Netkiller Linux 手札

Netkiller Linux Cookbook

Mr. Neo Chan, 陈景峰 (BG7NYT)

中国广东省深圳市宝安区龙华镇

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 Tue Dec 6 12:12:43 UTC 2011

内容摘要

本文档讲述Linux系统涵盖了系统管理与配置包括:

对初学Linux的爱好者忠告

玩Linux最忌reboot（重新启动）这是windows玩家坏习惯

Linux只要接上电源你就不要再想用reboot,shutdown,halt,poweroff命令,Linux系统和应用软件一般备有reload,reconfigure,restart/start/stop...不需要安装软件或配置服务器后使用reboot重新引导计算机

在Linux系统里SIGHUP信号被定义为刷新配置文件,有些程序没有提供reload参数,你可以给进程发送HUP信号,让它刷新配置文件,而不用restart.通过pkill,killall,kill 都可以发送HUP信号例如: pkill -HUP httpd

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 MySQL 手札	Netkiller LDAP 手札	Netkiller Security 手札	Netkiller Version 手札
Netkiller Intranet 手札	Netkiller Cisco IOS 手札	Netkiller Writer 手札	Netkiller Studio Linux 手札

鸣谢

目录

表格清单

范例清单

下一页

自述

自述

目录

1. 本文目的

为什么写这篇文章

有很多想法,不能实现.工作中也用不到,所以想写出来,和大家分享.有一点写一点,写得也不好,就当学习笔记了.

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。也想写写摄影方面的心得体会。

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.

2. 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

3. 读者对象

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。

4. 作者简介

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

陈景峰 (ㄔㄣ ㄐㄧㄥ 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

4.1. 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

第 1 章 Introduction

目录

1. Distribution Version

Debian/Ubuntu

http://www.ubuntu.com

Gentoo

http://www.gentoo.org/

Scientific Linux (SL)

http://www.scientificlinux.org/

CentOS

http://www.centos.org/

Debian/Ubuntu适合做实验，快速安装定制，Gentoo适合DIY

如果是企业服务器还是建议使用CentOS，Scientific Linux

2. Distribution information

To find your Ubuntu version: lsb_release -a

```
[root@localhost ~]# lsb_release -a
LSB Version:    :core-3.1-ia32:core-3.1-noarch:graphics-3.1-ia32:graphics-3.1-noarch
Distributor ID: CentOS
Description:    CentOS release 5.2 (Final)
Release:        5.2
Codename:       Final


neo@netkiller:~$ lsb_release -a

No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04.1
Release:        8.04
Codename:       hardy
```

```
$ head -n1 /etc/issue
Ubuntu 10.04 LTS \n \l
```

3. Linux Installation

3.1. HDD Partition

partition

表 1.1. Linux partition

volume	size
/boot	500M
/	50G
/opt	remainder
swap	memory * 2

部分 I. System Administrator

目录

第 2 章 Kernel

```
wget -q -c http://www.kernel.org/pub/linux/kernel/v3.0/linux-3.0.1.tar.bz2
tar jxvf linux-3.0.1.tar.bz2

cd linux-3.0.1
make clean
make mrproper
make menuconfig
make
make modules_install
make install
```

第 3 章 System Infomation

目录

1. Cpu Bit

```
neo@netkiller:~$ uname -a
Linux netkiller 2.6.28-15-server #52-Ubuntu SMP Wed Sep 9 11:34:09 UTC 2009 x86_64 GNU/Linux

neo@netkiller:~$ getconf LONG_BIT
64
```

第 4 章 shutdown

```
shutdown -h now
shutdown -h 10:00        10点关机
shutdown -h +10          10mins后关机
shutdown -r now          reboot at once
shutdown -r +30          'System will reboot in 30mins'
shutdown -k              'System will reboot'
```

第 5 章 Profile

目录

1. shell

```
$ chsh /bin/bash
```

第 6 章 Device information

目录

1. dmesg - print or control the kernel ring buffer

dmesg

```
neo@shenzhen:~/doc/Linux/xhtml$ dmesg
```

2. smartctl - Control and Monitor Utility for SMART Disks

```
# smartctl -i /dev/sda
smartctl version 5.38 [x86_64-redhat-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF INFORMATION SECTION ===
Model Family:     Western Digital Caviar Second Generation Serial ATA family
Device Model:     WDC WD1600AAJS-75M0A0
Serial Number:    WD-WCAV35616755
Firmware Version: 02.03E02
User Capacity:    160,000,000,000 bytes
Device is:        In smartctl database [for details use: -P show]
ATA Version is:   8
ATA Standard is:  Exact ATA specification draft version not indicated
Local Time is:    Wed May  5 13:05:18 2010 CST
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

如果 SMART support is: Disabled 使用下面命令启用

```
# smartctl --smart=on --offlineauto=on --saveauto=on /dev/hdb
```

健康情况

```
# smartctl -H /dev/sda
smartctl version 5.38 [x86_64-redhat-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED
```

PASSED，这表示硬盘健康状态良好,Failure 最好立刻给服务器更换硬盘

3. lspci - list all PCI devices

```
$ lspci
00:00.0 Host bridge: Intel Corporation 82945G/GZ/P/PL Memory Controller Hub (rev 02)
00:02.0 VGA compatible controller: Intel Corporation 82945G/GZ Integrated Graphics Controller
(rev 02)
00:1b.0 Audio device: Intel Corporation 82801G (ICH7 Family) High Definition Audio Controller
(rev 01)
00:1c.0 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 1 (rev 01)
00:1c.2 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 3 (rev 01)
00:1c.3 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 4 (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #3 (rev 01)
00:1d.3 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #4 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801G (ICH7 Family) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev e1)
00:1f.0 ISA bridge: Intel Corporation 82801GB/GR (ICH7 Family) LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801G (ICH7 Family) IDE Controller (rev 01)
00:1f.2 IDE interface: Intel Corporation 82801GB/GR/GH (ICH7 Family) SATA IDE Controller (rev
01)
00:1f.3 SMBus: Intel Corporation 82801G (ICH7 Family) SMBus Controller (rev 01)
01:00.0 Ethernet controller: Realtek Semiconductor Co., Ltd. RTL8111/8168B PCI Express Gigabit
Ethernet controller (rev 02)
04:00.0 Ethernet controller: Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+ (rev 10)
```

```
$ lspci -tv
-[0000:00]-+-00.0  Intel Corporation 82945G/GZ/P/PL Memory Controller Hub
           +-02.0  Intel Corporation 82945G/GZ Integrated Graphics Controller
           +-1b.0  Intel Corporation N10/ICH 7 Family High Definition Audio Controller
           +-1c.0-[0000:01]----00.0  Realtek Semiconductor Co., Ltd. RTL8111/8168B PCI Express
Gigabit Ethernet controller
           +-1c.2-[0000:02]--
           +-1c.3-[0000:03]--
           +-1d.0  Intel Corporation N10/ICH7 Family USB UHCI Controller #1
           +-1d.1  Intel Corporation N10/ICH 7 Family USB UHCI Controller #2
           +-1d.2  Intel Corporation N10/ICH 7 Family USB UHCI Controller #3
           +-1d.3  Intel Corporation N10/ICH 7 Family USB UHCI Controller #4
           +-1d.7  Intel Corporation N10/ICH 7 Family USB2 EHCI Controller
           +-1e.0-[0000:04]----00.0  Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
           +-1f.0  Intel Corporation 82801GB/GR (ICH7 Family) LPC Interface Bridge
           +-1f.1  Intel Corporation 82801G (ICH7 Family) IDE Controller
           +-1f.2  Intel Corporation N10/ICH7 Family SATA IDE Controller
           \-1f.3  Intel Corporation N10/ICH 7 Family SMBus Controller
```

4. dmidecode - DMI table decoder

dmidecode

```
# dmidecode |more

# dmidecode 2.2
SMBIOS 2.4 present.
62 structures occupying 3161 bytes.
Table at 0xCFFBC000.
Handle 0xDA00
        DMI type 218, 11 bytes.
        OEM-specific Type
                Header And Data:
                        DA 0B 00 DA B2 00 17 00 0E 20 00
Handle 0x0000
        DMI type 0, 24 bytes.
        BIOS Information
                Vendor: Dell Inc.
                Version: 1.2.0
                Release Date: 10/18/2006
                Address: 0xF0000
                Runtime Size: 64 kB
                ROM Size: 1024 kB
                Characteristics:
                        ISA is supported
                        PCI is supported
                        PNP is supported
                        BIOS is upgradeable
                        BIOS shadowing is allowed
                        ESCD support is available
                        Boot from CD is supported
                        Selectable boot is supported
                        EDD is supported
                        Japanese floppy for Toshiba 1.2 MB is supported (int 13h)
                        5.25"/360 KB floppy services are supported (int 13h)
                        5.25"/1.2 MB floppy services are supported (int 13h)
                        3.5"/720 KB floppy services are supported (int 13h)
                        Print screen service is supported (int 5h)
                        8042 keyboard services are supported (int 9h)
                        Serial services are supported (int 14h)
                        Printer services are supported (int 17h)
                        CGA/mono video services are supported (int 10h)
                        ACPI is supported
                        USB legacy is supported
                        BIOS boot specification is supported
                        Function key-initiated network boot is supported
```

5. 鉴别eth(x)

```
 简单的方法:
一个插网线，一个不插，运行 mii-tool 或 ethtool eth0，看状态是否连接

另一种方法是:
tail -f /var/log/messages，当你向其中一个网口做插拔网线的动作时，屏幕上会看到提示信息
```

最好的方法是将mac地址写在启动脚本内.

6. usb device

lsusb

```
neo@netkiller:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 005 Device 002: ID 0dda:0301 Integrated Circuit Solution, Inc. MP3 Player
Bus 005 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 004 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 003 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

```
$ lsusb -tv
/:  Bus 05.Port 1: Dev 1, Class=root_hub, Driver=uhci_hcd/2p, 12M
/:  Bus 04.Port 1: Dev 1, Class=root_hub, Driver=uhci_hcd/2p, 12M
/:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=uhci_hcd/2p, 12M
/:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=uhci_hcd/2p, 12M
/:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=ehci_hcd/8p, 480M
```

```
$ sudo lsusb -v

Bus 005 Device 001: ID 0000:0000
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               2.00
  bDeviceClass            9 Hub
  bDeviceSubClass         0 Unused
  bDeviceProtocol         1 Single TT
  bMaxPacketSize0        64
  idVendor           0x0000
  idProduct          0x0000
  bcdDevice            2.06
  iManufacturer           3 Linux 2.6.24-22-generic ehci_hcd
  iProduct                2 EHCI Host Controller
  iSerial                 1 0000:00:1d.7
  bNumConfigurations      1
  Configuration Descriptor:
    bLength                 9
    bDescriptorType         2
    wTotalLength           25
    bNumInterfaces          1
    bConfigurationValue     1
    iConfiguration          0
    bmAttributes         0xe0
      Self Powered
      Remote Wakeup
    MaxPower                0mA
    Interface Descriptor:
      bLength                 9
      bDescriptorType         4
      bInterfaceNumber        0
      bAlternateSetting       0
      bNumEndpoints           1
      bInterfaceClass         9 Hub
      bInterfaceSubClass      0 Unused
      bInterfaceProtocol      0 Full speed (or root) hub
      iInterface              0
      Endpoint Descriptor:
        bLength                 7
        bDescriptorType         5
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0004  1x 4 bytes
        bInterval              12
Hub Descriptor:
  bLength              11
  bDescriptorType      41
  nNbrPorts             8
  wHubCharacteristic 0x000a
    No power switching (usb 1.0)
    Per-port overcurrent protection
    TT think time 8 FS bits
```

```
  bPwrOn2PwrGood       10 * 2 milli seconds
  bHubContrCurrent      0 milli Ampere
  DeviceRemovable    0x00 0x00
  PortPwrCtrlMask    0xff 0xff
 Hub Port Status:
   Port 1: 0000.0100 power
   Port 2: 0000.0100 power
   Port 3: 0000.0100 power
   Port 4: 0000.0100 power
   Port 5: 0000.0100 power
   Port 6: 0000.0100 power
   Port 7: 0000.0100 power
   Port 8: 0000.0100 power
Device Status:     0x0003
  Self Powered
  Remote Wakeup Enabled

Bus 004 Device 001: ID 0000:0000
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               1.10
  bDeviceClass            9 Hub
  bDeviceSubClass         0 Unused
  bDeviceProtocol         0 Full speed (or root) hub
  bMaxPacketSize0        64
  idVendor           0x0000
  idProduct          0x0000
  bcdDevice            2.06
  iManufacturer           3 Linux 2.6.24-22-generic uhci_hcd
  iProduct                2 UHCI Host Controller
  iSerial                 1 0000:00:1d.3
  bNumConfigurations      1
  Configuration Descriptor:
    bLength                 9
    bDescriptorType         2
    wTotalLength           25
    bNumInterfaces          1
    bConfigurationValue     1
    iConfiguration          0
    bmAttributes         0xe0
      Self Powered
      Remote Wakeup
    MaxPower                0mA
    Interface Descriptor:
      bLength                 9
      bDescriptorType         4
      bInterfaceNumber        0
      bAlternateSetting       0
      bNumEndpoints           1
      bInterfaceClass         9 Hub
      bInterfaceSubClass      0 Unused
      bInterfaceProtocol      0 Full speed (or root) hub
      iInterface              0
      Endpoint Descriptor:
        bLength                 7
        bDescriptorType         5
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0002  1x 2 bytes
        bInterval             255
Hub Descriptor:
  bLength               9
  bDescriptorType      41
  nNbrPorts             2
  wHubCharacteristic 0x000a
    No power switching (usb 1.0)
    Per-port overcurrent protection
  bPwrOn2PwrGood        1 * 2 milli seconds
  bHubContrCurrent      0 milli Ampere
  DeviceRemovable    0x00
  PortPwrCtrlMask    0xff
 Hub Port Status:
   Port 1: 0000.0100 power
   Port 2: 0000.0100 power
Device Status:     0x0003
  Self Powered
  Remote Wakeup Enabled

Bus 003 Device 001: ID 0000:0000
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               1.10
  bDeviceClass            9 Hub
  bDeviceSubClass         0 Unused
  bDeviceProtocol         0 Full speed (or root) hub
  bMaxPacketSize0        64
  idVendor           0x0000
  idProduct          0x0000
  bcdDevice            2.06
  iManufacturer           3 Linux 2.6.24-22-generic uhci_hcd
  iProduct                2 UHCI Host Controller
  iSerial                 1 0000:00:1d.2
  bNumConfigurations      1
  Configuration Descriptor:
    bLength                 9
    bDescriptorType         2
    wTotalLength           25
    bNumInterfaces          1
    bConfigurationValue     1
    iConfiguration          0
```

```
    bmAttributes         0xe0
      Self Powered
      Remote Wakeup
    MaxPower                0mA
    Interface Descriptor:
      bLength                 9
      bDescriptorType         4
      bInterfaceNumber        0
      bAlternateSetting       0
      bNumEndpoints           1
      bInterfaceClass         9 Hub
      bInterfaceSubClass      0 Unused
      bInterfaceProtocol      0 Full speed (or root) hub
      iInterface              0
      Endpoint Descriptor:
        bLength                 7
        bDescriptorType         5
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0002  1x 2 bytes
        bInterval             255
Hub Descriptor:
  bLength               9
  bDescriptorType      41
  nNbrPorts             2
  wHubCharacteristic 0x000a
    No power switching (usb 1.0)
    Per-port overcurrent protection
  bPwrOn2PwrGood        1 * 2 milli seconds
  bHubContrCurrent      0 milli Ampere
  DeviceRemovable    0x00
  PortPwrCtrlMask    0xff
 Hub Port Status:
   Port 1: 0000.0100 power
   Port 2: 0000.0100 power
Device Status:     0x0003
  Self Powered
  Remote Wakeup Enabled

Bus 002 Device 001: ID 0000:0000
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               1.10
  bDeviceClass            9 Hub
  bDeviceSubClass         0 Unused
  bDeviceProtocol         0 Full speed (or root) hub
  bMaxPacketSize0        64
  idVendor           0x0000
  idProduct          0x0000
  bcdDevice            2.06
  iManufacturer           3 Linux 2.6.24-22-generic uhci_hcd
  iProduct                2 UHCI Host Controller
  iSerial                 1 0000:00:1d.1
  bNumConfigurations      1
  Configuration Descriptor:
    bLength                 9
    bDescriptorType         2
    wTotalLength           25
    bNumInterfaces          1
    bConfigurationValue     1
    iConfiguration          0
    bmAttributes         0xe0
      Self Powered
      Remote Wakeup
    MaxPower                0mA
    Interface Descriptor:
      bLength                 9
      bDescriptorType         4
      bInterfaceNumber        0
      bAlternateSetting       0
      bNumEndpoints           1
      bInterfaceClass         9 Hub
      bInterfaceSubClass      0 Unused
      bInterfaceProtocol      0 Full speed (or root) hub
      iInterface              0
      Endpoint Descriptor:
        bLength                 7
        bDescriptorType         5
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0002  1x 2 bytes
        bInterval             255
Hub Descriptor:
  bLength               9
  bDescriptorType      41
  nNbrPorts             2
  wHubCharacteristic 0x000a
    No power switching (usb 1.0)
    Per-port overcurrent protection
  bPwrOn2PwrGood        1 * 2 milli seconds
  bHubContrCurrent      0 milli Ampere
  DeviceRemovable    0x00
  PortPwrCtrlMask    0xff
 Hub Port Status:
   Port 1: 0000.0100 power
   Port 2: 0000.0100 power
Device Status:     0x0003
  Self Powered
```

```
  Remote Wakeup Enabled

Bus 001 Device 001: ID 0000:0000
Device Descriptor:
  bLength                 18
  bDescriptorType          1
  bcdUSB                1.10
  bDeviceClass             9 Hub
  bDeviceSubClass          0 Unused
  bDeviceProtocol          0 Full speed (or root) hub
  bMaxPacketSize0         64
  idVendor           0x0000
  idProduct          0x0000
  bcdDevice            2.06
  iManufacturer            3 Linux 2.6.24-22-generic uhci_hcd
  iProduct                 2 UHCI Host Controller
  iSerial                  1 0000:00:1d.0
  bNumConfigurations       1
  Configuration Descriptor:
    bLength                 9
    bDescriptorType         2
    wTotalLength           25
    bNumInterfaces          1
    bConfigurationValue     1
    iConfiguration          0
    bmAttributes         0xe0
      Self Powered
      Remote Wakeup
    MaxPower                0mA
    Interface Descriptor:
      bLength                 9
      bDescriptorType         4
      bInterfaceNumber        0
      bAlternateSetting       0
      bNumEndpoints           1
      bInterfaceClass         9 Hub
      bInterfaceSubClass      0 Unused
      bInterfaceProtocol      0 Full speed (or root) hub
      iInterface              0
      Endpoint Descriptor:
        bLength                 7
        bDescriptorType         5
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0002  1x 2 bytes
        bInterval             255
Hub Descriptor:
  bLength               9
  bDescriptorType      41
  nNbrPorts             2
  wHubCharacteristic 0x000a
    No power switching (usb 1.0)
    Per-port overcurrent protection
  bPwrOn2PwrGood        1 * 2 milli seconds
  bHubContrCurrent      0 milli Ampere
  DeviceRemovable    0x00
  PortPwrCtrlMask    0xff
 Hub Port Status:
   Port 1: 0000.0100 power
   Port 2: 0000.0100 power
Device Status:     0x0003
  Self Powered
  Remote Wakeup Enabled
```

7. SCSI

```
# cat /proc/scsi/scsi
Attached devices:
Host: scsi0 Channel: 02 Id: 00 Lun: 00
  Vendor: DELL     Model: PERC H700        Rev: 2.10
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi0 Channel: 02 Id: 01 Lun: 00
  Vendor: DELL     Model: PERC H700        Rev: 2.10
  Type:   Direct-Access                    ANSI SCSI revision: 05
```

8. HBA

```
# dmesg | grep QLogic
QLogic Fibre Channel HBA Driver: 8.03.01.05.06.0-k8
 QLogic Fibre Channel HBA Driver: 8.03.01.05.06.0-k8
  QLogic QLE2562 - PCI-Express Dual Channel 8Gb Fibre Channel HBA
 QLogic Fibre Channel HBA Driver: 8.03.01.05.06.0-k8
  QLogic QLE2562 - PCI-Express Dual Channel 8Gb Fibre Channel HBA


# dmesg | grep qla
qla2xxx 0000:04:00.0: PCI INT A -> GSI 38 (level, low) -> IRQ 38
qla2xxx 0000:04:00.0: Found an ISP2532, irq 38, iobase 0xffffc90016e76000
qla2xxx 0000:04:00.0: irq 61 for MSI/MSI-X
qla2xxx 0000:04:00.0: irq 62 for MSI/MSI-X
qla2xxx 0000:04:00.0: Configuring PCI space...
qla2xxx 0000:04:00.0: setting latency timer to 64
qla2xxx 0000:04:00.0: Configure NVRAM parameters...
qla2xxx 0000:04:00.0: Verifying loaded RISC code...
qla2xxx 0000:04:00.0: firmware: requesting ql2500_fw.bin
qla2xxx 0000:04:00.0: FW: Loading via request-firmware...
qla2xxx 0000:04:00.0: Allocated (64 KB) for FCE...
qla2xxx 0000:04:00.0: Allocated (64 KB) for EFT...
qla2xxx 0000:04:00.0: Allocated (1350 KB) for firmware dump...
qla2xxx 0000:04:00.0: Unable to read FCP priority data.
scsi0 : qla2xxx
qla2xxx 0000:04:00.0:
qla2xxx 0000:04:00.1: PCI INT B -> GSI 45 (level, low) -> IRQ 45
qla2xxx 0000:04:00.1: Found an ISP2532, irq 45, iobase 0xffffc90016e06000
qla2xxx 0000:04:00.1: irq 63 for MSI/MSI-X
qla2xxx 0000:04:00.1: irq 64 for MSI/MSI-X
qla2xxx 0000:04:00.1: Configuring PCI space...
qla2xxx 0000:04:00.1: setting latency timer to 64
qla2xxx 0000:04:00.1: Configure NVRAM parameters...
qla2xxx 0000:04:00.1: Verifying loaded RISC code...
qla2xxx 0000:04:00.1: FW: Loading via request-firmware...
qla2xxx 0000:04:00.1: Allocated (64 KB) for FCE...
qla2xxx 0000:04:00.1: Allocated (64 KB) for EFT...
qla2xxx 0000:04:00.1: Allocated (1350 KB) for firmware dump...
qla2xxx 0000:04:00.1: Unable to read FCP priority data.
scsi1 : qla2xxx
qla2xxx 0000:04:00.1:
qla2xxx 0000:04:00.0: LIP reset occurred (f700).
qla2xxx 0000:04:00.1: LIP reset occurred (f700).
qla2xxx 0000:04:00.0: LOOP UP detected (8 Gbps).
qla2xxx 0000:04:00.1: LOOP UP detected (8 Gbps).
```

9. kudzu - detects and configures new and/or changed hardware on a system

```
# kudzu -p | more
```

network

```
# kudzu --class=network -p
```

第 7 章 Locale

目录

1. time zone

选择用户时区

```
$ tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?
```

tzconfig

```
netkiller@shenzhen:~$ tzconfig
Your current time zone is set to US/Eastern
Do you want to change that? [n]: y

Please enter the number of the geographic area in which you live:


        1) Africa                       7) Australia

        2) America                      8) Europe

        3) US time zones                9) Indian Ocean

        4) Canada time zones            10) Pacific Ocean

        5) Asia                         11) Use System V style time zones

        6) Atlantic Ocean               12) None of the above


Then you will be shown a list of cities which represent the time zone
in which they are located. You should choose a city in your time zone.

Number: 5

Aden Almaty Amman Anadyr Aqtau Aqtobe Ashgabat Ashkhabad Baghdad Bahrain
Baku Bangkok Beirut Bishkek Brunei Calcutta Choibalsan Chongqing Chungking
Colombo Dacca Damascus Dhaka Dili Dubai Dushanbe Gaza Harbin Hong_Kong
Hovd Irkutsk Istanbul Jakarta Jayapura Jerusalem Kabul Kamchatka Karachi
Kashgar Katmandu Krasnoyarsk Kuala_Lumpur Kuching Kuwait Macao Macau
Magadan Makassar Manila Muscat Nicosia Novosibirsk Omsk Oral Phnom_Penh
Pontianak Pyongyang Qatar Qyzylorda Rangoon Riyadh Riyadh87 Riyadh88
```

```
Riyadh89 Saigon Sakhalin Samarkand Seoul Shanghai Singapore Taipei
Tashkent Tbilisi Tehran Tel_Aviv Thimbu Thimphu Tokyo Ujung_Pandang
Ulaanbaatar Ulan_Bator Urumqi Vientiane Vladivostok Yakutsk Yekaterinburg
Yerevan

Please enter the name of one of these cities or zones
You just need to type enough letters to resolve ambiguities
Press Enter to view all of them again
Name: [] Harbin
Your default time zone is set to 'Asia/Harbin'.
Local time is now:      Tue Mar 11 10:46:46 CST 2008.
Universal Time is now:  Tue Mar 11 02:46:46 UTC 2008.
```

tzdata

dpkg-reconfigure tzdata

```
$ sudo dpkg-reconfigure tzdata
```

上一页 上一级 下一页

9. kudzu - detects and configures new and/or changed hardware on a system

起始页

2. to change system date/time

2. to change system date/time

date

e.g. date -s month/day/year

```
# date -s 1/18/2008
```

time

e.g. date -s hour:minute:second

```
# date -s 11:12:00
```

writing CMOS

```
# clock -w
```

2.1. NTP Server

更新网络时间

ntpdate - client for setting system time from NTP servers

```
$ sudo ntpdate asia.pool.ntp.org
21 May 10:34:18 ntpdate[6687]: adjust time server 203.185.69.60 offset 0.031079 sec
$ sudo hwclock -w
```

3. Language

默认语言

```
export LANG=en_US
export LC_ALL=en_US
```

永久更改

```
sudo vi /etc/default/locale

LANG="en_US.UTF-8"
LANGUAGE="en_US:en"
```

改为中文环境

```
sudo apt-get install language-support-zh
LANG="zh_CN.UTF-8"
LANGUAGE="zh_CN:zh"
```

第 8 章 console / terminal

目录

1. serial console

gurb

```
$ sudo vim /boot/grub/menu.lst

title           Ubuntu 8.04.1, kernel 2.6.24-21-generic
root            (hd0,5)
kernel          /boot/vmlinuz-2.6.24-21-generic root=UUID=3d5dd6c0-bbd2-4ddf-9b71-1c7b78e8de3b
ro quiet splash

console=tty0 console=ttyS0,38400
initrd          /boot/initrd.img-2.6.24-21-generic
quiet
```

tty6

```
$ sudo vim /etc/event.d/tty6

respawn
#exec /sbin/getty 38400 tty6
exec /sbin/getty -L /dev/ttyS0 38400 vt100
```

other terminal: VT100, VT220, VT320, VT420

securetty

```
$ cat /etc/securetty
# for people with serial port consoles
ttyS0
```

2. console timeout

查看当前的$TMOUT环境变量设置

echo $TMOUT

TMOUT=3600

export TMOUT

netkiller@Linux-server:~$ sudo dpkg-reconfigure en_US.UTF-8

3. TUI (Text User Interface)

SVGATextMode

```
$ sudo apt-get install svgatextmode
$ SVGATextMode 80x25x9
```

4. framebuffer

在grub.conf中的kernel行后面写上vga=0x317就行了，也可以用vga=ask，让系统启动的时候询问你用多大的分辨率

第 9 章 Harddisk

目录

主分区最多4个

逻辑分区:

- SCSI 最多 16 个
- IDE 最多 63 个

1. 查看分区分区 UUID

```
$ blkid
/dev/sda1: UUID="a457213b-e72d-4c9c-953d-b438ec554d3c" SEC_TYPE="ext2" TYPE="ext3"
/dev/sda5: UUID="cc2c1be9-a6e0-4494-a5f0-76b39d3fc1f0" TYPE="swap"
/dev/sda6: UUID="3c9a1484-1295-4fb9-9c94-f9c69ae7e770" TYPE="ext3"
/dev/sda7: UUID="ade7b5e7-a311-45de-9b24-e16be73de715" TYPE="swap"

$ ls -l /dev/disk/by-uuid
total 0
lrwxrwxrwx 1 root root 10 2009-07-11 00:52 3c9a1484-1295-4fb9-9c94-f9c69ae7e770 -> ../../sda6
lrwxrwxrwx 1 root root 10 2009-07-11 00:52 a457213b-e72d-4c9c-953d-b438ec554d3c -> ../../sda1
lrwxrwxrwx 1 root root 10 2009-07-11 00:52 ade7b5e7-a311-45de-9b24-e16be73de715 -> ../../sda7
lrwxrwxrwx 1 root root 10 2009-07-11 00:52 cc2c1be9-a6e0-4494-a5f0-76b39d3fc1f0 -> ../../sda5
```

---

2. Label

2.1. Ext2

e2label - Change the label on an ext2/ext3 filesystem

2.1.1. 查看卷标

```
# e2label /dev/sda1
/boot
```

2.1.2. 更改卷标

```
# man e2label
# e2label /dev/sda5 /www

# e2label /dev/sda5
/www
```

测试

```
# mount /app
```

3. 临时增加 swap 分区

```
dd if=/dev/zero of=/root/swap0 bs=1M count=2048
mkswap /root/swap0
swapon /root/swap0
```

4. Show partition

show all of disk and partition

```
neo@master:~$ sudo sfdisk -s
/dev/sda:   8388608
/dev/sdb:   2097152
total: 10485760 blocks
```

or

```
neo@master:~$ sudo fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x000301bd

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         993     7976241   83  Linux
/dev/sda2             994        1044      409657+   5  Extended
/dev/sda5             994        1044      409626   82  Linux swap / Solaris

Disk /dev/sdb: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000

Disk /dev/sdb doesn't contain a valid partition table
neo@master:~$
```

show partition /dev/sda

```
neo@master:~$ sudo fdisk -l /dev/sda

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x000301bd

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         993     7976241   83  Linux
/dev/sda2             994        1044      409657+   5  Extended
/dev/sda5             994        1044      409626   82  Linux swap / Solaris
neo@master:~$
```

5. Create partition

```
$ sudo cfdisk /dev/sdb
```

```
Command (m for help): p

Disk /dev/sda: 146.1 GB, 146163105792 bytes
255 heads, 63 sectors/track, 17769 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          25      200781   83  Linux
/dev/sda2              26        3849    30716280   83  Linux
/dev/sda3            3850       17769   111812400   83  Linux

Command (m for help): d
Partition number (1-4): 3

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (3850-17769, default 3850):
Using default value 3850
Last cylinder or +size or +sizeM or +sizeK (3850-17769, default 17769): +32000M

Command (m for help): p

Disk /dev/sda: 146.1 GB, 146163105792 bytes
255 heads, 63 sectors/track, 17769 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          25      200781   83  Linux
/dev/sda2              26        3849    30716280   83  Linux
/dev/sda3            3850        7740    31254457+  83  Linux
```

6. Clone partition

/dev/sda 克隆到 /dev/sdb

```
$ sudo dd if=/dev/sda of=/dev/sdb
```

备份 mbr 主引导记录

```
$ dd if=/dev/sda of=/root/disk.mbr bs=512 count=1
```

```
$ dd if=/root/disk.mbr of=/dev/sda bs=512 count=1
```

软盘镜像

```
$ dd if=/dev/fd0 of=floppy.img bs=1440k
```

7. Format partition

format /dev/sdb1

7.1. ext3

```
neo@master:~$ sudo mkfs.ext3 /dev/sdb1
```

7.2. ReiserFS

you also can using other file system

reiserfs

```
neo@master:~$ sudo mkfs.reiserfs /dev/sdb1
```

8. estimate disk / directory / file space usage

total for a directory

```
du -h --max-depth=0
```

9. Convert from ext3 to ext4 File system

step 1

```
$ sudo tune2fs -O extents,uninit_bg,dir_index /dev/sda7
tune2fs 1.41.4 (27-Jan-2009)

Please run e2fsck on the filesystem.
```

step 2

```
$ sudo e2fsck -fD /dev/sda7
e2fsck 1.41.4 (27-Jan-2009)
/dev/sda7 is mounted.

WARNING!!!  Running e2fsck on a mounted filesystem may cause
SEVERE filesystem damage.

Do you really want to continue (y/n)? yes

/dev/sda7: recovering journal
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 3A: Optimizing directories
Pass 4: Checking reference counts
Pass 5: Checking group summary information
Block bitmap differences:  -3913734 +3925302
Fix<y>? yes


/dev/sda7: ***** FILE SYSTEM WAS MODIFIED *****
/dev/sda7: 77282/2293760 files (15.7% non-contiguous), 4584313/9163066 blocks
```

step 3

```
$ sudo cp /etc/fstab /etc/fstab.old
$ sudo vim /etc/fstab

# /dev/sda7
UUID=16089544-6fbf-400e-a63a-fa6159e271e5 /home           ext4    relatime,errors=remount-ro 0
1
```

step 4

```
$ sudo reboot
```

10. GPT

```
$ sudo parted /dev/sda
GNU Parted 2.3
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted)
```

10.1. 查看分区

```
(parted) print
Model: DELL PERC 6/i (scsi)
Disk /dev/sda: 2498GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size    File system     Name     Flags
 1      1049kB  50.0GB  50.0GB  ext4                     boot
 2      50.0GB  66.0GB  16.0GB  linux-swap(v1)
 3      66.0GB  2498GB  2432GB  ext4            /backup
```

空闲空间

```
(parted) print free
Model: DELL PERC 6/i (scsi)
Disk /dev/sda: 2498GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size    File system     Name     Flags
        17.4kB  1049kB  1031kB  Free Space
 1      1049kB  50.0GB  50.0GB  ext4                     boot
 2      50.0GB  66.0GB  16.0GB  linux-swap(v1)
 3      66.0GB  2498GB  2432GB  ext4            /backup
        2498GB  2498GB  1032kB  Free Space
```

10.2. 创建分区

```
(parted) mkpart
Partition name?  []? /www
File system type?  [ext2]?
Start? 10GB
End? 50GB
```

例 9.1. GPT Example

```
(parted) print devices
/dev/sdb (9999GB)
/dev/sda (2498GB)

(parted) select /dev/sdb
Using /dev/sdb

(parted) mklabel gpt
Warning: The existing disk label on /dev/sdb will be destroyed and all data on this disk will
be
lost. Do you want to continue?
Yes/No? yes

(parted) mkpart
Partition name?  []? /md1200
File system type?  [ext2]? ext4
Start? 0GB
End? 9999GB
```

```
(parted) print list
Model: DELL PERC H800 (scsi)
Disk /dev/sdb: 9999GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size    File system  Name     Flags
 1      1049kB  9999GB  9999GB               /md1200


Model: DELL PERC 6/i (scsi)
Disk /dev/sda: 2498GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size    File system     Name     Flags
 1      1049kB  50.0GB  50.0GB  ext4                     boot
 2      50.0GB  66.0GB  16.0GB  linux-swap(v1)
 3      66.0GB  2498GB  2432GB  ext4            /backup


(parted)
```

10.3. 退出

```
(parted) quit
```

10.4. mount

```
neo@backup:~$ sudo blkid
[sudo] password for neo:
/dev/sda1: UUID="2fc411ec-9f6e-4e04-9270-11d23a9b0668" TYPE="ext4"
/dev/sda2: UUID="f5175b7a-4c87-471c-ab9f-9d601bc5e6e2" TYPE="swap"
/dev/sda3: UUID="3217bdd9-1beb-494a-a428-8d1c09eaa1af" TYPE="ext4"

neo@backup:~$ sudo vim /etc/fstab
UUID=3217bdd9-1beb-494a-a428-8d1c09eaa1af /backup ext4 errors=remount-ro 0       1
```

11. loop devices

If you are using the loadable module you must have the module loaded first with the command:

```
$ sudo modprobe loop
```

The following commands can be used as an example of using the loop device.

```
$ dd if=/dev/zero of=file bs=1k count=100
100+0 records in
100+0 records out
102400 bytes (102 kB) copied, 0.00126554 s, 80.9 MB/s

$ sudo losetup /dev/loop0 file

$ sudo mkfs.ext3 /dev/loop0
mke2fs 1.40.8 (13-Mar-2008)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
16 inodes, 100 blocks
5 blocks (5.00%) reserved for the super user
First data block=1
1 block group
8192 blocks per group, 8192 fragments per group
16 inodes per group

Writing inode tables: done

Filesystem too small for a journal
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 24 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

mount loop device

```
$ sudo mkdir /mnt/loop
$ sudo mount /dev/loop0 /mnt/loop
```

Now! you can using it as harddisk.

umount loop device

```
$ sudo umount /mnt/loop/
$ sudo losetup -d /dev/loop0
```

Maybe also encryption modules are needed.

