register and try again.
To register, please visit http://www.nessus.org/register/
```

https://localhost:8834

---

2. OpenVAS

第 5 章 Network Management Software & Network Monitoring

目录

1. Webmin

网站

http://www.webmin.com/

过程 5.1. Webmin 安装步骤:

1. Debian Package
2. 命令:

sudo dpkg --install webmin_1.380_all.deb

sudo apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl libmd5-perl

Webmin install complete. You can now login to https://netkiller.8800.org:10000/ as root with your root password, or as any user who can use sudo to run commands as root.

3. script

   Usage: /etc/init.d/webmin { start | stop }

4. nmap localhost

1.1. webalizer

```
#apt-get install webmin-webalizer
```

2. Mrtg

```
$ sudo apt-get install mrtg
$ sudo mkdir /etc/mrtg/
$ sudo sh -c 'cfgmaker --global "HtmlDir: /var/www/mrtg" \
--global "ImageDir: /var/www/mrtg" \
--global "LogDir: /var/lib/mrtg" \
--global "ThreshDir: /var/lib/mrtg" \
--global "Options[_]: growright,bits"  \
--ifref=name --ifdesc=descr --show-op-down \
public@172.16.0.254 > /etc/mrtg/firewall.cfg'

$ sudo mkdir -p /var/www/mrtg
$ sudo indexmaker --output=/var/www/mrtg/firewall.html /etc/mrtg/firewall.cfg
```

例 5.1. mrtg

3. Cacti

Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices.

homepage: http://www.cacti.net/

Cacti requires MySQL, PHP, RRDTool, net-snmp, and a webserver that supports PHP such as Apache.

```
sudo apt-get install rrdtool
sudo apt-get install snmp snmpd
sudo apt-get install php5-snmp
```

At first, install snmp for linux

1. wget http://www.cacti.net/downloads/cacti-0.8.7b.tar.gz
2. tar zxvf cacti-0.8.7b.tar.gz
3. mv cacti-0.8.7b /home/netkiller/public_html/cacti
4. mysqladmin --user=root create cacti
5. mysql -uroot -p cacti < cacti.sql
6. echo "GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'somepassword';" | mysql -uroot -p
7. echo "flush privileges;" | mysql -uroot -p
8. vi include/config.php

例 5.2. cacti config.php

```
$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "somepassword";
$database_port = "3306";
```

9. crontab -e

   */5 * * * * php /var/www/neo.6600.org/html/cacti/poller.php > /dev/null 2>&1

   or

   /etc/crontab

```
*/5 * * * * nobody php /home/netkiller/public_html/cacti/poller.php > /dev/null 2>&1
```

10. mkdir -p /var/log/cacti/

configure cacti

http://your-server/cacti/

3.1. Template

MySQL Template: http://code.google.com/p/mysql-cacti-templates/

```
$ cd /usr/local/src/
$ wget http://mysql-cacti-templates.googlecode.com/files/better-cacti-templates-
1.1.7.tar.gz
$ tar zxvf better-cacti-templates-1.1.7.tar.gz
$ cd better-cacti-templates-1.1.7/
$ cp scripts/ss_get_mysql_stats.php /usr/share/cacti/site/scripts
```

default password

```
vim /usr/share/cacti/site/scripts/ss_get_mysql_stats.php.cnf
<?php
$mysql_user = "root";
$mysql_pass = "s3cret";
?>
```

Import Templates

```
Import/Export -> Import Templates -> Import Template from Local File -> Save
```

设置模版

```
Templates ->

X MyISAM Indexes DT
X MyISAM Key Cache DT
X MySQL Binary/Relay Logs DT
X MySQL Command Counters DT
X MySQL Connections DT
X MySQL Files and Tables DT
X MySQL Handlers DT
X MySQL Network Traffic DT
X MySQL Processlist DT
X MySQL Query Cache DT
X MySQL Query Cache Memory DT
X MySQL Replication DT
X MySQL Select Types DT
X MySQL Sorts DT
X MySQL Table Locks DT
X MySQL Temporary Objects DT
X MySQL Threads DT
X MySQL Transaction Handler DT

->

Custom Data
Hostname
Username        #单击复选框，并输入默认用户名
Password        #单击复选框，并输入默认密码
Port

-> Save
```

4. Nagios

homepage: http://www.nagios.org/

4.1. Install Nagios

Nagios 是一种开放源代码监视软件，它可以扫描主机、服务、网络方面存在的问题。Nagios 与其他类似的包之间的主要区别在于，Nagios 将所有的信息简化为“工作（working）”、“可疑的（questionable）”和“故障（failure）”状态，并且 Nagios 支持由插件组成的非常丰富的“生态系统”。这些特性使得用户能够进行有效安装，在此过程中无需过多地关心细节内容，只提供他们所需的信息即可。

install

```
$ sudo apt-get install nagios3 nagios-nrpe-plugin
```

add user nagiosadmin for nagios

```
$ sudo htpasswd -c /etc/nagios2/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
```

Create a new nagcmd group for allowing external commands to be submitted through the web interface. Add both the nagios user and the apache user to the group.

```
$ groupadd nagcmd
$ sudo usermod -a -G nagcmd nagios
$ sudo usermod -a -G nagcmd www-data
$ cat /etc/group
nagcmd:x:1003:nagios,www-data
```

reload apache

```
$ sudo /etc/init.d/apache2 reload
 * Reloading web server config apache2                    [ OK ]
```

4.2. 配置 Nagios

```
$ sudo vim /etc/nagios3/nagios.cfg

cfg_dir=/etc/nagios3/hosts
cfg_dir=/etc/nagios3/servers
cfg_dir=/etc/nagios3/switches
cfg_dir=/etc/nagios3/routers

admin_email=nagios, neo.chen@zoshow.com
```

4.2.1. authorized

add user neo for nagios

```
```

```
$ sudo htpasswd /etc/nagios3/htpasswd.users neo
New password:
Re-type new password:
Adding password for user neo
```

```
$ sudo vim /etc/nagios3/cgi.cfg

authorized_for_all_services=nagiosadmin,neo
authorized_for_all_hosts=nagiosadmin,neo
```

4.2.2. contacts

```
$ sudo vim /etc/nagios3/conf.d/contacts_nagios2.cfg

###############################################################################
# contacts.cfg
###############################################################################

define contact{
        contact_name                    neo
        alias                           Neo
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-service-by-email
        host_notification_commands      notify-host-by-email
        email                           neo.chen@example.com
        }

###############################################################################
###############################################################################
#
# CONTACT GROUPS
#
###############################################################################
###############################################################################

# We only have one contact in this simple configuration file, so there is
# no need to create more than one contact group.

define contactgroup{
        contactgroup_name       admins
        alias                   Nagios Administrators
        members                 root, neo
        }
```

当服务出现w—报警(warning),u—未知(unkown),c—严重(critical),r—从异常恢复到正常，在这四种情况下通知联系人

当主机出现d－当机(down),u—返回不可达(unreachable),r—从异常情况恢复正常,在这3种情况下通知联系人

确认 contact_groups 已经设置

```
neo@monitor:/etc/nagios3$ grep admins conf.d/generic-host_nagios2.cfg
                contact_groups                  admins
neo@monitor:/etc/nagios3$ grep admins conf.d/generic-service_nagios2.cfg
                contact_groups                  admins
```

4.2.3. hostgroups

```
$ sudo vim /etc/nagios3/conf.d/hostgroups_nagios2.cfg

define hostgroup {
        hostgroup_name  mysql-servers
                alias           MySQL Servers
                members         *
        }
```

4.2.4. generic-service

```
$ cat /etc/nagios3/conf.d/generic-service_nagios2.cfg
# generic service template definition
define service{
        name                            generic-service ; The 'name' of this
service template
        active_checks_enabled           1       ; Active service checks are
enabled
        passive_checks_enabled          1       ; Passive service checks are
enabled/accepted
        parallelize_check               1       ; Active service checks should be
parallelized (disabling this can lead to major performance problems)
        obsess_over_service             1       ; We should obsess over this
service (if necessary)
        check_freshness                 0       ; Default is to NOT check service
'freshness'
        notifications_enabled           1       ; Service notifications are
enabled
        event_handler_enabled           1       ; Service event handler is
enabled
        flap_detection_enabled          1       ; Flap detection is enabled
        failure_prediction_enabled      1       ; Failure prediction is enabled
        process_perf_data               1       ; Process performance data
        retain_status_information       1       ; Retain status information across
program restarts
        retain_nonstatus_information    1       ; Retain non-status information
across program restarts
                notification_interval           0               ; Only send
notifications on status change by default.
                is_volatile                     0
                check_period                    24x7
                normal_check_interval           5
                retry_check_interval            1
                max_check_attempts              4
                notification_period             24x7
                notification_options            w,u,c,r
                contact_groups                  admins
        register                        0       ; DONT REGISTER THIS DEFINITION -
ITS NOT A REAL SERVICE, JUST A TEMPLATE!
        }
```

- notification_interval 报警发送间隔，单位分钟
- normal_check_interval 间隔时间
- retry_check_interval 重试间隔时间
- max_check_attempts 检查次数，4次失败后报警

4.2.5. SOUND OPTIONS

发出警报声

```
$ sudo vim /etc/nagios3/cgi.cfg

# SOUND OPTIONS
# These options allow you to specify an optional audio file
# that should be played in your browser window when there are
# problems on the network.  The audio files are used only in
# the status CGI.  Only the sound for the most critical problem
# will be played.  Order of importance (higher to lower) is as
# follows: unreachable hosts, down hosts, critical services,
# warning services, and unknown services. If there are no
# visible problems, the sound file optionally specified by
# 'normal_sound' variable will be played.
#
#
# <varname>=<sound_file>
#
# Note: All audio files must be placed in the /media subdirectory
# under the HTML path (i.e. /usr/local/nagios/share/media/).
```

```
host_unreachable_sound=hostdown.wav
host_down_sound=hostdown.wav
service_critical_sound=critical.wav
service_warning_sound=warning.wav
service_unknown_sound=warning.wav
normal_sound=noproblem.wav
```

4.2.6. SMS 短信

```
vim /etc/nagios3/commands.cfg

# 'notify-host-by-sms' command definition
define command{
        command_name    notify-host-by-sms
        command_line    /srv/sms/sms "Host: $HOSTNAME$\nState:
$HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time:
$LONGDATETIME$\n"
        }

# 'notify-service-by-sms' command definition
define command{
        command_name    notify-service-by-sms
        command_line    /srv/sms/sms "Service: $SERVICEDESC$\nHost:
$HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time:
$LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$"
        }
```

```
sudo vim /etc/nagios3/conf.d/contacts_nagios2.cfg
define contact{
        contact_name                    neo
        alias                           Neo
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-service-by-email, notify-service-
by-sms
        host_notification_commands      notify-host-by-email, notify-host-by-sms
        email                           neo.chen@xiu.com
        }
```

4.3. 配置监控设备

4.3.1. routers

```
vim /etc/nagios3/routers/firewall.cfg

define host{

        use             generic-host; Inherit default values from a template

        host_name       firewall         ; The name we're giving to this switch

        alias           Cisco PIX 515E Firewall ; A longer name associated with
the switch

        address         172.16.1.254            ; IP address of the switch

        hostgroups      all,networks            ; Host groups this switch is
associated with

        }

define service{

        use                     generic-service ; Inherit values from a template

        host_name                       firewall ; The name of the host the
service is associated with

        service_description     PING            ; The service description

        check_command           check_ping!200.0,20%!600.0,60%  ; The command
```

```
used to monitor the service

        normal_check_interval   5       ; Check the service every 5 minutes under
normal conditions

        retry_check_interval    1       ; Re-check the service every minute until
its final/hard state is determined

        }

define service{

        use                     generic-service ; Inherit values from a template

        host_name                       firewall

        service_description     Uptime

        check_command           check_snmp!-C public -o sysUpTime.0

        }
```

4.3.2. hosts / service

4.3.2.1. http

hosts

```
$ cat /etc/nagios3/hosts/www.example.com.cfg
define host{

        use             generic-host            ; Inherit default values from a
template

        host_name       www.example.com             ; The name we're giving to
this host

        alias           Some Remote Host        ; A longer name associated with
the host

        address         120.132.14.6           ; IP address of the host

        hostgroups      all,http-servers        ; Host groups this host is
associated with