```
$ sudo modprobe cryptoloop
$ sudo modprobe des
```

enable data encryption

```
$ dd if=/dev/zero of=encryption_file bs=1k count=100
100+0 records in
100+0 records out
```

```
102400 bytes (102 kB) copied, 0.00130537 s, 78.4 MB/s
$ sudo losetup -e des /dev/loop0 encryption_file
```

If you are using the loadable module you may remove the module with the command

```
$ sudo rmmod loop des cryptoloop
```

11.1. losetup - set up and control loop devices

EXAMPLE

```
       If you are using the loadable module you must have the module loaded first with the
command

               # insmod loop.o

       Maybe also encryption modules are needed.

               # insmod des.o # insmod cryptoloop.o

       The following commands can be used as an example of using the loop device.

               # dd if=/dev/zero of=/file bs=1k count=100
               # losetup -e des /dev/loop0 /file
               Password:
               Init (up to 16 hex digits):
               # mkfs -t ext2 /dev/loop0 100
               # mount -t ext2 /dev/loop0 /mnt
                ...
               # umount /dev/loop0
               # losetup -d /dev/loop0

       If you are using the loadable module you may remove the module with the command

               # rmmod loop
```

第 10 章 Removable Storage

目录

eject - eject removable media

```
$ eject
```

1. usb flash

mount NTFS filesystem

```
sudo mount -t ntfs-3g /dev/sdb1 /mnt/usbflash/ -o force
```

2. CD / DVD

2.1. Mount an ISO file

To mount the ISO image file.iso to the mount point /media/cdrom use this :

```
$ mount -o loop -t iso9660 file.iso /media/cdrom
```

2.2. create iso file from CD

```
$ dd if=/dev/cdrom of=isofile.iso
```

2.3. burner

2.4. ISO Mirror

```
$ mkisofs -V LABEL -r /mnt/cdrom | gzip > cdrom.iso.gz
```

mount iso file

```
$ mount -t iso9660 -o loop cdrom.iso /mnt/cdrom
```

第 11 章 File System

目录

1. Mount partition

1.1. Mount

```
sudo mount /dev/sdb1 /mnt/mount1
```

支持UTF-8

```
mount -o iocharset=utf8 /dev/sda5 /mnt/usb
```

1.2. Umount

umount - unmount file systems

```
sudo umount /mnt/mount1
```

1.3. bind directory

```
mount --bind /foo /home/neo/foo
```

挂载目录将不能被删除，但目录下文件可以删除

```
# rm -rf /home/neo/foo
rm: cannot remove directory '/home/neo/foo': Device or resource busy
```

/etc/fstab

```
/foo /home/neo/foo    none    bind    0 0
```

1.4. /etc/fstab

```
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
```

mount point

```
该字段描述希望的文件系统加载的目录，对于swap设备，该字段为none
```

file system

```
例如/dev/cdrom或/dev/sdb,除了使用设备名，你可以使用设备的UUID或设备的卷标签，例如，LABAL=root 或
UUID=7f91104e-8187-4ccf-8215-6e2e641f32e3
```

type

定义了该设备上的文件系统,系统可用文件系统

```
$ cat /proc/filesystems
nodev   sysfs
nodev   rootfs
nodev   bdev
nodev   proc
nodev   cgroup
nodev   cpuset
nodev   tmpfs
nodev   devtmpfs
nodev   debugfs
nodev   securityfs
nodev   sockfs
nodev   pipefs
nodev   anon_inodefs
nodev   inotifyfs
nodev   devpts
        ext3
        ext2
        ext4
nodev   ramfs
nodev   hugetlbfs
nodev   ecryptfs
nodev   fuse
        fuseblk
nodev   fusectl
nodev   mqueue
nodev   rpc_pipefs
nodev   nfs
nodev   nfs4
        reiserfs
        xfs
        jfs
        msdos
        vfat
        ntfs
        minix
        hfs
        hfsplus
        qnx4
        ufs
        btrfs
        iso9660
```

options

```
选项                    含义
```

```
ro     以只读模式加载该文件系统
sync    不对该设备的写操作进行缓冲处理，这可以防止在非正常关机时情况下破坏文件系统，但是却降低了计算机速度
user    允许普通用户加载该文件系统
quota    强制在该文件系统上进行磁盘定额限制
noauto   不再使用mount -a命令（例如系统启动时）加载该文件系统
noatime/nodiratime       禁止更新访问时间
```

dump

```
dump - 该选项被"dump"命令使用来检查一个文件系统应该以多快频率进行转储，若不需要转储就设置该字段为0
```

pass

```
该字段被fsck命令用来决定在启动时需要被扫描的文件系统的顺序，根文件系统"/"对应该字段的值应该为1，其他文件系统应该为2。若该文件系统无需在启动时扫描则设置该字段为0
```

noatime/nodiratime

```
/dev/sda2 /data ext3 defaults 0 2
/dev/sda2 /data ext3 defaults,noatime,nodiratime 0 2
```

```
mount -o remount /data
mount -o noatime -o nodiratime -o remount /data
```

---

2. RAM FS

```
# mkdir -p /mnt/ram1
# mount -t ramfs none /mnt/ram1 -o maxsize=10000
```

3. tmpfs

```
# mkdir -p /mnt/tmpfs
# mount tmpfs /mnt/tmpfs -t tmpfs
# mount tmpfs /mnt/tmpfs -t tmpfs -o size=32m
```

4. ftp fs

安装

```
sudo apt-get install curlftpfs
```

挂载

```
sudo curlftpfs ftp://username:password@172.16.0.1 /mnt/ftp
```

卸载

```
sudo fusermount -u /mnt/ftp
```

权限设置

```
sudo curlftpfs -o rw,allow_other,uid=500,gid=500 ftp://neo:chen@172.16.1.1 /mnt/ftp
sudo curlftpfs ftp://host/sub_dir mount_point -o user="ftp_username:ftp_password", uid=user_id,
gid=group_id, allow_other
```

fstab 开机自动挂载

```
sudo echo "curlftpfs#username:password@172.16.0.1 /mnt/ftp fuse
allow_other,uid=userid,gid=groupid 0 0" >> /etc/fstab
```

5. SSHFS (sshfs - filesystem client based on SSH File Transfer Protocol)

```
$ sudo apt-get install sshfs
$ sudo sshfs root@172.16.0.5:/home/neo /mnt
$ sudo fusermount -u /mnt
```

第 12 章 Networking

目录

1. Hostname

1.1. /etc/hostname

```
# cat /etc/hostname
web1.example.com
```

1.2. /etc/host.conf

解析顺序配置文件

```
[root@development bin]# cat /etc/host.conf
order hosts,bind
```

首先在/etc/hosts文件中寻找，如果不存在，再去DNS服务器中寻找

1.3. /etc/hosts

IP地址后面TAB符，然后写主机地址

```
127.0.0.1       localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
192.168.1.10    development.example.com development
```

1.4. hosts.allow / hosts.deny

/etc/hosts.allow 和 /etc/hosts.deny

许可IP／禁止IP，相当于黑白名单

1.5. /etc/resolv.conf

```
search example.com
nameserver 208.67.222.222
nameserver 208.67.220.220
```

上一页 上一级 下一页

5. SSHFS (sshfs - filesystem client based on SSH File Transfer Protocol) 起始页 2. Network adapter

2. Network adapter

ethtool eth1

```
neo@shenzhen:~/doc/Linux/xhtml$ sudo ethtool eth1
Settings for eth1:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Full
        Port: MII
        PHYAD: 32
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: pumbg
        Wake-on: d
        Current message level: 0x00000007 (7)
        Link detected: yes
```

mii-tool

```
neo@shenzhen:~/doc/Linux/xhtml$ sudo mii-tool
eth1: negotiated 100baseTx-FD, link ok
```

3. Ethernet Interfaces

restart

```
sudo /etc/init.d/networking restart
```

3.1. ifquery

```
$ sudo ifquery --list
lo
eth0
eth1
```

3.2. DHCP

DHCP

```
sudo vi /etc/network/interfaces

# The primary network interface - use DHCP to find our address
auto eth0
iface eth0 inet dhcp
```

3.3. Static IP

Static IP

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.3.90
gateway 192.168.3.1
netmask 255.255.255.0
network 192.168.3.0
broadcast 192.168.3.255
```

Setting up Second IP address or Virtual IP address in Ubuntu

```
sudo vi /etc/network/interfaces

auto eth0:1
iface eth0:1 inet static
address 192.168.1.60
netmask 255.255.255.0
network x.x.x.x
broadcast x.x.x.x
gateway x.x.x.x
```

4. Mask

举例说明该算法。

例：给定一 class c address : 192.168.5.0 ，要求划分20个子网，每个子网5个主机。

解：因为4 <5 < 8 ，用256－8＝248 ---->即是所求的子网掩码，对应的子网数也就出来了。这是针对C类地址。针对B类地址的做法。对于B类地址，假如主机数小于或等于254，与C类地址算法相同。对于主机数大于254的，如需主机 700台，50个子网（相当大了），512 < 700< 1024

256－（1024/256）=256－4＝252 ---->即是所求的子网掩码，对应的子网数也就出来了。上面256－4中的4（2的2次幂）是指主机数用2进制表示时超过8位的位数，即超过2位，掩码为剩余的前6位，即子网数为2（6）－2＝62个。

```
Append :Host/Subnet Quantities Table

-----------------------------------------------------------------------
Class A                     Effective  Effective
# bits         Mask          Subnets     Hosts
-------  ---------------  ---------  ---------
  2      255.192.0.0            2      4194302
  3      255.224.0.0            6      2097150
  4      255.240.0.0           14      1048574
  5      255.248.0.0           30       524286
  6      255.252.0.0           62       262142
  7      255.254.0.0          126       131070
  8      255.255.0.0          254        65536
  9      255.255.128.0        510        32766
  10     255.255.192.0       1022        16382
  11     255.255.224.0       2046         8190
  12     255.255.240.0       4094         4094
  13     255.255.248.0       8190         2046
  14     255.255.252.0      16382         1022
  15     255.255.254.0      32766          510
  16     255.255.255.0      65536          254
  17     255.255.255.128   131070          126
  18     255.255.255.192   262142           62
  19     255.255.255.224   524286           30
  20     255.255.255.240  1048574           14
  21     255.255.255.248  2097150            6
  22     255.255.255.252  4194302            2

Class B                     Effective  Effective
# bits         Mask          Subnets     Hosts
-------  ---------------  ---------  ---------
  2      255.255.192.0          2       16382
  3      255.255.224.0          6        8190
  4      255.255.240.0         14        4094
  5      255.255.248.0         30        2046
  6      255.255.252.0         62        1022
  7      255.255.254.0        126         510
  8      255.255.255.0        254         254
  9      255.255.255.128      510         126
  10     255.255.255.192     1022          62
  11     255.255.255.224     2046          30
  12     255.255.255.240     4094          14
  13     255.255.255.248     8190           6
  14     255.255.255.252    16382           2

Class C                     Effective  Effective
# bits         Mask          Subnets     Hosts
-------  ---------------  ---------  ---------
  2      255.255.255.192       2          62
  3      255.255.255.224       6          30
  4      255.255.255.240      14          14
```

```
  5      255.255.255.248      30          6
  6      255.255.255.252      62          2

*Subnet all zeroes and all ones excluded.
*Host all zeroes and all ones excluded.
```

5. Gateway

default gateway

```
$ sudo route add default gw 172.16.0.1
```

```
$ sudo ip route default via 172.16.0.1 dev eth0
```

6. Configuring Name Server Lookups

Setting up DNS

```
When it comes to DNS setup Ubuntu doesn't differ from other distributions. You can add hostname
and IP addresses to the file /etc/hosts for static lookups.

To cause your machine to consult with a particular server for name lookups you simply add their
addresses to /etc/resolv.conf.

For example a machine which should perform lookups from the DNS server at IP address 192.168.3.2
would have a resolv.conf file looking like this

sudo vi /etc/resolv.conf

enter the following details

search test.com
nameserver 192.168.3.2
```

```
domain domain.com
search www.domain.com domain.com
nameserver 202.96.128.86
nameserver 202.96.134.133
```

7. sysctl

enable IP forwarding

```
neo@shenzhen:~$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
```

```
# enable IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
```

ubuntu

```
sysctl -w net.ipv4.ip_forward=1
```

8. bonding

绑定的前提条件：芯片组型号相同，而且网卡应该具备自己独立的BIOS芯片。

#vi ifcfg-bond0

```
# cat ifcfg-bond0
DEVICE=bond0
BOOTPROTO=static
IPADDR=172.16.0.1
NETMASK=255.255.252.0
BROADCAST=172.16.3.254
ONBOOT=yes
TYPE=Ethernet
```

这里要主意，不要指定单个网卡的IP 地址、子网掩码。将上述信息指定到虚拟适配器(bonding)中即可

```
[root@rhas-13 network-scripts]# cat ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp

[root@rhas-13 network-scripts]# cat ifcfg-eth1
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=dhcp
```

编辑 /etc/modules.conf 文件，加入如下一行内容，以使系统在启动时加载bonding模块，对外虚拟网络接口设备为 bond0.加入下列两行:

* /etc/modules.conf 文件已经不再使用

```
cat >> /etc/modprobe.d/bonding.conf <<EOF
alias bond0 bonding
options bond0 miimon=100 mode=1
EOF
```

说明：miimon是用来进行链路监测的。比如:miimon=100，那么系统每100ms监测一次链路连接状态，如果有一条线路不通就转入另一条线路；mode的值表示工作模式，他共有0， 1,2,3四种模式，常用的为0,1两种。mode=0表示load balancing (round-robin)为负载均衡方式，两块网卡都工作。mode=1表示fault-tolerance (active-backup)提供冗余功能，工作方式是主备的工作方式,也就是说默认情况下只有一块网卡工作,另一块做备份。bonding只能提供链路监测，即从主机到交换机的链路是否接通。如果只是交换机对外的链路down掉了，而交换机本身并没有故障，那么bonding会认为链路没有问题而继续使用。

vi /etc/rc.d/rc.local

```
ifenslave bond0 eth0 eth1
route add -net 172.31.3.254 netmask 255.255.255.0 bond0
```

到这时已经配置完毕 重新启动机器。重启会看见以下信息就表示配置成功了

```
................
Bringing up interface bond0 OK
Bringing up interface eth0 OK
Bringing up interface eth1 OK
................
```

mode=1工作在主备模式下,这时eth1作为备份网卡是no arp的 [root@rhas-13 network-scripts]# ifconfig 验证网卡的配置信息

那也就是说在主备模式下,当一个网络接口失效时(例如主交换机掉电等),不回出现网络中断, 系统会按照cat /etc/rc.d/rc.local里指定网卡的顺序工作,机器仍能对外服务,起到了失效保护的功能。在mode=0 负载均衡工作模式,他能提供两倍的带宽,下我们来看一下网卡的配置信息:

在这种情况下出现一块网卡失效,仅仅会是服务器出口带宽下降,也不会影响网络使用。通过查看bond0的工作状态查询能详细的掌握bonding的工作状态

Linux下通过网卡邦定技术既增加了服务器的可靠性,又增加了可用网络带宽,为用户提供不间断的关键服务。

8.1. Ubuntu

ifenslave

```
apt-get install ifenslave-2.6
```

/etc/modules

```
bonding
```

modprobe bonding

/etc/modprobe.d/aliases

```
alias bond0 bonding
options bonding mode=0 miimon=100

or

options bonding mode=1 miimon=100 downdelay=200 updelay=200
```

例 12.1. bonding example

/etc/network/interfaces

```
auto lo
iface lo inet loopback

iface eth0 inet dhcp
iface eth1 inet dhcp

auto bond0
iface bond0 inet static
address 172.16.0.1
netmask 255.255.255.0
gateway 172.16.0.254
up ifenslave bond0 eth0 eth1
down ifenslave -d bond0 eth0 eth1
```

9. Finding optimal MTU

```
$ ping -c 1 -s $((1500-28)) -M do www.debian.org
PING www.debian.org (140.112.8.139) 1472(1500) bytes of data.
1480 bytes from linux3.cc.ntu.edu.tw (140.112.8.139): icmp_seq=1 ttl=47 time=52.7 ms

--- www.debian.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 52.778/52.778/52.778/0.000 ms
```

Try 1454 instead of 1500

第 13 章 syslog, klogctl - read and/or clear kernel message ring buffer; set console_loglevel

目录

1. /etc/sysconfig/syslog

enables logging from remote machines

```
# vim /etc/sysconfig/syslog

#SYSLOGD_OPTIONS="-m 0"
SYSLOGD_OPTIONS="-r -m 0"
```

```
# /etc/init.d/syslog restart
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
```

2. /etc/syslog.conf

```
*.*                     @172.16.0.9
```

所有日志将被重定向到172.16.0.9

```
[root@dev1 test]# service syslog restart
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
[root@dev1 test]#
```

3. logger

日志的级别

```
emerg 系统已经不可用，级别为紧急
alert 警报，需要立即处理和解决
crit 既将发生，得需要预防。事件就要发生
warnig 警告
err 错误信息，普通的错误信息
notice 提醒信息，很重要的信息
info 通知信息，属于一般信息
debug 这是调试类信息
```

```
#vi /etc/syslog.conf

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none;local1.none;local3.none /var/log/messages

#my log
local3.* /var/log/my.log
```

```
# service syslog restart
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
```

```
ping 192.168.0.1 | logger -it logger_test -p local3.notice
```

```
# cat /var/log/my.log
Jan 12 18:06:03 dev1 logger_test[10991]: PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
Jan 12 18:06:03 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.746
ms
Jan 12 18:06:04 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.713
ms
Jan 12 18:06:05 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.924
ms
Jan 12 18:06:06 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.819
ms
Jan 12 18:06:08 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.667
ms
Jan 12 18:06:09 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=0.626
ms
Jan 12 18:06:10 dev1 logger_test[10991]: 64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=0.665
ms
```

4. To Log Messages Over UDP Network

第 14 章 logrotate - rotates, compresses, and mails system logs

目录

logrotate 是linux系统自带的日志分割与压缩程序，通过crontab每日运行一次。

```
$ cat /etc/cron.daily/logrotate
#!/bin/sh

test -x /usr/sbin/logrotate || exit 0
/usr/sbin/logrotate /etc/logrotate.conf
```

1. /etc/logrotate.conf

```
$ cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

# system-specific logs may be configured here
```

2. /etc/logrotate.d/

2.1. apache2

```
$ cat /etc/logrotate.d/apache2
/var/log/apache2/*.log {
        weekly
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                if [ -f "`. /etc/apache2/envvars ; echo ${APACHE_PID_FILE:-
/var/run/apache2.pid}`" ]; then
                        /etc/init.d/apache2 reload > /dev/null
                fi
        endscript
}
```

```
/var/log/httpd/*log {
    missingok
    notifempty
    sharedscripts
    postrotate
        /sbin/service httpd reload > /dev/null 2>/dev/null || true
    endscript
}
```

2.2. mysql

```
$ cat /etc/logrotate.d/mysql-server
# - I put everything in one block and added sharedscripts, so that mysql gets
#   flush-logs'd only once.
#   Else the binary logs would automatically increase by n times every day.
# - The error log is obsolete, messages go to syslog now.
/var/log/mysql.log /var/log/mysql/mysql.log /var/log/mysql/mysql-slow.log {
        daily
        rotate 7
        missingok
        create 640 mysql adm
        compress
        sharedscripts
        postrotate
                test -x /usr/bin/mysqladmin || exit 0
                # If this fails, check debian.conf!
                MYADMIN="/usr/bin/mysqladmin --defaults-file=/etc/mysql/debian.cnf"
                if [ -z "`$MYADMIN ping 2>/dev/null`" ]; then
                  # Really no mysqld or rather a missing debian-sys-maint user?
                  # If this occurs and is not a error please report a bug.
                  #if ps cax | grep -q mysqld; then
                  if killall -q -s0 -umysql mysqld; then
                    exit 1
                  fi
                else
                  $MYADMIN flush-logs
                fi
        endscript
}
```

2.3. cacti

```
/var/log/cacti/*.log {
        weekly
        missingok
        rotate 52
        compress
        notifempty
        create 640 www-data www-data
        sharedscripts
}
```

第 15 章 remote syslog

目录

1. syslog-ng

2. rsyslog

www.rsyslog.com

第 16 章 Service

目录

1. update-rc.d - install and remove System-V style init script links

for example:

```
Insert links using the defaults:
   update-rc.d foobar defaults
Equivalent command using explicit argument sets:
   update-rc.d foobar start 20 2 3 4 5 . stop 20 0 1 6 .
More typical command using explicit argument sets:
   update-rc.d foobar start 30 2 3 4 5 . stop 70 0 1 6 .
Insert links at default runlevels when B requires A
   update-rc.d script_for_A defaults 80 20
   update-rc.d script_for_B defaults 90 10
Insert a link to a service that (presumably) will not be needed by any other daemon
   update-rc.d top_level_app defaults 98 02
Insert links for a script that requires services that start/stop at sequence number 20
   update-rc.d script_depends_on_svc20 defaults 21 19
Remove all links for a script (assuming foobar has been deleted already):
   update-rc.d foobar remove
Example of disabling a service:
   update-rc.d -f foobar remove
   update-rc.d foobar stop 20 2 3 4 5 .
Example of a command for installing a system initialization-and-shutdown script:
   update-rc.d foobar start 45 S . stop 31 0 6 .
Example of a command for disabling a system initialization-and-shutdown script:
   update-rc.d -f foobar remove
   update-rc.d foobar stop 45 S .
```

set default

```
update-rc.d nginx defaults
```

remove

```
update-rc.d -f lighttpd remove
$ sudo update-rc.d -f avahi-daemon remove
```

2. invoke-rc.d - executes System-V style init script actions

```
$ sudo invoke-rc.d mysql restart
```

3. runlevel

```
$ runlevel
N 2

# runlevel
N 3
```

```
$ sudo vim /etc/init.d/rcS
#! /bin/sh
#
# rcS
#
# Call all S??* scripts in /etc/rcS.d/ in numerical/alphabetical order
#

exec /etc/init.d/rc S
```

the default is S (/etc/rcS.d/)

the redhat linux in the /etc/inittab

switch runlevel

```
/etc/init.d/rc 3
```

4. sysv-rc-conf

(ubuntu下sysv-rc-conf命令等同redhat下chkconfig命令)

```
sysv-rc-conf gmond on
sysv-rc-conf --list gmond
```

5. xinetd - replacement for inetd with many enhancements

```
$ sudo apt-get install xinetd
```

5.1. tftpd

```
apt-get install xinetd
apt-get install tftpd tftp
```

/etc/xinetd.d/tftp

```
service tftp
{
        disable=no
        socket_type=dgram
        protocol =udp
        wait=yes
        user=root
        server=/usr/sbin/in.tftpd
        server_args =-s /home/neo/tftpboot -c
        per_source=11
        cps=100 2
        flags=IPv4
}
```

6. Scheduled Tasks

6.1. crontab - maintain crontab files for individual users

To see what crontabs are currently running on your system, you can open a terminal and run:

```
$  crontab -l
# m h  dom mon dow   command
#* */30 * * * /home/neo/dyndns
```

if you want to see root user, please add 'sudo' in the prefix.

To edit the list of cron jobs you can run:

```
$ crontab -e
```

As you can see there are 5 stars. The stars represent different date parts in the following order:

1. minute (from 0 to 59)
2. hour (from 0 to 23)
3. day of month (from 1 to 31)
4. month (from 1 to 12)
5. day of week (from 0 to 6) (0=Sunday)

By default cron jobs sends a email to the user account executing the cronjob. If this is not needed put the following command At the end of the cron job line .

```
>/dev/null 2>&1
```

6.2. at, batch, atq, atrm - queue, examine or delete jobs for later execution

部分 II. Network Application

目录

第 17 章 network tools

目录

1. curl / w3m / lynx

curl

```
curl http://netkiller.8800.org
```

w3m

```
w3m http://netkiller.8800.org
```

lynx

```
lynx http://netkiller.8800.org
```

第 18 章 OpenNTPD

目录

http://www.pool.ntp.org/

1. install

ubuntu

```
sudo apt-get install openntpd
```

centos / redhat

```
yum install ntp -y
```

2. ntpdate

```
# ntpdate 172.16.3.51
```

3. ntpd.conf / ntp.conf

```
# $OpenBSD: ntpd.conf,v 1.7 2004/07/20 17:38:35 henning Exp $
# sample ntpd configuration file, see ntpd.conf(5)

# Addresses to listen on (ntpd does not listen by default)
listen on *
#listen on 127.0.0.1
#listen on ::1

# sync to a single server
#server ntp.example.org

# use a random selection of 4 public stratum 2 servers
# see http://twiki.ntp.org/bin/view/Servers/NTPPoolServers
# and http://www.pool.ntp.org/
#server 0.debian.pool.ntp.org
#server 1.debian.pool.ntp.org
#server 2.debian.pool.ntp.org
#server 3.debian.pool.ntp.org

server 0.asia.pool.ntp.org
server 1.asia.pool.ntp.org
server 2.asia.pool.ntp.org
server 3.asia.pool.ntp.org
```

3.1. server 配置

server your_ip_address

```
server 172.16.0.1
server 172.16.0.2
```

3.2. ntp 安全设置

允许192.168.1.0段访问ntp

```
restrict default ignore
# Hosts on local network are less restricted.
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

第 19 章 Linux IP And Router

目录

1. netmask

```
# iptab
+-----------------------------------------------+
| addrs   bits   pref   class  mask             |
+-----------------------------------------------+
|     1      0    /32          255.255.255.255  |
|     2      1    /31          255.255.255.254  |
|     4      2    /30          255.255.255.252  |
|     8      3    /29          255.255.255.248  |
|    16      4    /28          255.255.255.240  |
|    32      5    /27          255.255.255.224  |
|    64      6    /26          255.255.255.192  |
|   128      7    /25          255.255.255.128  |
|   256      8    /24      1C  255.255.255.0    |
|   512      9    /23      2C  255.255.254.0    |
```

```
|     1K      10     /22       4C  255.255.252.0    |
|     2K      11     /21       8C  255.255.248.0    |
|     4K      12     /20      16C  255.255.240.0    |
|     8K      13     /19      32C  255.255.224.0    |
|    16K      14     /18      64C  255.255.192.0    |
|    32K      15     /17     128C  255.255.128.0    |
|    64K      16     /16       1B  255.255.0.0      |
|   128K      17     /15       2B  255.254.0.0      |
|   256K      18     /14       4B  255.252.0.0      |
|   512K      19     /13       8B  255.248.0.0      |
|     1M      20     /12      16B  255.240.0.0      |
|     2M      21     /11      32B  255.224.0.0      |
|     4M      22     /10      64B  255.192.0.0      |
|     8M      23      /9     128B  255.128.0.0      |
|    16M      24      /8       1A  255.0.0.0        |
|    32M      25      /7       2A  254.0.0.0        |
|    64M      26      /6       4A  252.0.0.0        |
|   128M      27      /5       8A  248.0.0.0        |
|   256M      28      /4      16A  240.0.0.0        |
|   512M      29      /3      32A  224.0.0.0        |
|  1024M      30      /2      64A  192.0.0.0        |
|  2048M      31      /1     128A  128.0.0.0        |
|  4096M      32      /0     256A  0.0.0.0          |
+-----------------------------------------------+
```

上一页 上一级 下一页

3. ntpd.conf / ntp.conf 起始页 2. arp - manipulate the system ARP cache

2. arp - manipulate the system ARP cache

2.1. display hosts

display (all) hosts in alternative (BSD) style

```
[root@dev2 ~]# arp -a
? (192.168.3.253) at 00:1D:0F:82:05:DC [ether] on eth0
? (192.168.3.48) at 00:25:64:9A:D7:CC [ether] on eth0
? (192.168.3.101) at 00:25:64:A3:65:93 [ether] on eth0
nis.example.com (192.168.3.5) at 00:25:64:9A:D7:E0 [ether] on eth0
? (192.168.3.1) at 00:0F:E2:71:8E:FB [ether] on eth0
? (192.168.3.153) at B8:AC:6F:25:D2:2E [ether] on eth0
```

display (all) hosts in default (Linux) style

```
[root@dev2 ~]# arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.3.48             ether   00:25:64:9A:D7:CC   C                     eth0
192.168.3.101            ether   00:25:64:A3:65:93   C                     eth0
nis.example.com          ether   00:25:64:9A:D7:E0   C                     eth0
192.168.3.1              ether   00:0F:E2:71:8E:FB   C                     eth0
10.0.0.1                 ether   00:1F:12:55:A9:02   C                     eth0
192.168.3.153            ether   B8:AC:6F:25:D2:2E   C                     eth0
```

don't resolve names

```
[root@dev2 ~]# arp -a -n
? (192.168.3.253) at 00:1D:0F:82:05:DC [ether] on eth0
? (192.168.3.48) at 00:25:64:9A:D7:CC [ether] on eth0
? (192.168.3.101) at 00:25:64:A3:65:93 [ether] on eth0
? (192.168.3.5) at 00:25:64:9A:D7:E0 [ether] on eth0
? (192.168.3.1) at 00:0F:E2:71:8E:FB [ether] on eth0
? (192.168.3.153) at B8:AC:6F:25:D2:2E [ether] on eth0
```

2.2. delete a specified entry

```
[root@dev2 ~]# arp -d 192.168.3.101
[root@dev2 ~]# arp -i eth1 -d 10.0.0.1
```

2.3. /proc/net/arp

```
[root@dev2 ~]# cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.3.48     0x1         0x2         00:25:64:9A:D7:CC     *        eth0
192.168.3.101    0x1         0x2         00:1E:7A:E0:47:40     *        eth0
192.168.3.5      0x1         0x2         00:25:64:9A:D7:E0     *        eth0
192.168.3.1      0x1         0x2         00:0F:E2:71:8E:FB     *        eth0
192.168.3.153    0x1         0x2         B8:AC:6F:25:D2:2E     *        eth0
```

2.4. /etc/ethers

```
# Ethernet-address  IP-number
00:25:64:9A:D7:CC       192.168.3.48
```

read new entries from file or from /etc/ethers

```
# arp -f
```

3. iproute2

```
add 增加路由
del 删除路由
via 网关出口 IP地址
dev 网关出口 物理设备名
```

3.1. 添加路由

```
ip route add 192.168.0.0/24 via 192.168.0.1
ip route add 192.168.1.1 dev 192.168.0.1
```

3.2. 删除路由

```
ip route del 192.168.0.0/24 via 192.168.0.1
```

3.3. 变更路由

```
[root@router ~]# ip route
192.168.5.0/24 dev eth0  proto kernel  scope link  src 192.168.5.47
192.168.3.0/24 dev eth0  proto kernel  scope link  src 192.168.3.47
default via 192.168.3.1 dev eth0

[root@router ~]# ip route change default via 192.168.5.1 dev eth0

[root@router ~]# ip route list
192.168.5.0/24 dev eth0  proto kernel  scope link  src 192.168.5.47
192.168.3.0/24 dev eth0  proto kernel  scope link  src 192.168.3.47
default via 192.168.5.1 dev eth0
```

3.4. 替换已有的路由

```
 ip route replace
```

3.5. 增加默认路由

192.168.0.1 是我的默认路由器

```
ip route add default via 192.168.0.1 dev eth0
```

3.6. cache

```
ip route flush cache
```

4. 策略路由

```
比如我们的LINUX有3个网卡
eth0: 192.168.1.1    (局域网)
eth1: 172.17.1.2     (default gw=172.17.1.1, 可以上INTERNET)
eth2: 192.168.10.2    (连接第二路由192.168.10.1, 也可以上INTERNET)

实现两个目的
1、让192.168.1.66从第二路由上网, 其他人走默认路由
2、让所有人访问192.168.1.1的FTP时, 转到192.168.10.96上

配置方法:
vi /etc/iproute2/rt_tables

#
# reserved values
#
255     local
254     main
253     default
100     ROUTE2

# ip route default via 172.17.1.1 dev eth1
# ip route default via 192.168.10.1 dev eth2 table ROUTE2
# ip rule add from 192.168.1.66 pref 1001 table ROUTE2
# ip rule add to 192.168.10.96 pref 1002 table ROUTE2
# echo 1 >; /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING -j MASQUERADE
# iptables -t nat -A PREROUTING -d 192.168.1.1 -p tcp --dport 21 -j DNAT --to 192.168.10.96
# ip route flush cache
```

```
http://phorum.study-area.org/viewtopic.php?t=10085
引用: # 對外網卡
EXT_IF="eth0"

# HiNet IP
EXT_IP1="111.111.111.111"
EXT_MASK1="24"
GW1="111.111.111.1"

# SeedNet IP
EXT_IP2="222.222.222.222"
EXT_MASK2="24"
GW2="222.222.222.1"

# ?#93;定 ip
ip addr add $EXT_IP1/$EXT_MASK1 dev $EXT_IF
ip addr add $EXT_IP2/$EXT_MASK2 dev $EXT_IF

# ?#93;定 HiNet routing
ip rule add to $EXT_IP1/$EXT_MASK1 lookup 201
ip route add default via $GW1 dev $EXT_IF table 201

# ?#93;定 SeedNet routing
ip rule add to $EXT_IP2/$EXT_MASK2 lookup 202
ip route add default via $GW2 dev $EXT_IF table 202

# ?#93;定 Default route
ip route replace default equalize \
   nexthop via $GW1 dev $EXT_IF \
   nexthop via $GW2 dev $EXT_IF

# 清除 route cache
ip route flush cache


它这里的ip rule也是这么使用的
```

5. 负载均衡

```
ip route add default scope global nexthop dev ppp0 nexthop dev ppp1
```

```
neo@debian:~$ sudo ip route add default scope global nexthop via 192.168.3.1 dev eth0 weight 1
\
nexthop via 192.168.5.1 dev eth2 weight 1

neo@debian:~$ sudo ip route
192.168.5.0/24 dev eth1  proto kernel  scope link  src 192.168.5.9
192.168.4.0/24 dev eth0  proto kernel  scope link  src 192.168.4.9
192.168.3.0/24 dev eth0  proto kernel  scope link  src 192.168.3.9
172.16.0.0/24 dev eth2  proto kernel  scope link  src 172.16.0.254
default
        nexthop via 192.168.3.1  dev eth0 weight 1
        nexthop via 192.168.5.1  dev eth1 weight 1
```

```
ip route add default scope global nexthop via $P1 dev $IF1 weight 1 \
nexthop via $P2 dev $IF2 weight 1
```

6. MASQUERADE

```
iptables-tnat-APOSTROUTING-d192.168.1.0/24-s0/0-oppp0-jMASQUERD
iptables-tnat-APOSTROUTING-s192.168.1.0/24-jSNAT-to202.103.224.58
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE
```

```
#ip route add via ppp0 dev eth0
#ip route add via 202.103.224.58 dev eth0
```

7. ip tunnel

ipip 是IP隧道模块

过程 19.1. ip tunnel IP隧道配置步骤

1. server 1

```
modprobe ipip
ip tunnel add mytun mode ipip remote 220.201.35.11 local 211.100.37.167 ttl 255
ifconfig mytun 10.42.1.1
route add -net 10.42.1.0/24 dev mytun
```

2. server 2

```
modprobe ipip
ip tunnel add mytun mode ipip remote 211.100.37.167 local 220.201.35.11 ttl 255
ifconfig mytun 10.42.1.2
route add -net 10.42.1.0/24 dev mytun
```

3. nat

```
/sbin/iptables -t nat -A POSTROUTING -s 10.42.1.0/24 -j MASQUERADE
/sbin/iptables -t nat -A POSTROUTING -s 211.100.37.0/24 -j MASQUERADE
```

删除路由表

```
route del -net 10.42.1.0/24 dev mytun
```

修改IP隧道的IP

```
ifconfig mytun 10.10.10.220
route add -net 10.10.10.0/24 dev mytun
```

ip 伪装

```
/sbin/iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -j MASQUERADE
```

8. VLAN

首先需确保加载了内核模块 802.1q

```
[root@development ~]# lsmod | grep 8021q
[root@development ~]# modprobe 8021q
```

加载后会生成目录/proc/net/vlan

```
[root@development ~]# cat /proc/net/vlan/config
VLAN Dev name    | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
```

9. Zebra

http://www.zebra.org/

第 20 章 DHCP

目录

1. DHCP Server

eth0 公网ip

eth1 192.168.0.1 255.255.255.0

eth2 192.168.1.1 255.255.255.0

```
dhcpd.conf配置内容如下:

#Sample /etc/dhcpd.conf
default-lease-time 1200;
max-lease-time 19200;
option domain-name-servers 202.102.192.68,202.102.199.68;
#option domain-name "test.test";
ddns-update-style ad-hoc;

subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.20 192.168.0.200;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.0.255;
        option routers 192.168.0.1;
}
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.20 192.168.1.200;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.1.255;
        option routers 192.168.1.1;
}
```

2. dhclient

all interface

```
$ sudo dhclient
```

eth0

```
$ sudo dhclient eth0
```

3. release matching connections

windows

```
> ipconfig /release
> ipconfig /renew
```

第 21 章 DNS/Bind

目录

1. 安装 bind9

neo@master:~$ # apt-get install bind9

named.conf.local.neo.org

```
neo@master:~$ cat /etc/bind/named.conf.local.neo.org

zone "neo.org" in {
     type master;
     file "db.neo.org";
};

zone "0.16.172.in-addr.arpa" in {
    type master;
    file "db.172.16.0";
};
```

/var/cache/bind/db.neo.org

```
neo@master:~$ cat /var/cache/bind/db.neo.org
@ IN SOA        neo.org. root.neo.org. (
                          200211131 ; serial, todays date + todays serial #
                          28800 ; refresh, seconds
                          7200 ; retry, seconds
                          3600000 ; expire, seconds
                          86400 ) ; minimum, seconds
        NS ns.neo.org.
@       IN A         172.16.0.1
www     IN A         172.16.0.1
mail    IN A         172.16.0.1
@       MX 10 mail.neo.org.
```

/var/cache/bind/db.172.16.0

```
neo@master:~$ cat /var/cache/bind/db.172.16.0
@ IN SOA neo.org root.neo.org. (
                                2002111300 ; Serial
                                28800 ; Refresh
                                14400 ; Retry
                                3600000 ; Expire
                                86400 ) ; Minimum
                                IN NS ns.neo.org.

1 PTR www1.neo.org.
2 PTR www2.neo.org.
3 PTR www3.neo.org.
neo@master:~$
```

/etc/resolv.conf

```
neo@master:~$ cat /etc/resolv.conf
search neo.org
nameserver 172.16.0.2
neo@master:~$
```

---

2. forwarders

```
options {
    directory "/var/named";
    forwarders { 192.168.24.35; 192.168.24.36; };
};
```

3. Load Balancing

Load Balancing (DNS 轮循负载均衡)

Bind 8

```
neo@master:~$ cat /var/cache/bind/db.neo.org
@ IN SOA        neo.org. root.neo.org. (
                          200211131 ; serial, todays date + todays serial #
                          28800 ; refresh, seconds
                          7200 ; retry, seconds
                          3600000 ; expire, seconds
                          86400 ) ; minimum, seconds
        NS ns.neo.org.
@       IN A         192.168.0.1
web     IN A         192.168.0.1
mail    IN A         192.168.0.1
@       MX 10 mail.neo.org.

www1 IN A         172.16.0.1
www2 IN A         172.16.0.2
www3 IN A         172.16.0.3
www4 IN A         172.16.0.4

www    IN CNAME        www1.neo.org.
www    IN CNAME        www2.neo.org.
www    IN CNAME        www3.neo.org.
www    IN CNAME        www4.neo.org.
neo@master:~$
```

Bind 9

```
neo@master:~$ cat /var/cache/bind/db.neo.org
@ IN SOA        neo.org. root.neo.org. (
                          200211131 ; serial, todays date + todays serial #
                          28800 ; refresh, seconds
                          7200 ; retry, seconds
                          3600000 ; expire, seconds
                          86400 ) ; minimum, seconds
        NS ns.neo.org.
@       IN A         192.168.0.1
web     IN A         192.168.0.1
mail    IN A         192.168.0.1
@       MX 10 mail.neo.org.

www IN A         172.16.0.1
www IN A         172.16.0.2
www IN A         172.16.0.3
www IN A         172.16.0.4
www IN A         10.50.1.110
www IN A         10.50.1.131
www IN A         10.50.1.122
neo@master:~$
```

4. view

```
acl "cnc_view" {
          220.250.21.86;
          216.93.170.17;
          216.93.160.16;
          210.53.31.2;
          218.104.224.106;
          218.66.59.233;
          218.66.102.93;
          202.101.98.55;
          };

view "cnc" {
match-clients { "cnc_view"; };
recursion yes;
zone "." { type hint; file "named.root"; };
zone "netkiller.org.cn" { type master; file "cnc/netkiller.org.cn" ; };
};

view "no_cnc" {
match-clients { any; };
recursion yes;
zone "netkiller.org.cn" { type master; file "telecom/netkiller.org.cn"; };
zone "." { type hint; file "named.root"; };
};
```

5. Master / Slave

5.1. master /etc/named.conf

```
# cat /etc/named.conf

        zone "example.com" {
                type master;
                file "/var/named/example.com.zone";
                allow-transfer { 172.16.1.23; 120.100.100.23; };
        };
```

notify 指令会自动通知所有这个域的所有在ns记录上的机器，also-notify指令可以用来通知所有不在ns记录上的dns服务器

```
        zone "example.com" {
                type master;
                file "xiu.com.zone";
                allow-transfer { 172.16.1.23; };
                notify yes;
                also-notify { 172.16.1.23; };
        };

                zone "1.16.172.in-addr.arpa" IN {
                        type master;
                        file "1.16.172";
                        allow-transfer { 172.16.1.23 ; };
                        notify yes;
                        also-notify { 172.16.1.23 ; };
                };
```

5.2. /var/named/example.com.zone

```
$TTL    86400
@               IN SOA  example.com. root.example.com. (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
                IN NS           ns1.example.com.
                IN NS           ns2.example.com.
@               IN A 120.100.100.6
@               IN MX 10 mx.corpease.net.

ns1             IN A 120.100.100.20
ns2             IN A 120.100.100.23
www            IN A 120.100.100.6
images         IN A 120.100.100.6
```

5.3. slave /etc/named.conf

```
                zone "example.com" {
                        type slave;
                        file "/var/named/slaves/example.com.zone";
                        masters { 172.16.1.20; 120.100.100.20; };
                };
```

6. DNS tools

6.1. dig - DNS lookup utility

dig

dig @<name server> <domain name>

```
[root@testing neo]# dig @202.96.134.133 netkiller.8800.org

; <<>> DiG 9.2.4 <<>> @202.96.134.133 netkiller.8800.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47971
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;netkiller.8800.org.            IN      A

;; ANSWER SECTION:
netkiller.8800.org.     14353   IN      A       220.201.35.11

;; AUTHORITY SECTION:
8800.org.               86398   IN      NS      ns1.3322.net.
8800.org.               86398   IN      NS      ns2.3322.net.

;; ADDITIONAL SECTION:
ns1.3322.net.           166302  IN      A       61.177.95.125
ns2.3322.net.           166298  IN      A       222.185.245.254

;; Query time: 4 msec
;; SERVER: 202.96.134.133#53(202.96.134.133)
;; WHEN: Fri May 11 22:25:54 2007
;; MSG SIZE  rcvd: 128

[root@testing neo]#
```

6.1.1. any

```
$ dig any google.com

; <<>> DiG 9.7.0-P1 <<>> any google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3225
;; flags: qr rd ra; QUERY: 1, ANSWER: 21, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             300     IN      A       74.125.71.104
google.com.             300     IN      A       74.125.71.99
google.com.             300     IN      A       74.125.71.106
google.com.             300     IN      A       74.125.71.105
google.com.             300     IN      A       74.125.71.103
google.com.             300     IN      A       74.125.71.147
google.com.             86400   IN      SOA     ns1.google.com. dns-admin.google.com.
2011128000 7200 1800 1209600 300
google.com.             3600    IN      TXT     "v=spf1 include:_netblocks.google.com
ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all"
google.com.             345600  IN      NS      ns2.google.com.
google.com.             600     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             345600  IN      NS      ns1.google.com.
google.com.             345600  IN      NS      ns4.google.com.
google.com.             345600  IN      NS      ns3.google.com.
google.com.             600     IN      MX      10 aspmx.l.google.com.
google.com.             600     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             600     IN      MX      30 alt2.aspmx.l.google.com.
```

```
google.com.             600     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             300     IN      A       74.125.71.104
google.com.             300     IN      A       74.125.71.99
google.com.             300     IN      A       74.125.71.106
google.com.             300     IN      A       74.125.71.105

;; Query time: 432 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Tue Nov 29 18:06:43 2011
;; MSG SIZE  rcvd: 508
```

6.1.2. ns

```
$ dig ns google.com

; <<>> DiG 9.7.0-P1 <<>> ns google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57275
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             171085  IN      NS      ns2.google.com.
google.com.             171085  IN      NS      ns1.google.com.
google.com.             171085  IN      NS      ns3.google.com.
google.com.             171085  IN      NS      ns4.google.com.

;; Query time: 402 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Tue Nov 29 18:06:07 2011
;; MSG SIZE  rcvd: 100
```

6.1.3. mx

```
$ dig mx google.com

; <<>> DiG 9.7.0-P1 <<>> mx google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27428
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             525     IN      MX      10 aspmx.l.google.com.
google.com.             525     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             525     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             525     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             525     IN      MX      50 alt4.aspmx.l.google.com.

;; Query time: 359 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Tue Nov 29 18:05:54 2011
;; MSG SIZE  rcvd: 136
```

6.2. nslookup

6.2.1. 刷新 DNS 解析缓存

```
C:\Users\neo>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

6.2.2. 查看NS记录

-qt=ns 查看NS记录

```
C:\Users\neo>nslookup -qt=ns 163.com
服务器:  resolver1.opendns.com
Address:  208.67.222.222

非权威应答:
163.com nameserver = ns3.nease.net
163.com nameserver = ns2.nease.net
163.com nameserver = ns4.nease.net
```

```
C:\Users\neo>nslookup -qt=ns 163.com
服务器:  ns.szptt.net.cn
Address:  202.96.134.133

非权威应答:
163.com nameserver = ns3.nease.net
163.com nameserver = ns4.nease.net
163.com nameserver = ns2.nease.net

ns4.nease.net   internet address = 61.135.255.140
ns2.nease.net   internet address = 114.113.197.12
ns3.nease.net   internet address = 220.181.28.4
```

6.2.3. Mx 记录

```
C:\Users\neo>nslookup -qt=mx 163.com
服务器:  ns.szptt.net.cn
Address:  202.96.134.133

非权威应答:
163.com MX preference = 10, mail exchanger = 163mx03.mxmail.netease.com
163.com MX preference = 10, mail exchanger = 163mx04.mxmail.netease.com
163.com MX preference = 50, mail exchanger = 163mx00.mxmail.netease.com
163.com MX preference = 10, mail exchanger = 163mx01.mxmail.netease.com
163.com MX preference = 10, mail exchanger = 163mx02.mxmail.netease.com

163mx04.mxmail.netease.com      internet address = 220.181.12.78
163mx04.mxmail.netease.com      internet address = 220.181.12.79
163mx04.mxmail.netease.com      internet address = 220.181.12.80
163mx04.mxmail.netease.com      internet address = 220.181.12.81
163mx04.mxmail.netease.com      internet address = 220.181.12.83
163mx04.mxmail.netease.com      internet address = 220.181.12.84
163mx04.mxmail.netease.com      internet address = 220.181.12.85
163mx04.mxmail.netease.com      internet address = 220.181.12.70
163mx04.mxmail.netease.com      internet address = 220.181.12.71
163mx04.mxmail.netease.com      internet address = 220.181.12.72
163mx04.mxmail.netease.com      internet address = 220.181.12.76
163mx04.mxmail.netease.com      internet address = 220.181.12.77
163mx00.mxmail.netease.com      internet address = 220.181.12.87
163mx00.mxmail.netease.com      internet address = 220.181.12.88
163mx00.mxmail.netease.com      internet address = 220.181.12.89
163mx00.mxmail.netease.com      internet address = 220.181.12.90
163mx00.mxmail.netease.com      internet address = 220.181.12.91
163mx00.mxmail.netease.com      internet address = 220.181.12.52
163mx00.mxmail.netease.com      internet address = 220.181.12.53
163mx00.mxmail.netease.com      internet address = 220.181.12.55
163mx00.mxmail.netease.com      internet address = 220.181.12.56
163mx00.mxmail.netease.com      internet address = 220.181.12.57
```

7. DNS

7.1. OpenDNS

```
208.67.222.222
208.67.220.220
```

7.2. Google DNS

```
8.8.8.8
8.8.4.4
```

第 22 章 dnsmasq

目录

1. Install

1.1. CentOS / Redhat

```
yum -y install dnsmasq
```

1.2. Debian / Ubuntu

```
apt-get install dnsmasq
```

1.3. Firewall 设置

```
iptables -A INPUT -p udp -m udp –dport 53 -j ACCEPT
```

2. /etc/dnsmasq.conf

一般配置下面三处即可

```
# vim /etc/dnsmasq.conf

resolv-file=/etc/dnsmasq.resolv.conf
addn-hosts=/etc/dnsmasq.hosts
conf-dir=/etc/dnsmasq.d

/etc/init.d/dnsmasq restart
```

3. dnsmasq.resolv.conf

让dnsmasq 接管DNS解析

```
# vim /etc/dnsmasq.conf

resolv-file=/etc/dnsmasq.resolv.conf
resolv-file
```

```
sudo cp /etc/resolv.conf /etc/dnsmasq.resolv.conf

cat > /etc/dnsmasq.resolv.conf <<EOF
nameserver 208.67.222.222
nameserver 208.67.220.220
EOF
```

或者

```
nameserver 8.8.8.8
nameserver 4.4.4.4
```

/etc/resolv.conf设置用本机做解析

```
echo "nameserver 127.0.0.1" > /etc/resolv.conf
or
sudo vim /etc/resolv.conf
nameserver 127.0.0.1
```

reload

```
/etc/init.d/dnsmasq reload
or
sudo killall -s SIGHUP dnsmasq
```

4. dnsmasq.hosts

dnsmasq 默认会读取 /etc/hosts 如果你不想让它解析/etc/hosts文件，可以自己定义一个文件。

```
# vim /etc/dnsmasq.conf
no-hosts
addn-hosts=/etc/dnsmasq.hosts
```

```
echo "172.16.0.1 test.example.com" > /etc/dnsmasq.hosts
```

重新起动

```
/etc/init.d/dnsmasq restart
```

查看日志

```
cat /var/log/message

Sep 15 18:17:24 J10-51-MemCache dnsmasq[13799]: read /etc/hosts - 2 addresses
Sep 15 18:17:24 J10-51-MemCache dnsmasq[13799]: read /etc/dnsmasq.hosts - 40 addresses
```

使用nslookup测试

```
nslookup test.example.com 172.16.3.51
```

提示

注释no-hosts选项，可以实现 /etc/hosts 与 /etc/dnsmasq.hosts 共用

5. /etc/dnsmasq.d/dnsmasq.server.conf

配置域名使用那些DNS解析

```
vim /etc/dnsmasq.d/dnsmasq.server.conf

server=/google.com/8.8.8.8
server=/yahoo.com/4.4.4.4
server=/qq.com/202.96.134.133
server=/com.cn/202.96.128.68
server=/us/208.67.222.222
server=/uk/208.67.220.220
```

反向解析

```
# Add other name servers here, with domain specs if they are for
# non-public domains.
#server=/localnet/192.168.0.1

# Example of routing PTR queries to nameservers: this will send all
# address->name queries for 192.168.3/24 to nameserver 10.1.2.3
#server=/3.168.192.in-addr.arpa/10.1.2.3
```

6. /etc/dnsmasq.d/dnsmasq.address.conf

```
vim /etc/dnsmasq.d/dnsmasq.address.conf

address=/www.mydomain.com/172.16.0.254
```

deny domain

```
address=/www.facebook.com/127.0.0.1
address=/www.google.com/127.0.0.1
```

6.1. 域名劫持

将域名解析到错误的地址，这样可以屏蔽一些网站。

```
address=/www.facebook.com/127.0.0.1
address=/www.google.com/127.0.0.1
```

例如：在企业网络中不想让员下载安装软件，可以将下载网站解析到错误的地址上去，做到网址屏蔽

```
address=/www.download.com/127.0.0.1
```

7. FAQ

dnsdomainname: Unknown host

```
# hostname -i
hostname: Unknown host

echo "127.0.0.1     `hostname`" >> /etc/hosts

# hostname -i
127.0.0.1
```

什么时候使用 reload / restart

开启或禁用选项必须使用restart, 更新配置可以使用reload

第 23 章 Firewall

摘要

Linux Firewall 安装与配置

目录

1. sysctl - configure kernel parameters at runtime

checking status

```
$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

or just checking out the value in the /proc system

```
$ cat /proc/sys/net/ipv4/ip_forward
0
```

enable

```
sysctl -w net.ipv4.ip_forward=1
```

or

```
#redhat
echo 1 > /proc/sys/net/ipv4/ip_forward
#debian/ubuntu
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward;
```

disable

```
sysctl -w net.ipv4.ip_forward=0
```

or

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

without rebooting the system

1.1. net.ipv4.ip_forward

表 23.1. net.ipv4.ip_forward

user	route	wan
192.168.0.2	eth0:192.168.0.1 eth1:172.16.0.1	172.16.0.254

```
$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

try out ping host from 192.168.0.2 to 192.168.0.1 , 172.16.0.1 and 172.16.0.254

you can access 192.168.0.1 , 172.16.0.1, but 172.16.0.254 time out

sysctl -w net.ipv4.ip_forward=1

try again ping 172.16.0.254

1.2. net.ipv4.icmp_echo_ignore_all

如果希望屏蔽别人 ping 你的主机，则加入以下代码：

```
# Disable ping requests
net.ipv4.icmp_echo_ignore_all = 1
```

2. iptables - administration tools for packet filtering and NAT

Linux Iptables Manual

```
      Incoming
       Traffic
          |
          |
          V
     +----------+
     |PREROUTING|
     +----------+
     |   raw    |  <--------------+
     |  mangle  |                 |
     |   nat    |                 |
     +----------+                 |
          |                       |
       Routing                    |
    +- Decision -+                |
    |            |                |
    |            |                |
    V            V                |
  Local        Remote             |
Destination   Destination         |
    |            |                |
    |            |                |
    V            V                |
+--------+  +---------+           |
| INPUT  |  | FORWARD |           |
+--------+  +---------+           |
| mangle |  | mangle  |           |
| filter |  | filter  |           |
+--------+  +---------+           |
    |            |                |
    |            |                |
    V            |                |
  Local          |                |
 Machine         |                |
    |            |                |
    |            |                |
    V            |                |
 Routing         |                |
 Decision        |                |
    |            |                |
```

```
    V             |                 |
+--------+        |                 |
| OUTPUT |        |                 |
+--------+        |                 |
|  raw   |        |                 |
| mangle |        |                 |
|  nat   |        |                 |
| filter |        |                 |
+--------+        |                 |
    |             |                 |
    |       +-------------+         |
    |       | POSTROUTING |       Local
    +----> +-------------+ --> Traffic
            |   mangle    |
            |     nat     |
            +-------------+
                  |
                  V
              Outgoing
              Traffic
```

2.1. Getting Started

Redhat / CentOS

You can check to see if iptables is installed on your system by:

```
[root@database ~]# rpm -q iptables
iptables-1.3.5-5.3.el5_4.1
```

And to see if iptables is actually running, we can check that the iptables modules are loaded and use the -L switch to inspect the currently loaded rules:

```
[root@database ~]# lsmod | grep ip_tables
ip_tables              55201  2 iptable_nat,iptable_filter
x_tables               50505  6 ipt_MASQUERADE,iptable_nat,xt_state,ipt_REJECT,xt_tcpudp,ip_tables
```

```
[root@database ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere            udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere            udp dpt:bootps
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:bootps

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             192.168.122.0/24    state RELATED,ESTABLISHED
ACCEPT     all  --  192.168.122.0/24     anywhere
ACCEPT     all  --  anywhere             anywhere
```

```
REJECT     all  --  anywhere             anywhere            reject-with icmp-port-unreachable
REJECT     all  --  anywhere             anywhere            reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

If iptables is not running, you can enable it by running:

```
# system-config-securitylevel
```

2.2. User-defined Chain

2.2.1. Chains List

列出规则链

```
 列出INPUT,OUTPUT,FORWARD规则
iptables -L

列出NAT规则
iptables -t nat -L

列出过滤规则
iptables -t filter -L
```

2.2.2. Chains Refresh

刷新规则

```
/sbin/iptables -F
/sbin/iptables -F -t filter
/sbin/iptables -F -t nat
/sbin/iptables -t nat -P PREROUTING ACCEPT
/sbin/iptables -t nat -P POSTROUTING ACCEPT
/sbin/iptables -t nat -P OUTPUT ACCEPT
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
```

2.2.3. Chains Admin

创建新链

```
iptables -N netkiller
```

删除新链

```
# iptables -X netkiller
```

2.3. Common Chains Filtering

2.3.1. INPUT Rule Chains

2.3.1.1. OpenSSH

```
# Accept tcp packets on destination port 22 (SSH)
 iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# Accept tcp packets on destination port 22 (SSH) from private LAN
 iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 22 -j ACCEPT
```

2.3.1.2. FTP

```
/sbin/iptables -A INPUT -p tcp --dport 21 -j ACCEPT
/sbin/iptables -A INPUT -p tcp --dport 20 -j ACCEPT
```

2.3.1.3. DNS

```
iptables -A INPUT -i eth0 -p tcp --dport 53   -j ACCEPT
iptables -A INPUT -i eth0 -p udp --dport 53   -j ACCEPT
```

2.3.1.4. WWW

```
# WWW
/sbin/iptables -A INPUT -p tcp --dport 80 -j ACCEPT
# HTTPS
/sbin/iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

```
# Tomcat
/sbin/iptables -A INPUT -p tcp --dport 8080 -j ACCEPT
```

2.3.1.5. SOCKS5

```
/sbin/iptables -A INPUT -p tcp --dport 1080 -j ACCEPT
```

2.3.1.6. Mail Server

```
# SMTP
/sbin/iptables -A INPUT -p tcp --dport 25 -j ACCEPT
# SMTPS
/sbin/iptables -A INPUT -p tcp --dport 465 -j ACCEPT
# POP3
/sbin/iptables -A INPUT -p tcp --dport 110 -j ACCEPT
# POP3S
/sbin/iptables -A INPUT -p tcp --dport 995 -j ACCEPT
# IMAP
/sbin/iptables -A INPUT -p tcp --dport 143 -j ACCEPT
# IMAPS
/sbin/iptables -A INPUT -p tcp --dport 993 -j ACCEPT
```

2.3.1.7. MySQL

```
/sbin/iptables -A INPUT -p tcp --dport 3306 -j ACCEPT
```

2.3.1.8. PostgreSQL

```
/sbin/iptables -A INPUT -p tcp --dport 5432 -j ACCEPT
```

2.3.1.9. DHCP

```
iptables -A INPUT -p UDP -i eth0 --dport 67 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 --dport 68 -j ACCEPT
```

2.3.1.10. Samba

```
/sbin/iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 137 -j ACCEPT
```

```
iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 145 -j ACCEPT
iptables -A INPUT -p udp -s 192.168.0.0/24 --dport 138 -j ACCEPT
iptables -A INPUT -p udp -s 192.168.0.0/24 --dport 139 -j ACCEPT
```

2.3.1.11. ICMP

accept_redirects

echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects

or

sysctl net.ipv4.conf.all.accept_redirects="0"

```
使自己不能ping 通 127.0.0.1
iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP

192.168.0.0/24 网段无法ping能本机
iptables -A INPUT -s 192.168.0.0/24 -p icmp -j DROP

禁所有机器
# iptables -A INPUT -s 0/0 -p icmp -j DROP

# ICMP(PING) 接受 ! echo-request
iptables -A INPUT -p icmp --icmp-type ! echo-request -j ACCEPT
```

2.3.1.12. 禁止IP访问自己

```
$sudo iptables -A INPUT -d 192.168.0.253 -j DROP
```

2.3.1.13. DENY

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j DROP
```

2.3.2. OUTPUT Rule Chains

2.3.2.1. outbound

```
# Open ports for outbound established connections
$IPT -A OUTPUT -p tcp -s $NET -d 0/0 --destination-port 1:65535 -j ACCEPT
$IPT -A OUTPUT -p udp -s $NET -d 0/0 --destination-port 1:65535 -j ACCEPT
```

2.3.2.2. ICMP

本地不允许ping 192.168.0.0/24

iptables -A OUTPUT -s 192.168.0.0/24 -p icmp -j DROP

禁所本地ping任何机器

iptables -A OUTPUT -s 0/0 -p icmp -j DROP

ICMP(PING) 接受 ! echo-request

iptables -A OUTPUT -p icmp --icmp-type ! echo-request -j ACCEPT

2.3.2.3. 禁止自己访问某个IP

```
# iptables -A OUTPUT -d 192.168.0.253 -j DROP
iptables -A OUTPUT -p udp -j DROP
iptables -A OUTPUT -d 125.211.210.46 -j DROP
```

2.3.3. Forward

```
iptables -A FORWARD -i eth1 -j ACCEPT
```

```
# Network 1 forwarded outgoing client request to network 2
iptables -A FORWARD -i eth1 -p tcp -s 192.168.1.0/24 -d 192.168.2.0/24 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -o eth1 -p tcp -s 192.168.2.0/24 -d 192.168.1.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2.3.3.1. TCPMSS

```
iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
```

2.3.4. Malicious Software and Spoofed IP Addresses

```
# The following rules drop all TCP traffic that attempts to use port 31337:
iptables -A OUTPUT -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
iptables -A FORWARD -o eth0 -p tcp --dport 31337 --sport 31337 -j DROP
```

2.4. Interfaces

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -i ppp0 -j ACCEPT
```

2.5. IP Addresses

```
# Accept packets from trusted IP addresses
 iptables -A INPUT -s 192.168.0.4 -j ACCEPT # change the IP address as appropriate

# Accept packets from trusted IP addresses
 iptables -A INPUT -s 192.168.0.0/24 -j ACCEPT  # using standard slash notation
 iptables -A INPUT -s 192.168.0.0/255.255.255.0 -j ACCEPT # using a subnet mask


# Accept packets from trusted IP addresses
 iptables -A INPUT -s 192.168.0.4 -m mac --mac-source 00:50:8D:FD:E6:32 -j ACCEPT
```

2.6. Ports and Protocols

```
# Accept tcp packets on destination port 6881 (bittorrent)
 iptables -A INPUT -p tcp --dport 6881 -j ACCEPT

# Accept tcp packets on destination ports 6881-6890
 iptables -A INPUT -p tcp --dport 6881:6890 -j ACCEPT
```

2.7. IPTables and Connection Tracking

NEW — A packet requesting a new connection, such as an HTTP request.

ESTABLISHED — A packet that is part of an existing connection.

RELATED — A packet that is requesting a new connection but is part of an existing connection. For example, FTP uses port 21 to establish a connection, but data is transferred on a different port (typically port 20).

INVALID — A packet that is not part of any connections in the connection tracking table.

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2.8. NAT

2.8.1. Redirect

重定向规则

```
端口重定向
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 21 -j REDIRECT --to-port 2401

将80端口重定向到8080
# iptables -t nat -A PREROUTING -j REDIRECT -p tcp --destination-port 80 --to-ports 8080
```

端口转发

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -d 192.168.3.9 -p tcp -m tcp --dport 1000 -j DNAT --to-destination 192.168.3.137:8080
iptables -t nat -A POSTROUTING -s 192.168.3.0/255.255.255.0 -d 192.168.3.137 -p tcp -m tcp --dport 8080 -j SNAT --to-source 192.168.3.9
```

2.8.2. Postrouting and IP Masquerading

```
iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -t nat -I POSTROUTING -j MASQUERADE
sudo iptables -t nat -A POSTROUTING -j MASQUERADE -s 172.16.0.0/24 -d 0.0.0.0/0
sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o eth1 -s 172.16.1.0/24 -d 0.0.0.0/0
sudo iptables -t nat -A POSTROUTING -j MASQUERADE -p tcp -o eth1 -s 172.16.1.0/24 -d 0.0.0.0/0
```

2.8.3. Prerouting

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 172.31.0.23:80
```

If you have a default policy of DROP in your FORWARD chain, you must append a rule to forward all incoming HTTP requests so that destination NAT routing is possible. To do this, use the following command:

```
iptables -A FORWARD -i eth0 -p tcp --dport 80 -d 172.31.0.23 -j ACCEPT
```

This rule forwards all incoming HTTP requests from the firewall to the intended destination; the Apache HTTP Server behind the firewall.

2.8.4. DNAT and SNAT

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -d 202.103.96.10 -j DNAT --to-destination 192.168.0.10
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j SNAT --to-source 202.96.244.56
```

2.8.5. DMZ zone

```
#
# DMZ zone
#
$iptables -t nat -A PREROUTING -p TCP -m multiport -i eth0 --dport 22,25,113,80,8080 -j DNAT --to 10.0.0.10
$iptables -t nat -A PREROUTING -p UDP -i eth0 --dport 25 -j DNAT --to-destination 10.0.0.10
```

DNAT ppp0/eth0

```
```

```
iptables -t nat -A PREROUTING -p tcp -i ppp0 --dport 80 -j DNAT --to-destination <web server ip>
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 10.0.4.2:80
```

2.9. IPV6

```
[root@linux iptables]# modprobe ipv6
[root@linux iptables]# modprobe ip6_tables
[root@linux iptables]# [ ! -f /proc/net/ip6_tables_names ] && echo "Current kernel doesn't support? 'ip6tables' firewalling (IPv6)!"
[root@linux iptables]# ip6tables -A INPUT -i eth0 -p tcp -s 3ffe:ffff:100::1/128 --dport 22 -j ACCEPT
```

2.10. iptables-xml - Convert iptables-save format to XML

2.11. Example

例 23.1.

```
/sbin/iptables -F
/sbin/iptables -F -t filter
/sbin/iptables -F -t nat
/sbin/iptables -t nat -P PREROUTING ACCEPT
/sbin/iptables -t nat -P POSTROUTING ACCEPT
/sbin/iptables -t nat -P OUTPUT ACCEPT
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT

-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

sysctl net.ipv4.ip_forward=1
```

3. ulogd - The Netfilter Userspace Logging Daemon

ulogd homepage: http://www.gnumonks.org/projects/

1. Installation

   $ sudo apt-get install ulogd

   $ sudo apt-get install ulogd-mysql

2. Configure LOGEMU

```
plugin="/usr/lib/ulogd/ulogd_LOGEMU.so"
```

3. Configure MYSQL

   $ sudo vim /etc/ulogd.conf

```
plugin="/usr/lib/ulogd/ulogd_MYSQL.so"
[MYSQL]
table="ulog"
pass="ulog"
user="ulog"
db="ulogd"
host="localhost"
```

   create database

```
neo@master:~$ mysql -u root -p -A mysql
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5.1-log (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> create database ulogd;
Query OK, 1 row affected (0.07 sec)

mysql> grant all privileges on ulogd.* to ulog@localhost identified by 'ulog';
Query OK, 0 rows affected (0.09 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.02 sec)

mysql> source /usr/share/doc/ulogd-mysql/mysql.table
Query OK, 0 rows affected (0.05 sec)

mysql> exit;
Bye
neo@master:~$
```

4. Iptables

```
iptables -A INPUT -p tcp --dport 80 -j ULOG
iptables -A FORWARD -j ULOG
```

5. Starting

   $ sudo /etc/init.d/ulogd start

6. testing

   logemu

```
neo@master:~$ tail -f /var/log/ulog/syslogemu.log
Oct 20 12:54:07 master IN=eth0 OUT= MAC=00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00
SRC=192.168.245.1 DST=192.168.245.129 LEN=40 TOS=00 PREC=0x00 TTL=128 ID=30048 DF PROTO=TCP
SPT=2080 DPT=80 SEQ=1732529774 ACK=1543952440 WINDOW=64608 ACK URGP=0
Oct 20 12:54:22 master IN=eth0 OUT= MAC=00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00
SRC=192.168.245.1 DST=192.168.245.129 LEN=40 TOS=00 PREC=0x00 TTL=128 ID=30294 DF PROTO=TCP
SPT=2080 DPT=80 SEQ=1732529774 ACK=1543952441 WINDOW=64608 ACK URGP=0
Oct 20 12:54:32 master IN=eth0 OUT= MAC=00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00
SRC=192.168.245.1 DST=192.168.245.129 LEN=40 TOS=00 PREC=0x00 TTL=128 ID=30481 DF PROTO=TCP
SPT=2080 DPT=80 SEQ=1732529774 ACK=1543952441 WINDOW=64608 ACK FIN URGP=0
Oct 20 12:55:27 master IN=eth0 OUT= MAC=00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00
SRC=192.168.245.1 DST=192.168.245.129 LEN=48 TOS=00 PREC=0x00 TTL=128 ID=31444 DF PROTO=TCP
SPT=2087 DPT=80 SEQ=866215326 ACK=0 WINDOW=65535 SYN URGP=0
```

   mysql

```
mysql> select count(*) from ulog;
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.03 sec)

mysql> select id, raw_mac from ulog;
+----+---------------------------------------------+
| id | raw_mac                                     |
+----+---------------------------------------------+
|  1 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  2 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  3 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  4 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  5 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  6 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  7 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  8 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
|  9 | 00:0c:29:b0:6b:d0:00:50:56:c0:00:08:08:00  |
+----+---------------------------------------------+
9 rows in set (0.00 sec)
```