        }

define service{

        use             generic-service         ; Inherit default values from a
template

        host_name               www.example.com

        service_description     HTTP

        check_command   check_http

        }
```

HTTP状态

```
neo@monitor:~$ /usr/lib/nagios/plugins/check_http -H www.example.com -I 172.16.0.8
-s "HTTs"
HTTP CRITICAL: HTTP/1.1 404 Not Found - string not found - 336 bytes in 0.001
second response time |time=0.000733s;;;0.000000 size=336B;;;0

neo@monitor:~$ /usr/lib/nagios/plugins/check_http -H www.example.com -I 172.16.0.8
-e '404'
HTTP OK: Status line output matched "404" - 336 bytes in 0.001 second response
time |time=0.000715s;;;0.000000 size=336B;;;0
```

4.3.2.2. mysql hosts

```
$ sudo vim /etc/nagios3/hosts/mysql.cfg


define host{

        use             generic-host            ; Inherit default values from a
template

        host_name       mysql-master.example.com            ; The name we're
giving to this host

        alias           Some Remote Host        ; A longer name associated with
the host

        address         172.16.1.6             ; IP address of the host

        hostgroups      all,mysql-servers       ; Host groups this host is
associated with

        }

define service{

        use             generic-service         ; Inherit default values from a
template

        host_name               mysql-master.example.com

        service_description     MySQL

        check_command   check_mysql_database!user!passwd!database

        }
```

4.4. Monitor Client nrpe

4.4.1. Nagios3 nrpe plugins

nrpe 插件接收来自nagios-nrpe-server数据报告

```
cat /etc/nagios3/hosts/host.example.org.cfg

define host{

        use             generic-host            ; Inherit default values from a
template

        host_name       host.example.org        ; The name we're giving to this
host

        alias           Some Remote Host        ; A longer name associated with
the host

        address         172.16.1.3              ; IP address of the host

        hostgroups      all                     ; Host groups this host is
associated with

        }

# NRPE disk check.
define service {
        use                             generic-service
        host_name                       backup
        service_description             nrpe-disk
        check_command                   check_nrpe_1arg!check_all_disks!172.16.1.3
}
define service {
        use                             generic-service
        host_name                       backup
        service_description             nrpe-users
        check_command                   check_nrpe_1arg!check_users!172.16.1.3
}
define service {
        use                             generic-service
        host_name                       backup
        service_description             nrpe-swap
```

```
        check_command                   check_nrpe_1arg!check_swap!172.16.1.3
}
define service {
        use                             generic-service
        host_name                       backup
        service_description             nrpe-procs
        check_command                   check_nrpe_1arg!check_procs!172.16.1.3
}
```

4.4.2. nagios-nrpe-server

nagios-nrpe-server 的功能是向服务器发送监控数据

```
sudo apt-get install nagios-nrpe-server nagios-plugins
```

/etc/nagios/nrpe.cfg

/etc/nagios/nrpe_local.cfg

```
$ sudo vim /etc/nagios/nrpe_local.cfg
allowed_hosts=172.16.1.2

command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
command[check_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
command[check_swap]=/usr/lib/nagios/plugins/check_swap -w 20% -c 10%
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
command[check_disk_root]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /
command[check_disk_home]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /home
command[check_sda_iostat]=/usr/lib/nagios/plugins/check_iostat -d sda -w 100 -c
200
command[check_sdb_iostat]=/usr/lib/nagios/plugins/check_iostat -d sdb -w 100 -c
200
# command[check_uri_user]=/usr/lib/nagios/plugins/check_http -I 127.0.0.1 -p 80 -u
http://example.com/test/ok.php
# command[check_mysql]=/usr/lib/nagios/plugins/check_mysql -H localhost -u root -
ppassword test -P 3306
```

重启后生效

```
/etc/init.d/nagios-nrpe-server restart
```

4.5. Monitoring Windows Machines

4.5.1. NSClient++

http://sourceforge.net/projects/nscplus

4.5.2. check_nt

Define windows services that should be monitored.

```
# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
use             windows-server              ; Inherit default values from a
template
host_name   remote-windows-host      ; The name we're giving to this host
alias            Remote Windows Host     ; A longer name associated with the host
address       192.168.1.4                   ; IP address of the remote windows
host
}

define service{
use                     generic-service
host_name               remote-windows-host
```

```
service_description     NSClient++ Version
check_command           check_nt!CLIENTVERSION
}
define service{
use                     generic-service
host_name               remote-windows-host
service_description     Uptime
check_command           check_nt!UPTIME
}
define service{
use                     generic-service
host_name               remote-windows-host
service_description     CPU Load
check_command           check_nt!CPULOAD!-l 5,80,90
}
define service{
use                     generic-service
host_name               remote-windows-host
service_description     Memory Usage
check_command           check_nt!MEMUSE!-w 80 -c 90
}
define service{
use                     generic-service
host_name               remote-windows-host
service_description     C:\ Drive Space
check_command           check_nt!USEDDISKSPACE!-l c -w 80 -c 90
}
define service{
use                     generic-service
host_name               remote-windows-host
service_description     W3SVC
check_command           check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
}
define service{
use                     generic-service
host_name               remote-windows-host
service_description     Explorer
check_command           check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}
```

4.5.3. Enable Password Protection

```
define command{
command_name    check_nt
command_line    $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s My2Secure$Password -
v $ARG1$ $ARG2$
}
```

4.6. Nagios Plugins

检查命令配置文件 /etc/nagios-plugins/config/

4.6.1. http.cfg

```
define command{
        command_name    check_http_404
        command_line    /usr/lib/nagios/plugins/check_http -H '$HOSTADDRESS$' -I
'$HOSTADDRESS$' -e '404'
        }

define command{
        command_name    check_http_status
        command_line    /usr/lib/nagios/plugins/check_http -H '$HOSTADDRESS$' -I
'$HOSTADDRESS$' -e '$ARG1$'
        }

define command{
        command_name    check_http_url
        command_line    /usr/lib/nagios/plugins/check_http -H '$HOSTADDRESS$' -I
'$HOSTADDRESS$'  -u '$ARG1$'
        }
```

默认HTTP健康检查超时时间是10秒，如果你的网站需要更长的时间才能打开可以使用-t参数修改默认Timeout时间

```
# 'check_http' command definition
define command{
        command_name    check_http
        command_line    /usr/lib/nagios/plugins/check_http -t 30 -H
'$HOSTADDRESS$' -I '$HOSTADDRESS$'
        }
```

4.6.1.1. check_http

```
neo@monitor:~$ /usr/lib/nagios/plugins/check_http -H www.example.com -I 172.16.0.8
-s "HTTs"
HTTP CRITICAL: HTTP/1.1 404 Not Found - string not found - 336 bytes in 0.001
second response time |time=0.000733s;;;0.000000 size=336B;;;0

neo@monitor:~$ /usr/lib/nagios/plugins/check_http -H www.example.com -I 172.16.0.8
-e '404'
HTTP OK: Status line output matched "404" - 336 bytes in 0.001 second response
time |time=0.000715s;;;0.000000 size=336B;;;0
```

4.6.2. mysql.cfg

/etc/nagios-plugins/config/mysql.cfg

4.6.2.1. check_mysql

```
$ /usr/lib64/nagios/plugins/check_mysql --hostname=172.16.1.5 --port=3306 --
username=monitor --password=monitor
Uptime: 27001  Threads: 8  Questions: 25280156  Slow queries: 14941  Opens:
1389932  Flush tables: 3  Open tables: 128  Queries per second avg: 936.267
```

4.6.2.2. mysql.cfg check_mysql_replication

```
cat >> /usr/lib64/nagios/plugins/check_mysql_replication <<EOF
#!/bin/bash

declare -a slave_is

slave_is=($(mysql -h$1 -umonitor -pxmNhj -e "show slave status\G"|grep Running
|awk '{print $2}'))

if [ "${slave_is[0]}" = "Yes" -a "${slave_is[1]}" = "Yes" ]
     then
     echo "OK - Slave is running"
     exit 0
else
     echo "Critical - Slave is error"
     exit 2
fi
EOF
```

```
sudo chmod +x /usr/lib64/nagios/plugins/check_mysql_replication
/usr/lib64/nagios/plugins/check_mysql_replication 172.16.1.4
Critical - slave is error
```

```
vim /etc/nagios-plugins/config/mysql.cfg

# 'check_mysql_replication' command definition
define command{
        command_name    check_mysql_replication
        command_line    /usr/lib/nagios/plugins/check_mysql_replication
$HOSTADDRESS$
}
define command{
        command_name    check_mysql_replication_host
        command_line    /usr/lib/nagios/plugins/check_mysql_replication '$ARG1$'
}
```

```

```

4.6.2.3. nrpe.cfg check_mysql_replication

nrpe.cfg

```
cat >> /usr/lib64/nagios/plugins/check_mysql_replication <<EOF
#!/bin/bash

declare -a slave_is

slave_is=($(mysql -umonitor -pxmNhj -e "show slave status\G"|grep Running |awk
'{print $2}'))

if [ "${slave_is[0]}" = "Yes" -a "${slave_is[1]}" = "Yes" ]
     then
     echo "OK - slave is running"
     exit 0
else
     echo "Critical - slave is error"
     exit 2
fi
EOF

command[check_mysql_slave]=/usr/lib64/nagios/plugins/check_mysql_replication

/usr/local/nagios/libexec/check_nrpe -H 192.168.1.1
/usr/local/nagios/libexec/check_nrpe -H 192.168.1.1 -c check_mysql_replication


define service {
        host_name 192.168.10.232
        service_description check_mysql_replication
        check_period 24x7
        max_check_attempts 5
        normal_check_interval 3
        retry_check_interval 2
        contact_groups mygroup
        notification_interval 5
        notification_period 24x7
        notification_options w,u,c,r
        check_command check_nrpe!check_mysql_replication
}
```

4.6.3. Disk

4.6.3.1. disk.cfg

```
$ cat /etc/nagios-plugins/config/disk.cfg
# 'check_disk' command definition
define command{
        command_name    check_disk
        command_line    /usr/lib/nagios/plugins/check_disk -w '$ARG1$' -c '$ARG2$'
-e -p '$ARG3$'
        }

# 'check_all_disks' command definition
define command{
        command_name    check_all_disks
        command_line    /usr/lib/nagios/plugins/check_disk -w '$ARG1$' -c '$ARG2$'
-e
        }

# 'ssh_disk' command definition
define command{
        command_name    ssh_disk
        command_line    /usr/lib/nagios/plugins/check_by_ssh -H '$HOSTADDRESS$' -C
'/usr/lib/nagios/plugins/check_disk -w '\''$ARG1$' -c '\''$ARG2$'\'' -e -p
'\''$ARG3$'\'
        }

####
# use these checks, if you want to test IPv4 connectivity on IPv6 enabled systems
####
```

```
# 'ssh_disk_4' command definition
define command{
        command_name    ssh_disk_4
        command_line    /usr/lib/nagios/plugins/check_by_ssh -H '$HOSTADDRESS$' -C
'/usr/lib/nagios/plugins/check_disk -w '\''$ARG1$'\'' -c '\''$ARG2$'\'' -e -p
'\''$ARG3$'\' -4
        }
```

4.6.3.2. check_disk

WARNING/CRITICAL 报警阀值

```
-w 10% -c 5%
-w 100M -c 50M
```

-p, --path=PATH, --partition=PARTITION 参数监控路径，可以一次写多个参数

```
$ /usr/lib/nagios/plugins/check_disk -w 10% -c 5% -p / -p /opt -p /boot
DISK OK - free space: / 23872 MB (66% inode=92%); /opt 99242 MB (47% inode=93%);
/boot 276 MB (63% inode=99%);| /=11767MB;33792;35669;0;37547
/opt=110882MB;199232;210300;0;221369 /boot=160MB;414;437;0;460

$ /usr/lib/nagios/plugins/check_disk -w 100M -c 50M -p / -p /opt -p /boot
DISK OK - free space: / 23872 MB (66% inode=92%); /opt 99242 MB (47% inode=93%);
/boot 276 MB (63% inode=99%);| /=11768MB;37447;37497;0;37547
/opt=110882MB;221269;221319;0;221369 /boot=160MB;360;410;0;460
```

-x, --exclude_device=PATH 排除监控路径

```
/usr/lib64/nagios/plugins/check_disk -w 10% -c 5% -e -x /bak -x /u01
```

4.6.3.3. disk-smb.cfg