共有四个参数可供使用:

1.--ulog-nlgroup

iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-nlgroup 2

指定向哪个netlink组发送包，比如-- ulog-nlgroup 2。一共有32个netlink组，它们被简单地编号位1-32。默认值是1。

2.--ulog-prefix

iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-prefix "SSH connection attempt: "

指定记录信息的前缀，以便于区分不同的信息。使用方法和 LOG的prefix一样，只是长度可以达到32个字符。

3.--ulog-cprange

iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-cprange 100

指定每个包要向“ULOG在用户空间的代理”发送的字节数，如--ulog-cprange 100，
表示把整个包的前100个字节拷贝到用户空间记录下来，其中包含了这个包头，还有一些包的引导数据。默认值是0，表示拷贝整个包，不管它有多大。

4.--ulog-qthreshold

iptables -A INPUT -p TCP --dport 22 -j ULOG --ulog-qthreshold 10

告诉ULOG在向用户空间发送数据以供记录之前，要在内核里收集的包的数量，如--ulog-qthreshold 10。
这表示先在内核里积聚10个包，再把它们发送到用户空间里，它们会被看作同一个netlink的信息，只是由好几部分组成罢了。
默认值是1，这是为了向后兼容，因为以前的版本不能处理分段的信息

---

4. ufw - program for managing a netfilter firewall

1. Installation

   sudo apt-get install ufw

2. Enable | Disable

   sudo ufw enable | disable

```
neo@master:~$ sudo ufw enable
Firewall started and enabled on system startup
```

3. Default Rule

   sudo ufw default deny

   sudo ufw default allow

```
neo@master:~$ sudo ufw default deny
Default policy changed to 'deny'
(be sure to update your rules accordingly)
```

4. Rule Allow|Deny

   sudo ufw allow|deny [service]

   打开或关闭某个端口，例如：

sudo ufw allow smtp 允许所有的外部IP访问本机的25/tcp (smtp)端口

sudo ufw allow 22/tcp 允许所有的外部IP访问本机的22/tcp (ssh)端口

sudo ufw allow 53 允许外部访问53端口(tcp/udp)

sudo ufw allow from 172.16.1.100 允许此IP访问所有的本机端口

sudo ufw allow proto udp 192.168.0.1 port 53 to 192.168.0.2 port 53

sudo ufw deny smtp 禁止外部访问smtp服务

sudo ufw delete allow smtp 删除上面建立的某条规则

   UFW 使用范例

UFW 使用范例：

允许 53 端口

$ sudo ufw allow 53

禁用 53 端口

$ sudo ufw delete allow 53

允许 80 端口

$ sudo ufw allow 80/tcp

禁用 80 端口

$ sudo ufw delete allow 80/tcp

允许 smtp 端口

$ sudo ufw allow smtp

删除 smtp 端口的许可

$ sudo ufw delete allow smtp

允许某特定 IP

$ sudo ufw allow from 192.168.254.254

删除上面的规则

$ sudo ufw delete allow from 192.168.254.254

$ sudo ufw allow ssh

$ sudo ufw allow www

$ sudo ufw allow smtp

```
neo@master:~$ sudo ufw allow ssh
Rule added
```

5. Status

sudo ufw status

```
neo@master:~$ sudo ufw allow www
Rule added
neo@master:~$ sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
25:tcp                     ALLOW   Anywhere
22:tcp                     ALLOW   Anywhere
22:udp                     ALLOW   Anywhere
80:tcp                     ALLOW   Anywhere
80:udp                     ALLOW   Anywhere
```

6. Rule Delete

sudo ufw delete allow|deny RULE

```
neo@master:~$ sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
25:tcp                     ALLOW   Anywhere
22:tcp                     ALLOW   Anywhere
22:udp                     ALLOW   Anywhere
80:tcp                     ALLOW   Anywhere
80:udp                     ALLOW   Anywhere

neo@master:~$ sudo ufw delete allow smtp
Rule deleted
neo@master:~$ sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
22:tcp                     ALLOW   Anywhere
22:udp                     ALLOW   Anywhere
80:tcp                     ALLOW   Anywhere
80:udp                     ALLOW   Anywhere
```

7. logging

sudo ufw logging on|off

```
neo@master:~$ sudo ufw logging ON
Logging enabled
```

8. iptales

```
neo@master:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere

Chain ufw-after-forward (1 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            limit: avg 3/min burst 10 LOG
level warning prefix `[UFW BLOCK FORWARD]: '
RETURN     all  --  anywhere             anywhere
```

```
Chain ufw-after-input (1 references)
target     prot opt source               destination
RETURN     udp  --  anywhere             anywhere            udp dpt:netbios-ns
RETURN     udp  --  anywhere             anywhere            udp dpt:netbios-dgm
RETURN     tcp  --  anywhere             anywhere            tcp dpt:netbios-ssn
RETURN     tcp  --  anywhere             anywhere            tcp dpt:microsoft-ds
RETURN     udp  --  anywhere             anywhere            udp dpt:bootps
RETURN     udp  --  anywhere             anywhere            udp dpt:bootpc
LOG        all  --  anywhere             anywhere            limit: avg 3/min burst 10 LOG
level warning prefix `[UFW BLOCK INPUT]: '
RETURN     all  --  anywhere             anywhere

Chain ufw-after-output (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere

Chain ufw-before-forward (1 references)
target     prot opt source               destination
ufw-user-forward  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain ufw-before-input (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere            ctstate RELATED,ESTABLISHED
DROP       all  --  anywhere             anywhere            ctstate INVALID
ACCEPT     icmp --  anywhere             anywhere            icmp destination-unreachable
ACCEPT     icmp --  anywhere             anywhere            icmp source-quench
ACCEPT     icmp --  anywhere             anywhere            icmp time-exceeded
ACCEPT     icmp --  anywhere             anywhere            icmp parameter-problem
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     udp  --  anywhere             anywhere            udp spt:bootps dpt:bootpc
ufw-not-local  all  --  anywhere             anywhere
ACCEPT     all  --  base-address.mcast.net/4  anywhere
ACCEPT     all  --  anywhere             base-address.mcast.net/4
ufw-user-input  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain ufw-before-output (1 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW,RELATED,ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere            state NEW,RELATED,ESTABLISHED
ufw-user-output  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain ufw-not-local (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere            ADDRTYPE match dst-type LOCAL
RETURN     all  --  anywhere             anywhere            ADDRTYPE match dst-type
MULTICAST
RETURN     all  --  anywhere             anywhere            ADDRTYPE match dst-type
BROADCAST
LOG        all  --  anywhere             anywhere            limit: avg 3/min burst 10 LOG
level warning prefix `[UFW BLOCK NOT-TO-ME]: '
DROP       all  --  anywhere             anywhere

Chain ufw-user-forward (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere

Chain ufw-user-input (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www
ACCEPT     udp  --  anywhere             anywhere            udp dpt:www
RETURN     all  --  anywhere             anywhere

Chain ufw-user-output (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
```

4.1. /etc/default/ufw

```
$ sudo vim /etc/default/ufw
# /etc/default/ufw
#

# set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=no

# set the default input policy to ACCEPT, DROP or REJECT.  Please note that if
# you change this you will most likely want to adjust your rules
DEFAULT_INPUT_POLICY="DROP"

# set the default output policy to ACCEPT, DROP, or REJECT.  Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_OUTPUT_POLICY="ACCEPT"

# set the default forward policy to ACCEPT, DROP or REJECT.  Please note that
# if you change this you will most likely want to adjust your rules
#DEFAULT_FORWARD_POLICY="DROP"
DEFAULT_FORWARD_POLICY="ACCEPT"

# set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
```

```
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
DEFAULT_APPLICATION_POLICY="SKIP"

# By default, ufw only touches its own chains. Set this to 'yes' to have ufw
# manage the built-in chains too. Warning: setting this to 'yes' will break
# non-ufw managed firewall rules
MANAGE_BUILTINS=no

#
# IPT backend
#
# only enable if using iptables backend
IPT_SYSCTL=/etc/ufw/sysctl.conf

# extra connection tracking modules to load
IPT_MODULES="nf_conntrack_ftp nf_nat_ftp nf_conntrack_irc nf_nat_irc"
```

4.2. ip_forward

```
$ sudo vim /etc/ufw/sysctl.conf
net/ipv4/ip_forward=1
```

4.3. DHCP

```
neo@netkiller:~$ sudo ufw allow 67/udp
Rules updated
neo@netkiller:~$ sudo ufw allow 68/udp
Rules updated
```

4.4. Samba

```
neo@netkiller:~$ sudo ufw allow 137/tcp
Rule added
neo@netkiller:~$ sudo ufw allow 445/tcp
Rule added
neo@netkiller:~$ sudo ufw allow 138/udp
Rule added
neo@netkiller:~$ sudo ufw allow 139/udp
Rule added
```

5. Shorewall

Shorewall

5.1. Installation Instructions

5.1.1. Install using RPM

```
# rpm -ivh http://slovakia.shorewall.net/pub/shorewall/CURRENT_STABLE_VERSION_IS_4.4/shorewall-
4.4.25/shorewall-4.4.25-3.noarch.rpm
Retrieving http://slovakia.shorewall.net/pub/shorewall/CURRENT_STABLE_VERSION_IS_4.4/shorewall-
4.4.25/shorewall-4.4.25-3.noarch.rpm
warning: /var/tmp/rpm-tmp.qc6WVw: Header V4 DSA/SHA1 Signature, key ID 6c562ac4: NOKEY
Preparing...                ########################################### [100%]
   1:shorewall              ########################################### [100%]
```

5.1.2. Install using apt-get

```
netkiller@shenzhen:~$ apt-cache search shorewall
shorewall - Shoreline Firewall (Shorewall), a high-level tool for configuring Netfilter
shorewall-doc - documentation for Shorewall firewall
shorewall-lite - Shorewall (lite version), a high-level tool for configuring Netfilter
netkiller@shenzhen:~$
```

install

```
sudo apt-get install shorewall
```

copy config file to /etc/shorewall/

```
sudo cp /usr/share/doc/shorewall/default-config/modules /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/policy /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/nat /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/zones /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/maclist /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/blacklist /etc/shorewall/

sudo cp /usr/share/doc/shorewall/default-config/interfaces /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/rules /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/hosts /etc/shorewall/
sudo cp /usr/share/doc/shorewall/default-config/masq /etc/shorewall/
```

5.2. Configuring Shorewall

过程 23.1. shorewall.conf

1. STARTUP_ENABLED

   STARTUP_ENABLED=No

改为

STARTUP_ENABLED=Yes

2. IP_FORWARDING

IP_FORWARDING关闭与开启

IP_FORWARDING=On

IP_FORWARDING=Off

```
IP_FORWARDING=On
```

3.

```

```

4.

```

```

5.

```

```

6.

```

```

7. 启动防火墙

sudo shorewall start

5.2.1. zones

```
# cat /etc/shorewall/zones
#
# Shorewall version 4 - Zones File
#
# For information about this file, type "man shorewall-zones"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-zones.html
#
###############################################################################
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
#fw     firewall
ouside  wan
inside  lan
dmz     dmz
```

5.2.2. policy

```
# cat /etc/shorewall/policy
#
# Shorewall version 4 - Policy File
#
# For information about entries in this file, type "man shorewall-policy"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#
###############################################################################
#SOURCE DEST    POLICY          LOG     LIMIT:          CONNLIMIT:
#                               LEVEL   BURST           MASK
inside  outside ACCEPT
dmz     outside ACCEPT
inside  dmz     ACCEPT
```

```
outside all     DROP
all     all     REJECT
```

5.2.3. interfaces

```
# cat /etc/shorewall/interfaces
#
# Shorewall version 4 - Interfaces File
#
# For information about entries in this file, type "man shorewall-interfaces"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
outside eth0    detect
inside  eth1    detect
dmz     eth2    detect
```

5.2.4. masq

```
# cat /etc/shorewall/masq
#
# Shorewall version 4 - Masq file
#
# For information about entries in this file, type "man shorewall-masq"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-masq.html
#
#######################################################################################
#INTERFACE:DEST         SOURCE          ADDRESS         PROTO   PORT(S) IPSEC   MARK    USER/
#                                                                                        GROUP
eth0    192.168.0.0/24
```

5.2.5. rules

```
# cat /etc/shorewall/rules
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
#######################################################################################################

#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE          ORIGINAL
RATE            USER/   MARK    CONNLIMIT       TIME         HEADERS         SWITCH
#                                                       PORT    PORT(S)         DEST
LIMIT           GROUP
#SECTION BLACKLIST
#SECTION ALL
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
ACCEPT  any     outside tcp     http
ACCEPT  any     inside  tcp     http
ACCEPT  dmz     inside  tcp     smtp
ACCEPT  any     inside  tcp     ssh
ACCEPT  any     dmz             tcp     ssh
ACCEPT  dmz     any             tcp     ssh
SSH(ACCEPT) net all        -           -            -         -                s:1/min:3
```

5.2.6. params

```
# cat /etc/shorewall/params
#
# Shorewall version 4 - Params File
#
# /etc/shorewall/params
#
#       Assign any variables that you need here.
#
#       It is suggested that variable names begin with an upper case letter
#       to distinguish them from variables used internally within the
#       Shorewall programs
#
#       Example:
```

```
#
#                NET_IF=eth0
#                NET_BCAST=130.252.100.255
#                NET_OPTIONS=routefilter,norfc1918
#
#        Example (/etc/shorewall/interfaces record):
#
#                net     $NET_IF         $NET_BCAST      $NET_OPTIONS
#
#        The result will be the same as if the record had been written
#
#                net     eth0            130.252.100.255 routefilter,norfc1918
#
################################################################################

#LAST LINE -- DO NOT REMOVE
```

---

6. Firewall GUI Tools

KMyFirewall

Firestarter

Firewall Builder

7. Endian Firewall

http://www.endian.com/

8. Smooth Firewall

第 24 章 Stunnel - universal SSL tunnel

Homepage: http://www.stunnel.org/

Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. Stunnel can allow you to secure non-SSL aware daemons and protocols (like POP, IMAP, LDAP, etc) by having Stunnel provide the encryption, requiring no changes to the daemon's code.

1. install

```
$ sudo apt-get install stunnel4
```

2. enable stunnel

```
$ vim /etc/default/stunnel4
# /etc/default/stunnel
# Julien LEMOINE <speedblue@debian.org>
# September 2003

# Change to one to enable stunnel
ENABLED=0
FILES="/etc/stunnel/*.conf"
OPTIONS=""

# Change to one to enable ppp restart scripts
PPP_RESTART=0
```

edit /etc/default/stunnel4 file and change ENABLED=0 to ENABLED=1 to enable Stunnel

3. config

```
$ sudo vim /etc/stunnel/stunnel.conf
[pop3s]
accept  = 995
connect = 110

[imaps]
accept  = 993
connect = 143

[ssmtp]
accept  = 465
connect = 25

[https]
accept  = 443
connect = 80
```

4. start

```
$ sudo /etc/init.d/stunnel4 start
```

第 25 章 OpenVPN (openvpn - Virtual Private Network daemon)

目录

http://openvpn.net/

1. 源码安装

过程 25.1. OpenVPN 编译安装步骤

1. 安装liblzo,libssl支持库

```
netkiller@neo:~$ sudo apt-get install liblzo-dev
netkiller@neo:~$ sudo apt-get install libssl-dev
```

2. 取得安装包

```
netkiller@neo:/usr/local$ sudo chmod 777 /usr/local/src/
netkiller@neo:~$ cd /usr/local/src/
netkiller@neo:/usr/local/src$ wget http://openvpn.net/release/openvpn-2.0.9.tar.gz
netkiller@neo:/usr/local/src$ tar zxvf openvpn-2.0.9.tar.gz
netkiller@neo:/usr/local/src$ cd openvpn-2.0.9/
netkiller@neo:/usr/local/src/openvpn-2.0.9$
```

3. 编译安装

```
netkiller@neo:/usr/local/src/openvpn-2.0.9$ ./configure --prefix=/usr/local/openvpn-2.0.9 -
-enable-pthread
netkiller@neo:/usr/local/src/openvpn-2.0.9$ make
netkiller@neo:/usr/local/src/openvpn-2.0.9$ sudo make install
```

4. 配置文件

```
netkiller@neo:/usr/local/src/openvpn-2.0.9$ sudo ln -s /usr/local/openvpn-2.0.9/
/usr/local/openvpn
netkiller@neo:/usr/local/src/openvpn-2.0.9$ cd /usr/local/openvpn
netkiller@neo:/usr/local/openvpn$ sudo mkdir etc
netkiller@neo:/usr/local/openvpn$ sudo mkdir log
netkiller@neo:/usr/local/openvpn$ sudo vi etc/openvpn.conf
```

例 25.1. openvpn.conf

```

```

sudo cp ca.crt dh1024.pem server.crt server.key /usr/local/openvpn/etc/

5. 创建证书

修改vars文件的环境变量

```
netkiller@neo:/usr/share/openvpn$ sudo vi vars
export KEY_COUNTRY=CN
export KEY_PROVINCE=GD
export KEY_CITY=Shenzhen
export KEY_ORG=http://netkiller.sourceforge.net/
export KEY_EMAIL=openunix@163.com
```

```
netkiller@neo:/usr/local/openvpn$ cd /usr/share/openvpn/
netkiller@neo:/usr/share/openvpn$

netkiller@neo:~/openvpn-2.1_rc1/easy-rsa/2.0$ sudo make install DESTDIR=/usr/share/openvpn
install -c --directory "/usr/share/openvpn/"
install -c --mode=0755 build-* "/usr/share/openvpn/"
install -c --mode=0755 clean-all list-crl inherit-inter pkitool revoke-full sign-req
whichopensslcnf "/usr/share/openvpn/"
install -c --mode=0644 openssl-0.9.6.cnf openssl.cnf README vars "/usr/share/openvpn/"
netkiller@neo:~/openvpn-2.1_rc1/easy-rsa/2.0$

netkiller@neo:/usr/share/openvpn$ sudo chmod +x vars
netkiller@neo:/usr/share/openvpn$
netkiller@neo:/usr/share/openvpn$ sudo ./clean-all

netkiller@neo:/usr/share/openvpn$ sudo ./build-ca
netkiller@neo:/usr/share/openvpn$ sudo ./build-key-server server
netkiller@neo:/usr/share/openvpn$ sudo ./build-key client1

netkiller@neo:/usr/share/openvpn$ sudo mkdir /etc/openvpn
netkiller@neo:/usr/share/openvpn$ cd /etc/openvpn/
netkiller@neo:/etc/openvpn$ sudo vi server.ovpn
netkiller@neo:/etc/openvpn$ sudo cp /usr/share/openvpn/keys/dh1024.pem .
netkiller@neo:/etc/openvpn$ sudo cp /usr/share/openvpn/keys/server.crt .
netkiller@neo:/etc/openvpn$ sudo cp /usr/share/openvpn/keys/server.key .
netkiller@neo:/etc/openvpn$ sudo cp /usr/share/openvpn/keys/ca.crt .

root@neo:/home/netkiller/openvpn-2.1_rc1/sample-config-files# cp * /etc/openvpn/
root@neo:/home/netkiller/openvpn-2.1_rc1/sample-config-files# cd /etc/openvpn/
```

6. 启动

```
/usr/local/openvpn/sbin/openvpn --config /usr/local/openvpn/etc/openvpn.conf
```

7. Script

/etc/init.d/openvpn

```
#!/bin/bash
# vpn init file for OpenVPN
#
# chkconfig: - 100 100
# description: OpenVPN is a full-featured SSL VPN solution which can accomodate a wide
range of configurations,
#                                 including remote access, site-to-site VPNs, WiFi security,
#                                 and enterprise-scale remote access solutions with load
balancing, failover,
#                                 and fine-grained access-controls
#                                 as it is designed and optimized for high performance
environments.
# author: Neo Chen<openunix@163.com>
#
# processname: $PROG
# config:
# pidfile: /var/run/openvpn

# source function library
. /etc/init.d/functions

PREFIX=/usr/local/openvpn
PROG=$PREFIX/sbin/openvpn
OPTIONS="-f /usr/local/openvpn/etc/openvpn.conf"
USER=daemon
RETVAL=0
prog="openvpn"

start() {
        echo -n $"Starting $prog: "
        if [ $UID -ne 0 ]; then
                RETVAL=1
                failure
        else
                daemon --user=$USER $PROG $OPTIONS
                RETVAL=$?
                [ $RETVAL -eq 0 ] && touch /var/lock/subsys/openvpn
        fi;
        echo
        return $RETVAL
}

stop() {
        echo -n $"Stopping $prog: "
        if [ $UID -ne 0 ]; then
                RETVAL=1
                failure
        else
                killproc $PROG
                RETVAL=$?
                [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/openvpn
        fi;
        echo
        return $RETVAL
}

reload(){
        echo -n $"Reloading $prog: "
        killproc $PROG -HUP
        RETVAL=$?
        echo
        return $RETVAL
}

restart(){
        stop
        start
}

condrestart(){
    [ -e /var/lock/subsys/openvpn ] && restart
    return 0
}

case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart)
        restart
        ;;
  reload)
```

```
        reload
        ;;
  condrestart)
        condrestart
        ;;
  status)
        status openvpn
        RETVAL=$?
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart|reload}"
        RETVAL=1
esac

exit $RETVAL
```

添加x权限

```
sudo chmod +x /etc/init.d/openvpn
```

2. Openvpn Server

Ubuntu/Debian 环境安装

过程 25.2. Openvpn Server 安装步骤

- 相关软件包

```
netkiller@shenzhen:~$ apt-cache search openvpn
carpaltunnel - Configuration helper for OpenVPN
kvpnc - vpn clients frontend for KDE
network-manager-openvpn - network management framework (OpenVPN plugin)
openvpn - Virtual Private Network daemon
tunneldigger - Configures OpenVPN tunnel networks
tunneldigger-utils - Utilities for TunnelDigger-configured OpenVPN tunnels
You have new mail in /var/mail/netkiller
netkiller@shenzhen:~$
```

This is for Dapper ubuntu and openvpn

```
netkiller@shenzhen:~$ sudo apt-get install openvpn
```

- config file

  /etc/openvpn/

- share

  /usr/share/openvpn/

- doc

  /usr/share/doc/openvpn/

- example

  /usr/share/doc/openvpn/examples/

2.1. create keys for the server

过程 25.3. CREATE KEYS FOR THE SERVER AND THE CLIENTS

1. Change to the directory /usr/share/doc/openvpn/examples/easy-rsa/2.0

```
netkiller@shenzhen:~$ cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
```

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ ls
build-ca  build-dh  build-inter  build-key  build-key-pass  build-key-pkcs12  build-key-
server  build-req  build-req-pass  clean-all  inherit-inter  list-crl  Makefile  openssl-
0.9.6.cnf.gz  openssl.cnf  pkitool  README.gz  revoke-full  sign-req  vars  whichopensslcnf
```

backup vars to vars.original

```
sudo cp vars vars.original
```

vi vars and change with you

```
export KEY_COUNTRY="CN"
export KEY_PROVINCE="GD"
export KEY_CITY="Shenzhen"
export KEY_ORG="http://netkiller.sourceforge.net/"
export KEY_EMAIL="openunix@163.com"
```

type the commands

- vars
- clean-all
- build-ca
- build-key-server server
- build-key client1
- build-dh

2. vars and clean-all

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on
/usr/share/doc/openvpn/examples/easy-rsa/2.0/keys
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ ./clean-all

$ sudo mkdir keys
$ sudo chown neo.neo keys
```

3. build-ca

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ ./build-ca
Generating a 1024 bit RSA private key
.........................++++++
............++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [http://netkiller.8800.org]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [http://netkiller.8800.org CA]:
Email Address [openunix@163.com]:
```

4. build-key-server server

You will have to answer the same questions above. It will ask you for a password, I suggest you don’t put a

password when it ask.

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ ./build-key-server server
Generating a 1024 bit RSA private key
.....................................++++++
.............................................++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [http://netkiller.8800.org]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Email Address [openunix@163.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/share/doc/openvpn/examples/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Shenzhen'
organizationName      :PRINTABLE:'http://netkiller.8800.org'
commonName            :PRINTABLE:'server'
emailAddress          :IA5STRING:'openunix@163.com'
Certificate is to be certified until Nov 10 18:09:52 2017 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

enter yes to sign the certificate.

5. build-dh

```
# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.........................+..............................+.....................................
```

2.2. create keys for the clients

过程 25.4. create keys for the clients

1. build-key client1

Now to build the client files

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ ./build-key client1
Generating a 1024 bit RSA private key
.++++++
...........++++++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [http://netkiller.8800.org]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [client1]:
```

```
Email Address [openunix@163.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/share/doc/openvpn/examples/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Shenzhen'
organizationName      :PRINTABLE:'http://netkiller.8800.org'
commonName            :PRINTABLE:'client1'
emailAddress          :IA5STRING:'openunix@163.com'
Certificate is to be certified until Nov 10 18:15:39 2017 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

And once again you will need to answer the questions above. I still don’t recommend you putting a password as it can cause problems when I have tried.

注意在进入 Common Name (eg, your name or your server’s hostname) []: 的输入时, 每个证书输入的名字必须不同.

2. All the files you just generated are located in /usr/share/doc/openvpn/examples/easy-rsa/2.0/keys

If you do a list command in the keys folder you should have something like:

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ ls keys/
01.pem  ca.crt  client1.crt  client1.key  index.txt       index.txt.attr.old  serial
server.crt  server.key
02.pem  ca.key  client1.csr  dh1024.pem   index.txt.attr  index.txt.old       serial.old
server.csr
```

Copy the files ca.crt, ca.key, dh1024.pem, server.crt, and server.key to the /etc/openvpn/keys

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0$ cd keys/
netkiller@shenzhen:/usr/share/doc/openvpn/examples/easy-rsa/2.0/keys$ sudo cp keys/ca.key
keys/ca.crt keys/dh1024.pem keys/server.key keys/server.crt /etc/openvpn/
```

We will worry about the client files after we configure the client config file.

3. CONFIGURE THE SERVER

Change to the directory /usr/share/doc/openvpn/examples/sample-config-files

```
netkiller@shenzhen:/usr/share/doc/openvpn/examples/sample-config-files$ sudo gunzip
server.conf.gz
netkiller@shenzhen:/usr/share/doc/openvpn/examples/sample-config-files$ sudo cp server.conf
/etc/openvpn/
netkiller@shenzhen:/usr/share/doc/openvpn/examples/sample-config-files$ cd /etc/openvpn/
netkiller@shenzhen:/etc/openvpn$
```

为用户添加路由

push "route 192.168.1.0 255.255.255.0"

例 25.2. server.conf

```
#####################################################
```

```
# Sample OpenVPN 2.0 config file for            #
# multi-client server.                          #
#                                                #
# This file is for the server side               #
# of a many-clients <-> one-server               #
# OpenVPN configuration.                        #
#                                                #
# OpenVPN also supports                          #
# single-machine <-> single-machine             #
# configurations (See the Examples page         #
# on the web site for more info).                #
#                                                #
# This config should work on Windows            #
# or Linux/BSD systems.  Remember on            #
# Windows to quote pathnames and use            #
# double backslashes, e.g.:                     #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                                #
# Comments are preceded with '#' or ';'          #
##################################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d
;local 192.168.1.7

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh1024.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
```

```
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"
push "route 192.168.1.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248

# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2


# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# the TUN/TAP interface to the internet in
# order for this to work properly).
# CAVEAT: May break client's network config if
# client's local DHCP server packets get routed
# through the tunnel.  Solution: make sure
# client's local DHCP server is reachable via
# a more specific route than the default route
# of 0.0.0.0/0.0.0.0.
;push "redirect-gateway"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
;push "dhcp-option DNS 10.8.0.1"
;push "dhcp-option WINS 10.8.0.1"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
```

```
# UNCOMMENT THIS LINE OUT.
;duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

test

```
netkiller@shenzhen:/etc/openvpn$ sudo openvpn --config /etc/openvpn/server.conf
Tue Nov 13 14:12:33 2007 OpenVPN 2.0.9 i486-pc-linux-gnu [SSL] [LZO] [EPOLL] built on Mar
2 2007
Tue Nov 13 14:12:33 2007 Diffie-Hellman initialized with 1024 bit key
Tue Nov 13 14:12:33 2007 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Tue Nov 13 14:12:33 2007 TUN/TAP device tun0 opened
Tue Nov 13 14:12:33 2007 ifconfig tun0 10.8.0.1 pointopoint 10.8.0.2 mtu 1500
Tue Nov 13 14:12:33 2007 route add -net 10.8.0.0 netmask 255.255.255.0 gw 10.8.0.2
```

```
Tue Nov 13 14:12:33 2007 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0
AF:3/1 ]
Tue Nov 13 14:12:33 2007 UDPv4 link local (bound): [undef]:1194
Tue Nov 13 14:12:33 2007 UDPv4 link remote: [undef]
Tue Nov 13 14:12:33 2007 MULTI: multi_init called, r=256 v=256
Tue Nov 13 14:12:33 2007 IFCONFIG POOL: base=10.8.0.4 size=62
Tue Nov 13 14:12:33 2007 IFCONFIG POOL LIST
Tue Nov 13 14:12:33 2007 Initialization Sequence Completed
```

4. Start

```
netkiller@shenzhen:~$ sudo /etc/init.d/openvpn start
Starting virtual private network daemon: server(OK).
```

---

3. 吊销(revoke)用户证书

```
$ . vars
$ ./revoke-full client1
$ sudo cp keys/crl.pem /etc/openvpn/
```

命令执行完成之后， 会在 keys 目录下面， 生成一个 crl.pem 文件,这个文件中包含了吊销证书的名单。

确认成功注销某个证书，可以打开keys/index.txt 文件，可以看到前面已被标记为R的注销证书

```
$ grep ^R keys/index.txt
R       200908052722Z   110218014133Z   04      unknown
/C=CN/ST=GD/L=Shenzhen/O=EXAMPLE.COM/CN=client1/emailAddress=client1@EXAMPLE.com
```

在服务端的配置文件 server.conf 中，加入这样一行：

```
crl-verify crl.pem
```

4. Openvpn Client

```
$ cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
$ cp keys/ca.crt keys/client1.crt keys/client1.key /etc/openvpn/
```

过程 25.5. Openvpn Client 安装步骤

1. CONFIGURE THE CLIENTS

   修改 remote my-server-1 1194

   例 25.3. client.conf

```
#############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
#############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote vpn.netkiller.8800.org 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind
```

```
# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client1.crt
key client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

2. 禁止Server端 redirect-gateway def1

```
redirect-gateway local
```

5. OpenVPN GUI for Windows

5.1. Windows Server

过程 25.6. For Windows Server

1. http://openvpn.se/

   http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

   下载安装后,会在系统托盘上显示图标.这时并不能使用,使用创建配置文件后托盘图标才会显示连接菜单

2. 创建证书

```
C:\Documents and Settings\Neo>cd "\Program Files\OpenVPN\easy-rsa"
C:\Program Files\OpenVPN\easy-rsa>
C:\Program Files\OpenVPN\easy-rsa>init-config.bat
```

编辑vars.bat

```
set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=Shenzhen
set KEY_ORG=netkiller.org.cn
set KEY_EMAIL=openunix@163.com
```

```
C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
C:\Program Files\OpenVPN\easy-rsa>vars.bat
```

创建CA证书

```
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......++++++
......++++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [netkiller.org.cn]:
Organizational Unit Name (eg, section) []:vpn
Common Name (eg, your name or your server's hostname) []:netkiller.org.cn
Email Address [openunix@163.com]:

C:\Program Files\OpenVPN\easy-rsa>
```

dh

```
C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
Loading 'screen' into random state - done
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.........................+...................+...............................
...............................+...........+....................+.......+....
.....................................................................+..+.............
.+.....................................+.................................
...+..+...........+..............................+...........................
.............................................+.....+.......................
.............................................+.....+......+..................
.....................................+.........................................
.......................................................................+.....+
.....................................+....................+..................
....+.............................................................................
.....................+..............................+...........................
.................................................................................
.................................................................................
...........................+.................+.......................+......+...
............+...................+.........................................
................+.................................................+..................
.................................................................................
...............................+....+................+.......................
..................+.......+.....................................................
..+..............+...............................................................
.................................................................................
.............................................................+................
.......+.......................................................++*++*++*

C:\Program Files\OpenVPN\easy-rsa>
```

server key

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
........++++++
....................++++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [netkiller.org.cn]:
Organizational Unit Name (eg, section) []:vpn
Common Name (eg, your name or your server's hostname) []:netkiller.org.cn
Email Address [openunix@163.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chen
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Shenzhen'
organizationName      :PRINTABLE:'netkiller.org.cn'
organizationalUnitName:PRINTABLE:'vpn'
commonName            :PRINTABLE:'netkiller.org.cn'
emailAddress          :IA5STRING:'openunix@163.com'
Certificate is to be certified until Jun  9 03:14:55 2017 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

client key

```
C:\Program Files\OpenVPN\easy-rsa>build-key.bat client
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......++++++
....................++++++
writing new private key to 'keys\client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Shenzhen]:
Organization Name (eg, company) [netkiller.org.cn]:
Organizational Unit Name (eg, section) []:vpn
Common Name (eg, your name or your server's hostname) []:netkiller.org.cn
Email Address [openunix@163.com ]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chen
An optional company name []:
Using configuration from openssl.cnf
Loading 'screen' into random state - done
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Shenzhen'
organizationName      :PRINTABLE:'netkiller.org.cn'
organizationalUnitName:PRINTABLE:'vpn'
commonName            :PRINTABLE:'netkiller.org.cn'
emailAddress          :IA5STRING:'openunix@163.com^I'
Certificate is to be certified until Jun  9 03:17:55 2017 GMT (3650 days)
Sign the certificate? [y/n]:y
failed to update database
TXT_DB error number 2

C:\Program Files\OpenVPN\easy-rsa>
```

3. 配置

例 25.4. server.ovpn

```
#################################################
# Sample OpenVPN 2.0 config file for            #
# multi-client server.                          #
#                                               #
# This file is for the server side              #
# of a many-clients <-> one-server              #
# OpenVPN configuration.                        #
#                                               #
# OpenVPN also supports                         #
# single-machine <-> single-machine             #
# configurations (See the Examples page         #
# on the web site for more info).               #
#                                               #
# This config should work on Windows            #
# or Linux/BSD systems.  Remember on            #
# Windows to quote pathnames and use            #
# double backslashes, e.g.:                     #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                               #
# Comments are preceded with '#' or ';'         #
#################################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
```

```
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh1024.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
```

```
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2

# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# the TUN/TAP interface to the internet in
# order for this to work properly).
# CAVEAT: May break client's network config if
# client's local DHCP server packets get routed
# through the tunnel.  Solution: make sure
# client's local DHCP server is reachable via
# a more specific route than the default route
# of 0.0.0.0/0.0.0.0.
;push "redirect-gateway"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
;push "dhcp-option DNS 10.8.0.1"
;push "dhcp-option WINS 10.8.0.1"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
;client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.
;duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nobody
```

```
# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

5.2. Windows Client

过程 25.7. For Windows Client

1. 配置文件

   将C:\Program Files\OpenVPN\sample-config目录下的client.ovpn复制到C:\Program Files\OpenVPN\config

   ca.crt, client.crt, client.key 三个文件复制到 C:\Program Files\OpenVPN\config

   修改;remote my-server-1 1194

```
remote vpn.netkiller.8800.org 1194
```

   编辑client.ovpn文件

   例 25.5. client.ovpn

```
#################################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
################################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
```

```
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote netkiller.8800.org 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client1.crt
key client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

2. 连接到VPN服务器

托盘图标上->右键->选择 [Connect] 菜单

5.2.1. 客户端路由设置

client.ovpn 中加入

```
# Silence repeating messages
;mute 20
up client.ovpn_up.bat
```

client.ovpn_up.bat

```


@echo off
@echo 5秒后执行添加路由
set t=5
ping -n %t% 127.0.0.1>nul
@echo 开始执行添加路由

route ADD 0.0.0.0 MASK 0.0.0.0 192.168.90.254

route DELETE 0.0.0.0 MASK 128.0.0.0 10.8.0.21
route DELETE 128.0.0.0 MASK 128.0.0.0 10.8.0.21


rem route ADD 10.0.0 MASK 255.0.0.0 192.168.90.252
rem route ADD 192.168.0 MASK 255.255.0.0 192.168.90.252
rem route ADD 202.96.0.0 MASK 255.255.0.0 192.168.90.252
```

---

6. point-to-point VPNs

过程 25.8. This example demonstrates a bare-bones point-to-point OpenVPN configuration.

1. Generate a static key

```
$ cd /etc/openvpn/
$ sudo openvpn --genkey --secret static.key
```

2. server configuration file

```
$ cd /usr/share/doc/openvpn/examples/sample-config-files
$ sudo cp static-office.conf office.up /etc/openvpn/
```

static-office.conf

```
$ sudo vim static-office.conf
```

3. client configuration file

```
$ cd /usr/share/doc/openvpn/examples/sample-config-files
$ sudo cp static-home.conf home.up /etc/openvpn/
$ cd /etc/openvpn/
$ scp user@netkiller.8800.org:/etc/openvpn/static.key .
```

static-home.conf

```
remote netkiller.8800.org
```

OpenVPN GUI for Windows

```
copy C:\Program Files\OpenVPN\sample-config\sample.ovpn C:\Program Files\OpenVPN\config
```

7. VPN 案例

7.1. server and client vpn

```
office (linux)                                      home (xp)
--------------                                      ----------
172.16.0.1 eth0                                     192.168.0.1
    ^                                                   ^
    |                                                   |
10.8.0.1 tun0  --> 10.8.0.2 <---> 10.8.0.5 <--   10.8.0.6

testing home - > office
-------------------------------------------------------

ping 10.8.0.1 OK
ping 172.16.0.1 OK
ping 172.16.0.254 OK
```

例 25.6. office.conf

office

```
$ sudo sysctl -w net.ipv4.ip_forward=1
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
#################################################
# Sample OpenVPN 2.0 config file for            #
# multi-client server.                          #
#                                               #
# This file is for the server side              #
# of a many-clients <-> one-server              #
# OpenVPN configuration.                        #
#                                               #
# OpenVPN also supports                         #
# single-machine <-> single-machine             #
# configurations (See the Examples page         #
# on the web site for more info).               #
#                                               #
# This config should work on Windows            #
# or Linux/BSD systems.  Remember on            #
# Windows to quote pathnames and use            #
# double backslashes, e.g.:                     #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                               #
# Comments are preceded with '#' or ';'         #
#################################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
```

```
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh1024.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"
push "route 172.16.0.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
```

```
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
route 192.168.102.0 255.255.255.0
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2

# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"
;push "redirect-gateway"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.
;duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
```

```
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
log         openvpn.log
log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

例 25.7. home.ovpn

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
```

```
remote netkiller.8800.org 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client.crt
key client.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

7.2. Ethernet Bridging Example

过程 25.9. server

1.
```
yum -y install bridge-utils
```

2. server.conf

```
dev tap0
server-bridge 192.168.3.5 255.255.255.0 192.168.3.200  192.168.3.250
push "redirect-gateway local def1"
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"
```

3.

```
cp /usr/share/doc/openvpn-2.1.1/sample-scripts/bridge-st* /etc/openvpn/

chmod +x /etc/openvpn/bridge*
```

config bridge-start

```
vim /etc/openvpn/bridge-start
eth="eth0"
eth_ip="192.168.3.5"
eth_netmask="255.255.255.0"
eth_broadcast="192.168.3.255"
```

4. start

```
/etc/openvpn/bridge-start
/etc/init.d/openvpn start
```

5. stop

```
/etc/init.d/openvpn stop
/etc/openvpn/bridge-stop
```

过程 25.10. client

1. client.ovpn

```
dev tap
dev-node tap-bridge
```

2. 网上邻居右键，选择属性，TAP-Win32 Adapter V8 重命名为 tap-bridge

vista windows7 操作系统注意：

```
OpenVPN GUI 右键“以管理员身份运行”

client.ovpn 中加入
route-method exe
route-delay 2
```

7.3. IDC Example

```
                Internet
                        |
                        V
                ethernet 0 : 120.132.x.x
        Cisco PIX Firewall      NAT(120.132.x.x TO 172.16.1.2)
                ethernet 1 : 172.16.1.254
                        |
                        V
Cisco Catalyst 3750 Switch
                g0/0/1 : 172.16.1.1
                        |
                        V
        eth0 : 172.16.1.2
        OpenVPN Server
```

VPN 拨通后不能正常访问172.16.1.0

/etc/openvpn/server.conf

```
push "redirect-gateway def1 bypass-dhcp"
```

```
$ sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

第 26 章 pptpd

目录

过程 26.1. pptpd 安装步骤

1. install

```
$ sudo apt-get install pptpd
```

2. $ sudo vim /etc/pptpd.conf

```
localip 172.16.0.1
remoteip 172.16.0.50-100
```

3. $ sudo vim /etc/ppp/pptpd-options

```
ms-dns 208.67.222.222
ms-dns 208.67.220.220
```

4. $ sudo vim /etc/ppp/chap-secrets

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
neo pptpd chen *
```

5. restart

```
sudo /etc/init.d/pptpd restart
Restarting PPTP:
Stopping PPTP: pptpd.
Starting PPTP Daemon: pptpd.
```

6.

```
# ifconfig ppp0

ppp0      Link encap:Point-to-Point Protocol
          inet addr:192.168.3.9  P-t-P:192.168.3.15  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1396  Metric:1
          RX packets:1545 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1008 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:342505 (334.4 KiB)  TX bytes:239324 (233.7 KiB)
```

7. $ sudo vim /etc/sysctl.conf

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

refresh status

```
$ sudo sysctl -p
net.ipv4.ip_forward = 1
```

8. NAT

```
$ sudo iptables -t nat -A POSTROUTING -s 172.16.0.0/24 -o eth0 -j MASQUERADE
$ sudo iptables-save > /etc/iptables-rules
```

$ sudo vim /etc/network/interfaces

```
pre-up iptables-restore < /etc/iptables-rules
```

9. firewall

```
$ sudo ufw allow 1723
Rules updated
```

MTU

```
$ sudo iptables -A FORWARD -s 10.100.0.0/24 -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --
set-mss 1200
还有一个最简单的修改mtu的办法:
$ sudo vim /etc/ppp/ip-up.local

!/bin/bash

/sbin/ifconfig $1 mtu 1496
```

1. FAQ

错误：800

运行 ipconfig /flushdns 后，再试

第 27 章 l2tpd - dummy package for l2tpd to xl2tpd transition

过程 27.1. install l2tpd

1. install

```
# apt-get install l2tpd
```

2. /etc/xl2tpd/xl2tpd.conf

```
# cp /etc/xl2tpd/xl2tpd.conf /etc/xl2tpd/xl2tpd.conf.original
# vim /etc/xl2tpd/xl2tpd.conf

[global]
port = 1701
auth file = /etc/xl2tpd/l2tp-secrets

[lns default]
ip range = 192.168.3.200-192.168.3.250
local ip = 192.168.3.9
require chap = yes
refuse pap = yes
require authentication = yes
name = vpn.example.com
pppoptfile = /etc/ppp/options.l2tpd.lns
```

3. /etc/ppp/options.l2tpd.lns

```
vim /etc/ppp/options.l2tpd.lns

ipcp-accept-local
ipcp-accept-remote
ms-dns 208.67.222.222
ms-dns 208.67.220.220
ms-wins 192.168.3.4
noccp
auth
crtscts
idle 1800
mtu 1410
mru 1410
nodefaultroute
debug
lock
proxyarp
connect-delay 5000
```

4. /etc/xl2tpd/l2tp-secrets

```
vim /etc/xl2tpd/l2tp-secrets

neo     *       chen    *
```

5. start

```
/etc/init.d/xl2tpd start
```

第 28 章 Ipsec VPN

目录

1. openswan - IPSEC utilities for Openswan

http://www.openswan.org/

2. strongswan - IPSec utilities for strongSwan

http://www.strongswan.org/

3. ipsec-tools - IPsec tools for Linux

https://trac.ipsec-tools.net/

第 29 章 Point to Point

目录

1. download

1.1. rtorrent - ncurses BitTorrent client based on LibTorrent

```
$ apt-cache search rtorrent
rtorrent - ncurses BitTorrent client based on LibTorrent
rtpg-www - web based front end for rTorrent
```

1.2. mldonkey-server - Door to the 'donkey' network

```
$ sudo apt-get install mldonkey-server

$ sudo cat /etc/default/mldonkey-server
# MLDonkey configuration file
# This file is loaded by /etc/init.d/mldonkey-server.
# This file is managed using ucf(1).

MLDONKEY_DIR=/var/lib/mldonkey
MLDONKEY_USER=mldonkey
MLDONKEY_GROUP=mldonkey
MLDONKEY_UMASK=0022
LAUNCH_AT_STARTUP=false
MLDONKEY_NICENESS=0
```

Initial Setup

Once the daemon is running, connect to it as the admin user and change the password:

```
$ telnet 127.0.0.1 4000
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Welcome to MLDonkey 2.8.5
Welcome on mldonkey command-line

Use ? for help

MLdonkey command-line:
> auth admin ""
Full access enabled
```

```
MLdonkey command-line:
> passwd newpasswd
Password of user admin changed

MLdonkey command-line:
>
```

1.3. amule - client for the eD2k and Kad networks, like eMule

```
$ apt-cache search amule
amule - client for the eD2k and Kad networks, like eMule
amule-adunanza - client for the eD2k and Kadu networks for for Fastweb clients
amule-adunanza-daemon - non-graphic version of aMule-AdunanzA, a client for the eD2k and
amule-adunanza-utils - utilities for aMule-AdunanzA (command-line version)
amule-adunanza-utils-gui - graphic utilities for aMule-AdunanzA
amule-common - common files for the rest of aMule packages
amule-daemon - non-graphic version of aMule, a client for the eD2k and Kad networks
amule-emc - list ed2k links inside emulecollection files
amule-gnome-support - ed2k links handling support for GNOME web browsers
amule-utils - utilities for aMule (command-line version)
amule-utils-gui - graphic utilities for aMule
```

第 30 章 News Group (innd)

目录

homepage: http://www.isc.org/inn.html

过程 30.1. innd

1. debian 安装

```
sudo apt-get install inn2
```

2. 配置

a. inn.conf

```
cd /etc/news/
chown news.news inn.conf
domain:                 example.org
server:                 localhost
fromhost:               news.example.org
moderatormailer:        openunix@163.com
```

b. storage.conf

```
vi storage.conf
method tradspool {
        newsgroups: *
        class: 0
}
```

c. readers.conf

```
vi readers.conf
auth "local" {
        hosts: "*"
        default: "*"
}

access "local" {
        users: "*"
        newsgroups: "*"
}
```

3. start

/etc/init.d/innd start

```
service innd start
Starting INND system:                                      [  OK  ]
```

sudo ufw allow nntp

news://news.example.org

1. User Authentication

过程 30.2. Authinfo

1. ckpasswd

```
chown root /usr/lib/news/bin/auth/passwd/ckpasswd
chmod 4555 /usr/lib/news/bin/auth/passwd/ckpasswd
```

2. shadow auth

```
$ sudo vim /etc/news/readers.conf

auth local {
        auth: "ckpasswd -s"
}

access local {
        users: "neo"
        newsgroups: "*,!junk,!control,!control.*"
}
```

3. passwd file

```
auth local {
       auth: "ckpasswd -f /etc/news/newsusers"
}

access local {
        users: "neo"
        newsgroups: "*,!junk,!control,!control.*"
}
```

4. dbm,ndbm

```
auth: "ckpasswd -d /etc/news/newsusers.ndbm"
```

2. usenet 管理

```
Usenet新闻组有以下几大类:
  ●comp    计算机科学及相关的话题
  ●news    一般性的新闻话题
  ●rec     个人爱好、娱乐活动、艺术话题
  ●sci     科学研究、工程技术
  ●soc     社会类话题
  ●biz     商业类话题
  ●talk    有争议的话题
  ●misc    不属于以上几类的或有交叉的话题
  后来又增加了一类“alt”，这是一个范围较小、使用的人也较少的一个新闻组，
“alt”是“altemative” 的简写，是“替代”的意思，在这个组可以讨论各类话题。
```

创建组

```
sudo ctlinnd newgroup comp.lang.php
sudo ctlinnd newgroup comp.lang.perl
sudo ctlinnd newgroup comp.lang.python

sudo ctlinnd newgroup rec.photography
sudo ctlinnd newgroup rec.photographic.equipment
sudo ctlinnd newgroup rec.photographic.equipment.35mm
sudo ctlinnd newgroup rec.photographic.equipment.digital
sudo ctlinnd newgroup rec.photographic.equipment.lens
```

ctlinnd 手册

```
使用 ctlinnd 这个指令的大部份功能都只会在 INND 开启后才可以使用，例如就是新增
Newsgroup ，您可以参考 ctlinnd 的系统手册。以下是一些常用的功能解释及例子。

格式： ctlinnd newgroup [groupname]
例子： ctlinnd newgroup group.readers.discuss


这个作法是新增一个名为 "group.readers.discuss" 的 Newsgroup

格式:  ctlinnd rmgroup [groupname]
例子:  ctlinnd rmgroup group.test.unused


这个指令是可以删除 [groupname] 的 Newsgroup。

格式:  ctlinnd cannel [message-id]
例子:  ctlinnd cancel 3BCBF4B3.8AD48C8F@linux.org.hk


把 Message-ID 为 "3BCBF4B3.8AD48C8F@linux.org.hk" 的文章删除，而这个 Message-ID 可以在
"View Source" 时看到，就如图二中是在 Netscape 中的画面，图中打圈的就是 Message-ID 的
位置，不过要注意是某些的 Message-ID 是包括了 "$" 号的，这时可别忘记在 "$" 号前加
上 "\" ，也就是 "\$"。

格式:  ctlinnd pause [reason]
例子:  ctlinnd pause maintenance


暂停一切的连线及不准许新的文章，这个适合作为暂时性的服务暂停。而 [reason] 部
份是关键钥，您可以输入任何的 [reason] ，下文再谈。

格式:  ctlinnd throttle [reason]
例子:  ctlinnd throttle upgrade


暂停一切的连线及不准许新的文章，并且也会关闭 INND 的 "history" 檔案。这个适合
作为长时期的服务暂停。而 [reason] 部份是关键钥，您可以输入任何的 [reason] ，下文
再谈。

格式:  ctlinnd go [reason]
例子:  ctlinnd go maintenance


这个 "go" 功能是使已暂停服务的 innd 继续服务，例如是在 "pause" 或是 "throttle" 后，可
以使用这个功能，但是要注意笔者刚才提过 [reason] 一事，在 "go" 中使用的 [reason] 必
须要与 "pause" 或是 "throttle" 中的 [reason] 相同。
```

3. 通过SSL连接

```
$ cat /etc/news/sasl.conf
```

创建证书

```
$ sudo openssl req -new -x509 -nodes \
-out cert.pem -days 366 \
-keyout cert.pem

Generating a 1024 bit RSA private key
....................++++++
.............................++++++
writing new private key to 'cert.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CN
State or Province Name (full name) [Berkshire]:Guang dong
Locality Name (eg, city) [Newbury]:Shen Zhen
Organization Name (eg, company) [My Company Ltd]:netkiller
Organizational Unit Name (eg, section) []:netkiller
Common Name (eg, your name or your server's hostname) []:netkiller.8800.org
Email Address []:openunix@163.com
```

设置权限

```
$ sudo chmod 640 cert.pem
```

4. src.rpm 安装

下载文件

```
wget ftp://rpmfind.net/linux/redhat/enterprise/4/en/os/i386/SRPMS/inn-2.3.5-12.src.rpm
cd /usr/src/redhat/SPECS
rpmbuild --ba inn.spec
cd /usr/src/redhat/RPMS/i386/
rpm -ivh *
```

makedbz

```
cd /var/lib/news
chmod 664 active
sudo -u news /usr/lib/news/bin/makedbz -i
mv history.n.dir history.dir
mv history.n.hash history.hash
mv history.n.index history.index
```

inncheck

```
sudo -u news /usr/lib/news/bin/inncheck
```

5. 常用新闻组

news://news.newsfan.net

news://news.nntp.hk

news://news.idsam.com

第 31 章 IRC - Internet Relay Chat

目录

IRC Protcol

irc://chat.freenode.net/wikipedia-zh

irc://host/channel

```
irc://chat.freenode.net/wikipedia-zh
```

2. IRC Commands

IRC常用命令

```
如果已经进入了 UTF-8 频道，却不知道自己是否正使用 UTF-8 编码，可以输入
/charset utf-8
/serv irc.freenode.net
/nick 更改昵称
/join 加入/建立聊天室
/mode +(-)i 锁住聊天室
/mode +(-)o 设定管理员权限
/knock 要求进入私人聊天室
/invite 邀请用户进入私人聊天室
/privmsg 悄悄话
/ignore 忽略
/away 暂时离开
/whois 查询用户信息
/names 列出所有在线用户
/topic 更换聊天室主题
/kick 把用户踢出聊天室
/quit 退出聊天室
```

```
IRC命令有二点值得您注意:
所有的IRC命令都是由“/”引导。
在不引起混淆的情况下，IRC命令允许简写。例如，/join 命令可以简写为/j，/jo或者/joi。
/nick
更改昵称的基本方法是: /n(ick) 新的昵称
您的昵称可以包含英文字母，数字，汉字及下划线等。但是，昵称不能超过50个（每个字符和汉字都算一个字），而且不能包含$，+，！和空格。
/nick 命令等价于工具按钮中的“改变别名”。
/join
/join命令的格式是: /j(oin) 聊天室名
如果聊天室已经存在，您就进入该聊天室。此时，/join 命令等价于聊天室列表工具按钮中的“进入”。
如果聊天室不存在，您就建立了一个新的聊天室并进入。此时，/join 命令等价于工具按钮中的“建聊天室”。
聊天室的名字可以包含英文字母，数字，汉字及下划线等。但是，不能超过50个字（每个字符和汉字都算一个字），而且不能包含$，+，！和空格。
/mode +(-)i
/mode +(-)i 命令可以用来锁住（解锁）用户自建的聊天室（私人聊天室）。其命令格式是:/m(ode)
+i 或 /m(ode) -i
只有用户自建的聊天室才能加锁。
未经管理员邀请，其他用户不能进入私人聊天室。
/mode +(-)o
/mode +(-)o 命令可以让聊天室管理员赋予或者剥夺其他用户的管理员身份。其命令格式是: /m(ode)
+o 用户昵称或/m(ode)-o用户昵称只有聊天室管理员才能使用这个命令。
/knock
```

/knock 命令可以让您询问私人聊天室管理员是否可以进入该私人聊天室。其命令格式是: /k(nock) 房间名

消息]

/invite

/invite 命令可以让聊天室管理员邀请其他用户进入私人聊天室。其命令格式是:/i(nvite) 用户昵称

只有私人聊天室的管理员才能使用这个命令。

/privmsg

/privmsg 命令用来向在同一间聊天室的某个用户发送私人消息（悄悄话）。也就是说，您的消息只送给指定的人，而不会显示给其他用户。

/privmsg 命令的基本格式是: /p(rivmsg) 用户昵称 消息

接受您的私人消息的用户必须和您在同一间聊天室。

“用户昵称”和“消息”这两个参数是不能省略的。
如果某个用户的昵称太长，在不会产生混淆的情况下，您可以只输入用户昵称的头几个字母，系统会进行自动匹配。

例如：聊天室里除了您之外还有两个用户，他们的昵称分别是xiaobao和softman。您若想给softman发送悄悄话，可以在输入框里输入下面的命令:

/p s Have you etanged today?
由于xiaobao和softman的第一个字母就不一样，所以系统会把您输入的昵称“s”自动匹配为“softman”。另外，“/p”是“/privmsg”的缩写。

/ignore

/ignore 命令用来把某个用户加入您的“坏人黑名单”。一旦某个用户进入了您的黑名单，他说的任何话都将不会显示在您的终端上。

/ignore 命令的基本格式是: /ig(nore) 用户昵称

用户昵称所代表的用户必须和您在同一个聊天室。

/ignore 命令等价于用户列表工具按钮中的“忽略”。

如果某个用户的昵称太长，在不会产生混淆的情况下，您可以只输入用户昵称的头几个字母，系统会进行自动匹配。

在您的用户列表中，如果某个用户昵称前有一个#，表示该用户已经被您列入黑名单。

如果一个用户已经在您的黑名单中，您可以用 /ignore 用户昵称 把他从黑名单中去掉。

/away

/away 命令用来把自己设为“暂时离开”状态，并可以留言给其他用户。当其他用户和您说悄悄话时，您预先设置的留言会自动回复给其他用户。

/away 命令的基本格式是: /a(way) [留言]

“留言”这个参数是可选的。如果有这个参数，您的状态会被设置为“暂时离开”。否则，您的状态会被设置为“我回来了”。

当您暂时离开聊天室时，用户列表中您的昵称前会出现一个?，表示您处于“离开”状态。工具按钮中的“暂时离开”也会变为“我回来了”。

当您回来继续聊天时，您可以点击工具按钮中的“我回来了”，或者在输入框里输入 /away 命令，将自己设置为正常状态。

/away 命令等价于工具按钮中的“暂时离开”

/whois

/whois 命令用来查询某个用户的信息，包括用户的亿唐ID，IP地址，目前所在的聊天室和发呆时间。

/whois 命令的基本格式是: /w(hois) 用户昵称

/whois命令等价于用户列表工具按钮中的“查询”。

/names

/names 命令用来查看当前所有（或某个聊天室内）的在线聊天用户。其命令格式是: /na(mes) [聊天室]

/topic

/topic 命令用来设定当前聊天室的主题。

/topic 命令的基本格式是: /t(opic) 聊天室主题

只有当前聊天室的管理员（op）才有权利设定聊天室主题。

聊天室的创建者就是该聊天室的管理员。

管理员权限可以通过 /mode +o 命令转交。

/kick

/kick 命令用来把某个用户踢出当前聊天室。

/kick 命令的基本格式是: /ki(ck) 用户昵称 [消息]

只有当前聊天室的管理员（op）才有权利把其他用户踢出当前聊天室。

聊天室的创建者就是该聊天室的管理员。

管理员权限可以通过/mode +o命令转交。

请诸位网友慎用这个命令。“君子动口不动手”嘛!

/quit

/quit 命令用来退出聊天室。

`/quit` 命令的基本格式是: `/q(uit) [消息]`

“消息”这个参数是可选的。如果您指定退出时的消息，该消息会发送给当前聊天室中的其他用户。您可以使用这个消息向其他用户道别。

`/quit` 命令等价于工具按钮中的“结束聊天”。

---

3. ircd-irc2 - The original IRCNet IRC server daemon

Installation

```
sudo apt-get install ircd-irc2
```

Configuration

```
$ sudo vim /etc/ircd/ircd.conf
$ sudo /etc/init.d/ircd-irc2 start
```

4. ircd-hybrid

install

```
netkiller@shenzhen:~$ sudo apt-get install ircd-hybrid
```

script file

```
netkiller@shenzhen:~$ /etc/init.d/ircd-hybrid
Usage: /etc/init.d/ircd-hybrid {start|stop|restart|reload|force-reload}
```

config file

```
netkiller@shenzhen:~$ sudo ls /etc/ircd-hybrid/
cresv.conf  dline.conf  ircd.conf  ircd.motd  kline.conf  nresv.conf  rkline.conf  rxline.conf
xline.conf
```

5. IRC Client

Client

5.1. ircII - interface to the Internet Relay Chat system

TUI client

```
$ sudo apt-get install ircii
```

/etc/irc/servers

remove the string: change_this_in_etc_irc_servers

add default irc server.

```
172.16.0.1
```

running irc client

```
$ irc -c '#system' neo 192.168.3.9
```

freenode.net

```
$ irc -c '#debian' neo chat.freenode.net
```

5.2. HydraIRC

http://www.hydrairc.com

第 32 章 jabber

目录

jabber homepage

1. ejabberd - Distributed, fault-tolerant Jabber/XMPP server written in Erlang

http://www.ejabberd.im/

1. install

```
$ sudo apt-get install ejabberd
```

2. configure.

```
$ sudo cp /etc/ejabberd/ejabberd.cfg /etc/ejabberd/ejabberd.cfg.old
$ sudo ls /etc/ejabberd/
ejabberd.cfg  ejabberd.cfg.old  ejabberd.pem  inetrc

$ sudo vim /etc/ejabberd/ejabberd.cfg

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% Options which are set by Debconf and managed by ucf

%% Admin user
{acl, admin, {user, "neo", "netkiller.8800.org"}}.

%% Hostname
{hosts, ["netkiller.8800.org"]}.

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

3. create a admin

ejabberdctl register <username> <server> <password># ejabberdctl unregister <username> <server>

```
$ sudo ejabberdctl register neo netkiller.8800.org your_password
```

admin page: http://localhost:5280/admin/

4. firewall

```
$ sudo ufw allow xmpp-server
Rule added

$ sudo ufw allow xmpp-client
Rule added
```

5. test

```
$ sudo apt-get install sendxmpp
```

Create config file ~/.sendxmpprc

```
$ vim ~/.sendxmpprc

#account@host:port password
neo@netkiller.8800.org chen

$ sudo chmod 600 .sendxmpprc
```

send messages

```
$ echo -n hi | sendxmpp -r echocmd neo@netkiller.8800.org
```

1.1. ejabberdctl

set-password

```
$ sudo ejabberdctl set-password eva netkiller.8800.org eva
```

2. DJabberd

http://www.danga.com/djabberd/

3. freetalk - A console based Jabber client

```
$ sudo apt-get install freetalk
$ freetalk
```

4. library

4.1. python-xmpp

```
$ sudo apt-get install python-xmpp
```

```
$ cat jabber.py
import xmpp
jid=xmpp.protocol.JID('neo@netkiller.8800.org')
cl=xmpp.Client(jid.getDomain(),debug=[])
cl.connect()
cl.auth(jid.getNode(),'chen')
cl.send(xmpp.protocol.Message('neo@netkiller.8800.org','hi there'))
cl.disconnect()
```

第 33 章 NET SNMP (Simple Network Management Protocol)

目录

1. 安装SNMP

search package

```
netkiller@neo:~$ apt-cache search snmp
libsnmp-base - NET SNMP (Simple Network Management Protocol) MIBs and Docs
libsnmp-perl - NET SNMP (Simple Network Management Protocol) Perl5 Support
libsnmp-session-perl - Perl support for accessing SNMP-aware devices
libsnmp9 - NET SNMP (Simple Network Management Protocol) Library
libsnmp9-dev - NET SNMP (Simple Network Management Protocol) Development Files
snmp - NET SNMP (Simple Network Management Protocol) Apps
snmpd - NET SNMP (Simple Network Management Protocol) Agents
php5-snmp - SNMP module for php5
tcpdump - A powerful tool for network monitoring and data acquisition
```

安装

```
netkiller@neo:~$ sudo apt-get install snmp snmpd
```

2. snmpd.conf

配置 /etc/snmp/snmpd.conf

配置agentAddress

```
agentAddress  udp:172.16.1.3:161
```

```
#       sec.name  source          community
com2sec paranoid  default          chen

#           incl/excl subtree                          mask
view all    included  .1                               80
view system included  .iso.org.dod.internet.mgmt.mib-2.system
view system included  .iso.org.dod.internet.mgmt.mib-2.host
view system included  .iso.org.dod.internet.mgmt.mib-2.interfaces
```

.iso.org.dod.internet.mgmt.mib-2.host 可以使用命令 snmptranslate -Onf -IR hrStorageDescr得到

参考:http://www.mkssoftware.com/docs/man1/snmptranslate.1.asp

3. 列出MBI

$ snmpwalk -c public -v 1 127.0.0.1 1.3.6.1.2.1.1

```
netkiller@neo:/etc/snmp$ snmpwalk -c public -v 1 127.0.0.1 1.3.6.1.2.1.1
SNMPv2-MIB::sysDescr.0 = STRING: Linux neo.example.org 2.6.17-10-server #2 SMP Tue Dec 5
22:29:32 UTC 2006 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (120146) 0:20:01.46
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmpd.local.conf)
SNMPv2-MIB::sysName.0 = STRING: neo.example.org
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (configure /etc/snmp/snmpd.local.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (18) 0:00:00.18
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module to describe generic objects for network
interface sub-layers
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.7 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.9 = STRING: The management information definitions for the SNMP User-
based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (12) 0:00:00.12
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (12) 0:00:00.12
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (12) 0:00:00.12
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (12) 0:00:00.12
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (12) 0:00:00.12
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (12) 0:00:00.12
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (18) 0:00:00.18
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (18) 0:00:00.18
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (18) 0:00:00.18
End of MIB
netkiller@neo:/etc/snmp$ snmpget -v 1 -c public localhost sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Linux neo.example.org 2.6.17-10-server #2 SMP Tue Dec 5
22:29:32 UTC 2006 i686
netkiller@neo:/etc/snmp$
```

snmpget -v 1 -c public localhost sysDescr.0

```
snmpwalk -v 1 -c OFcx6CvN 127.0.0.1 extEntry
```

4. SNMP v3

```
neo@debian:~$ sudo /etc/init.d/snmpd stop
Stopping network management services: snmpd snmptrapd.

neo@debian:~$ sudo net-snmp-config --create-snmpv3-user -ro -a "netadminpassword" netadmin
adding the following line to /var/lib/snmp/snmpd.conf:
   createUser netadmin MD5 "netadminpassword" DES
adding the following line to /usr/share/snmp/snmpd.conf:
   rouser netadmin

neo@debian:~$ sudo /etc/init.d/snmpd start
Starting network management services: snmpd.
```

test

```
neo@debian:~$ snmpget -v 3 -u netadmin -l authNoPriv -a MD5 -A <passwd> 127.0.0.1 sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (6342) 0:01:03.42
```

With a different password this fails:

```
neo@debian:~$ snmpget -v 3 -u netadmin -l authNoPriv -a MD5 -A nopasswd 127.0.0.1 sysUpTime.0
snmpget: Authentication failure (incorrect password, community or key) (Sub-id not found: (top)
-> sysUpTime)
```

Note that this can be stuck in a snmp.conf file in ~/.snmp:

```
neo@debian:~$ mkdir ~/.snmp
neo@debian:~$ vim ~/.snmp/snmp.conf
defSecurityName netadmin
defContext ""
defAuthType MD5
defSecurityLevel authNoPriv
defAuthPassphrase <netadminpassword>
defVersion 3
```

test

```
neo@debian:~$ snmpget 127.0.0.1 sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (39471) 0:06:34.71
```

5. Cacti

Cacti

```
#access  notConfigGroup ""      any       noauth    exact  systemview none none
access  notConfigGroup ""      any       noauth    exact  all none none
view all    included  .1                                  80
```

6. Cisco

```
snmpwalk -c public -v2c 172.16.1.1
```

system.sysDescr

```
$ snmpget -v2c -c public 172.16.1.1 system.sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: 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

$ snmpget -v2c -c public 172.16.1.1 sysName.0
SNMPv2-MIB::sysName.0 = STRING: Switch-3750-LAN

$ snmpwalk -v2c -c public 172.16.1.1 interfaces.ifTable.ifEntry.ifDescr
IF-MIB::ifDescr.1 = STRING: Vlan1
IF-MIB::ifDescr.2 = STRING: Vlan2
IF-MIB::ifDescr.3 = STRING: Vlan3
IF-MIB::ifDescr.4 = STRING: Vlan4
IF-MIB::ifDescr.5 = STRING: Vlan5
IF-MIB::ifDescr.5179 = STRING: StackPort1
IF-MIB::ifDescr.5180 = STRING: StackSub-St1-1
IF-MIB::ifDescr.5181 = STRING: StackSub-St1-2
IF-MIB::ifDescr.10101 = STRING: GigabitEthernet1/0/1
IF-MIB::ifDescr.10102 = STRING: GigabitEthernet1/0/2
IF-MIB::ifDescr.10103 = STRING: GigabitEthernet1/0/3
IF-MIB::ifDescr.10104 = STRING: GigabitEthernet1/0/4
IF-MIB::ifDescr.10105 = STRING: GigabitEthernet1/0/5
IF-MIB::ifDescr.10106 = STRING: GigabitEthernet1/0/6
IF-MIB::ifDescr.10107 = STRING: GigabitEthernet1/0/7
IF-MIB::ifDescr.10108 = STRING: GigabitEthernet1/0/8
IF-MIB::ifDescr.10109 = STRING: GigabitEthernet1/0/9
IF-MIB::ifDescr.10110 = STRING: GigabitEthernet1/0/10
IF-MIB::ifDescr.10111 = STRING: GigabitEthernet1/0/11
IF-MIB::ifDescr.10112 = STRING: GigabitEthernet1/0/12
IF-MIB::ifDescr.10113 = STRING: GigabitEthernet1/0/13
IF-MIB::ifDescr.10114 = STRING: GigabitEthernet1/0/14
IF-MIB::ifDescr.10115 = STRING: GigabitEthernet1/0/15
IF-MIB::ifDescr.10116 = STRING: GigabitEthernet1/0/16
IF-MIB::ifDescr.10117 = STRING: GigabitEthernet1/0/17
IF-MIB::ifDescr.10118 = STRING: GigabitEthernet1/0/18
IF-MIB::ifDescr.10119 = STRING: GigabitEthernet1/0/19
IF-MIB::ifDescr.10120 = STRING: GigabitEthernet1/0/20
IF-MIB::ifDescr.10121 = STRING: GigabitEthernet1/0/21
IF-MIB::ifDescr.10122 = STRING: GigabitEthernet1/0/22
IF-MIB::ifDescr.10123 = STRING: GigabitEthernet1/0/23
IF-MIB::ifDescr.10124 = STRING: GigabitEthernet1/0/24
IF-MIB::ifDescr.10125 = STRING: GigabitEthernet1/0/25
IF-MIB::ifDescr.10126 = STRING: GigabitEthernet1/0/26
IF-MIB::ifDescr.10127 = STRING: GigabitEthernet1/0/27
IF-MIB::ifDescr.10128 = STRING: GigabitEthernet1/0/28
IF-MIB::ifDescr.14501 = STRING: Null0


$ snmpget -v2c -c public 172.16.1.1 interfaces.ifNumber.0
IF-MIB::ifNumber.0 = INTEGER: 37
```

7. Linux

```
$ snmpwalk -c public -v2c 172.16.1.10 hrSWRunPerfMem | awk 'BEGIN {total_mem=0} { if ($NF ==
"KBytes") {total_mem=total_mem+$(NF-1)}}  END {print total_mem}'
655784
```

第 34 章 Network Authentication

目录

1. Network Information Service (NIS)

1.1. 安装NIS服务器

过程 34.1. 安装NIS服务器

1. ypserv

```
# yum install ypserv -y
```

2. /etc/hosts

```
[root@nis ~]# hostname nis.example.com
[root@nis ~]# echo "192.168.3.5 nis.example.com" >> /etc/hosts
[root@nis ~]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1 datacenter.example.com datacenter localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
127.0.0.1 kerberos.example.com
192.168.3.5 nis.example.com
```

3. 设置NIS域名

```
# nisdomainname example.com
# nisdomainname
example.com
```

加入 /etc/rc.local 开机脚本

```
# echo '/bin/nisdomainname example.com' >> /etc/rc.local
# echo 'NISDOMAIN=example.com' >> /etc/sysconfig/network
```

4. 设置/etc/ypserv.conf主配置文件

```
# vim /etc/ypserv.conf

127.0.0.0/255.255.255.0 : * : * : none
192.168.3.0/255.255.255.0 : * : * : none
* : * : * : deny
```

5. 创建 /var/yp/securenets 文件

securenets 安全配置文件

```
# vim /var/yp/securenets
host 127.0.0.1
255.255.255.0 192.168.3.0
```

6. 启动NIS服务器

NIS服务器需要portmap服务的支持，并且需要启动ypserv和yppasswdd两个服务

```
[root@nis ~]# service portmap status
portmap (pid 2336)
is running...
[root@nis ~]# service ypserv start
Starting YP
server services: [ OK ]
[root@nis ~]# service yppasswdd start
Starting YP passwd service: [ OK ]
```

7. 构建NIS数据库

32bit: /usr/lib/yp/ypinit -m

64bit: /usr/lib64/yp/ypinit -m

```
[root@nis ~]# /usr/lib64/yp/ypinit -m

At this point, we have to construct a list of the hosts which will run NIS
servers.  nis.example.com is in the list of NIS server hosts.  Please continue to add
the names for the other hosts, one per line.  When you are done with the
list, type a <control D>.
        next host to add:  nis.example.com
        next host to add:
        next host to add:
The current list of NIS servers looks like this:

nis.example.com


Is this correct?  [y/n: y]
We need a few minutes to build the databases...
Building /var/yp/example.com/ypservers...
Running /var/yp/Makefile...
gmake[1]: Entering directory `/var/yp/example.com'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gmake[1]: Leaving directory `/var/yp/example.com'

nis.example.com has been set up as a NIS master server.