```
$ cat disk-smb.cfg
# 'check_disk_smb' command definition
define command{
        command_name    check_disk_smb
        command_line    /usr/lib/nagios/plugins/check_disk_smb -H '$ARG1$' -s
'$ARG2$'
        }


# 'check_disk_smb_workgroup' command definition
define command{
        command_name    check_disk_smb_workgroup
        command_line    /usr/lib/nagios/plugins/check_disk_smb -H '$ARG1$' -s
'$ARG2$' -W '$ARG3$'
        }


# 'check_disk_smb_host' command definition
define command{
        command_name    check_disk_smb_host
        command_line    /usr/lib/nagios/plugins/check_disk_smb -a '$HOSTADDRESS$'
-H '$ARG1$' -s '$ARG2$'
        }


# 'check_disk_smb_workgroup_host' command definition
define command{
        command_name    check_disk_smb_workgroup_host
        command_line    /usr/lib/nagios/plugins/check_disk_smb -a '$HOSTADDRESS$'
-H '$ARG1$' -s '$ARG2$' -W '$ARG3$'
        }


# 'check_disk_smb_user' command definition
define command{
        command_name    check_disk_smb_user
        command_line    /usr/lib/nagios/plugins/check_disk_smb -H '$ARG1$' -s
'$ARG2$' -u '$ARG3$' -p '$ARG4$' -w '$ARG5$' -c '$ARG6$'
        }
```

```
# 'check_disk_smb_workgroup_user' command definition
define command{
        command_name    check_disk_smb_workgroup_user
        command_line    /usr/lib/nagios/plugins/check_disk_smb -H '$ARG1$' -s
'$ARG2$' -W '$ARG3$' -u '$ARG4$' -p '$ARG5$'
        }


# 'check_disk_smb_host_user' command definition
define command{
        command_name    check_disk_smb_host_user
        command_line    /usr/lib/nagios/plugins/check_disk_smb -a '$HOSTADDRESS$'
-H '$ARG1$' -s '$ARG2$' -u '$ARG3$' -p '$ARG4$'
        }


# 'check_disk_smb_workgroup_host_user' command definition
define command{
        command_name    check_disk_smb_workgroup_host_user
        command_line    /usr/lib/nagios/plugins/check_disk_smb -a '$HOSTADDRESS$'
-H '$ARG1$' -s '$ARG2$' -W '$ARG3$' -u '$ARG4$' -p '$ARG5$'
        }
```

4.6.4. tcp_udp.cfg

4.6.4.1. check_tcp

```
$ /usr/lib/nagios/plugins/check_tcp -H 172.16.1.2 -p 80
TCP OK - 0.000 second response time on port 80|time=0.000369s;;;0.000000;10.000000
```

4.6.4.2. Memcache

```
$ /usr/lib64/nagios/plugins/check_tcp -H localhost -p 11211 -t 5 -E -s
'stats\r\nquit\r\n' -e 'uptime' -M crit
TCP OK - 0.001 second response time on port 11211 [STAT pid 29253
STAT uptime 36088
STAT time 1311100189
STAT version 1.4.5
STAT pointer_size 64
STAT rusage_user 3.207512
STAT rusage_system 50.596308
STAT curr_connections 10
STAT total_connections 97372
STAT connection_structures 84
STAT cmd_get 84673
STAT cmd_set 273
STAT cmd_flush 0
STAT get_hits 84336
STAT get_misses 337
STAT delete_misses 0
STAT delete_hits 0
STAT incr_misses 0
STAT incr_hits 0
STAT decr_misses 0
STAT decr_hits 0
STAT cas_misses 0
STAT cas_hits 0
STAT cas_badval 0
STAT auth_cmds 0
STAT auth_errors 0
STAT bytes_read 49280152
STAT bytes_written 46326517326
STAT limit_maxbytes 4294967296
STAT accepting_conns 1
STAT listen_disabled_num 0
STAT threads 4
STAT conn_yields 0
STAT bytes 1345
STAT curr_items 14
STAT total_items 241
STAT evictions 0
STAT reclaimed 135
END]|time=0.000658s;;;0.000000;5.000000
```

5. Munin

5.1. Installation Monitor Server

```
$ sudo apt-get install munin

neo@monitor:~$ sudo vim /etc/munin/munin.conf
neo@monitor:~$ sudo service munin-node restart


[example.com]
        address 127.0.0.1
        use_node_name yes

[web2]
    address 172.16.1.2
    use_node_name yes

[web3]
    address 172.16.1.3
    use_node_name yes

[database]
    address 172.16.1.10
    use_node_name yes
```

5.2. Installation Node

```
sudo apt-get install munin-node

vim /etc/munin/munin-node.conf

allow ^172\.16\.1\.2$
```

5.3. Additional Plugins

```
sudo apt-get install munin-plugins-extra
```

5.4. plugins

5.4.1. mysql

```
ln -s /usr/share/munin/plugins/mysql_* /etc/munin/plugins/
```

/etc/munin/plugin-conf.d/munin-node

```
$ sudo vim /etc/munin/plugin-conf.d/munin-node

[mysql*]
user root
env.mysqlopts --defaults-file=/etc/mysql/debian.cnf
env.mysqluser debian-sys-maint
env.mysqlconnection DBI:mysql:mysql;mysql_read_default_file=/etc/mysql/debian.cnf

[mysql*]
```

```
env.mysqlopts -h 192.168.3.40 -uneo -pchen
```

5.4.2. apache

```
$ sudo vim /etc/munin/plugin-conf.d/munin-node

[apache_*]
env.url   http://127.0.0.1/server-status?auto
env.ports 80
```

6. Zabbix

6.1. Installing and Configuring Zabbix

```
neo@monitor:~$ apt-cache search zabbix
zabbix-agent - network monitoring solution - agent
zabbix-frontend-php - network monitoring solution - PHP front-end
zabbix-proxy-mysql - network monitoring solution - proxy (using MySQL)
zabbix-proxy-pgsql - network monitoring solution - proxy (using PostgreSQL)
zabbix-server-mysql - network monitoring solution - server (using MySQL)
zabbix-server-pgsql - network monitoring solution - server (using PostgreSQL)
```

```
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost' IDENTIFIED BY 'chen'
WITH GRANT OPTION;
FLUSH PRIVILEGES;
```

```
sudo apt-get install zabbix-server-mysql zabbix-frontend-php
```

如果上述过程中遇到一些问题，可以手工安装数据库

```
$ sudo mysql -uroot -p -e"create database zabbix;"
$ sudo mysql -uroot -p -e"grant all privileges on zabbix.* to zabbix@localhost
identified by 'enter-password-here';"
$ mysql -uzabbix -p zabbix < /usr/share/zabbix-server/mysql.sql
$ mysql -uzabbix -p zabbix < /usr/share/zabbix-server/data.sql
$ sudo dpkg-reconfigure zabbix-server-mysql
```

```
cat >> /etc/services <<EOF

zabbix-agent    10050/tcp                       #Zabbix Agent
zabbix-agent    10050/udp                       #Zabbix Agent
zabbix-trapper  10051/tcp                       #Zabbix Trapper
zabbix-trapper  10051/udp                       #Zabbix Trapper
EOF
```

6.2. web ui

http://localhost/zabbix/

user: admin

passwd: zabbix

6.3. zabbix-agent

```
# sudo apt-get install zabbix-agent
```

/etc/zabbix/zabbix_agent.conf

```
#Server=localhost
Server=your_server_ip_address
```

```
# vim /etc/services

zabbix-agent    10050/tcp                       #Zabbix Agent
zabbix-agent    10050/udp                       #Zabbix Agent
```

```
# sudo /etc/init.d/zabbix-agent restart
```

7. Ganglia

Ganglia是一个集群监控软件

Ganglia 是一个开源项目，它为高性能计算系统（例如集群和网格）提供了一个免费的可扩展分布式监视系统。

7.1. Server

```
sudo apt-get install ganglia-monitor ganglia-webfrontend

Restart apache2? 选择 Yes

sudo ln -s /usr/share/ganglia-webfrontend/ /var/www/ganglia
```

/etc/ganglia/gmond.conf

```
name = "my servers"   （只改了这个地方，改成"my cluster”）
```

在浏览器输入”http://localhost/ganglia”就可以看到Web UI

7.2. Client

```
# apt-get install ganglia-monitor
$ sudo vim /etc/ganglia/gmond.conf
sudo cp /etc/ganglia/gmond.conf  /etc/ganglia/gmond.conf.old

sudo cp /etc/ganglia/gmetad.conf /etc/ganglia/gmetad.conf.old
sudo vim /etc/ganglia/gmetad.conf

$ sudo  /etc/init.d/gmetad restart

$ sudo  /etc/init.d/ganglia-monitor restart
```

ip route add 239.2.11.71 dev eth1

7.3. Plugin

7.4. Installing Ganglia on Centos

http://www.jansipke.nl/installing-ganglia-on-centos

启动

```
# service gmond start
Starting GANGLIA gmond:                                    [  OK  ]
# chkconfig --list gmond
gmond           0:off   1:off   2:off   3:off   4:off   5:off   6:off
# chkconfig gmond on
# chkconfig --list gmond
gmond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

8. lvs-rrd

http://tepedino.org/lvs-rrd/

9. Ntop

9.1. Installation

```
$ sudo apt-get install ntop
```

设置管理员密码

```
$ sudo ntop --set-admin-password
```

```
$ sudo /etc/init.d/ntop start
```

9.2. Web UI

http://localhost:3000/

10. Observium

http://www.observium.org

10.1. Installation

```
aptitude install libapache2-mod-php5 php5-cli php5-mysql php5-gd php5-snmp \
php-pear snmp graphviz subversion mysql-server mysql-client rrdtool \
fping imagemagick whois mtr-tiny nmap ipmitool
```

```
Install the IPv4 and IPv6 pear libraries:
$ sudo pear install Net_IPv6
$ sudo pear install Net_IPv4
```

http://www.observium.org/observium-latest.tar.gz

```
$ wget http://www.observium.org/observium-latest.tar.gz
$ tar zxvf observium-latest.tar.gz
$ sudo mv observium /opt
$ cd /opt/observium/
$ cp config.php.default config.php
$ sudo mkdir graphs rrd
$ chown www-data.www-data graphs rrd
$ mkdir /opt/observium/logs
```

```

CREATE DATABASE observium;
GRANT ALL PRIVILEGES ON observium.* TO 'observium'@'localhost'
IDENTIFIED BY '<observium db password>';


```

```

$ mysql -uroot -p
Enter password: <mysql root password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 238145
Server version: 5.1.41-3ubuntu12.10 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE observium;
Query OK, 1 row affected (0.10 sec)

mysql> GRANT ALL PRIVILEGES ON observium.* TO 'observium'@'localhost' IDENTIFIED
BY 'observium';
Query OK, 0 rows affected (0.06 sec)


```

```
$ vim config.php

### Database config
$config['db_host'] = "localhost";
$config['db_user'] = "observium";
$config['db_pass'] = "observium";
$config['db_name'] = "observium";

### List of networks to allow scanning-based discovery
$config['nets'][] = "172.16.1.0/24";
```

```
$config['nets'][] = "172.16.3.0/24";

or
$config['nets'][] = "172.16.0.0/16";
```

```
$ mysql -uobservium -pobservium observium < database-schema.sql
```

```
$ sudo vim /etc/apache2/sites-available/observium

<VirtualHost *:80>
       ServerAdmin webmaster@localhost
       ServerName  observium.domain.com
       DocumentRoot /opt/observium/html
       <Directory />
               Options FollowSymLinks
               AllowOverride None
       </Directory>
       <Directory /opt/observium/html/>
               Options Indexes FollowSymLinks MultiViews
               AllowOverride All
               Order allow,deny
               allow from all
       </Directory>
       ErrorLog /var/log/apache2/error.log
       LogLevel warn
       CustomLog /var/log/apache2/access.log combined
       ServerSignature On
</VirtualHost>
```

```
$ sudo a2enmod rewrite
Enabling module rewrite.
Run '/etc/init.d/apache2 restart' to activate new configuration!

$ sudo a2ensite observium
Enabling site observium.
Run '/etc/init.d/apache2 reload' to activate new configuration!

$ sudo apache2ctl restart
```

```
$ ./adduser.php
Add User Tool
Usage: ./adduser.php <username> <password> <level 1-10> [email]

$ ./adduser.php neo chen 1 neo.chen@example.com

$ ./adduser.php netkiller 3655927 10 neo.chen@xiu.com
User netkiller added successfully




$ ./addhost.php

Observium v0.11.9.2439 Add Host Tool

Usage: ./addhost.php <hostname> [community] [v1|v2c] [port] [udp|udp6|tcp|tcp6]

$ ./addhost.php localhost public v2c
Trying community public
Added device localhost (1)
```

```
./discovery.php -h all
./poller.php -h all
```

```
$ crontab -e
```

```
33 */6   * * *   cd /opt/observium/ && ./discovery.php -h all >> /dev/null 2>&1
*/5 *    * * *   cd /opt/observium/ && ./discovery.php -h new >> /dev/null 2>&1
*/5 *    * * *   cd /opt/observium/ && ./poller.php -h all >> /dev/null 2>&1

$ sudo /etc/init.d/cron reload
```