Now you can run ypinit -s nis.example.com on all slave server.
```

检查

```
# ls /var/yp/
binding example.com Makefile nicknames securenets ypservers
```

8. Service

```
[root@datacenter ~]# chkconfig --list | grep yp
ypbind          0:off   1:off   2:off   3:off   4:off   5:off   6:off
yppasswdd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
ypserv          0:off   1:off   2:off   3:off   4:off   5:off   6:off
ypxfrd          0:off   1:off   2:off   3:off   4:off   5:off   6:off

[root@nis ~]# chkconfig ypserv on
[root@nis ~]# chkconfig yppasswdd on
```

1.2. Slave NIS Server

Now you can run ypinit -s nis.example.com on all slave server.

```
# ypinit -s nis.example.com
```

1.3. 客户机软件安装

过程 34.2. 安装NIS客户端软件

1. NIS客户机需要安装ypbind和yp-tools两个软件包

```
# yum install ypbind yp-tools -y
```

2. NIS域名

```
# nisdomainname example.com
```

3. /etc/hosts

```
192.168.3.5 nis.example.com
```

4. /etc/yp.conf

```
# vim /etc/yp.conf
domain example.com server nis.example.com
```

5. /etc/nsswitch.conf

```
# vim /etc/nsswitch.conf
passwd: files nis
shadow: files nis
group: files nis
hosts: files nis dns
```

6. 启动ypbind服务程序

```
[root@test ~]# service portmap status
portmap is stopped
[root@test ~]# service portmap start
Starting portmap: [ OK ]
[root@test ~]# service ypbind start
Turning on allow_ypbind SELinux boolean
Binding to the NIS domain: [ OK ]
Listening for an NIS domain server..
```

7. yp-tools 测试工具

yptest 命令可对NIS服务器进行自动测试

```
# yptest
```

ypwhich 命令可显示NIS客户机所使用的NIS服务器的主机名称和数据库文件列表

```
# ypwhich
# ypwhich -x
```

ypcat命令显示数据库文件列表和指定数据库的内容

```
# ypcat -x
# ypcat passwd
```

8. NIS Client Service

```
# chkconfig ypbind on
```

1.4. Authentication Configuration

```
# authconfig-tui
```

Use NIS

```
                 ┤ Authentication Configuration ├
  User Information          Authentication
  [ ] Cache Information     [*] Use MD5 Passwords
  [ ] Use Hesiod            [*] Use Shadow Passwords
  [ ] Use LDAP              [ ] Use LDAP Authentication
  [*] Use NIS               [ ] Use Kerberos
  [ ] Use Winbind           [ ] Use SMB Authentication
                            [ ] Use Winbind Authentication
                            [ ] Local authorization is sufficient

            Cancel                        Next
```

NIS Settings

```
                    ┤ NIS Settings ├
  Domain: example.com
  Server: nis.example.com

          Back                  Ok
```

1.5. application example

nis server:

在NIS服务器上创建一个test用户

```
# adduser test
# passwd test
# /usr/lib64/yp/ypinit -m
```

nis client

使用test用户登录到客户机

```
ssh test@client.example.com
```

测试

```
[root@test ~]# yptest
Test 1: domainname
Configured domainname is "example.com"

Test 2: ypbind
Used NIS server:
nis.example.com

Test 3: yp_match
WARNING: No such key in map (Map
passwd.byname, key nobody)

Test 4: yp_first
neo
neo:$1$e1nd3pts$s7NikMnKwpL4vUp2LM/N9.:500:500::/home/neo:/bin/bash

Test 5: yp_next
test
test:$1$g4.VCB7i$I/N5W/imakprFdtP02i8/.:502:502::/home/test:/bin/bash
svnroot svnroot:!!:501:501::/home/svnroot:/bin/bash

Test 6: yp_master
nis.example.com

Test 7: yp_order
1271936660

Test 8: yp_maplist
rpc.byname
protocols.bynumber
ypservers
passwd.byname
hosts.byname
rpc.bynumber
group.bygid
services.byservicename
mail.aliases
passwd.byuid
services.byname
netid.byname
protocols.byname
group.byname
hosts.byaddr

Test 9: yp_all
neo
```

```
neo:$1$e1nd3pts$s7NikMnKwpL4vUp2LM/N9.:500:500::/home/neo:/bin/bash
test
test:$1$g4.VCB7i$I/N5W/imakprFdtP02i8/.:502:502::/home/test:/bin/bash
svnroot svnroot:!!:501:501::/home/svnroot:/bin/bash
1 tests failed
```

更改密码

```
$ yppasswd
Changing NIS account information for test on nis.example.com.
Please enter old password:
Changing NIS password for test on
nis.example.com.
Please enter new password:
Please retype new password:

The NIS password has been changed on nis.example.com.
```

```
-bash-3.2$ ypcat hosts
127.0.0.1 localhost.localdomain localhost
127.0.0.1 kerberos.example.com
192.168.3.5 nis.example.com

-bash-3.2$ ypcat passwd
neo:$1$e1nd3pts$s7NikMnKwpL4vUp2LM/N9.:500:500::/home/neo:/bin/bash
test:$1$g4.VCB7i$I/N5W/imakprFdtP02i8/.:502:502::/home/test:/bin/bash
svnroot:!!:501:501::/home/svnroot:/bin/bash
```

```
-bash-3.2$
ypwhich
nis.example.com

ypwhich -x
Use "ethers" for map "ethers.byname"
Use "aliases" for map "mail.aliases"
Use "services" for map "services.byname"
Use "protocols" for map "protocols.bynumber"
Use "hosts" for map "hosts.byname"
Use "networks" for map "networks.byaddr"
Use "group" for map "group.byname"
Use "passwd" for map "passwd.byname"
```

1.6. Mount /home volume from NFS

在NIS服务器中将“/home”输出为NFS共享目录

```
# vi /etc/exports
/home 192.168.3.0/24(sync,rw,no_root_squash)
```

重启NFS服务

```
# service nfs restart
```

在NIS客户端中挂载“/home”目录

```
                # vi /etc/fstab
192.168.1.10:/home/ /home nfs   defaults 0 0
```

mount home volume

```
```

```
# mount /home
```

2. OpenLDAP

2.1. Server

1. First, install the OpenLDAP server daemon slapd and ldap-utils, a package containing LDAP management utilities:

```
sudo apt-get install slapd ldap-utils
```

By default the directory suffix will match the domain name of the server. For example, if the machine's Fully Qualified Domain Name (FQDN) is ldap.example.com, the default suffix will be dc=example,dc=com. If you require a different suffix, the directory can be reconfigured using dpkg-reconfigure. Enter the following in a terminal prompt:

```
sudo dpkg-reconfigure slapd
```

2. example.com.ldif

```
dn: ou=people,dc=example,dc=com
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups

dn: uid=john,ou=people,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: john.doe@example.com
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: JD

dn: cn=example,ou=groups,dc=example,dc=com
objectClass: posixGroup
cn: example
gidNumber: 10000
```

3. To add the entries to the LDAP directory use the ldapadd utility:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f example.com.ldif
```

We can check that the content has been correctly added with the tools from the ldap-utils package. In order to execute a search of the LDAP directory:

```
ldapsearch -xLLL -b "dc=example,dc=com" uid=john sn givenName cn

dn: uid=john,ou=people,dc=example,dc=com
cn: John Doe
sn: Doe
givenName: John
```

Just a quick explanation:

-x: will not use SASL authentication method, which is the default.

-LLL: disable printing LDIF schema information.

2.2. Client

1. libnss-ldap

```
sudo apt-get install libnss-ldap
```

2. reconfigure ldap-auth-config

```
sudo dpkg-reconfigure ldap-auth-config
```

3. auth-client-config

```
sudo auth-client-config -t nss -p lac_ldap
```

4. pam-auth-update.

```
sudo pam-auth-update
```

2.3. User and Group Management

```
sudo apt-get install ldapscripts
```

/etc/ldapscripts/ldapscripts.conf

```
SERVER=localhost
BINDDN='cn=admin,dc=example,dc=com'
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX='dc=example,dc=com'
GSUFFIX='ou=Groups'
USUFFIX='ou=People'
MSUFFIX='ou=Computers'
GIDSTART=10000
UIDSTART=10000
MIDSTART=10000
```

Now, create the ldapscripts.passwd file to allow authenticated access to the directory:

```
sudo sh -c "echo -n 'secret' > /etc/ldapscripts/ldapscripts.passwd"
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

3. Kerberos

（Kerberos: Network Authentication Protocol）

http://web.mit.edu/Kerberos/

kerberos是由MIT开发的提供网络认证服务的系统，很早就听说过它的大名，但一直没有使用过它。 它可用来为网络上的各种server提供认证服务,使得口令不再是以明文方式在网络上传输，并且联接之间通讯是加密的； 它和PKI认证的原理不一样，PKI使用公钥体制(不对称密码体制)，kerberos基于私钥体制(对称密码体制)。

3.1. Kerberos 安装

3.1.1. CentOS 安装

获得krb5的安装包

yum search krb5

```
[root@centos ~]# yum search krb5
============================================ Matched: krb5 ============================================
krb5-auth-dialog.x86_64 : Kerberos 5 authentication dialog
krb5-devel.i386 : Development files needed to compile Kerberos 5 programs.
krb5-devel.x86_64 : Development files needed to compile Kerberos 5 programs.
krb5-libs.i386 : The shared libraries used by Kerberos 5.
krb5-libs.x86_64 : The shared libraries used by Kerberos 5.
krb5-server.x86_64 : The KDC and related programs for Kerberos 5.
krb5-workstation.x86_64 : Kerberos 5 programs for use on workstations.
pam_krb5.i386 : A Pluggable Authentication Module for Kerberos 5.
pam_krb5.x86_64 : A Pluggable Authentication Module for Kerberos 5.
```

安装

yum install krb5-server.i386

```
[root@centos ~]# yum install krb5-server
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package krb5-server.x86_64 0:1.6.1-36.el5_4.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=================================================================================================
 Package                 Arch                Version                        Repository
Size
=================================================================================================
Installing:
 krb5-server             x86_64              1.6.1-36.el5_4.1               updates
914 k

Transaction Summary
=================================================================================================
Install      1 Package(s)
```

```
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 914 k
Is this ok [y/N]: y
Downloading Packages:
krb5-server-1.6.1-36.el5_4.1.x86_64.rpm                                          | 914 kB     00:01
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : krb5-server
1/1

Installed:
  krb5-server.x86_64 0:1.6.1-36.el5_4.1

Complete!
[root@datacenter ~]#Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package krb5-server.x86_64 0:1.6.1-36.el5_4.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=================================================================================================

 Package                 Arch               Version                       Repository
Size
=================================================================================================

Installing:
 krb5-server             x86_64             1.6.1-36.el5_4.1              updates
914 k

Transaction Summary
=================================================================================================

Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 914 k
Is this ok [y/N]: y
Downloading Packages:
krb5-server-1.6.1-36.el5_4.1.x86_64.rpm                                          | 914 kB     00:01
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : krb5-server
1/1

Installed:
  krb5-server.x86_64 0:1.6.1-36.el5_4.1

Complete!
```

yum install krb5-workstation

```
[root@centos ~]# yum install krb5-workstation
```

yum install krb5-libs

```

```

3.1.2. Install by apt-get

过程 34.3. installation

1.
```
$ sudo apt-get install krb5-admin-server
```

2. Configuring

```
  ┌──────────────────────────────┤ Configuring krb5-admin-server
├──────────────────────────────┐
  │
```

```
│
│ Setting up a Kerberos Realm
│
│
│ This package contains the administrative tools required to run the Kerberos master
server.    │
│
│ However, installing this package does not automatically set up a Kerberos realm.  This
can    │
│ be done later by running the "krb5_newrealm" command.
│
│
│ Please also read the /usr/share/doc/krb5-kdc/README.KDC file and the administration
guide    │
│ found in the krb5-doc package.
│
│
│                                                <Ok>
│
│
│
└──────────────────────────────────────────────────────────────────────────────────────────
```

OK

```
┌──────────────────────────────┤ Configuring krb5-admin-server
├──────────────────────────────┐
│
│
│ Kadmind serves requests to add/modify/remove principals in the Kerberos database.
│
│
│
│ It is required by the kpasswd program, used to change passwords. With standard setups,
this    │
│ daemon should run on the master KDC.
│
│
│
│ Run the Kerberos V5 administration daemon (kadmind)?
│
│
│
│                            <Yes>                               <No>
│
│
│
└──────────────────────────────────────────────────────────────────────────────────────────
```

Yes

3.2. Kerberos Server

过程 34.4. Kerberos Server 配置步骤

1. Create the Database

   创建Kerberos的本地数据库

kdb5_util create -r EXAMPLE.COM -s

```
[root@datacenter ~]# kdb5_util create -r EXAMPLE.COM -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

2. /etc/krb5.conf

```
# cp /etc/krb5.conf /etc/krb5.conf.old
# vim /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 EXAMPLE.COM = {
  kdc = kerberos.example.com:88
  admin_server = kerberos.example.com:749
  default_domain = example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

检查下面配置文件 /var/kerberos/krb5kdc/kadm5.acl

```
[root@datacenter ~]# cat /var/kerberos/krb5kdc/kadm5.acl
*/admin@EXAMPLE.COM     *
```

格式

```
The format of the file is:

     Kerberos_principal      permissions     [target_principal] [restrictions]
```

3. Add Administrators to the Kerberos Database

创建账号

```
[root@datacenter ~]# kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local:  addprinc admin/admin@EXAMPLE.COM
WARNING: no policy specified for admin/admin@EXAMPLE.COM; defaulting to no policy
Enter password for principal "admin/admin@EXAMPLE.COM":
Re-enter password for principal "admin/admin@EXAMPLE.COM":
Principal "admin/admin@EXAMPLE.COM" created.
kadmin.local:
```

也同样可以使用下面命令

kadmin.local -q "addprinc username/admin"

```
[root@datacenter ~]# kadmin.local -q "addprinc krbuser"
Authenticating as principal admin/admin@EXAMPLE.COM with password.
WARNING: no policy specified for krbuser@EXAMPLE.COM; defaulting to no policy
Enter password for principal "krbuser@EXAMPLE.COM":
Re-enter password for principal "krbuser@EXAMPLE.COM":
Principal "krbuser@EXAMPLE.COM" created.
```

4. Create a kadmind Keytab

```
[root@datacenter ~]# kadmin.local -q  "ktadd -k /var/kerberos/krb5kdc/kadm5.keytab =>
kadmin/admin kadmin/changepw"
```

```
Authenticating as principal admin/admin@EXAMPLE.COM with password.
kadmin.local: Principal => does not exist.
Entry for principal kadmin/admin with kvno 3, encryption type Triple DES cbc mode with
HMAC/sha1 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type DES cbc mode with CRC-32
added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc mode with
HMAC/sha1 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode with CRC-32
added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
```

5. Start the Kerberos Daemons on the Master KDC

   启动 Kerberos进程

```
[root@datacenter ~]# sudo /etc/init.d/krb524 start
Starting Kerberos 5-to-4 Server:                            [  OK  ]

[root@datacenter ~]# sudo /etc/init.d/krb5kdc restart
Stopping Kerberos 5 KDC:                                    [  OK  ]
Starting Kerberos 5 KDC:                                    [  OK  ]

[root@datacenter ~]# sudo /etc/init.d/kadmin start
Starting Kerberos 5 Admin Server:                           [  OK  ]
```

6. Log 文件

```
[root@datacenter ~]# cat /var/log/krb5kdc.log

[root@datacenter ~]# cat /var/log/krb5libs.log

[root@datacenter ~]# cat /var/log/kadmind.log
```

3.3. Kerberos Client

过程 34.5. Kerberos Client 配置步骤

1. Ticket Management

   a. Obtaining Tickets with kinit

```
[root@datacenter ~]# kinit admin/admin
Password for admin/admin@EXAMPLE.COM:
```

   b. Viewing Your Tickets with klist

```
[root@datacenter ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin/admin@EXAMPLE.COM

Valid starting     Expires            Service principal
03/25/10 16:15:18  03/26/10 16:15:18  krbtgt/EXAMPLE.COM@ZEXAMPLECOM


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

   c. Destroying Your Tickets with kdestroy

```
[root@datacenter ~]# kdestroy
[root@datacenter ~]# klist
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_0)


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

2. Password Management

Changing Your Password

```
[root@datacenter ~]# kpasswd
Password for admin/admin@EXAMPLE.COM:
Enter new password:
Enter it again:
Password changed.
```

3.4. Kerberos Management

3.4.1. ktutil - Kerberos keytab file maintenance utility

```
[root@datacenter ~]# ktutil
ktutil: rkt /var/kerberos/krb5kdc/kadm5.keytab
ktutil:  l
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    3                  kadmin/admin@EXAMPLE.COM
   2    3                  kadmin/admin@EXAMPLE.COM
   3    3               kadmin/changepw@EXAMPLE.COM
   4    3               kadmin/changepw@EXAMPLE.COM
ktutil: q
```

3.4.2. klist - list cached Kerberos tickets

```
[root@datacenter ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin/admin@EXAMPLE.COM

Valid starting     Expires            Service principal
03/25/10 16:53:02  03/26/10 16:53:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
03/25/10 17:02:10  03/26/10 16:53:02  host/172.16.0.8@


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

3.5. OpenSSH Authentications

3.5.1. Configuring the Application server system

```
[root@datacenter ~]# kinit   admin/admin
Password for admin/admin@EXAMPLE.COM:

[root@datacenter ~]# kadmin.local -q "addprinc -randkey host/172.16.0.8"
Authenticating as principal admin/admin@EXAMPLE.COM with password.
WARNING: no policy specified for host/172.16.0.8@EXAMPLE.COM; defaulting to no policy
Principal "host/172.16.0.8@EXAMPLE.COM" created.

[root@datacenter ~]# kadmin.local -q " ktadd -k /var/kerberos/krb5kdc/kadm5.keytab
host/172.16.0.8"
Authenticating as principal admin/admin@EXAMPLE.COM with password.
Entry for principal host/172.16.0.8 with kvno 3, encryption type Triple DES cbc mode with
HMAC/sha1 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal host/172.16.0.8 with kvno 3, encryption type DES cbc mode with CRC-32 added
to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
[root@datacenter ~]# ktutil
ktutil:  rkt /var/kerberos/krb5kdc/kadm5.keytab
ktutil:  l
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    3                  kadmin/admin@EXAMPLE.COM
   2    3                  kadmin/admin@EXAMPLE.COM
   3    3               kadmin/changepw@EXAMPLE.COM
   4    3               kadmin/changepw@EXAMPLE.COM
   5    3               host/172.16.0.8@EXAMPLE.COM
   6    3               host/172.16.0.8@EXAMPLE.COM
ktutil:  q
[root@datacenter ~]#
```

3.5.2. Configuring the Application client system

/etc/ssh/sshd_config

```
KerberosAuthentication yes
```

4. FreeRADIUS (Remote Authentication Dial In User Service)

I want to authorize Wi-Fi Protected Access with freeradius for Wi-Fi Route.

- debian/ubuntu
- FreeRADIUS
- D-Link DI-624+A

some package of freeradius.

```
netkiller@shenzhen:~$ apt-cache search freeradius
freeradius - a high-performance and highly configurable RADIUS server
freeradius-dialupadmin - set of PHP scripts for administering a FreeRADIUS server
freeradius-iodbc - iODBC module for FreeRADIUS server
freeradius-krb5 - kerberos module for FreeRADIUS server
freeradius-ldap - LDAP module for FreeRADIUS server
freeradius-mysql - MySQL module for FreeRADIUS server
```

install

```
netkiller@shenzhen:~$ sudo apt-get install freeradius
```

OK, we have installed let's quickly test it. the '******' is your password.

```
netkiller@shenzhen:~$ radtest netkiller ****** localhost 0 testing123
Sending Access-Request of id 237 to 127.0.0.1 port 1812
        User-Name = "netkiller"
        User-Password = "******"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=237, length=20
```

if you can see 'Access-Accept', you have succeed

let me to input an incorrect password.

```
netkiller@shenzhen:~$ radtest netkiller ****** localhost 0 testing123
Sending Access-Request of id 241 to 127.0.0.1 port 1812
        User-Name = "netkiller"
        User-Password = "******"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
Re-sending Access-Request of id 241 to 127.0.0.1 port 1812
        User-Name = "netkiller"
        User-Password = "******"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1:1812, id=241, length=20
```

you will see 'Access-Reject'.

```
# vim /etc/freeradius/clients.conf
```

```
client 172.16.0.0/24 {
        secret          = testing123
        shortname       = freeradius.example.com
}
```

4.1. ldap

4.2. mysql

4.3. WAP2 Enterprise

WRT54G

上一页 上一级 下一页

3. Kerberos 起始页 5. SASL (Simple Authentication and Security Layer)

5. SASL (Simple Authentication and Security Layer)

6. GSSAPI (Generic Security Services Application Program Interface)

第 35 章 OpenSSH

目录

安装

sudo apt-get install ssh

1. maximum number of authentication

限制SSH验证重试次数:

```
# vi /etc/ssh/sshd_config
MaxAuthTries 6
```

2. disable root SSH login

禁止root用户登录

```
PermitRootLogin no
```

3. 忽略known_hosts文件

/etc/ssh/sshd_config

```
IgnoreUserKnownHosts yes
```

4. Automatic SSH / SSH without password

config /etc/ssh/sshd_config

```
$ sudo vim /etc/ssh/sshd_config

AuthorizedKeysFile  %h/.ssh/authorized_keys

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

ssh-keygen

ssh-keygen -d

master server

```
[netkiller@master ~]$ ssh-keygen -d
Generating public/private dsa key pair.
Enter file in which to save the key (/home/netkiller/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/netkiller/.ssh/id_dsa.
Your public key has been saved in /home/netkiller/.ssh/id_dsa.pub.
The key fingerprint is:
bf:a9:21:2c:82:77:2d:71:33:12:20:10:93:5f:cb:74 netkiller@master
[netkiller@master ~]$
[netkiller@master ~]$ cp .ssh/id_dsa.pub .ssh/authorized_keys
[netkiller@master ~]$ chmod 600 .ssh/authorized_keys
[netkiller@master ~]$ ls -l .ssh/
total 12
-rw-------  1 netkiller netkiller 612 Mar 27 15:31 authorized_keys
-rw-------  1 netkiller netkiller 736 Mar 27 15:24 id_dsa
-rw-r--r--  1 netkiller netkiller 612 Mar 27 15:24 id_dsa.pub
[netkiller@master ~]$
```

backup server

```
[netkiller@backup ~]$ ssh-keygen -d
Generating public/private dsa key pair.
Enter file in which to save the key (/home/netkiller/.ssh/id_dsa):
Created directory '/home/netkiller/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/netkiller/.ssh/id_dsa.
Your public key has been saved in /home/netkiller/.ssh/id_dsa.pub.
The key fingerprint is:
c5:2f:0e:4e:b0:46:47:ec:19:30:be:9c:20:ad:9c:51 netkiller@backup
[netkiller@backup ~]$ cp .ssh/id_dsa.pub .ssh/authorized_keys
[netkiller@backup ~]$ chmod 600 .ssh/authorized_keys
[netkiller@backup ~]$ ls -l .ssh/
total 16
-rw-------  1 netkiller netkiller 609 Mar 27 15:31 authorized_keys
-rw-------  1 netkiller netkiller 736 Mar 27 15:27 id_dsa
-rw-r--r--  1 netkiller netkiller 609 Mar 27 15:27 id_dsa.pub
```

交换公钥证书

master => backup

```
[netkiller@master ~]$ scp .ssh/id_dsa.pub netkiller@backup.example.org:.ssh/master.pub
netkiller@backup.example.org's password:
id_dsa.p                                                  100%  612     0.6KB/s   00:00
```

```
[netkiller@master ~]$

[netkiller@backup ~]$ cat .ssh/master.pub >> .ssh/authorized_keys
```

test

```
[netkiller@master ~]$ ssh backup.example.org
Enter passphrase for key '/home/netkiller/.ssh/id_dsa':
Last login: Tue Mar 27 15:26:35 2007 from master.example.org
[netkiller@backup ~]$
```

master <= backup

```
[netkiller@backup ~]$ scp .ssh/id_dsa.pub netkiller@master.example.org:.ssh/backup.pub
netkiller@master.example.org's password:
id_dsa.pub                                                    100%  609     0.6KB/s   00:00
[netkiller@backup ~]$

[netkiller@master ~]$ cat .ssh/backup.pub >> .ssh/authorized_keys
```

test

```
[netkiller@backup ~]$ ssh master.example.org
Enter passphrase for key '/home/netkiller/.ssh/id_dsa':
Last login: Tue Mar 27 15:44:37 2007 from backup.example.org
[netkiller@master ~]$
```

注意：authorized_keys权限必须为600，否则可能登陆的时候还会让你输入密码，但是一旦改成600以后并且成功登陆，此问题不再出现。

script

```
ssh-keygen -d
cp .ssh/id_dsa.pub .ssh/authorized_keys
chmod 600 .ssh/authorized_keys
ls -l .ssh/
```

---

5. disable password authentication

建议你使用证书登录，并禁用密码认证 PasswordAuthentication yes，这样更安全，且不会骇客穷举你的口令。

```
PasswordAuthentication no
```

6. Putty

1. config /etc/ssh/sshd_config

```
$ sudo vim /etc/ssh/sshd_config

AuthorizedKeysFile  %h/.ssh/authorized_keys

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

2. ssh-keygen

```
neo@master:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/neo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/neo/.ssh/id_rsa.
Your public key has been saved in /home/neo/.ssh/id_rsa.pub.
The key fingerprint is:
98:35:81:56:fd:b5:87:e4:94:e4:54:b8:b9:0a:4e:80 neo@master
```

3. authorized_keys

```
$ mv .ssh/id_rsa.pub .ssh/authorized_keys
```

or

```
$ cat .ssh/id_rsa.pub > .ssh/authorized_keys
```

4. PuTTYgen

Load an existing private key file

to click 'Load' button and then open 'id_rsa'

'Save public key' and 'Save private key'

closing PuTTYgen

5. Pageant

opening Pageant

to click mouse right key and then select 'Add Key', opening above private key.

6. Putty

Host Name: your ip address

Connection -> Data -> Auto-login username: your username

Connection -> SSH -> Auth -> Allow agent forwarding, you must checked it

Now, You may click 'Open' to login linux system

---

7. OpenSSH Tunnel

mysql tunnel

```
$ ssh -L 3306:127.0.0.1:3306 user@example.org
```

testing

```
$ mysql -h 127.0.0.1 -uroot -p test
```

7.1. SOCKS v5 Tunnel

```
ssh -D 1080 <远程主机地址>
or
ssh -D 7070 <远程主机地址>
```

I prefer 1080 to 7070. the reason is 1080 default for SOCKS port.

8. ssh-copy-id - install your public key in a remote machine's authorized_keys

```
ssh-copy-id [-i [identity_file]] [user@]machine
```

9. ssh-agent

```
$ ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-JvfzN17863/agent.17863; export SSH_AUTH_SOCK;
SSH_AGENT_PID=17864; export SSH_AGENT_PID;
echo Agent pid 17864;
```

```
eval `ssh-agent`
```

9.1. ssh-add

```
neo@netkiller:~$ ssh-add
Identity added: /home/neo/.ssh/id_dsa (/home/neo/.ssh/id_dsa)

neo@netkiller:~$ ssh-add -l
1024 e5:16:5a:ca:5c:ca:a6:66:89:2d:bf:f2:22:94:3c:d6 /home/neo/.ssh/id_dsa (DSA)
```

let's add a few one-off keys

```
$ ssh-add ssh-keys/id*
```

Delete all keys from the agent

```
neo@netkiller:~$ ssh-add -D
All identities removed.
```

9.2. Lock / Unlock agent

```
neo@netkiller:~$ ssh-add -x
Enter lock password:
Again:
Agent locked.
neo@netkiller:~$ ssh-add -X
Enter lock password:
Agent unlocked.
```

9.3. Set lifetime (in seconds) when adding identities.

```
neo@netkiller:~$ ssh-add -t 10
Identity added: /home/neo/.ssh/id_dsa (/home/neo/.ssh/id_dsa)
Lifetime set to 10 seconds

neo@netkiller:~$ ssh-add -l
1024 e5:16:5a:ca:5c:ca:a6:66:89:2d:bf:f2:22:94:3c:d6 /home/neo/.ssh/id_dsa (DSA)

neo@netkiller:~$ ssh-add -l
The agent has no identities.
```

remote machine’s authorized_keys

10. OpenSSH for Windows

homepage: http://sshwindows.sourceforge.net/

第 36 章 Proxy Server

目录

1. Apache Proxy

```
netkiller@Linux-server:/etc/apache2$ sudo a2enmod proxy
Module proxy installed; run /etc/init.d/apache2 force-reload to enable.
netkiller@Linux-server:/etc/apache2$ sudo a2enmod proxy_connect
Module proxy_connect installed; run /etc/init.d/apache2 force-reload to enable.
netkiller@Linux-server:/etc/apache2$ sudo a2enmod proxy_http
Module proxy_http installed; run /etc/init.d/apache2 force-reload to enable.
netkiller@Linux-server:/etc/apache2$
```

proxy.conf

ProxyRequests On

ProxyPass /mirror/1/ http://netkiller.hikz.com/

ProxyPassReverse /mirror/1/ http://netkiller.hikz.com/

```
netkiller@Linux-server:/etc/apache2$ cat mods-available/proxy.conf
<IfModule mod_proxy.c>

        #turning ProxyRequests on and allowing proxying from all may allow
        #spammers to use your proxy to send email.

        #ProxyRequests Off
        ProxyRequests On

        <Proxy *>
                Order deny,allow
                Deny from all
                #Allow from .your_domain.com
                Allow from all
        </Proxy>

        # Enable/disable the handling of HTTP/1.1 "Via:" headers.
        # ("Full" adds the server version; "Block" removes all outgoing Via: headers)
        # Set to one of: Off | On | Full | Block

        ProxyVia On

        # To enable the cache as well, edit and uncomment the following lines:
        # (no cacheing without CacheRoot)

        CacheRoot "/var/cache/apache2/proxy"
        CacheSize 5
        CacheGcInterval 4
        CacheMaxExpire 24
        CacheLastModifiedFactor 0.1
        CacheDefaultExpire 1
        # Again, you probably should change this.
        #NoCache a_domain.com another_domain.edu joes.garage_sale.com

</IfModule>
```

VirtualHost

```
<VirtualHost *>
    ServerAdmin openunix@163.com
    DocumentRoot /home/netkiller/public_html
    ServerName netkiller.8800.org
    ErrorLog /home/netkiller/log/netkiller.8800.org-error_log
    CustomLog /home/netkiller/log/netkiller.8800.org-access_log common
    ProxyPass   /mirror/1/ http://netkiller.hikz.com/
    ProxyPassReverse    /mirror/1/ http://netkiller.hikz.com/

    <Location /repos>
      DAV svn
      SVNPath /home/netkiller/repos

    </Location>
</VirtualHost>
<VirtualHost *:*>
```

```
    ServerAdmin openunix@163.com
    ServerName mirror.netkiller.8800.org
    ErrorLog /home/netkiller/log/netkiller.8800.org-error_log
    CustomLog /home/netkiller/log/netkiller.8800.org-access_log common
    ProxyPass   / http://netkiller.hikz.com/
    ProxyPassReverse    / http://netkiller.hikz.com/
</VirtualHost>
```

测试http://netkiller.8800.org/mirror/1/, mirror.netkiller.8800.org

---

2. Squid - Internet Object Cache (WWW proxy cache)

如果apache 安装了gzip,deflate需要开启cache_vary

cache_vary on

2.1. 源码安装

```
wget http://www.squid-cache.org/Versions/v2/2.6/squid-2.6.STABLE13.tar.gz
./configure --prefix=/usr/local/squid-2.6
make all
make install

mkdir -p /usr/local/squid-2.6/var/cache
chown nobody.nobody -R /usr/local/squid-2.6/var/
ln -s /usr/local/squid-2.6 /usr/local/squid
cd /usr/local/squid

./squid -NCd1
```

2.2. debian/ubuntu 安装

$ sudo apt-get install squid

```
$ sudo apt-get install squid3
$ sudo apt-get install squidclient
```

2.3. 配置

查看当前配置参数

当你打开squid.conf文件时，你会头大，因为文件太长了，并且已经启用了部分参数。你可以使用下面命令查看那些参数被开启。

```
$ grep '^[a-z]' squid.conf
```

下面是安装squid3后的默认开启选项

```
$ grep '^[a-z]' squid.conf
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
```

```
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
icp_access deny all
htcp_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
access_log /var/log/squid3/access.log squid
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern (cgi-bin|\?)    0       0%      0
refresh_pattern .               0       20%     4320
icp_port 3130
coredump_dir /var/spool/squid3
```

修改squid.conf之前请做好备份。

```
netkiller@Linux-server:/etc/squid$ sudo cp squid.conf squid.conf.old
netkiller@Linux-server:/etc/squid$ sudo vi squid.conf
```

生成自己的squid.conf文件,这样比较清晰

```
$ grep '^[a-z]' squid.conf.old > squid.conf
```

2.3.1. 正向代理

```
# cat squid.conf
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow all
#http_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
coredump_dir /var/spool/squid3
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0

refresh_pattern -i \.css$       1440 50% 129600 reload-into-ims
refresh_pattern -i \.js$        1440 90% 129600 reload-into-ims
refresh_pattern -i \.hml$       1440 90% 129600 reload-into-ims
refresh_pattern -i \.html$      1440 90% 129600 reload-into-ims
refresh_pattern -i \.shtml$ 1440 90% 129600 reload-into-ims
refresh_pattern -i \.xml$       1440 50% 129600 reload-into-ims
refresh_pattern -i \.jpg$       1440 90% 129600 reload-into-ims
refresh_pattern -i \.png$       1440 90% 129600 ignore-reload
refresh_pattern -i \.gif$       1440 90% 129600 ignore-reload
refresh_pattern -i \.bmp$       1440 90% 129600 ignore-reload

refresh_pattern -i \.mp3$       1440 50% 2880 ignore-reload
refresh_pattern -i \.wmv$       1440 50% 2880 ignore-reload
refresh_pattern -i \.rm$        1440 50% 2880 ignore-reload
refresh_pattern -i \.swf$       1440 50% 2880 ignore-reload
refresh_pattern -i \.mpeg$      1440 50% 2880 ignore-reload

refresh_pattern -i \.doc$               1440    50%     2880      ignore-reload
refresh_pattern -i \.ppt$               1440    50%     2880      ignore-reload
refresh_pattern -i \.xls$               1440    50%     2880      ignore-reload
refresh_pattern -i \.pdf$               1440    50%     2880      ignore-reload
refresh_pattern -i \.rar$       1440    50%     2880      ignore-reload
refresh_pattern -i \.zip$               1440    50%     2880      ignore-reload
refresh_pattern -i \.txt$               1440    50%     2880      ignore-reload

refresh_pattern .               0       20%     4320
```

设置代理服务器

```
declare -x ftp_proxy="192.168.0.1:3128"
declare -x ftps_proxy="192.168.0.1:3128"
declare -x http_proxy="192.168.0.1:3128"
declare -x https_proxy="192.168.0.1:3128"
```

检查Cache工作情况

```
# declare -x http_proxy="172.16.0.5:3128"

# curl -I http://www.qq.com
HTTP/1.0 200 OK
Server: squid/3.0
Date: Wed, 15 Jun 2011 07:54:36 GMT
Content-Type: text/html; charset=GB2312
Vary: Accept-Encoding
Expires: Wed, 15 Jun 2011 08:09:36 GMT
Cache-Control: max-age=900
Vary: Accept-Encoding
X-Cache: HIT from rainny.qq.com
X-Cache: MISS from localhost
X-Cache-Lookup: MISS from localhost:3128
Via: 1.0 localhost (squid/3.1.6)
Proxy-Connection: keep-alive

# curl -I http://www.qq.com
HTTP/1.0 200 OK
Server: squid/3.0
Date: Wed, 15 Jun 2011 07:54:36 GMT
Content-Type: text/html; charset=GB2312
Vary: Accept-Encoding
Expires: Wed, 15 Jun 2011 08:09:36 GMT
Cache-Control: max-age=900
Vary: Accept-Encoding
X-Cache: HIT from rainny.qq.com
Age: 2
X-Cache: HIT from localhost
X-Cache-Lookup: HIT from localhost:3128
Via: 1.0 localhost (squid/3.1.6)
Proxy-Connection: keep-alive
```

当第二次请求同一个URL的时候X-Cache: 由MISS变为HIT，表示已经被缓存

2.3.2. 代理服务器

加入权限认证

```
netkiller@Linux-server:/etc/squid$ sudo htpasswd -c /etc/squid/squid_passwd neo
New password:
Re-type new password:
Adding password for user neo
netkiller@Linux-server:/etc/squid$


netkiller@Linux-server:/etc/squid$ sudo find / -name ncsa_auth
/usr/lib/squid/ncsa_auth

#
# Add this to the auth_param section of squid.conf
#
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd

#
# Add this to the bottom of the ACL section of squid.conf
#
acl ncsa_users proxy_auth REQUIRED
acl business_hours time M T W H F 9:00-17:00

#
# Add this at the top of the http_access section of squid.conf
#
http_access allow ncsa_users business_hours
```

extension_methods REPORT MERGE MKACTIVITY CHECKOUT # subversion

```
extension_methods REPORT MERGE MKACTIVITY CHECKOUT
```

默认端口 3128 如果你不想改squid.conf,可以使用iptables映射

iptables -t nat -A PREROUTING -i eth0 -p tcp -s 0.0.0.0/0.0.0.0 --dport 80 -j REDIRECT --to-ports 3128

设置你的浏览器，并测试

2.3.3. Squid作为反向代理Cache服务器(Reverse Proxy)

这里我们将apache和squid安装在一台服务器上

过程 36.1. 配置步骤

1. 配置Apache监听端口

```
netkiller@Linux-server:~$ cd /etc/apache2/
netkiller@Linux-server:/etc/apache2$ sudo cp ports.conf ports.conf.old
netkiller@Linux-server:/etc/apache2$ sudo vi ports.conf
Listen 8080
Listen 443
netkiller@Linux-server:/etc/apache2$ sudo /etc/init.d/apache2 restart
 * Forcing reload of apache 2.0 web server...
[ ok ]
netkiller@Linux-server:/etc/apache2$
```

restart/reload后测试一下

http://localhost:8080/

2. squid 2.5 之前的版本

```
netkiller@Linux-server:/etc/apache2$ cd ../squid/
netkiller@Linux-server:/etc/squid$ sudo vi squid.conf
http_port 80
httpd_accel_host localhost
httpd_accel_port 8080
httpd_accel_single_host on
httpd_accel_with_proxy on
httpd_accel_uses_host_header off
netkiller@Linux-server:/etc/squid$ sudo /etc/init.d/squid reload
 * Reloading Squid configuration files
   ...done.
netkiller@Linux-server:/etc/squid$
```

squid 2.5 之前的版本

对公网主机220.201.35.11:80做Cache

```
netkiller@Linux-server:/etc/apache2$ cd ../squid/
netkiller@Linux-server:/etc/squid$ sudo vi squid.conf
http_port 80
httpd_accel_host 220.201.35.11
httpd_accel_port 80
httpd_accel_single_host on
httpd_accel_with_proxy on
httpd_accel_uses_host_header off
netkiller@Linux-server:/etc/squid$ sudo /etc/init.d/squid reload
 * Reloading Squid configuration files
   ...done.
netkiller@Linux-server:/etc/squid$
```

多台主机做Cache

```
netkiller@Linux-server:/etc/apache2$ cd ../squid/
netkiller@Linux-server:/etc/squid$ sudo vi squid.conf
http_port 80
httpd_accel_host virtual
httpd_accel_port 8080
httpd_accel_single_host on
httpd_accel_with_proxy on
httpd_accel_uses_host_header off
netkiller@Linux-server:/etc/squid$ sudo /etc/init.d/squid reload
 * Reloading Squid configuration files
```

```
   ...done.
netkiller@Linux-server:/etc/squid$
```

3. squid 2.6之后版本的配置

   localhost

```
http_port 80 defaultsite=localhost vhost transparent
cache_peer localhost parent 8080 0 no-query originserver
```

   其它主机

```
http_port 80 defaultsite=192.168.1.2 vhost transparent
cache_peer 192.168.1.2 parent 80 0 no-query originserver
```

4. 2.7/3.0 版本

```
visible_hostname netkiller.8800.org

http_port 80 accel vhost vport

cache_peer 127.0.0.1 parent 8080 0 no-query originserver name=mainsite
cache_peer 127.0.0.1 parent 8080 0 no-query originserver name=site1
cache_peer_domain mainsite netkiller.8800.org
cache_peer_domain site1 neo.ohyeap.com
http_access allow all
```

5. 注意事项

   ERROR

   The requested URL could not be retrieved

   * Access Denied

   出现上面错说，关闭http_access deny all

   # And finally deny all other access to this proxy

   #http_access deny all

```
#squid.conf
#服务器IP 192.168.1.1
#监听服务器的80端口，透明代理，支持域名和IP的虚拟主机
http_port 192.168.1.1:80 transparent vhost vport

#限制同一IP客户端的最大连接数
acl OverConnLimit maxconn 16
http_access deny OverConnLimit

#防止天涯盗链，转嫁给百度
acl tianya referer_regex -i tianya
http_access deny tianya
deny_info http://www.baidu.com/logs.gif tianya

#防止被人利用为HTTP代理，设置允许访问的IP地址
acl myip dst 192.168.1.1
http_access deny !myip

#防止百度机器人爬死服务器
acl AntiBaidu req_header User-Agent Baiduspider
http_access deny AntiBaidu

#允许本地管理
acl Manager proto cache_object
acl Localhost src 127.0.0.1 192.168.1.1
http_access allow Manager Localhost
http_access deny Manager

#仅仅允许80端口的代理
acl Safe ports port 80 # http
```

```
http_access deny !Safe_ports
http_access allow all

#Squid信息设置
visible_hostname netkiller.8800.org
cache_mgr openunix@163.com

#基本设置
cache_effective_user squid
cache_effective_group squid
tcp_recv_bufsize 65535 bytes

#2.5的反向代理加速配置
#httpd_accel_host 127.0.0.1
#httpd_accel_port 80
#httpd_accel_single_host on
#httpd_accel_uses_host_header on
#httpd_accel_with_proxy on
#2.6的反向代理加速配置
#代理到本机的80端口的服务，仅仅做为原始内容服务器
cache_peer 127.0.0.1 parent 80 0 no-query originserver

#错误文档
error_directory /usr/local/squid/share/errors/Simplify_Chinese

#单台使用，不使用该功能
icp_port 0
```

2.3.4. 代理+反向代理

```
http_port 80 vhost vport defaultsite=220.201.35.11
http_port 88
......
......
acl Manager proto cache_object
acl Localhost src 127.0.0.1/32
acl Safe_ports port 80
acl all src 0.0.0.0/0.0.0.0
acl ACCEL_DST dst 127.0.0.1/32 220.201.35.11/32

acl ACCEL_MODE  myport 80
acl PROXY_MODE  myport 88
# Authentication
auth_param basic realm Please Login
auth_param basic program /usr/local/squid/libexec/ncsa_auth /usr/local/squid/etc/passwd
acl VALIDUSER proxy_auth plan9

# ACCEL MODE
# -----------------------------------------------------------------------------
cache_peer 10.34.2.93 parent 80 0 no-query originserver
cache_peer_access 220.201.35.11 allow ACCEL_MODE
cache_peer_access 220.201.35.11 deny all

http_access allow ACCEL_DST Safe_ports
http_access allow PROXY_MODE VALIDUSER
http_access deny !Safe_ports
http_access allow ACCEL_MODE
http_access allow Manager Localhost
http_access deny all
icp_access deny all
```

2.4. Squid 管理

2.4.1. squidclient

squidclient -- client interface to the squid cache

squidclient 使用方法

1. 运行状态信息： squidclient -p 80 mgr:info
2. 内存使用情况： squidclient -p 80 mgr:mem
3. 磁盘使用情况： squidclient -p 80 mgr:diskd
4. 已经缓存的列表： squidclient -p 80 mgr:objects. use it carefully,it may crash
5. 强制更新url：squidclient -p 80 -m PURGE http://netkiller.8800.org/index.html
6. 查看更多信息：squidclient -h 或者 squidclient -p 80 mgr:

```
debian:~# squidclient -p 80 mgr:squidaio_counts
HTTP/1.0 200 OK
Server: squid/2.6.STABLE5
Date: Sun, 29 Apr 2007 13:27:09 GMT
Content-Type: text/plain
Expires: Sun, 29 Apr 2007 13:27:09 GMT
Last-Modified: Sun, 29 Apr 2007 13:27:09 GMT
X-Cache: MISS from debian.example.org.example.org
X-Cache-Lookup: MISS from debian.example.org.example.org:80
Via: 1.0 debian.example.org.example.org:80 (squid/2.6.STABLE5)
Connection: close

ASYNC IO Counters:
Operation       # Requests
open    0
close   0
cancel  0
write   0
read    0
stat    0
unlink  0
check_callback  0
queue   0
debian:~#
```

squidclient -p 80 mgr:5min

2.4.2. reset cache

重做 cache

```
mkdir /var/spool/squid
chown proxy.proxy -R /var/spool/squid
netkiller@Linux-server:~$ sudo squid -z
netkiller@Linux-server:~$ sudo squid -k reconfigure
```

2.5. 禁止页面被Cache

加到head中

```
  HTML
          <META   HTTP-EQUIV="pragma" CONTENT="no-cache">
          <META   HTTP-EQUIV="Cache-Control" CONTENT="no-cache, must-revalidate">
          <META   HTTP-EQUIV="expires" CONTENT="Wed, 26 Feb 1978 08:21:57 GMT">
  ASP
  <%
          Response.Expires = -1
          Response.ExpiresAbsolute = Now() - 1
          Response.cachecontrol = "no-cache"
  %>
  PHP
          header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
          header("Cache-Control: no-cache, must-revalidate");
          header("Pragma: no-cache");
  JSP
          response.setHeader("Pragma","No-Cache");
          response.setHeader("Cache-Control","No-Cache");
          response.setDateHeader("Expires",   0);
  C#中禁止cache的方法!
          Response.Buffer=true;
          Response.ExpiresAbsolute=System.DateTime.Now.AddSeconds(-1);
          Response.Expires=0;
          Response.CacheControl="no-cache";
```

让浏览器发送no-cache头,只需Ctrl+f5刷新

2.6. Squid 实用案例

2.6.1. Squid Apache/Lighttpd 在同一台服务器上

squid 与 web server 在同一台服务器上,一般情况是squid 监听80端口, web server 监听其它端口(一般是8080)

用户访问时通过80端口访问服务器.不想让用户访问8080.

1. web server

   Apache httpd.conf文件Listen 8080 改成IP:Port,这样8080端口只允许本地访问

```
Listen 127.0.0.1:8080
```

   lighttpd

```
vi /etc/lighttpd/lighttpd.conf
server.port                = 8080
server.bind                = "localhost"

/etc/init.d/lighttpd reload
```

   本地测试

```
curl http://127.0.0.1:8080/
```

2. Squid

```
http_port 80 defaultsite=localhost vhost
cache_peer localhost parent 8080 0 no-query originserver

acl our_networks src 172.16.0.0/16
http_access allow our_networks
http_access allow all
```

   测试

```
curl http://127.0.0.1/
```

   在其它电脑上用IE访问http://your_ip/ 可以看到你的主页

   在其它电脑上用IE访问 http://ip:8080/ 应该是无法访问

3. 另一种方法是使用 iptables 实现

```
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 8080 -j DROP
/sbin/iptables -A INPUT -i lo -p tcp --dport 8080 -j ACCEPT
```

使用 nmap 工具还是可以看到8080存在的.

nmap localhost

```
debian:~# nmap localhost

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-04-29 08:28 EDT
Interesting ports on localhost (127.0.0.1):
Not shown: 1670 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
113/tcp  open  auth
548/tcp  open  afpovertcp
901/tcp  open  samba-swat
953/tcp  open  rndc
8080/tcp open  http-proxy

Nmap finished: 1 IP address (1 host up) scanned in 0.268 seconds
```

2.6.2. 用非 root 用户守护 Squid

squid.conf

```
http_port 3128 transparent vhost vport
```

iptables 做端口重定向

```
iptables -t nat -A PREROUTING -j REDIRECT -p tcp --destination-port 80 --to-ports 3128
```

3. Web page proxy

3.1. Surrogafier

homepage: http://bcable.net/project.php?surrogafier

Surrogafier，安装最简便。只需要下载一个PHP文件，上传到网站的某个目录，然后从浏览器里访问这个PHP脚本，就有了代理页面。

基本配置

```
# Default to simple mode when the page is loaded. [false]
define('DEFAULT_SIMPLE',true);
# Force the page to always be in simple mode (no advanced mode option). [false]
define('FORCE_SIMPLE',false);
# Width for the URL box when in simple mode (CSS "width" attribute). [300px]
define('SIMPLE_MODE_URLWIDTH','300px');

# Default value for tunnel server. []
define('DEFAULT_TUNNEL_PIP','');
# Default value for tunnel port. []
define('DEFAULT_TUNNEL_PPORT','');
# Should the tunnel fields be displayed? "false" value here will force the defaults above
[true]
define('FORCE_DEFAULT_TUNNEL',true);

# Default value for "Persistent URL" checkbox [true]
define('DEFAULT_URL_FORM',true);
# Default value for "Remove Cookies" checkbox [false]
define('DEFAULT_REMOVE_COOKIES',false);
# Default value for "Remove Referer Field" checkbox [false]
define('DEFAULT_REMOVE_REFERER',false);
# Default value for "Remove Scripts" checkbox [false]
define('DEFAULT_REMOVE_SCRIPTS',false);
# Default value for "Remove Objects" checkbox [false]
define('DEFAULT_REMOVE_OBJECTS',false);
# Default value for "Encrypt URLs" checkbox [false]
define('DEFAULT_ENCRYPT_URLS',true);
# Default value for "Encrypt Cookies" checkbox [false]
define('DEFAULT_ENCRYPT_COOKS',true);
```

高级选项

```
#从代理服务器到用户的传输用gzip压缩
define('GZIP_PROXY_USER',true);
# 如果可能，在代理获取的内容也用gzip压缩
define('GZIP_PROXY_SERVER',true);

#每次访问的超时计数，由10秒增加到20秒
define('TIME_LIMIT',20);
#域名解析缓存的时间，由原来的10分钟，改为90分钟
define('DNS_CACHE_EXPIRE',90);
```

3.2. CGIproxy

http://www.jmarshall.com/tools/cgiproxy/

3.3. PHPProxy

http://sourceforge.net/projects/poxy/

```
$ wget http://nchc.dl.sourceforge.net/sourceforge/poxy/poxy-0.5b2.zip
$ unzip poxy-0.5b2.zip
```

http://freshmeat.net/projects/phpproxy/

3.4. BBlocked

http://www.bblocked.org/

3.5. Glype

http://www.glype.com/

3.6. Zelune

---

4. SOCKS

4.1. Socks5

软件包socks5-v1.0r11他的主站已经无法访问,你可以搜一下.

安装

```
./configure --with-threads
make
make install
```

4.2. dante-server - SOCKS (v4 and v5) proxy daemon(danted)

1. install.

```
$ sudo apt-get install dante-server
```

2. configure.

```
$ sudo vim /etc/danted.conf

$ cat danted.conf | sed s/^#.*//g | sed -r /^$/d
logoutput: /tmp/socks.log
internal: eth0 port = 1080
external: 172.16.0.1
method: username none #rfc931
clientmethod: none
user.privileged: proxy
user.notprivileged: nobody
user.libwrap: nobody
client pass {
        from: 0.0.0.0/0 port 1-65535 to: 0.0.0.0/0
}
pass {
        from: 0.0.0.0/0 to: 0.0.0.0/0
        protocol: tcp udp
}
```

3. Once the config is complete. Start/Restart dante socks server:

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

check to see if server is listening on 1080

```
$ netstat -n -a |grep 1080
tcp        0      0 172.16.0.1:1080         0.0.0.0:*               LISTEN
tcp        0      0 172.16.0.1:1080         10.8.0.6:1485           TIME_WAIT
```

4. Make sure the firewall is open.

```
$ grep socks /etc/services
socks           1080/tcp                        # socks proxy server
socks           1080/udp

$ sudo ufw allow socks
Rule added
```

SSL Tunnel

```
internal: 127.0.0.1 port = 1080

ssh -L 1080:localhost:1080 username@yourserver

or

ssh user@server.com -D 1080
# -D is for Dynamic Port Forwarding.
```

4.3. hpsockd - HP SOCKS server

```
$ sudo apt-get install hpsockd
$ sudo cp /usr/share/doc/hpsockd/examples/hpsockd.conf /etc/hpsockd.conf
$ sudo vim /etc/hpsockd.conf
```

部分 III. Web Application

目录

第 37 章 web 服务器排名

http://news.netcraft.com/

第 38 章 LAMP

目录

1. Install

1.1. Quick install apache with aptitude

$ sudo apt-get install apache2$ sudo apt-get install apache2-mpm-worker

```
netkiller@Linux-server:~$ sudo apt-get install apache2
```

1.1.1. command

enable module: a2enmod

enable site: a2ensite

1.1.2. rewrite module

```
$ sudo a2enmod rewrite
```

1.1.3. PHP module

```
$ sudo a2enmod php5
```

1.1.4. deflate module

```
root@neo:/etc/apache2# a2enmod deflate
Module deflate installed; run /etc/init.d/apache2 force-reload to enable.
root@neo:/etc/apache2# /etc/init.d/apache2 force-reload
 * Forcing reload of apache 2.0 web server...                                                    [
ok ]
root@neo:/etc/apache2#
```

1.1.5. ssl module

a2enmod ssl

a2ensite ssl

/etc/apache2/httpd.conf 加入

```
ServerName 220.201.35.11
```

安全模块

```
netkiller@Linux-server:~$ sudo apt-get install libapache2-mod-security

netkiller@Linux-server:/etc/apache2$ sudo vi ports.conf
netkiller@Linux-server:/etc/apache2$ cat ports.conf
Listen 80
Listen 443

NameVirtualHost *
NameVirtualHost *:443


netkiller@Linux-server:/etc/apache2$ sudo apache2-ssl-certificate
or
netkiller@Linux-server:~$ apache2-ssl-certificate -days 365

netkiller@Linux-server:~$ a2enmod ssl
or
netkiller@Linux-server:/etc/apache2/mods-enabled$ sudo ln -s ../mods-available/ssl.conf
netkiller@Linux-server:/etc/apache2/mods-enabled$ sudo ln -s ../mods-available/ssl.load

netkiller@Linux-server:/etc/apache2/sites-enabled$ sudo mkdir ssl/
netkiller@Linux-server:/etc/apache2/sites-enabled$ sudo cp netkiller woodart ssl/


netkiller@Linux-server:/etc/apache2/mods-enabled$ sudo /etc/init.d/apache2 reload
 * Reloading apache 2.0 configuration...                                      [ ok ]
netkiller@Linux-server:/etc/apache2/mods-enabled$
```

1.1.6. VirtualHost

VirtualHost 虚拟主机

```
netkiller@Linux-server:/etc/apache2/sites-available$ sudo vi woodart

#NameVirtualHost neo.6600.org
<VirtualHost 220.201.35.11>
        ServerAdmin openx@163.com

        DocumentRoot /home/netkiller/www
        ServerName neo.6600.org
        ServerAlias www.neo.6600.org
        <Directory /home/netkiller/www>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
                # Uncomment this directive is you want to see apache2's
                # default start page (in /apache2-default) when you go to /
                #RedirectMatch ^/$ /apache2-default/
        </Directory>

#       ScriptAlias /cgi-bin/ /home/netkiller/www/
#       <Directory "/home/netkiller/www">
#               AllowOverride None
#               Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
#               Order allow,deny
#               Allow from all
#       </Directory>

        ErrorLog /var/log/apache2/neo.error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
#       LogLevel warn

        CustomLog /var/log/apache2/neo.access.log combined
#       ServerSignature On
```

```
</VirtualHost>

netkiller@Linux-server:/etc/apache2/sites-available$ sudo apache2 -k restart
```

1.1.7. ~userdir module - /public_html

~web环境

```
netkiller@Linux-server:~$ mkdir public_html
netkiller@Linux-server:~$ cd public_html/
netkiller@Linux-server:~/public_html$
netkiller@Linux-server:~/public_html$ echo helloworld>index.html
netkiller@Linux-server:~/public_html$ ls
index.html
```

http://xxx.xxx.xxx.xxx/~netkiller/

1.2. PHP 5

$ sudo apt-get install php5

```
netkiller@Linux-server:~$ sudo apt-get install php5
```

pgsql模块

```
netkiller@Linux-server:~$ sudo apt-get install php5-pgsql

netkiller@Linux-server:~$sudo cp /usr/lib/php5/20051025/pgsql.so /etc/php5/apache2/
```

php5-gd - GD module for php5

$ sudo apt-get install php5-gd

```
netkiller@Linux-server:~$ apt-cache search gd
libgdbm3 - GNU dbm database routines (runtime version)
libgd2-xpm - GD Graphics Library version 2
php5-gd - GD module for php5
pnm2ppa - PPM to PPA converter
postgresql-doc-8.1 - documentation for the PostgreSQL database management system
libruby1.8 - Libraries necessary to run Ruby 1.8
ruby1.8 - Interpreter of object-oriented scripting language Ruby 1.8
klogd - Kernel Logging Daemon
sysklogd - System Logging Daemon
upstart-logd - boot logging daemon
netkiller@Linux-server:~$ sudo apt-get install php5-gd

netkiller@Linux-server:~$
```

1.3. Compile and then install Apache

1.3.1. Apache 安装与配置

configure

--with-mpm=worker 进程,线程混合方式效率提高不少

--enable-modules='dir mime' 没有它就找不到index.*文件

--enable-rewrite=shared Rewrite用于表态化

--enable-expires=shared 禁止页面被 cache

--enable-authz_host=shared Order权限

--enable-setenvif=shared

--enable-log_config=shared 日志格式

--enable-speling=shared 允许自动修正拼错的URL

--enable-deflate=shared 压缩传送

--enable-mods-shared='cache file-cache disk-cache mem-cache proxy proxy-ajp proxy-balancer' 代理和缓存

```
tar zxvf httpd-2.2.4.tar.gz
cd httpd-2.2.4
./configure --prefix=/usr/local/httpd-2.2.4 \
--with-mpm=worker \
--enable-modules='dir mime' \
--enable-rewrite=shared \
--enable-authz_host=shared \
--enable-alias=shared \
--enable-setenvif=shared \
--enable-log_config=shared \
--enable-speling=shared \
--enable-filter=shared \
--enable-deflate=shared \
--enable-headers=shared \
--enable-expires=shared \
--enable-mods-shared='cache file-cache disk-cache mem-cache proxy proxy-ajp proxy-balancer' \
--disable-include \
--disable-actions \
--disable-alias \
--disable-asis \
--disable-autoindex \
--disable-auth_basic \
--disable-authn_file \
--disable-authn_default \
--disable-authz_groupfile \
--disable-authz_user \
--disable-authz_default \
--disable-cgi \
--disable-cgid \
--disable-env \
--disable-negotiation \
--disable-status \
--disable-userdir
```

make; make install

启动

```
ln -s /usr/local/httpd-2.2.4/ /usr/local/apache

/usr/local/httpd/bin/apachectl start
```

1.3.2. 优化编译条件

```
# vim server/mpm/worker/worker.c

# define DEFAULT_SERVER_LIMIT 256
# define MAX_SERVER_LIMIT 20000
# define DEFAULT_THREAD_LIMIT 512
# define MAX_THREAD_LIMIT 20000
```

1.3.3. PHP

过程 38.1. 安装PHP

1. 第一步

```
cd /usr/local/src
wget http://cn2.php.net/get/php-5.3.0.tar.bz2/from/cn.php.net/mirror
tar jxvf php-5.3.0.tar.bz2
cd php-5.3.0
```

2. 第二步

```
./configure --prefix=/usr/local/php-5.3.0 \
--with-config-file-path=/usr/local/php-5.3.0/etc \
--with-apxs2=/usr/local/apache/bin/apxs \
--with-curl \
--with-gd \
--with-ldap \
--with-snmp \
--enable-zip \
--enable-exif \
--with-libxml-dir \
--with-mysql \
--with-mysqli \
--with-pdo-mysql \
--with-pdo-pgsql

make
make test
make install
```

a. 建立符号连接

```
ln -s /usr/local/php-5.3.0 /usr/local/php
```

b. php.ini

```
cp php.ini-dist /usr/local/php/etc/php.ini
```

c. conf/httpd.conf

```
AddType application/x-httpd-php .php .phtml
AddType application/x-httpd-php-source .phps
```

reload apache

3. 最后一步

phpinfo() 测试文件复杂到apache目录

例 38.1. index.php

```
<?php phpinfo(); ?>
```

--with-snmp

redhat as4 启用 --with-snmp 需要安装下面包

```
rpm -i elfutils-libelf-devel-0.97.1-3.i386.rpm
rpm -i elfutils-devel-0.97.1-3.i386.rpm
```

```
rpm -i beecrypt-devel-3.1.0-6.i386.rpm
rpm -i net-snmp-devel-5.1.2-11.EL4.7.i386.rpm
```

1.3.4. Automation Installing

例 38.2. autolamp.sh

```
#!/bin/bash
HTTPD_SRC=httpd-2.2.15.tar.gz
PHP_SRC=php-5.2.13.tar.gz
MYSQL_SRC='mysql-5.1.45.tar.gz'
MYSQL_LIBS_SRC='mysql-5.1.45-linux-x86_64-glibc23.tar.gz'

SRC_DIR=$(pwd)
HTTPD_DIR=${HTTPD_SRC%%.tar.gz}
PHP_DIR=${PHP_SRC%%.tar.*}
MYSQL_DIR=${MYSQL_SRC%%.tar.*}
MYSQL_LIBS_DIR=${MYSQL_LIBS_SRC%%.tar.*}

function clean(){
        rm -rf $HTTPD_DIR
        rm -rf $PHP_DIR
        rm -rf $MYSQL_DIR
        rm -rf $MYSQL_LIBS_DIR
}
function mysql(){
rm -rf $MYSQL_DIR
tar zxf $MYSQL_SRC
cd $MYSQL_DIR
./configure \
--prefix=/usr/local/$MYSQL_DIR \
--with-mysqld-user=mysql \
--with-unix-socket-path=/tmp/mysql.sock \
--with-charset=utf8 \
--with-collation=utf8_general_ci \
--with-pthread \
--with-mysqld-ldflags \
--with-client-ldflags \
--with-openssl \
--without-docs \
--without-debug \
--without-ndb-debug \
--without-bench
#-–without-isam
#--without-innodb \
#--without-ndbcluster \
#--without-blackhole \
#--without-ibmdb2i \
#--without-federated \
#--without-example \
#--without-comment \
#--with-extra-charsets=gbk,gb2312,utf8 \

#--localstatedir=/usr/local/mysql/data
#--with-extra-charsets=all
make clean
make && make install
cd ..
/usr/local/$MYSQL_DIR/bin/mysql_install_db
}
function httpd(){
rm -rf $HTTPD_DIR
tar zxf $HTTPD_SRC
cd $HTTPD_DIR
./configure --prefix=/usr/local/$HTTPD_DIR \
--with-mpm=worker \
--enable-so \
--enable-mods-shared=all \
--disable-authn_file \
--disable-authn_default \
--disable-authz_groupfile \
--disable-authz_user \
--disable-authz_default \
--disable-auth_basic \
--disable-include \
--disable-env \
--disable-status \
--disable-autoindex \
--disable-asis \
--disable-cgi \
--disable-cgid \
--disable-negotiation \
--disable-actions \
--disable-userdir \
--disable-alias

make clean
make && make install
cd ..
}
function php(){
rm -rf $MYSQL_LIBS_DIR
tar zxf $MYSQL_LIBS_SRC
rm -rf $PHP_DIR
tar zxf $PHP_SRC
```

```
cd $PHP_DIR

./configure --prefix=/usr/local/$PHP_DIR \
--with-config-file-path=/usr/local/$PHP_DIR/etc \
--with-apxs2=/usr/local/$HTTPD_DIR/bin/apxs \
--with-curl \
--with-gd \
--with-jpeg-dir=/usr/lib64 \
--with-iconv \
--with-zlib-dir \
--with-pear \
--with-libxml \
--with-dom \
--with-xmlrpc \
--with-openssl \
--with-mysql=/usr/local/mysql-5.1.45-linux-x86_64-glibc23 \
--with-mysqli \
--with-pdo-mysql \
--enable-memcache \
--enable-zip \
--enable-sockets \
--enable-soap \
--enable-mbstring \
--enable-magic-quotes \
--enable-inline-optimization \
--enable-xml

#make && make test && make install
make &&  make install
cp /usr/local/src/$PHP_DIR/php.ini-dist /usr/local/$PHP_DIR/php.ini
}
function depend(){
        yum install gcc gcc-c++ -y
        yum install -y libxml2-devel libxslt-devel
        yum install curl-devel -y
        yum install gd-devel libjpeg-devel libpng-devel -y
        yum install ncurses-devel -y
        yum install mysql-devel -y
        yum install libevent-devel -y
}
function java(){
        #yum install java-1.6.0-openjdk -y
        chmod +x jdk-6u20-linux-x64.bin
        ./jdk-6u20-linux-x64.bin
        mv jdk1.6.0_20 ..
        ln -s /usr/local/jdk1.6.0_20 /usr/local/java
}
function memcached(){
        MEMCACHED_PKG=memcached-1.4.5.tar.gz
        MEMCACHED_SRC=memcached-1.4.5
        rm -rf $MEMCACHED_SRC
        tar zxf $MEMCACHED_PKG
        cd $MEMCACHED_SRC
        ./configure --prefix=/usr/local/memcached-1.4.5
        make && make install
}
# See how we were called.
case "$1" in
  clean)
        clean
        ;;
  httpd)
        httpd
        ;;
  php)
        php
        ;;
  mysql)
        if [ -f $0 ] ; then
                mysql
        fi
        ;;
  depend)
        depend
        ;;
  java)
        java
        ;;
  memcached)
        memcached
        ;;
  all)
        clean

        echo ##################################################
        echo # $MYSQL_DIR Installing...
        echo ##################################################
        mysql

        echo ##################################################
        echo # $HTTPD_DIR Installing...
        echo ##################################################
        httpd

        echo ##################################################
        echo # $PHP_DIR Installing...
        echo ##################################################
        php

        ln -s /usr/local/$HTTPD_DIR /usr/local/apache
        ln -s /usr/local/$MYSQL_DIR /usr/local/mysql
        ln -s /usr/local/$PHP_DIR /usr/local/php

        clean
        ;;
```

```
  *)
        echo $"Usage: $0 {httpd|php|mysql|all|clean}"
        RETVAL=2
        ;;
esac

exit $RETVAL
```

1.4. XAMPP

1.4.1. XAMPP for Linux

http://www.apachefriends.org/en/xampp-linux.html

install

```
tar xvfz xampp-linux-1.7.3a.tar.gz -C /opt
```

start

```
/opt/lampp/lampp start
```

stop

```
/opt/lampp/lampp stop
```

remove

```
rm -rf /opt/lampp
```

1.4.2. php5

```
./lampp php5
XAMPP: PHP 5.3.8 already active.

./lampp startapache
XAMPP: Starting Apache with SSL (and PHP5)...

./lampp startmysql
XAMPP: Starting MySQL...
```

2. Module

```
模块的做用如下:
mod_access        提供基于主机的访问控制命令
mod_actions 能够运行基于MIME类型的CGI脚本或HTTP请求方法
mod_alias         能执行URL重定向服务
mod_asis          使文档能在没有HTTP头标的情况下被发送到客户端
mod_auth          支持使用存储在文本文件中的用户名、口令实现认证
mod_auth_dbm 支持使用DBM文件存储基本HTTP认证
mod_auth_mysql 支持使用MySQL数据库实现基本HTTP认证
mod_auth_anon 允许以匿名方式访问需要认证的区域
mod_auth_external支持使用第三方认证
mod_autoindex 当缺少索引文件时，自动生成动态目录列表
mod_cern_meta 提供对元信息的支持
mod_cgi           支持CGI
mod_dir           能够重定向任何对不包括尾部斜杠字符命令的请求
mod_env           使你能够将环境变量传递给CGI或SSI脚本
mod_expires 让你确定Apache在服务器响应请求时如何处理Expires
mod_headers 能够操作HTTP应答头标
mod_imap          提供图形映射支持
mod_include 使支持SSI
mod_info          对服务器配置提供了全面的描述
mod_log_agent 允许在单独的日志文件中存储用户代理的信息
mod_log_config 支持记录日志
mod_log_referer 提供了将请求中的Referer头标写入日志的功能
mod_mime 用来向客户端提供有关文档的元信息
mod_negotiation 提供了对内容协商的支持
mod_setenvif 使你能够创建定制环境变量
mod_speling 使你能够处理含有拼写错误或大小写错误的URL请求
mod_status        允许管理员通过WEB管理Apache
mod_unique_id 为每个请求提供在非常特殊的条件下保证是唯一的标识
```

常用模块

```
LoadModule dir_module          modules/mod_dir.so
LoadModule mime_module         modules/mod_mime.so
LoadModule expires_module      modules/mod_expires.so
LoadModule config_log_module   modules/mod_log_config.so
LoadModule alias_module        modules/mod_alias.so
LoadModule rewrite_module      modules/mod_rewrite.so
LoadModule access_module       modules/mod_access.so
LoadModule auth_module         modules/mod_auth.so
```

2.1. Output a list of modules compiled into the server.

This will not list dynamically loaded modules included using the LoadModule directive.

```
[root@development bin]# httpd -l
Compiled in modules:
  core.c
  worker.c
  http_core.c
  mod_so.c
```

2.2. Core

2.2.1. Listen

绑定多个IP

```
#Listen 80
Listen 192.168.3.40:80
```

```
Listen 192.168.4.40:80
Listen 192.168.5.40:80
```

2.2.2. Filesystem and Webspace

ref: http://httpd.apache.org/docs/2.2/en/sections.html

Filesystem Containers

```
<Directory /var/web/dir1>
        Options +Indexes
</Directory>

<Files private.html>
        Order allow,deny
        Deny from all
</Files>

<Directory /var/web/dir1>
        <Files private.html>
                Order allow,deny
                Deny from all
        </Files>
</Directory>
```

Webspace Containers

```
<LocationMatch ^/private>
        Order Allow,Deny
        Deny from all
</LocationMatch>
```

Wildcards and Regular Expressions

```
A non-regex wildcard section that changes the configuration of all user directories could look
as follows:

<Directory /home/*/public_html>
Options Indexes
</Directory>
Using regex sections, we can deny access to many types of image files at once:

<FilesMatch \.(?i:gif|jpe?g|png)$>
Order allow,deny
Deny from all
</FilesMatch>
```

2.2.2.1. Options

```
<DirectoryMatch (/var/www/logs|/var/www/logs/*)>
        Options FollowSymLinks MultiViews Indexes

        DirectoryIndex index.html

        AllowOverride AuthConfig
        Order Allow,Deny
        Allow From All

        AuthName "Logs Access"
        AuthType Basic
        AuthUserFile /etc/nagios3/htpasswd.users
        require valid-user
</DirectoryMatch>
```

1. None是禁止所有

2. Indexes 当没有index.html 的时候列出目录

3. FollowSymLinks 允许符号连接，可以通过符号连接跨越DocumentRoot

4. AllowOverride 定义是否允许各个目录用目录中的.htaccess覆盖这里设定的Options

5.