11. BIG BROTHER

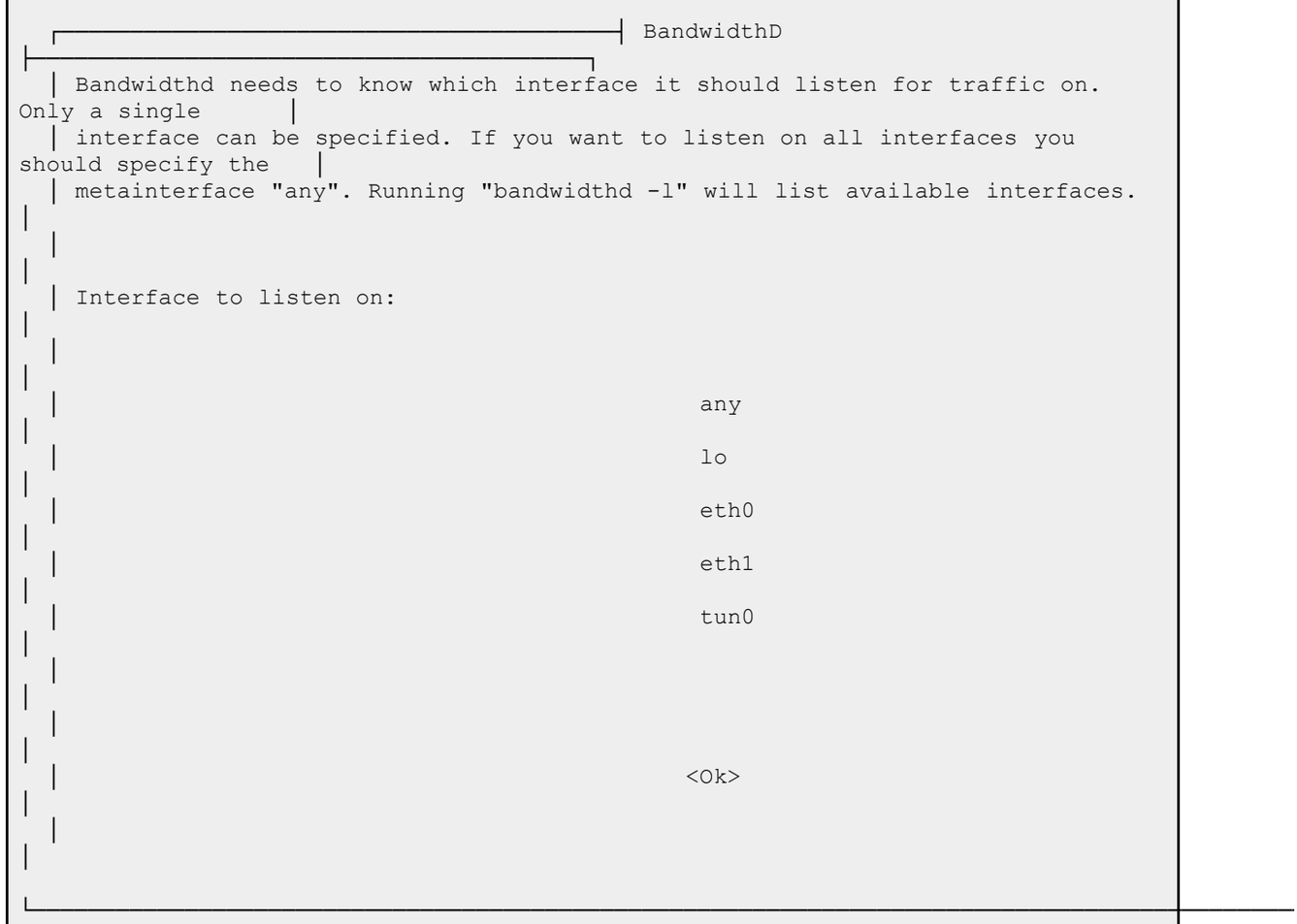
waiting ...

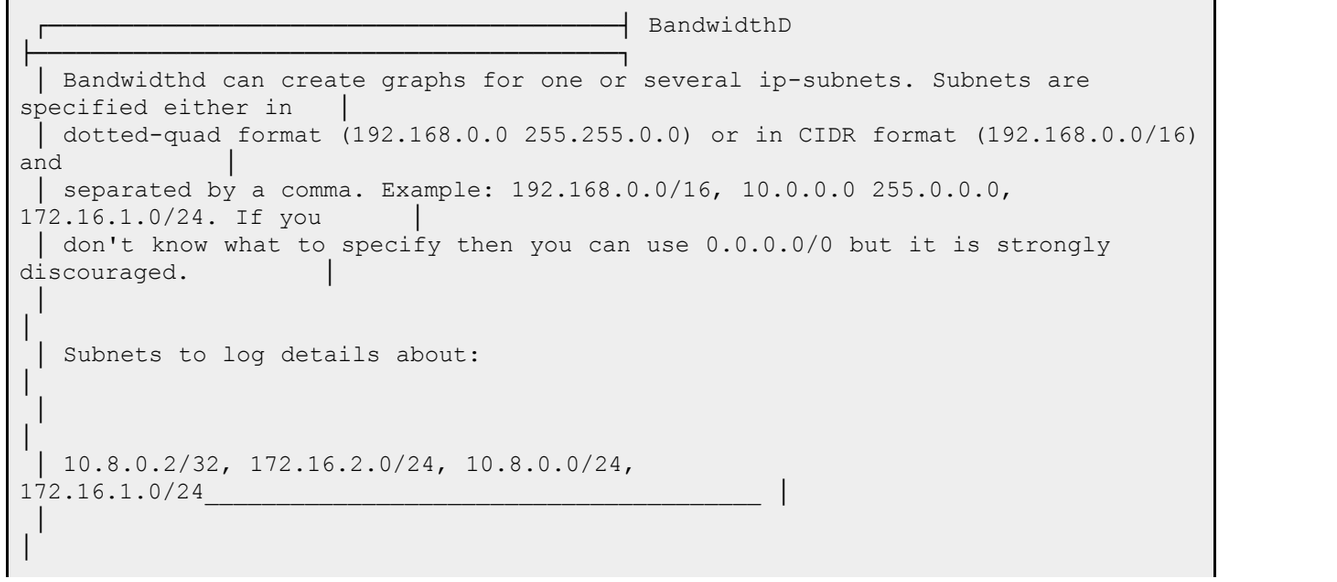
12. Bandwidth

http://bandwidthd.sourceforge.net/

```
$ apt-cache search bandwidthd
bandwidthd - Tracks usage of TCP/IP and builds html files with graphs
bandwidthd-pgsql - Tracks usage of TCP/IP and builds html files with graphs

$ sudo apt-get install bandwidthd
```





```
 |                                                  <Ok>
|
 |
|

└──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
```

```
$ sudo mkdir /www/bandwidth
$ sudo vim /etc/bandwidthd/bandwidthd.conf
htdocs_dir "/www/bandwidthd"

$ sudo /etc/init.d/bandwidthd restart
* Stopping BandwidthD bandwidthd               [ OK ]
* Starting BandwidthD bandwidthd               [ OK ]
```

http://localhost/bandwidthd/index.html

13. OpenNMS

http://www.opennms.org/

14. Performance Co-Pilot

http://oss.sgi.com/projects/pcp/

Performance Co-Pilot (PCP) provides a framework and services to support system-level performance monitoring and management. It presents a unifying abstraction for all of the performance data in a system, and many tools for interrogating, retrieving and processing that data.

15. Clumon Performance Monitor

http://clumon.ncsa.illinois.edu/

16. Zenoss

http://www.linuxjournal.com/article/10070

17. 商业软件

首选上ITM， OpenView

其次Solarwinds

国产 BTNM， siteview

18. OSSIM,Spiceworks,Splunk,FireGen,LANSweeper,OSSEC,HIDS

第 6 章 Web

目录

1. awstats

http://sourceforge.net/projects/awstats/

1. install

```
sudo apt-get install awstats
```

2. configure

sudo vim /etc/awstats/awstats.conf or awstats.conf.local

```
$ sudo vim /etc/awstats/awstats.conf.local

LogFile="/home/netkiller/logs/access_log"
SiteDomain="netkiller.8800.org"
```

or

```
# cd /usr/share/doc/awstats/examples/
#/usr/share/doc/awstats/examples$ perl awstats_configure.pl
```

3. apache

```
sudo cp /usr/share/doc/awstats/examples/apache.conf
/etc/apache2/conf.d/awstats.conf
```

4. how do I test awstats.

http://netkiller.8800.org/awstats/awstats.pl

5. Generating the First Stats

```
sudo -u www-data /usr/bin/perl /usr/lib/cgi-bin/awstats.pl -update -
config=netkiller.8800.org
```

6. Automatising the stats generation using Cron

If we check the file installed by awstats and search for the word cron using the following command line:

```
$ dpkg -L awstats | grep cron
/etc/cron.d
/etc/cron.d/awstats
```

sudo vim /etc/cron.d/awstats

```
0,10,20,30,40,50 * * * * www-data [ -x /usr/lib/cgi-bin/awstats.pl -a -f
/etc/awstats/awstats.conf -a -r /home/netkiller/logs/access.log ] &&
/usr/lib/cgi-bin/awstats.pl -config=netkiller.8800.org -update >/dev/null
```

7. web 测试

http://netkiller.8800.org/awstats/awstats.pl

http://netkiller.8800.org/awstats/awstats.pl?config=other.8800.org

1.1. 语言

```
awstats.pl -update -config=sitename -lang=cn
```

1.2. 输出HTML文档

```
perl awstats.pl -config=www.example.com -output -staticlinks -lang=cn >
awstats.example.html
```

1.3. 多站点配置

```
$ sudo gunzip /usr/share/doc/awstats/examples/awstats.model.conf.gz

$ sudo cp /usr/share/doc/awstats/examples/awstats.model.conf
/etc/awstats/awstats.www.example.com.conf
$ sudo cp /usr/share/doc/awstats/examples/awstats.model.conf
/etc/awstats/awstats.www.other.com.conf
```

```
neo@monitor:/etc/awstats$ vim awstats.www.example.com.conf
LogFile = /opt/logs/21/access.log
SiteDomain="www.example.com"

neo@monitor:/etc/awstats$ vim awstats.www.other.com.conf
LogFile = /opt/logs/22/access.log
SiteDomain="www.other.com"
```

```
$ sudo -u www-data /usr/bin/perl /usr/lib/cgi-bin/awstats.pl -update -
config=www.example.com
$ sudo -u www-data /usr/bin/perl /usr/lib/cgi-bin/awstats.pl -update -
config=www.other.com
```

```
http://localhost/cgi-bin/awstats.pl?config=www.example.com
http://localhost/cgi-bin/awstats.pl?config=www.other.com
```

批量生成

```
awstats_updateall.pl now -awstatsprog=/usr/lib/cgi-bin/awstats.pl -
configdir=/etc/awstats/
```

1.4. 合并日志

/usr/share/doc/awstats/examples/logresolvemerge.pl

```
$ vim awstats.www.example.com.conf
LogFile="/usr/share/doc/awstats/examples/logresolvemerge.pl
/var/log/*/access_log.* |"
LogFile="/usr/share/doc/awstats/examples/logresolvemerge.pl
/mnt/*/logs/www/access.%YYYY-24-%MM-24-%DD-24.log |"
```

```
sudo -u www-data /usr/bin/perl /usr/lib/cgi-bin/awstats.pl -update -
config=www.examples.com
```

http://localhost/cgi-bin/awstats.pl?config=www.example.com

```
$ grep -v "^#" awstats.www.example.com.conf | sed /^$/d
LogFile="/usr/share/doc/awstats/examples/logresolvemerge.pl
/mnt/*/logs/www/access.%YYYY-24-%MM-24-%DD-24.log |"
LogType=W
LogFormat=1
LogSeparator=" "
SiteDomain="www.example.com"
HostAliases="localhost 127.0.0.1 REGEX[myserver\.com$]"
DNSLookup=2
DirData="."
DirCgi="/cgi-bin"
DirIcons="/icon"
AllowToUpdateStatsFromBrowser=0
AllowFullYearView=2
EnableLockForUpdate=0
DNSStaticCacheFile="dnscache.txt"
DNSLastUpdateCacheFile="dnscachelastupdate.txt"
SkipDNSLookupFor=""
AllowAccessFromWebToAuthenticatedUsersOnly=0
AllowAccessFromWebToFollowingAuthenticatedUsers=""
AllowAccessFromWebToFollowingIPAddresses=""
CreateDirDataIfNotExists=0
BuildHistoryFormat=text
BuildReportFormat=html
SaveDatabaseFilesWithPermissionsForEveryone=0
PurgeLogFile=0
ArchiveLogRecords=0
KeepBackupOfHistoricFiles=0
DefaultFile="index.html"
SkipHosts=""
SkipUserAgents=""
SkipFiles=""
SkipReferrersBlackList=""
OnlyHosts=""
OnlyUserAgents=""
OnlyUsers=""
OnlyFiles=""
NotPageList="css js class gif jpg jpeg png bmp ico rss xml swf"
ValidHTTPCodes="200 304"
ValidSMTPCodes="1 250"
AuthenticatedUsersNotCaseSensitive=0
URLNotCaseSensitive=0
URLWithAnchor=0
URLQuerySeparators="?;"
URLWithQuery=0
URLWithQueryWithOnlyFollowingParameters=""
URLWithQueryWithoutFollowingParameters=""
URLReferrerWithQuery=0
WarningMessages=1
ErrorMessages=""
DebugMessages=0
NbOfLinesForCorruptedLog=50
WrapperScript=""
DecodeUA=0
MiscTrackerUrl="/js/awstats_misc_tracker.js"
LevelForBrowsersDetection=2         # 0 disables Browsers detection.
                                    # 2 reduces AWStats speed by 2%
                                    # allphones reduces AWStats speed by 5%
```

```
LevelForOSDetection=2                # 0 disables OS detection.
                                      # 2 reduces AWStats speed by 3%
LevelForRefererAnalyze=2             # 0 disables Origin detection.
                                      # 2 reduces AWStats speed by 14%
LevelForRobotsDetection=2            # 0 disables Robots detection.
                                      # 2 reduces AWStats speed by 2.5%
LevelForSearchEnginesDetection=2     # 0 disables Search engines detection.
                                      # 2 reduces AWStats speed by 9%
LevelForKeywordsDetection=2          # 0 disables Keyphrases/Keywords detection.
                                      # 2 reduces AWStats speed by 1%
LevelForFileTypesDetection=2         # 0 disables File types detection.
                                      # 2 reduces AWStats speed by 1%
LevelForWormsDetection=0             # 0 disables Worms detection.
                                      # 2 reduces AWStats speed by 15%
UseFramesWhenCGI=1
DetailedReportsOnNewWindows=1
Expires=0
MaxRowsInHTMLOutput=1000
Lang="auto"
DirLang="./lang"
ShowMenu=1
ShowSummary=UVPHB
ShowMonthStats=UVPHB
ShowDaysOfMonthStats=VPHB
ShowDaysOfWeekStats=PHB
ShowHoursStats=PHB
ShowDomainsStats=PHB
ShowHostsStats=PHBL
ShowAuthenticatedUsers=0
ShowRobotsStats=HBL
ShowWormsStats=0
ShowEMailSenders=0
ShowEMailReceivers=0
ShowSessionsStats=1
ShowPagesStats=PBEX
ShowFileTypesStats=HB
ShowFileSizesStats=0
ShowOSStats=1
ShowBrowsersStats=1
ShowScreenSizeStats=0
ShowOriginStats=PH
ShowKeyphrasesStats=1
ShowKeywordsStats=1
ShowMiscStats=a
ShowHTTPErrorsStats=1
ShowSMTPErrorsStats=0
ShowClusterStats=0
AddDataArrayMonthStats=1
AddDataArrayShowDaysOfMonthStats=1
AddDataArrayShowDaysOfWeekStats=1
AddDataArrayShowHoursStats=1
IncludeInternalLinksInOriginSection=0
MaxNbOfDomain = 10
MinHitDomain  = 1
MaxNbOfHostsShown = 10
MinHitHost    = 1
MaxNbOfLoginShown = 10
MinHitLogin   = 1
MaxNbOfRobotShown = 10
MinHitRobot   = 1
MaxNbOfPageShown = 10
MinHitFile    = 1
MaxNbOfOsShown = 10
MinHitOs      = 1
MaxNbOfBrowsersShown = 10
MinHitBrowser = 1
MaxNbOfScreenSizesShown = 5
MinHitScreenSize = 1
MaxNbOfWindowSizesShown = 5
MinHitWindowSize = 1
MaxNbOfRefererShown = 10
MinHitRefer   = 1
MaxNbOfKeyphrasesShown = 10
MinHitKeyphrase = 1
MaxNbOfKeywordsShown = 10
MinHitKeyword = 1
MaxNbOfEMailsShown = 20
MinHitEMail   = 1
FirstDayOfWeek=1
ShowFlagLinks=""
ShowLinksOnUrl=1
UseHTTPSLinkForUrl=""
MaxLengthOfShownURL=64
HTMLHeadSection=""
```

```
HTMLEndSection=""
Logo="awstats_logo6.png"
LogoLink="http://awstats.sourceforge.net"
BarWidth   = 260
BarHeight  = 90
StyleSheet=""
color_Background="FFFFFF"               # Background color for main page (Default
= "FFFFFF")
color_TableBGTitle="CCCCDD"             # Background color for table title
(Default = "CCCCDD")
color_TableTitle="000000"               # Table title font color (Default =
"000000")
color_TableBG="CCCCDD"                  # Background color for table (Default =
"CCCCDD")
color_TableRowTitle="FFFFFF"    # Table row title font color (Default = "FFFFFF")
color_TableBGRowTitle="ECECEC"  # Background color for row title (Default =
"ECECEC")
color_TableBorder="ECECEC"              # Table border color (Default = "ECECEC")
color_text="000000"                             # Color of text (Default =
"000000")
color_textpercent="606060"              # Color of text for percent values
(Default = "606060")
color_titletext="000000"                # Color of text title within colored
Title Rows (Default = "000000")
color_weekend="EAEAEA"                  # Color for week-end days (Default =
"EAEAEA")
color_link="0011BB"                             # Color of HTML links (Default =
"0011BB")
color_hover="605040"                    # Color of HTML on-mouseover links
(Default = "605040")
color_u="FFAA66"                                # Background color for number of
unique visitors (Default = "FFAA66")
color_v="F4F090"                                # Background color for number of
visites (Default = "F4F090")
color_p="4477DD"                                # Background color for number of
pages (Default = "4477DD")
color_h="66DDEE"                                # Background color for number of
hits (Default = "66DDEE")
color_k="2EA495"                                # Background color for number of
bytes (Default = "2EA495")
color_s="8888DD"                                # Background color for number of
search (Default = "8888DD")
color_e="CEC2E8"                                # Background color for number of
entry pages (Default = "CEC2E8")
color_x="C1B2E2"                                # Background color for number of
exit pages (Default = "C1B2E2")
ExtraTrackedRowsLimit=500
```

1.5. Flush history file on disk (unique url reach flush limit of 5000) 优化

```
$LIMITFLUSH=50000
```

1.6. JAWStats

http://www.jawstats.com/

---

2. webalizer

What is Webalizer?

The Webalizer is a fast, free web server log file analysis program. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser

1. install webalizer

```
sudo apt-get install webalizer
```

2. config

```
vim /etc/webalizer/webalizer.conf

LogFile /home/netkiller/logs/access.log
OutputDir /home/netkiller/public_html/webalizer
```

rotate log

```
Incremental yes
```

3. crontab

/etc/cron.daily/webalizer

```
netkiller@shenzhen:~$ cat /etc/cron.daily/webalizer
#!/bin/sh
# /etc/cron.daily/webalizer: Webalizer daily maintenance script
# This script was originally written by
# Remco van de Meent <remco@debian.org>
# and now, all rewrited by Jose Carlos Medeiros <jose@psabs.com.br>

# This script just run webalizer agains all .conf files in /etc/webalizer
directory

WEBALIZER=/usr/bin/webalizer
WEBALIZER_CONFDIR=/etc/webalizer

[ -x ${WEBALIZER} ] || exit 0;
[ -d ${WEBALIZER_CONFDIR} ] || exit 0;

for i in ${WEBALIZER_CONFDIR}/*.conf; do
  # run agains a rotated or normal logfile
  LOGFILE=`awk '$1 ~ /^LogFile$/ {print $2}' $i`;

  # empty ?
  [ -s "${LOGFILE}" ] || continue;
  # readable ?
  [ -r "${LOGFILE}" ] || continue;

  # there was a output ?
  OUTDIR=`awk '$1 ~ /^OutputDir$/ {print $2}' $i`;
  #  exists something ?
  [ "${OUTDIR}" != "" ] || continue;
  # its a directory ?
  [ -d ${OUTDIR} ] || continue;
  # its writable ?
  [ -w ${OUTDIR} ] || continue;

  # Run Really quietly, exit with status code if !0
```

```
  ${WEBALIZER} -c ${i} -Q || continue;
  RET=$?;

  # Non rotated log file
  NLOGFILE=`awk '$1 ~ /^LogFile$/ {gsub(/\.[0-9]+(\.gz)?/,""); print $2}'
$i`;

  # check current log, if last log is a rotated logfile
  if [ "${LOGFILE}" != "${NLOGFILE}" ]; then
    # empty ?
    [ -s "${NLOGFILE}" ] || continue;
    # readable ?
    [ -r "${NLOGFILE}" ] || continue;

    ${WEBALIZER} -c ${i} -Q ${NLOGFILE};
    RET=$?;
  fi;
done;

# exit with webalizer's exit code
exit $RET;
```

4. initialization

```
sudo /usr/bin/webalizer
```

5. http://netkiller.8800.org/webalizer/

```
最后附上Webalizer的参数表:
可以执行webalizer -h得到所有命令行参数:
Usage: webalizer [options] [log file]
-h = 打印帮助信息
-v -V = 打印版本信息
-d = 打印附加调试信息
-F type = 日志格式类型. type= (clf | ftp | squid)
-i = 忽略历史文件
-p = 保留状态 (递增模式)
-q = 忽略消息信息
-Q = 忽略所有信息
-Y = 忽略国家图形
-G = 忽略小时统计图形
-H = 忽略小时统计信息
-L = 忽略彩色图例
-l num = 在图形中使用数字背景线
-m num = 访问超时 (seconds)
-T = 打印时间信息
-c file = 指定配置文件
-n name = 使用的主机名
-o dir = 结果输出目录
-t name = 指定报告题目上的主机名
-a name = 隐藏用户代理名称
-r name = 隐藏访问链接
-s name = 隐藏客户
-u name = 隐藏URL
-x name = 使用文件扩展名
-P name = 页面类型扩展名
-I name = index别名
-A num = 显示前几名客户类型
-C num = 显示前几名国家
-R num = 显示前几名链接
-S num = 显示前几名客户
-U num = 显示前几名URLs
-e num = 显示前几名访问页面
-E num = 显示前几名不存在的页面
-X = 隐藏个别用户
-D name = 使用dns缓存文件
-N num = DNS 进程数 (0=禁用dns)
```

2.1. 手工生成

```
$ sudo webalizer -c /etc/webalizer/webalizer.conf -o /var/www/webalizer/web2
/opt/logs/web2/www/access_log
```

分析多个文件

```
# find ./ -exec sudo webalizer -p -c /etc/webalizer/webalizer.conf -o
/var/www/webalizer/my /mnt/logs/www/{} \;
```

2.2. 批量处理历史数据

下面脚本可以批量处理历史日志,等这个脚本运行完后在crontab中加入另一个脚本。

```
for f in /mnt/logs/cdn/*.gz ; do webalizer -c /etc/webalizer/webalizer.conf -o
/var/www/webalizer/cdn/ $f ; done
```

crontab

```
webalizer -c /etc/webalizer/webalizer.conf -o /var/www/webalizer/cdn/
/mnt/logs/cdn/$(date -d '-1 day' +'%Y-%m-%d').log.gz
```

多域名批量处理

```
for d in /mnt/cdn/* ; do
    htmldir=/var/www/webalizer/$(basename $d)
    mkdir -p $htmldir
    for f in $d/*.log.gz ; do webalizer -c /etc/webalizer/webalizer.conf -o
$htmldir $f ; done
done
```

crontab

```
#!/bin/bash
for d in /mnt/cdn/*;
do
    htmldir=/var/www/webalizer/$(basename $d)
    mkdir -p $htmldir
    webalizer -c /etc/webalizer/webalizer.conf -o $htmldir $d/$(date -d '-1 day'
+'%Y_%m_%d').log.gz
done
```

2.3. crontab

```
sudo webalizer  -F clf -p -t www.example.com -Q -c /etc/webalizer/webalizer.conf
-o /var/www/webalizer/xiu /mnt/logs/www/access.$(date -d '-1 day' +'%Y-%m-%d').log
```

第 7 章 SMS

目录

1. gnokii

http://www.gnokii.org

```
neo@monitor:~$ apt-cache search gnokii
opensync-plugin-gnokii - Opensync gnokii plugin
gnokii - Datasuite for mobile phone management
gnokii-cli - Datasuite for mobile phone management (console interface)
gnokii-common - Datasuite for mobile phone management (base files)
gnokii-smsd - SMS Daemon for mobile phones
gnokii-smsd-mysql - SMSD plugin for MySQL storage backend
gnokii-smsd-pgsql - SMSD plugin for PostgreSQL storage backend
libgnokii-dev - Gnokii mobile phone interface library (development files)
libgnokii5 - Gnokii mobile phone interface library
xgnokii - Datasuite for mobile phone management (X interface)


neo@monitor:~$ sudo apt-get install gnokii-cli
```

```

vim /etc/gnokiirc
or
vim ~/.gnokiirc

[global]
port = /dev/ttyS0
model = AT
initlength = default
connection = serial
serial_baudrate = 19200
smsc_timeout = 10
```

```

$ echo "This is a test message" | gnokii --sendsms +13113668890

$ gnokii --sendsms number <<EOF
hi neo,
This is a test message
EOF

$ gnokii --dialvoice number
```

2. AT Commands

```
AT
AT+CSCA=+86
AT+CMGF=1
AT+CMGS="13122993040"
Hello,This is the test of GSM module! Ctrl+z
```

第 8 章 IPMI (Intelligent Platform Management Interface)

目录


```
OpenIPMI: http://openipmi.sourceforge.net/
Ipmitool:  http://ipmitool.sourceforge.net/
ipmiutil:  http://ipmiutil.sourceforge.net/
```

1. OpenIPMI

```
# yum install OpenIPMI
```

start

```
/etc/init.d/ipmi start
Starting ipmi drivers:                                     [  OK  ]
```

2. freeipmi

```
# yum install freeipmi
```

2.1. ipmiping

```
# ipmiping 172.16.5.52
ipmiping 172.16.5.52 (172.16.5.52)
response received from 172.16.5.52: rq_seq=57
response received from 172.16.5.52: rq_seq=58
response received from 172.16.5.52: rq_seq=59
response received from 172.16.5.52: rq_seq=60
response received from 172.16.5.52: rq_seq=61
^C--- ipmiping 172.16.5.52 statistics ---
5 requests transmitted, 5 responses received in time, 0.0% packet loss
```

2.2. ipmimonitoring

```
# ipmimonitoring -h 172.16.1.23 -u root -pcalvin
Caching SDR repository information: /root/.freeipmi/sdr-cache/sdr-cache-J10-51-
Memcache-0.172.16.5.23
Caching SDR record 125 of 125 (current record ID 125)
Record_ID | Sensor Name | Sensor Group | Monitoring Status| Sensor Units | Sensor
Reading
7 | Ambient Temp | Temperature | Nominal | C | 27.000000
9 | CMOS Battery | Battery | Nominal | N/A | 'OK'
10 | VCORE PG | Voltage | Nominal | N/A | 'State Deasserted'
11 | VCORE PG | Voltage | Nominal | N/A | 'State Deasserted'
13 | 1.5V PG | Voltage | Nominal | N/A | 'State Deasserted'
14 | 1.8V PG | Voltage | Nominal | N/A | 'State Deasserted'
15 | 3.3V PG | Voltage | Nominal | N/A | 'State Deasserted'
16 | 5V PG | Voltage | Nominal | N/A | 'State Deasserted'
17 | 0.75VTT PG | Voltage | Nominal | N/A | 'State Deasserted'
19 | HEATSINK PRES | Entity Presence | Nominal | N/A | 'Entity Present'
20 | iDRAC6 Ent PRES | Entity Presence | Nominal | N/A | 'Entity Present'
21 | USB CABLE PRES | Entity Presence | Nominal | N/A | 'Entity Present'
22 | STOR ADAPT PRES | Entity Presence | Nominal | N/A | 'Entity Present'
23 | RISER2 PRES | Entity Presence | Nominal | N/A | 'Entity Present'
24 | RISER1 PRES | Entity Presence | Nominal | N/A | 'Entity Present'
25 | 0.75 VTT PG | Voltage | Nominal | N/A | 'State Deasserted'
26 | MEM PG | Voltage | Nominal | N/A | 'State Deasserted'
27 | MEM PG | Voltage | Nominal | N/A | 'State Deasserted'
28 | 0.9V PG | Voltage | Nominal | N/A | 'State Deasserted'
29 | VTT PG | Voltage | Nominal | N/A | 'State Deasserted'
30 | VTT PG | Voltage | Nominal | N/A | 'State Deasserted'
31 | 1.8 PLL PG | Voltage | Nominal | N/A | 'State Deasserted'
32 | 1.8 PLL PG | Voltage | Nominal | N/A | 'State Deasserted'
33 | 8.0V PG | Voltage | Nominal | N/A | 'State Deasserted'
34 | 1.1V PG | Voltage | Nominal | N/A | 'State Deasserted'
35 | 1.0V LOM PG | Voltage | Nominal | N/A | 'State Deasserted'
36 | 1.0V AUX PG | Voltage | Nominal | N/A | 'State Deasserted'
37 | 1.05V PG | Voltage | Nominal | N/A | 'State Deasserted'
38 | FAN MOD 1A RPM | Fan | Nominal | RPM | 5040.000000
39 | FAN MOD 2A RPM | Fan | Nominal | RPM | 7800.000000
40 | FAN MOD 3A RPM | Fan | Nominal | RPM | 8040.000000
41 | FAN MOD 4A RPM | Fan | Nominal | RPM | 8760.000000
42 | FAN MOD 5A RPM | Fan | Nominal | RPM | 8640.000000
43 | FAN MOD 6A RPM | Fan | Nominal | RPM | 5040.000000
44 | FAN MOD 1B RPM | Fan | Nominal | RPM | 3840.000000
45 | FAN MOD 2B RPM | Fan | Nominal | RPM | 6000.000000
46 | FAN MOD 3B RPM | Fan | Nominal | RPM | 6120.000000
47 | FAN MOD 4B RPM | Fan | Nominal | RPM | 6600.000000
48 | FAN MOD 5B RPM | Fan | Nominal | RPM | 6600.000000
```

```
49 | FAN MOD 6B RPM | Fan | Nominal | RPM | 3840.000000
50 | Presence | Entity Presence | Nominal | N/A | 'Entity Present'
51 | Presence | Entity Presence | Nominal | N/A | 'Entity Present'
52 | Presence | Entity Presence | Nominal | N/A | 'Entity Present'
53 | Presence | Entity Presence | Nominal | N/A | 'Entity Present'
54 | Presence  | Entity Presence | Nominal | N/A | 'Entity Present'
55 | Status | Processor | Nominal | N/A | 'Processor Presence detected'
56 | Status | Processor | Nominal | N/A | 'Processor Presence detected'
57 | Status | Power Supply | Nominal | N/A | 'Presence detected'
58 | Status | Power Supply | Critical | N/A | 'Presence detected' 'Power Supply
input lost (AC/DC)'
59 | Riser Config | Cable/Interconnect | Nominal | N/A | 'Cable/Interconnect is
connected'
60 | OS Watchdog | Watchdog 2 | Nominal | N/A | 'OK'
62 | Intrusion | Physical Security | Nominal | N/A | 'OK'
64 | Fan Redundancy | Fan | Nominal | N/A | 'Fully Redundant'
66 | Drive | Drive Slot | Nominal | N/A | 'Drive Presence'
67 | Cable SAS A | Cable/Interconnect | Nominal | N/A | 'Cable/Interconnect is
connected'
68 | Cable SAS B | Cable/Interconnect | Nominal | N/A | 'Cable/Interconnect is
connected'
116 | Current | Current | Nominal | A | 1.400000
118 | Voltage | Voltage | Nominal | V | 220.000000
120 | System Level | Current | Nominal | W | 329.000000
123 | ROMB Battery | Battery | Nominal | N/A | 'OK'
```

2.3. ipmi-sensors

```
# ipmi-sensors -h 172.16.5.23 -u root -pcalvin
1: Temp (Temperature): NA (NA/90.00): [NA]
2: Temp (Temperature): NA (NA/90.00): [NA]
3: Temp (Temperature): NA (NA/NA): [NA]
4: Ambient Temp (Temperature): NA (NA/NA): [NA]
5: Temp (Temperature): NA (NA/NA): [NA]
6: Ambient Temp (Temperature): NA (NA/NA): [NA]
7: Ambient Temp (Temperature): 27.00 C (3.00/47.00): [OK]
8: Planar Temp (Temperature): NA (3.00/97.00): [NA]
9: CMOS Battery (Battery): [OK]
10: VCORE PG (Voltage): [State Deasserted]
11: VCORE PG (Voltage): [State Deasserted]
12: IOH THERMTRIP (Temperature): [NA]
13: 1.5V PG (Voltage): [State Deasserted]
14: 1.8V PG (Voltage): [State Deasserted]
15: 3.3V PG (Voltage): [State Deasserted]
16: 5V PG (Voltage): [State Deasserted]
17: 0.75VTT PG (Voltage): [State Deasserted]
18: PFault Fail Safe (Voltage): [Unknown]
19: HEATSINK PRES (Entity Presence): [Entity Present]
20: iDRAC6 Ent PRES (Entity Presence): [Entity Present]
21: USB CABLE PRES (Entity Presence): [Entity Present]
22: STOR ADAPT PRES (Entity Presence): [Entity Present]
23: RISER2 PRES (Entity Presence): [Entity Present]
24: RISER1 PRES (Entity Presence): [Entity Present]
25: 0.75 VTT PG (Voltage): [State Deasserted]
26: MEM PG (Voltage): [State Deasserted]
27: MEM PG (Voltage): [State Deasserted]
28: 0.9V PG (Voltage): [State Deasserted]
29: VTT PG (Voltage): [State Deasserted]
30: VTT PG (Voltage): [State Deasserted]
31: 1.8 PLL PG (Voltage): [State Deasserted]
32: 1.8 PLL PG (Voltage): [State Deasserted]
33: 8.0V PG (Voltage): [State Deasserted]
34: 1.1V PG (Voltage): [State Deasserted]
35: 1.0V LOM PG (Voltage): [State Deasserted]
36: 1.0V AUX PG (Voltage): [State Deasserted]
37: 1.05V PG (Voltage): [State Deasserted]
38: FAN MOD 1A RPM (Fan): 5040.00 RPM (1920.00/NA): [OK]
39: FAN MOD 2A RPM (Fan): 8040.00 RPM (1920.00/NA): [OK]
40: FAN MOD 3A RPM (Fan): 7920.00 RPM (1920.00/NA): [OK]
41: FAN MOD 4A RPM (Fan): 9240.00 RPM (1920.00/NA): [OK]
42: FAN MOD 5A RPM (Fan): 9120.00 RPM (1920.00/NA): [OK]
43: FAN MOD 6A RPM (Fan): 5040.00 RPM (1920.00/NA): [OK]
44: FAN MOD 1B RPM (Fan): 3840.00 RPM (1920.00/NA): [OK]
45: FAN MOD 2B RPM (Fan): 6120.00 RPM (1920.00/NA): [OK]
46: FAN MOD 3B RPM (Fan): 6000.00 RPM (1920.00/NA): [OK]
47: FAN MOD 4B RPM (Fan): 6960.00 RPM (1920.00/NA): [OK]
48: FAN MOD 5B RPM (Fan): 6960.00 RPM (1920.00/NA): [OK]
49: FAN MOD 6B RPM (Fan): 3840.00 RPM (1920.00/NA): [OK]
50: Presence (Entity Presence): [Entity Present]
51: Presence (Entity Presence): [Entity Present]
52: Presence (Entity Presence): [Entity Present]
```

```
53: Presence (Entity Presence): [Entity Present]
54: Presence  (Entity Presence): [Entity Present]
55: Status (Processor): [Processor Presence detected]
56: Status (Processor): [Processor Presence detected]
57: Status (Power Supply): [Presence detected]
58: Status (Power Supply): [Presence detected][Power Supply input lost (AC/DC)]
59: Riser Config (Cable/Interconnect): [Cable/Interconnect is connected]
60: OS Watchdog (Watchdog 2): [OK]
61: SEL (Event Logging Disabled): [Unknown]
62: Intrusion (Physical Security): [OK]
63: PS Redundancy (Power Supply): [NA]
64: Fan Redundancy (Fan): [Fully Redundant]
65: CPU Temp Interf (Temperature): [NA]
66: Drive (Drive Slot): [Drive Presence]
67: Cable SAS A (Cable/Interconnect): [Cable/Interconnect is connected]
68: Cable SAS B (Cable/Interconnect): [Cable/Interconnect is connected]
69: DKM Status (OEM Reserved): [OEM State = 0000h]
79: ECC Corr Err (Memory): [Unknown]
80: ECC Uncorr Err (Memory): [Unknown]
81: I/O Channel Chk (Critical Interrupt): [Unknown]
82: PCI Parity Err (Critical Interrupt): [Unknown]
83: PCI System Err (Critical Interrupt): [Unknown]
84: SBE Log Disabled (Event Logging Disabled): [Unknown]
85: Logging Disabled (Event Logging Disabled): [Unknown]
86: Unknown (System Event): [Unknown]
87: CPU Protocol Err (Processor): [Unknown]
88: CPU Bus PERR (Processor): [Unknown]
89: CPU Init Err (Processor): [Unknown]
90: CPU Machine Chk (Processor): [Unknown]
91: Memory Spared (Memory): [Unknown]
92: Memory Mirrored (Memory): [Unknown]
93: Memory RAID (Memory): [Unknown]
94: Memory Added (Memory): [Unknown]
95: Memory Removed (Memory): [Unknown]
96: Memory Cfg Err (Memory): [Unknown]
97: Mem Redun Gain (Memory): [Unknown]
98: PCIE Fatal Err (Critical Interrupt): [Unknown]
99: Chipset Err (Critical Interrupt): [Unknown]
100: Err Reg Pointer (OEM Reserved): [Unknown]
101: Mem ECC Warning (Memory): [Unknown]
102: Mem CRC Err (Memory): [Unknown]
103: USB Over-current (Memory): [Unknown]
104: POST Err (System Firmware Progress): [Unknown]
105: Hdwr version err (Version Change): [Unknown]
106: Mem Overtemp (Memory): [Unknown]
107: Mem Fatal SB CRC (Memory): [Unknown]
108: Mem Fatal NB CRC (Memory): [Unknown]
109: OS Watchdog Time (Watchdog 1): [Unknown]
110: Non Fatal PCI Er (OEM Reserved): [Unknown]
111: Fatal IO Error (OEM Reserved): [Unknown]
112: MSR Info Log (OEM Reserved): [Unknown]
113: Temp (Temperature): NA (NA/NA): [NA]
114: Temp (Temperature): NA (3.00/47.00): [NA]
115: Temp (Temperature): NA (3.00/47.00): [NA]
116: Current (Current): 1.40 A (NA/NA): [OK]
117: Current (Current): NA (NA/NA): [Unknown]
118: Voltage (Voltage): 220.00 V (NA/NA): [OK]
119: Voltage (Voltage): NA (NA/NA): [Unknown]
120: System Level (Current): 329.00 W (NA/966.00): [OK]
121: Power Optimized (OEM Reserved): [Unrecognized State]
123: ROMB Battery (Battery): [OK]
125: vFlash (Module/Board): [OEM State = 0000h]
```

2.4. ipmi-locate

```
# ipmi-locate
Probing KCS device using DMIDECODE... done
IPMI Version: 2.0
IPMI locate driver: DMIDECODE
IPMI interface: KCS
BMC driver device:
BMC I/O base address: 0xCA8
Register spacing: 4

Probing SMIC device using DMIDECODE... FAILED

Probing BT device using DMIDECODE... FAILED

Probing SSIF device using DMIDECODE... FAILED

Probing KCS device using SMBIOS... done
```

```
IPMI Version: 2.0
IPMI locate driver: SMBIOS
IPMI interface: KCS
BMC driver device:
BMC I/O base address: 0xCA8
Register spacing: 4

Probing SMIC device using SMBIOS... FAILED

Probing BT device using SMBIOS... FAILED

Probing SSIF device using SMBIOS... FAILED

Probing KCS device using ACPI... FAILED

Probing SMIC device using ACPI... FAILED

Probing BT device using ACPI... FAILED

Probing SSIF device using ACPI... FAILED

Probing KCS device using PCI... FAILED

Probing SMIC device using PCI... FAILED

Probing BT device using PCI... FAILED

Probing SSIF device using PCI... FAILED

KCS device default values:
IPMI Version: 1.5
IPMI locate driver: DEFAULT
IPMI interface: KCS
BMC driver device:
BMC I/O base address: 0xCA2
Register spacing: 1

SMIC device default values:
IPMI Version: 1.5
IPMI locate driver: DEFAULT
IPMI interface: SMIC
BMC driver device:
BMC I/O base address: 0xCA9
Register spacing: 1

BT device default values:
SSIF device default values:
IPMI Version: 1.5
IPMI locate driver: DEFAULT
IPMI interface: SSIF
BMC driver device: /dev/i2c-0
BMC SMBUS slave address: 0x42
Register spacing: 1
```

3. ipmitool - utility for controlling IPMI-enabled devices

3.1. ipmitool

3.1.1. ubuntu

确定硬件是否支持 IPMI

```
neo@monitor:~$ sudo dmidecode |grep -C 5 IPMI
[sudo] password for neo:
Handle 0x2000, DMI type 32, 11 bytes
System Boot Information
        Status: No errors detected

Handle 0x2600, DMI type 38, 18 bytes
IPMI Device Information
        Interface Type: KCS (Keyboard Control Style)
        Specification Version: 2.0
        I2C Slave Address: 0x10
        NV Storage Device: Not Present
        Base Address: 0x0000000000000CA8 (I/O)
```

```
sudo apt-get install openipmi

sudo apt-get install ipmitool

sudo mkdir -p /var/lock/subsys/ipmi

$ sudo /etc/init.d/openipmi start
 * Starting ipmi drivers                  [ OK ]
```

3.1.2. CentOS

```
# yum search ipmi
============================================ Matched: ipmi
============================================
OpenIPMI.x86_64 : OpenIPMI (Intelligent Platform Management Interface) library and
tools
OpenIPMI-devel.i386 : The development environment for the OpenIPMI project.
OpenIPMI-devel.x86_64 : The development environment for the OpenIPMI project.
OpenIPMI-gui.x86_64 : IPMI graphical user interface tool
OpenIPMI-libs.i386 : The OpenIPMI runtime libraries
OpenIPMI-libs.x86_64 : The OpenIPMI runtime libraries
OpenIPMI-perl.x86_64 : OpenIPMI Perl language bindings
OpenIPMI-python.x86_64 : OpenIPMI Python language bindings
OpenIPMI-tools.x86_64 : OpenIPMI utilities and scripts from ipmitool
collectd-ipmi.x86_64 : IPMI module for collectd
freeipmi.i386 : FreeIPMI
freeipmi.x86_64 : FreeIPMI
freeipmi-bmc-watchdog.x86_64 : FreeIPMI BMC watchdog
freeipmi-devel.i386 : Development package for FreeIPMI
freeipmi-devel.x86_64 : Development package for FreeIPMI
freeipmi-ipmidetectd.x86_64 : IPMI node detection monitoring daemon
openhpi.i386 : openhpi Hardware Platform Interface (HPI) library and tools
openhpi.x86_64 : openhpi Hardware Platform Interface (HPI) library and tools
ripmime.x86_64 : Extract attachments out of a MIME encoded email packages
watchdog.x86_64 : Software and/or Hardware watchdog daemon

# yum install OpenIPMI OpenIPMI-tools -y
```

3.2. sensor

```
# ipmitool -I open sensor list
```

3.3. ipmitool shell

```
# ipmitool shell
```

mc info

```
ipmitool> mc info
Device ID                 : 32
Device Revision           : 0
Firmware Revision         : 1.54
IPMI Version              : 2.0
Manufacturer ID           : 674
Manufacturer Name         : DELL Inc
Product ID                : 256 (0x0100)
Product Name              : Unknown (0x100)
Device Available          : yes
Provides Device SDRs      : yes
Additional Device Support :
    Sensor Device
    SDR Repository Device
    SEL Device
    FRU Inventory Device
    IPMB Event Receiver
    Bridge
    Chassis Device
Aux Firmware Rev Info     :
    0x00
    0x0f
    0x00
    0x00


ipmitool> lan print 1
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD
Auth Type Enable        : Callback : MD2 MD5
                        : User     : MD2 MD5
                        : Operator : MD2 MD5
                        : Admin    : MD2 MD5
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 172.16.1.132
Subnet Mask             : 255.255.255.0
MAC Address             : 84:2b:2b:fd:e2:51
SNMP Community String   : public
IP Header               : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
Default Gateway IP      : 172.16.1.254
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14
Cipher Suite Priv Max   : aaaaaaaaaaaaaaa
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
```

3.4. ipmitool 访问远程主机

```
# ipmitool -H 172.16.1.155 -U root -P 123456 lan print 1
Set in Progress         : Set Complete
```

```
Auth Type Support       : NONE MD2 MD5 PASSWORD
Auth Type Enable        : Callback : MD2 MD5
                        : User     : MD2 MD5
                        : Operator : MD2 MD5
                        : Admin    : MD2 MD5
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 172.16.1.15
Subnet Mask             : 255.255.255.0
MAC Address             : 84:2b:2b:fc:fb:cc
SNMP Community String   : public
IP Header               : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
Default Gateway IP      : 172.16.1.254
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14
Cipher Suite Priv Max   : aaaaaaaaaaaaaaa
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
```

3.5. Get chassis status and set power state

```
# ipmitool -I open chassis
Chassis Commands:  status, power, identify, policy, restart_cause, poh, bootdev,
bootparam, selftest

# ipmitool -I open chassis status
System Power         : on
Power Overload       : false
Power Interlock      : inactive
Main Power Fault     : false
Power Control Fault  : false
Power Restore Policy : previous
Last Power Event     :
Chassis Intrusion    : inactive
Front-Panel Lockout  : inactive
Drive Fault          : false
Cooling/Fan Fault    : false
Sleep Button Disable : not allowed
Diag Button Disable  : allowed
Reset Button Disable : not allowed
Power Button Disable : allowed
Sleep Button Disabled: false
Diag Button Disabled : true
Reset Button Disabled: false
Power Button Disabled: false
```

3.6. Configure Management Controller

3.6.1. Management Controller status and global enables

```
# ipmitool -I open mc
MC Commands:
  reset <warm|cold>
  guid
  info
  watchdog <get|reset|off>
  selftest
  getenables
  setenables <option=on|off> ...
    recv_msg_intr         Receive Message Queue Interrupt
    event_msg_intr        Event Message Buffer Full Interrupt
    event_msg             Event Message Buffer
    system_event_log      System Event Logging
    oem0                  OEM 0
```

```
    oem1                   OEM 1
    oem2                   OEM 2
```

3.6.2. Configure LAN Channels

```
ipmitool -I open lan print 1                                显示BMC通道的信息，如果不知道BMC使用的是哪个通道，请使用下面的命令确认：
ipmitool -I open channel info 1
ipmitool -I open lan set 1 ipsrc static                     设置本地BMC地址为静态，才能设置IP
ipmitool -I open lan set 1 ipaddr 172.16.0.2                设置本地BMC的IP地址
ipmitool -I open lan set 1 netmask 255.255.255.0            子网掩码，别忘了设
ipmitool -I open lan set 1 defgw ipaddr 172.16.0.254        网关，可设可不设，不过一定要确保监控它的机器位于同一路由
```

3.6.3. Configure Management Controller users

```
ipmitool user list 1                                查看BMC的用户列表
ipmitool user set name 1 username                   对BMC的1号用户设置用户名username
ipmitool user set password 1 123456 对BMC的1号用户设置密码123456
```

3.6.4. Configure Management Controller channels

```
# ipmitool -I open channel info 1
Channel 0x1 info:
  Channel Medium Type   : 802.3 LAN
  Channel Protocol Type : IPMB-1.0
  Session Support       : multi-session
  Active Session Count  : 0
  Protocol Vendor ID    : 7154
  Volatile(active) Settings
    Alerting            : disabled
    Per-message Auth    : disabled
    User Level Auth     : enabled
    Access Mode         : always available
  Non-Volatile Settings
    Alerting            : disabled
    Per-message Auth    : disabled
    User Level Auth     : enabled
    Access Mode         : always available
```

3.7. Example for iDRAC

http://support.dell.com/support/edocs/software/smbmcmu/bmcmu_4_0/cs/ug/bmcugc0d.htm#wp1067804

3.7.1. 更改IP地址,子网掩码与网关

查看IP，子网掩码与网关

```
# ipmitool -I open lan print 1
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD
Auth Type Enable        : Callback : MD2 MD5
                        : User     : MD2 MD5
                        : Operator : MD2 MD5
                        : Admin    : MD2 MD5
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 172.16.5.23
Subnet Mask             : 255.255.255.0
MAC Address             : 18:03:73:f5:ee:82
SNMP Community String   : public
IP Header               : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
Default Gateway IP      : 172.16.5.254
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
```

```
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14
Cipher Suite Priv Max   : aaaaaaaaaaaaaaa
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
```

设置IP，子网掩码与网关

```
/usr/bin/ipmitool -I open lan set 1 ipaddr 172.16.8.200
/usr/bin/ipmitool -I open lan set 1 netmask 255.255.255.0
/usr/bin/ipmitool -I open lan set 1 defgw ipaddr 172.16.8.254
/usr/bin/ipmitool -I open lan set 1 access on
```

3.7.2. 更改 iDRAC LCD 显示屏

```
# ipmitool delloem lcd set mode userdefined test
# ipmitool delloem lcd info
LCD info
    Setting: User defined
    Text:    test
```

3.7.3. 更改 iDRAC 密码

```
# ipmitool user list 2
ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
2   root             true    true       true       ADMINISTRATOR
# ipmitool user set password 2 "mypasswd"
```

3.7.4. 关机/开机

```
服务器关机
#ipmitool -I lan -U root -P secpass -H 10.10.0.5 power off

服务器开机
#ipmitool -I lan -U root -P secpass -H 10.10.0.5 power on

服务器 reset
#ipmitool -I lan -U root -P secpass -H 10.10.0.5 power reset
```

第 9 章 NetFlow

目录

1. flow-tools - collects and processes NetFlow data

```
$ sudo apt-get install flow-tools
```

1.1. flow-capture

```
mkdir /opt/netflow
flow-capture -z 6 -n 143 -e 8928 -V 5 -w /opt/netflow 0/0/2055
```

2. netams - Network Traffic Accounting and Monitoring Software

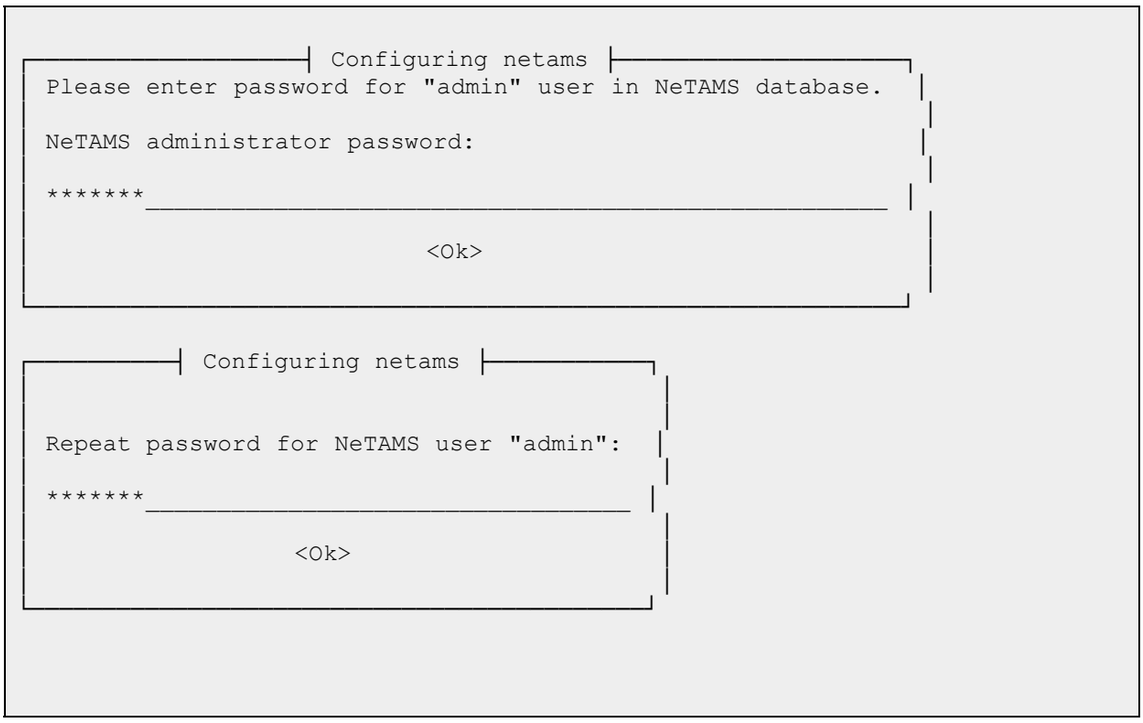
过程 9.1. 安装步骤

1. netams netams-web

```
$ sudo apt-get install netams netams-web
```

```
$ dpkg -s netams netams-web
```

2. NeTAMS administrator password



如果你想重新配置安装过程可以运行下面命令

```
$ sudo dpkg-reconfigure netams netams-web
```

3. 基本配置

```
$ sudo vim /etc/default/netams
RUN="yes"
```

```
$ sudo cp /etc/netams/netams.conf /etc/netams/netams.conf.old
$ sudo vim /etc/netams/netams.conf

$ sudo /etc/init.d/netams restart
```

```
$ cat /etc/apache2/conf.d/netams.conf
Alias /netams/images /usr/share/netams
Alias /netams/stat /var/lib/netams/stat
```

```
<Directory /var/lib/netams/stat/>
        Options -Indexes -FollowSymlinks

        DirectoryIndex index.html

        AllowOverride All
</Directory>

<Directory /usr/share/netams/>
        Options -Indexes -FollowSymlinks
        AllowOverride None
</Directory>
```

```
$ cat /etc/apache2/conf.d/netams-web.conf
ScriptAlias /netams/cgi-bin /usr/share/netams-web

# Uncomment the following if you have no netams package installed
#Alias /netams/images /usr/share/netams-web/images

<Directory /usr/share/netams-web>

        Options -Indexes +FollowSymlinks

        AddHandler cgi-script .cgi

        AllowOverride None

# By default we deny access from other hosts. May be you will need to
configure
# mod_auth_basic or mod_auth_mysql.
        Order deny,allow
        Deny from All
        Allow from 127.0.0.1

</Directory>
```

4. .netamsctl.rc

```
$ vim ~/.netamsctl.rc
login=admin
password=123456
host=localhost


$ netamsctl "show version"
NeTAMS 3.4.3 (3475.1) buildd@yellow / Tue 06 Apr 2010 03:40:49 +0000
Run time  22 mins 6.5699 secs
System time:  22 mins 1.2800 secs
Average CPU/system load: 0.10%
Process ID: 23647 RES: 9212K
Memory allocated: 3640404 (23161), freed (31) (0 NULL) [23130 used]
Total objects:
   Oids used: 9
   NetUnits: 4
   Policies: 3
   Services: 10
   Users: 1
   Connections: 1 active, 8 total

Services info:
 Storage ID=1 type mysql wr_q 0/0 rd_q 0/0
 Data-source ID=1 type LIBPCAP source eth0:0 loop 316382 average 4182 mcsec
    Perf: average skew delay 21580 mcsec, PPS: 77, BPS: 16788
Alerter 0 queue max: 255, current: 0
 Scheduled tasks: 1
```

2.1. netams-web

http://localhost/netams/stat/

http://localhost/netams/cgi-bin/login.cgi

第 10 章 Logs 分析

目录

1. php-syslog-ng

2. Apache Log

```
1、查看当天有多少个IP访问:
awk '{print $1}' log_file|sort|uniq|wc -l

2、查看某一个页面被访问的次数:
grep "/index.php" log_file | wc -l

3、查看每一个IP访问了多少个页面:
awk '{++S[$1]} END {for (a in S) print a,S[a]}' log_file

4、将每个IP访问的页面数进行从小到大排序:
awk '{++S[$1]} END {for (a in S) print S[a],a}' log_file | sort -n

5、查看某一个IP访问了哪些页面:
grep ^111.111.111.111 log_file| awk '{print $1,$7}'

6、去掉搜索引擎统计当天的页面:
awk '{print $12,$1}' log_file | grep ^\"Mozilla | awk '{print $2}' |sort | uniq |
wc -l

7、查看2009年6月21日14时这一个小时内有多少IP访问:
awk '{print $4,$1}' log_file | grep 21/Jun/2009:14 | awk '{print $2}'| sort |
uniq | wc -l
```

2.1. 删除日志

删除一个月前的日志

```
rm -f /www/logs/access.log.$(date -d '-1 month' +'%Y-%m')*
```

2.2. 统计爬虫

```
grep -E 'Googlebot|Baiduspider'  /www/logs/www.example.com/access.2011-02-23.log |
awk '{ print $1 }' | sort | uniq
```

2.3. 统计浏览器

```
cat /www/logs/example.com/access.2010-09-20.log | grep -v -E
'MSIE|Firefox|Chrome|Opera|Safari|Gecko|Maxthon' | sort | uniq -c | sort -r -n |
head -n 100
```

2.4. IP 统计

```
# cat /www/logs/www/access.2010-09-20.log | awk '{print $1}' | awk -F'.' '{print
$1"."$2"."$3".0"}' | sort | uniq -c | sort -r -n | head -n 200
```

2.5. 统计域名

```
# cat  /www/logs/access.2011-07-27.log |awk '{print $2}'|sort|uniq -c|sort -
rn|more
```

2.6. HTTP Status

```
# cat  /www/logs/access.2011-07-27.log |awk '{print $9}'|sort|uniq -c|sort -
rn|more
5056585 304
1125579 200
   7602 400
      5 301
```

2.7. URL 统计

```
cat  /www/logs/access.2011-07-27.log |awk '{print $7}'|sort|uniq -c|sort -rn|more
```

2.8. 文件流量统计

```
cat /www/logs/access.2011-08-03.log |awk '{sum[$7]+=$10}END{for(i in sum){print
sum[i],i}}'|sort -rn|more

grep ' 200 ' /www/logs/access.2011-08-03.log |awk '{sum[$7]+=$10}END{for(i in
sum){print sum[i],i}}'|sort -rn|more
```

2.9. 脚本运行速度

查出运行速度最慢的脚本

```
grep -v 0$ access.2010-11-05.log | awk -F '\" ' '{print $4" " $1}' web.log | awk
'{print $1" "$8}' | sort -n -k 1 -r | uniq > /tmp/slow_url.txt
```

3. Tomcat Log

3.1. 截取 0-3 点区间的日志

```
egrep '^2011-08-02 0[0-3].*' sale-debug.log
```