2.2.3. Etag

```
<Directory /www>
        <Files ~ "\.(gif|jpe?g|png|html|css|js)$">
                FileETag INode MTime Size
        </Files>
</Directory>
```

2.2.4. 隐藏 Apache 版本信息

```
ServerTokens ProductOnly
ServerSignature Off
```

2.3. worker

worker

```
# Server-pool management (MPM specific)
Include conf/extra/httpd-mpm.conf
```

conf/extra/httpd-mpm.conf

mpm_worker_module

```
<IfModule mpm_worker_module>
    ServerLimit          64
    ThreadLimit          256
    StartServers         8
    MaxClients           15000
    MinSpareThreads      100
    MaxSpareThreads      200
    ThreadsPerChild      256
    MaxRequestsPerChild   10000
</IfModule>
```

```
ServerLimit 默认是16，它决定系统最多启动几个httpd进程。
ThreadLimit 默认是64，
ThreadsPerChild* ServerLimit=系统支持的最大并发。
MaxClients<ThreadsPerChild* ServerLimit，MaxClients如果大于400将被限制在400.
400只是理论最大并发，实际并发就是MaxClients的值。
理论并发有什么用我不知道。


指令说明：
        StartServers：设置服务器启动时建立的子进程数量。因为子进程数量动态的取决于负载的轻重,所有一般没有必要调整这个参数。
        ServerLimit：服务器允许配置的进程数上限。只有在你需要将MaxClients和ThreadsPerChild设置成需要超过默认值16个子进程的时候才需要使用这个指令。不要将该指令的值设置的比MaxClients 和ThreadsPerChild需要的子进程数量高。修改此指令的值必须完全停止服务后再启动才能生效，以restart方式重启动将不会生效。
        ThreadLimit：设置每个子进程可配置的线程数ThreadsPerChild上限,该指令的值应当和ThreadsPerChild可能达到的最大值保持一致。修改此指令的值必须完全停止服务后再启动才能生效，以restart方式重启动将不会生效。
        MaxClients：用于伺服客户端请求的最大接入请求数量（最大线程数）。任何超过MaxClients限制的请求都将进入等候队列。默认值是"400"，16 (ServerLimit)乘以25(ThreadsPerChild)的结果。因此要增加MaxClients的时候，你必须同时增加 ServerLimit的值。笔者建议将初始值设为(以Mb为单位的最大物理内存/2),然后根据负载情况进行动态调整。比如一台4G内存的机器，那么初始值就是4000/2=2000。
        MinSpareThreads：最小空闲线程数,默认值是"75"。这个MPM将基于整个服务器监视空闲线程数。如果服务器中总的空闲线程数太少，子进程将产生新的空闲线程。
        MaxSpareThreads：设置最大空闲线程数。默认值是"250"。这个MPM将基于整个服务器监视空闲线程数。如果服务器中总的空闲线程数太多，子进程将杀死多余的空闲线程。MaxSpareThreads的取值范围是有限制的。Apache将按照如下限制自动修正你设置的值：worker要求其大于等于 MinSpareThreads加上ThreadsPerChild的和。
        ThreadsPerChild：每个子进程建立的线程数。默认值是25。子进程在启动时建立这些线程后就不再建立新的线程了。
```

```
每个子进程所拥有的所有线程的总数要足够大，以便可以处理可能的请求高峰。
        MaxRequestsPerChild：设置每个子进程在其生存期内允许伺服的最大请求数量。到达MaxRequestsPerChild的限制后，子进程将会结束。如果MaxRequestsPerChild为"0"，子进程将永远不会结束。将MaxRequestsPerChild设置成非零值有两个好处：可以防止(偶然的)内存泄漏无限进行而耗尽内存；
给进程一个有限寿命，从而有助于当服务器负载减轻的时候减少活动进程的数量。
如果设置为非零值，笔者建议设为10000-30000之间的一个值。
          公式：
          ThreadLimit >= ThreadsPerChild
          MaxClients <= ServerLimit * ThreadsPerChild 必须是ThreadsPerChild的倍数
          MaxSpareThreads >= MinSpareThreads+ThreadsPerChild
```

2.4. Apache Log

2.4.1. LogLevel

日志级别

语法：LogLevel level

```
可以选择下列level，依照重要性降序排列：
emerg   紧急(系统无法使用)
alert   必须立即采取措施
crit     致命情况
error   错误情况
warn     警告情况
notice   一般重要情况
info    普通信息
debug   调试信息
```

```
LogLevel crit
```

2.4.2. LogFormat

分割log日志文件

```
<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    #LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %{email}C
%{nickname}C" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog logs/access_log common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog logs/access_log combined

    #CookieLog logs/cookie_log
</IfModule>
```

2.4.3. Compressed

```
# compressed logs
$ CustomLog "|/usr/bin/gzip -c >> /var/log/access_log.gz" common
```

2.4.4. rotatelogs - Piped logging program to rotate Apache logs

rotatelogs是一个配合Apache管道日志功能使用的简单程序。举例：

```
rotatelogs logfile [ rotationtime [ offset ]] | [ filesizeM ]

选项
logfile
它加上基准名就是日志文件名。如果logfile中包含'%'，则它会被视为用于的strftime(3)的格式字串；否则，它会被自动加上以秒为单位的.nnnnnnnnnn后缀。这两种格式都表示新的日志开始使用的时间。
rotationtime
日志文件回卷的以秒为单位的间隔时间
offset
相对于UTC的时差的分钟数。如果省略，则假定为0，并使用UTC时间。比如，要指定UTC时差为-5小时的地区的当地时间，则此参数应为-300。
filesizeM
指定回卷时以兆字节为单位的后缀字母M的文件大小，而不是指定回卷时间或时差。

下列日志文件格式字串可以为所有的strftime(3)实现所支持，见各种扩展库对应的strftime(3)的手册。
%A 星期名全称(本地的)
%a 3个字符的星期名(本地的)
%B 月份名的全称(本地的)
%b 3个字符的月份名(本地的)
%c 日期和时间(本地的)
%d 2位数的一个月中的日期数
%H 2位数的小时数(24小时制)
%I 2位数的小时数(12小时制)
%j 3位数的一年中的日期数
%M 2位数的分钟数
%m 2位数的月份数
%p am/pm 12小时制的上下午(本地的)
%S 2位数的秒数
%U 2位数的一年中的星期数(星期天为一周的第一天)
%W 2位数的一年中的星期数(星期一为一周的第一天)
%w 1位数的星期几(星期天为一周的第一天)
%X 时间 (本地的)
%x 日期 (本地的)
%Y 4位数的年份

CustomLog "|bin/rotatelogs /var/logs/logfile 86400" common
此配置会建立文件"/var/logs/logfile.nnnn"，其中的nnnn是名义上的日志启动时的系统时间(此时间总是滚动时间的倍数，可以用于cron脚本的同步)。在滚动时间到达时(在此例中是24小时以后)，会产生一个新的日志。

CustomLog "|bin/rotatelogs /var/logs/logfile 5M" common
此配置会在日志文件大小增长到5兆字节时滚动该日志。

ErrorLog "|bin/rotatelogs /var/logs/errorlog.%Y-%m-%d-%H_%M_%S 5M"
此配置会在错误日志大小增长到5兆字节时滚动该日志，日志文件名后缀会按照如下格式创建：errorlog.YYYY-mm-dd-HH_MM_SS

ErrorLog "| /usr/local/apache/bin/rotatelogs /www/logs/www.example.com/error_%Y_%m_%d_log 86400 480"
CustomLog "| /usr/local/apache/bin/rotatelogs /www/logs/www.example.com/access_%Y_%m_%d_log 86400 480" common

CustomLog "|/usr/local/httpd/bin/rotatelogs /www/logs/www.example.com/access.%Y-%m-%d.log 86400 480" combined
```

2.4.5. cronolog

cronolog

```
cd /usr/local/src/
wget http://cronolog.org/download/cronolog-1.6.2.tar.gz
tar zxvf cronolog-1.6.2.tar.gz
cd cronolog-1.6.2
./configure --prefix=/usr/local/cronolog
make
make install
```

CustomLog "|/usr/local/cronolog/sbin/cronolog /opt/apache/logs/access_log.%Y%m%d" combined

2.4.6. 日志合并

合并多个服务器的日志文件（如log1、log2、log3），并输出到log_all中的方法是：

```
 $ sort -m -t " " -k 4 -o log_all log1 log2 log3
```

2.4.7. 日志归档

```
30 4 * * * /usr/bin/gzip -f /www/logs/access.`date -d yesterday +%Y-%m-%d`.log
```

2.4.8. logger

https://www.sit.auckland.ac.nz/Logging_to_syslog_with_Apache

```
Logging to syslog with Apache

First you will need to install syslog-ng. This is the logging server that will send the log
data to the syslog box.

apt-get update && apt-get install syslog-ng
syslog-ng uses a socket device to accept data from apache or whatever program is creating the
logs.

Use the configuration here: Syslog-ng default config.

The first part indicates what the socket will be called and where it will live. The second part
tells syslog-ng where to send the collected data. The restart syslog-ng (/etc/init.d/syslog-ng
restart)l.

Configure apache's logging

Add these directives to send apache's logs via a socket to syslog

CustomLog "|/usr/bin/logger -s -t 'monitor.cs.auckland.ac.nz' -p info -u
/var/log/apache_log.socket" Combined
ErrorLog "|/usr/bin/logger -s -t 'monitor.cs.auckland.ac.nz' -p err -u
/var/log/apache_log.socket"
Apache will then use the logger program to send data to syslog. /var/log/apache_log.socket
refers to the device that syslog-ng has created. Data sent to this device is sent over the
network to the main syslog box.

Troubleshooting

It seems that apache 2.0.54-5 does not like logging to a file and to a process at the same
time. In this case log entries will become re-ordered or missed out. You can use the test
scripts below to check if this is happening.

Testing

Here are some useful scripts that can help with testing to make sure the logging is working as
expected.

You can simulate http accesses using lynx with this command:

watch lynx -source http://monitor.cs.auckland.ac.nz/
Which will make a http request every two seconds. Or, for a better test:

for i in `seq 1 100`; do lynx -source http://monitor.cs.auckland.ac.nz/$i;sleep 3;done
The result of this test is a sequence of log entires from 1 to 100. If entries are missing or
in the wrong order, you know there is a problem.
```

2.4.9. other

```
CustomLog "|/usr/bin/your_script" Combined
ErrorLog "|/usr/bin/your_script"
```

2.5. mod_access

```
<Directory /www>
  Order Allow,Deny
</Directory>

<Directory /www>
        Order Deny,Allow
        Deny from all
        Allow from apache.org
</Directory>


<Directory /www>
        Order Allow,Deny
        Allow from apache.org
        Deny from foo.apache.org
</Directory>
```

```
A (partial) domain-name
Example: Allow from apache.org

A full IP address
Example: Allow from 10.1.2.3

A partial IP address
Example: Allow from 10.1

A network/netmask pair
Example: Allow from 10.1.0.0/255.255.0.0

A network/nnn CIDR specification
Example: Allow from 10.1.0.0/16
```

```
<DirectoryMatch (/usr/share/nagios3/htdocs|/usr/lib/cgi-bin/nagios3|/etc/nagios3/stylesheets)>
        Options FollowSymLinks

        DirectoryIndex index.html

        AllowOverride AuthConfig
        Order Allow,Deny
        Allow From All

        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /etc/nagios3/htpasswd.users
        # nagios 1.x:
        #AuthUserFile /etc/nagios/htpasswd.users
        require valid-user
</DirectoryMatch>
```

2.6. VirtualHost

conf/extra/httpd-vhosts.conf

or

/etc/httpd/conf.d/vhost.conf

```
NameVirtualHost *:80

<VirtualHost *:80>
    ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot "/usr/local/httpd-2.2.14/docs/dummy-host.example.com"
    ServerName dummy-host.example.com
    ServerAlias www.dummy-host.example.com
    ErrorLog "logs/dummy-host.example.com-error_log"
    CustomLog "logs/dummy-host.example.com-access_log" common
</VirtualHost>
```

2.6.1. ServerName/ServerAlias

```
ServerName dummy-host.example.com
ServerAlias www.dummy-host.example.com
```

2.6.2. rotatelogs

```
CustomLog "|/usr/local/httpd/bin/rotatelogs /www/logs/men.xiu.com/access.%Y-%m-%d.log 86400 480"
combined
ErrorLog "|/usr/local/httpd/bin/rotatelogs /www/logs/men.xiu.com/error.%Y-%m-%d.log 86400 480"
```

2.7. Alias / AliasMatch

```
Alias /image /ftp/pub/image
AliasMatch ^/icons(.*) /usr/local/apache/icons$1
```

```
cat /etc/httpd/conf.d/logs.conf

Alias /logs "/www/logs"

<Directory "/www/logs">
   Options FollowSymLinks MultiViews Indexes
   AllowOverride None
   Order allow,deny
   Allow from all
#  Order deny,allow
#  Deny from all
#  Allow from 127.0.0.1
#   AuthName "Logs Access"
#   AuthType Basic
#   AuthUserFile /etc/httpd/htpasswd.users
#   Require valid-user
</Directory>
```

2.8. Redirect / RedirectMatch

Redirect

```
Redirect /service http://foo2.example.com/service
Redirect permanent /one http://example.com/two
Redirect 303 /three http://example.com/other
```

RedirectMatch

```
RedirectMatch (.*)\.gif$ http://www.domain.com$1.jpg
```

```
<VirtualHost *:80>
     ServerName www.old.com
     DocumentRoot /path/to/htdocs
     ......
     <Directory "/path/to/htdocs">
         RedirectMatch ^/(.*)$ http://www.new.com/$1
     </Directory>
</VirtualHost>
```

2.9. Rewrite

Rewrite 需要 AllowOverride All

```
<Directory "/www">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.2/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    #AllowOverride None
    AllowOverride All

    #
    # Controls who can get stuff from this server.
    #
    Order allow,deny
    Allow from all
```

```
</Directory>
```

2.9.1. R=301

```
RewriteEngine on
RewriteCond %{HTTP_HOST} ^x.x.x.x [NC]
RewriteRule ^/(.*)$ http://www.example.com/$1 [L,R=301]
```

例 38.3. R=301

```
<VirtualHost *:80>
        ServerAdmin webmaster@example.com
        ServerName www.example.com
        ServerAlias www.second.com

    RewriteEngine On
    RewriteCond %{HTTP_HOST} ^www.example.com [NC]
    RewriteRule ^/(.*)$ http://www.other.com/$1 [L,R=301]
    RewriteCond %{HTTP_HOST} ^www.second.com [NC]
    RewriteRule ^/(.*)$ http://www.other.com/$1 [L,R=301]
</VirtualHost>
```

2.9.2. Rewrite + JkMount

JkMount 与 Rewrite 同时使用时

RewriteRule ^/communtiy/top/(.*)$ /community.do?method=activeContent&id=$1 [PT]

后面用[PT]

2.9.3. Apache redirect domain.com to www.domain.com

```
$ vi .htaccess
RewriteEngine on
RewriteCond %{HTTP_HOST} ^domain\.com
RewriteRule ^(.*)$ http://www.domain.com/$1 [R=permanent,L]
```

2.9.4. 正则匹配扩展名

```
<VirtualHost *:80>
    ServerAdmin webmaster@example.com
    DocumentRoot "/www/www.example.com/images"
    ServerName images.example.com
    RewriteEngine On
    RewriteRule ^(.+)(jpg|gif|bmp|jpeg|ico|png|css)$ http://images.other.com/$1$2 [R]
    ErrorLog "logs/images.example.com-error.log"
</VirtualHost>
```

```
<VirtualHost *:80>
        ServerAdmin webmaster@example.com
        ServerName images.example.com
        RewriteEngine On
        RewriteCond %{HTTP_HOST} ^images.example.com [NC]
        RewriteRule ^/(.*) http://images.other.com/$1 [L]
        CustomLog "|/usr/local/httpd/bin/rotatelogs /www/logs/images/access.%Y-%m-%d.log 100M"
common
</VirtualHost>
```

2.10. Proxy

```
ProxyRequests Off

<Proxy *>
        Order deny,allow
        Allow from all
</Proxy>
ProxyPass / http://your.domain.com:8080/
ProxyPassReverse / http://your.domain.com:8080/
```

2.10.1. Reverse proxy

/etc/httpd/conf.d/rails.conf

```
Listen 8080
ProxyRequests Off
<Proxy balancer://cluster>
        BalancerMember http://127.0.0.1:3001
        BalancerMember http://127.0.0.1:3002
        BalancerMember http://127.0.0.1:3003
        BalancerMember http://127.0.0.1:3004
        BalancerMember http://127.0.0.1:3005
</Proxy>

<VirtualHost *:8080>
        ServerName www.example.com:8080
        DocumentRoot /var/www/project/public
        ProxyPass /images !
        ProxyPass /stylesheets !
        ProxyPass /javascripts !
        ProxyPass / balancer://cluster/
        ProxyPassReverse / balancer://cluster/
        ProxyPreserveHost on
</VirtualHost>
```

2.11. Deflate

mod_deflate

httpd.conf中中加入下列语句:

```
<IfModule mod_deflate.c>
        SetOutputFilter DEFLATE
        DeflateCompressionLevel 9
        AddOutputFilterByType DEFLATE text/html text/plain text/xml application/x-httpd-php
        AddOutputFilter DEFLATE txt css js
        SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
        SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
        SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
        DeflateFilterNote Input input_info
        DeflateFilterNote Output output_info
        DeflateFilterNote Ratio ratio_info
        LogFormat '"%r" %{output_info}n/%{input_info}n (%{ratio_info}n%%)' deflate
        CustomLog logs/deflate_log.log deflate
</IfModule>
```

对目录/usr/local/apache/htdocs有效

```
<Directory "/usr/local/apache/htdocs">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
        SetOutputFilter DEFLATE
        DeflateCompressionLevel 9
        AddOutputFilterByType DEFLATE text/html text/plain text/xml application/x-httpd-php
        AddOutputFilter DEFLATE txt css js
```

```
        SetEnvIfNoCase Request_URI \
        \.(?:gif|jpe?g|png)$ no-gzip dont-vary
</Directory>
```

```
<Location />
        AddOutputFilterByType DEFLATE text/html text/plain text/xml text/css text/javascript
        AddOutputFilterByType DEFLATE application/javascript application/x-javascript
application/x-httpd-php
        AddOutputFilter DEFLATE txt css js
        SetOutputFilter DEFLATE
</Location>
```

Log定义

```
DeflateFilterNote Input instream   # 未压缩前
DeflateFilterNote Output outstream # 压缩后
DeflateFilterNote Ratio ratio   # 百分比
LogFormat '"%r" %{outstream}n/%{instream}n (%{ratio}n%%)' deflate # 格式定义

CustomLog logs/deflate_log.log deflate # 日志位置
CustomLog "|/usr/local/httpd/bin/rotatelogs /www/logs/deflate.%Y-%m-%d.log 86400 480" deflate #
分割日志位置
```

2.11.1. 测试 gzip,deflate 模块

telnet www.bg7nyt.cn 80

```
GET /index.html HTTP/1.0
Host: www.bg7nyt.cn
Accept-Encoding: gzip,deflate
```

你看到的是乱码,而不是HTML.

```
curl -H Accept-Encoding:gzip,defalte http://www.example.com/index.html | gunzip
```

gunzip 可以解压压缩内容

2.12. Expires

```
ExpiresActive On
ExpiresByType image/gif "access plus 1 month"
ExpiresByType image/jpeg "access plus 1 month"
ExpiresByType image/x-icon "access plus 1 month"
ExpiresByType image/png "access plus 1 month"
ExpiresByType text/html "access plus 30 minutes"
ExpiresByType text/css  "access plus 30 minutes"
ExpiresByType text/js   "access plus 30 minutes"
ExpiresByType application/x-javascript   "access plus 30 minutes"
ExpiresByType application/x-shockwave-flash     "access plus 30 minutes"

<FilesMatch “\.(ico|jpg|jpeg|png|gif|js|css|swf|html|htm|gzip)$”>
ExpiresActive on
ExpiresDefault “access plus 2 hours”
Header set Cache-Control “max-age=1800, public”
FileETag none
</FilesMatch>
```

2.13. Cache

htcacheclean -- program for cleaning the disk cache.

2.13.1. mod_disk_cache

```
<IfModule mod_cache.c>
    CacheDefaultExpire 86400
    <ifModule mod_disk_cache.c>
        CacheEnable disk /
        CacheRoot /tmp/apacheCache
        CacheDirLevels 5
        CacheDirLength 5
        CacheMaxFileSize 1048576
        CacheMinFileSize 10
    </ifModule mod_disk_cache.c>
</IfModule mod_cache.c>
```

2.13.2. mod_mem_cache

```
<IfModule mod_cache.c>
    <ifModule mod_mem_cache.c>
        CacheEnable mem /
        MCacheMaxObjectCount 20000
        MCacheMaxObjectSize 1048576
        MCacheMaxStreamingBuffer 65536
        MCacheMinObjectSize 10
        MCacheRemovalAlgorithm GDSF
        MCacheSize 131072
    </ifModule mod_disk_cache.c>
</IfModule mod_cache.c>
```

2.14. usertrack

跟踪用户信息

跟踪用户的cookie,使用log日志文件记录用户的cookie

```
LoadModule usertrack_module modules/mod_usertrack.so

CookieTracking on
CookieDomain .example.com
CookieExpires "10 years"
CookieStyle Cookie

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %{cookie}n" combined
```

2.15. Charset

Default charset

```
AddCharset UTF-8 .html

AddType 'text/html; charset=UTF-8' html

AddDefaultCharset UTF-8
```

Files match

```
<FilesMatch "\.(htm|html|css|js)$">
        ForceType 'text/html; charset=UTF-8'
</FilesMatch>

<FilesMatch "\.(htm|html|css|js)$">
        AddDefaultCharset UTF-8
</FilesMatch>
```

Changing the occasional file

```
<Files "example.html">
        AddCharset UTF-8 .html
</Files>
```

```
<Files "example.html">
        ForceType 'text/html; charset=UTF-8'
</Files>
```

2.16. Dir

```
<IfModule dir_module>
    DirectoryIndex index.html index.php
</IfModule>
```

2.17. Includes

```
<Directory "/www">
        Options Indexes FollowSymLinks +Includes
</Directory>
```

```
<IfModule mime_module>
        AddType text/html .shtml
    AddOutputFilter INCLUDES .shtml
</IfModule>
```

2.18. Apache Status

开启Apache的status模块，需要修改httpd.conf，增加以下配置段：

```
ExtendedStatus On
<Location /server-status>
  SetHandler server-status
  Order deny,allow
  Deny from all
  Allow from 125.76.229.113
</Location>
```

http://www.domain.com/server-status

2.19. Mod Perl

ref: http://search.cpan.org/~agrundma/Catalyst-Engine-Apache-1.07/lib/Catalyst/Engine/Apache2/MP20.pm

$ sudo apt-get install libapache2-mod-perl2 $ sudo apt-get install libcatalyst-engine-apache-perl

```
$ sudo vi /etc/apache2/sites-available/catalyst.conf
```

例 38.4. mod_perl.conf

```
PerlSwitches -I/var/www/MyApp/lib
# Preload your entire application
PerlModule MyApp

<VirtualHost 192.168.245.129:80>
        ServerName 192.168.245.129
        DocumentRoot /var/www/MyApp/root

        <Directory /var/www/MyApp/root>
                Options Indexes FollowSymLinks
                AllowOverride None
```

```
                Order allow,deny
                Allow from all
        </Directory>

        # If the server is started as:
        #       httpd -X -D PERLDB
        # then debugging will be turned on
#       <IfDefine PERLDB>
#               PerlRequire conf/db.pl
#               <Location />
#                       PerlFixupHandler Apache::DB
#               </Location>
#       </IfDefine>

        <Location />
                SetHandler modperl
                PerlResponseHandler MyApp
        </Location>

        Alias /static /var/www/MyApp/root/static
        <Location /static>
                SetHandler default-handler
        </Location>
</VirtualHost>
```

db.pl

```
use APR::Pool ();
use Apache::DB ();
Apache::DB->init();
```

enable site

```
$ sudo a2ensite mod_perl.conf
$ sudo /etc/init.d/apache2 restart
```

2.20. Module FAQ

```
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 358 of /etc/httpd/conf/httpd.conf:
Invalid command 'Order', perhaps mis-spelled or defined by a module not included
in the server configuration
[FAILED]
LoadModule access_module /etc/httpd/modules/mod_access.so
LoadModule auth_module /etc/httpd/modules/mod_auth.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 368 of /etc/httpd/conf/httpd.conf:
Invalid command 'UserDir', perhaps mis-spelled or defined by a module not includ
ed in the server configuration
[FAILED]
LoadModule userdir_module /etc/httpd/modules/mod_userdir.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 396 of /etc/httpd/conf/httpd.conf:
Invalid command 'DirectoryIndex', perhaps mis-spelled or defined by a module not
included in the server configuration
[FAILED]
LoadModule dir_module /etc/httpd/modules/mod_dir.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 419 of /etc/httpd/conf/httpd.conf:
Invalid command 'TypesConfig', perhaps mis-spelled or defined by a module not in
cluded in the server configuration
[FAILED]
LoadModule mime_module /etc/httpd/modules/mod_mime.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 491 of /etc/httpd/conf/httpd.conf:
Invalid command 'LogFormat', perhaps mis-spelled or defined by a module not incl
uded in the server configuration
[FAILED]
LoadModule log_config_module /etc/httpd/modules/mod_log_config.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 555 of /etc/httpd/conf/httpd.conf:
Invalid command 'Alias', perhaps mis-spelled or defined by a module not included
in the server configuration
[FAILED]
LoadModule alias_module /etc/httpd/modules/mod_alias.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 582 of /etc/httpd/conf/httpd.conf:
Invalid command 'SetEnvIf', perhaps mis-spelled or defined by a module not inclu
ded in the server configuration
[FAILED]
LoadModule setenvif_module /etc/httpd/modules/mod_setenvif.so
[root@srv-2 modules]# /etc/init.d/httpd start
```

```
Starting httpd: Syntax error on line 636 of /etc/httpd/conf/httpd.conf:
Invalid command 'IndexOptions', perhaps mis-spelled or defined by a module not i
ncluded in the server configuration
[FAILED]
LoadModule autoindex_module /etc/httpd/modules/mod_autoindex.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd: Syntax error on line 784 of /etc/httpd/conf/httpd.conf:
Invalid command 'LanguagePriority', perhaps mis-spelled or defined by a module n
ot included in the server configuration
[FAILED]
LoadModule negotiation_module /etc/httpd/modules/mod_negotiation.so
[root@srv-2 modules]# /etc/init.d/httpd start
Starting httpd:                                            [  OK  ]
[root@srv-2 modules]#
```

2.21. mod_setenvif

屏蔽爬虫

```
<directory "/www/example.com">
    Order allow,deny
    Allow from all
    BrowserMatchNoCase "iaskspider" badguy
    BrowserMatchNoCase "QihooBot" badguy
    BrowserMatchNoCase "larbin" badguy
    BrowserMatchNoCase "iearthworm" badguy
    BrowserMatchNoCase "Outfoxbot" badguy
    BrowserMatchNoCase "lanshanbot" badguy
    BrowserMatchNoCase "Arthur" badguy
    BrowserMatchNoCase "InfoPath" badguy
    BrowserMatchNoCase "DigExt" badguy
    BrowserMatchNoCase "Embedded" badguy
    BrowserMatchNoCase "EmbeddedWB" badguy
    BrowserMatchNoCase "Wget" badguy
    BrowserMatchNoCase "CNCDialer" badguy
    BrowserMatchNoCase "LWP::Simple" badguy
    BrowserMatchNoCase "WPS" badguy
    deny from env=badguy
</directory>
```

屏蔽下载

```
BrowserMatch "NetAnt" badguy
BrowserMatch "GetRight" badguy
BrowserMatch "JetCar" badguy
BrowserMatch "Mass Downloader" badguy
BrowserMatch "ReGet" badguy
BrowserMatch "DLExpert" badguy
BrowserMatch "FlashGet" badguy
BrowserMatch "Offline Explorer" badguy
BrowserMatch "Teleport" badguy
...........

order deny,allow
deny from env=badguy
allow from all
```

3. 设置Apache实现防盗连

```
SetEnvIf Referer "http://news.netkiller.com/" local_referal
SetEnvIf Referer "$" local_referral

Order Deny,Allow
Deny from all
Allow from env=local_referal
```

配置httpd.conf文件

#LoadModule rewrite_module modules/mod_rewrite.so

去掉前面的"#"注释

AllowOverride None

改为

AllowOverride All

配置.htaccess文件

```
RewriteEngine on
RewriteCond % !^http://xxx.cn/.*$        [NC]
RewriteCond % !^http://xxx.cn$                    [NC]
RewriteCond % !^http://www.xxx.cn/.*$    [NC]
RewriteCond % !^http://www.xxx.cn$       [NC]
RewriteRule .*\.(jpg|jpeg|gif|png|bmp|rar|zip|exe)$ http://download.example.com/err.html [R,NC]
```

4. Error Prompt

4.1. Invalid command 'Order', perhaps misspelled or defined by a module not included in the server configuration

没有加载 mod_authz_host 模块

```
LoadModule authz_host_module modules/mod_authz_host.so
```

4.2. Invalid command 'AuthUserFile', perhaps misspelled or defined by a module not included in the server configuration

```
LoadModule auth_basic_module /usr/lib/apache2/modules/mod_auth_basic.so
LoadModule authz_owner_module /usr/lib/apache2/modules/mod_authz_owner.so
LoadModule authn_file_module  /usr/lib/apache2/modules/mod_authn_file.so
```

第 39 章 Lighttpd

目录

1. 安装Lighttpd

1.1. quick install with aptitude

if you OS is Ubuntu/Debian

apt-get install lighttpd

```
netkiller@shenzhen:~$ sudo apt-get install lighttpd
```

the config file in /etc/lighttpd

```
netkiller@shenzhen:~/document/Docbook/Linux$ find /etc/lighttpd/
/etc/lighttpd/
/etc/lighttpd/lighttpd.conf
/etc/lighttpd/conf-enabled
/etc/lighttpd/conf-available
/etc/lighttpd/conf-available/10-userdir.conf
/etc/lighttpd/conf-available/10-fastcgi.conf
/etc/lighttpd/conf-available/10-cgi.conf
/etc/lighttpd/conf-available/README
/etc/lighttpd/conf-available/10-ssl.conf
```

```
/etc/lighttpd/conf-available/10-proxy.conf
/etc/lighttpd/conf-available/10-auth.conf
/etc/lighttpd/conf-available/10-simple-vhost.conf
/etc/lighttpd/conf-available/10-ssi.conf
```

Enabling and disabling modules could be done by provided e.g.

```
/usr/sbin/lighty-enable-mod fastcgi
/usr/sbin/lighty-disable-mod fastcgi
```

when you enabled a mod please force-reload it

```
netkiller@shenzhen:/etc/lighttpd$ sudo lighty-enable-mod fastcgi
Available modules: auth cgi fastcgi proxy simple-vhost ssi ssl userdir
Already enabled modules: userdir
Enabling fastcgi: ok
Run /etc/init.d/lighttpd force-reload to enable changes
netkiller@shenzhen:/etc/lighttpd$ sudo /etc/init.d/lighttpd force-reload
 * Stopping web server lighttpd
[ OK ]
 * Starting web server lighttpd
```

1.2. yum install

```
yum install lighttpd lighttpd-fastcgi -y
chkconfig lighttpd on
```

1.3. to compile and then install lighttpd

1. 下载相关软件

   立即下载

   ```
   $ sudo apt-get install libpcre3*

   cd /usr/local/src/
   wget http://www.lighttpd.net/download/lighttpd-1.4.15.tar.gz
   tar zxvf lighttpd-1.4.15.tar.gz
   cd lighttpd-1.4.15
   ```

2. 编译安装

   ```
   ./configure --prefix=/usr/local/lighttpd-1.4.15 \
   --with-bzip2 \
   --with-memcache
   make
   make install
   ```

3. 创建目录与配置文件

   ```
   ln -s /usr/local/lighttpd-1.4.15/ /usr/local/lighttpd
   mkdir -p /www/pages
   mkdir /www/logs
   mkdir /usr/local/lighttpd/htdocs
   mkdir /usr/local/lighttpd/logs
   mkdir /usr/local/lighttpd/etc
   cp ./doc/lighttpd.conf /usr/local/lighttpd/etc/
   cd /usr/local/lighttpd/
   ```

4. 配置lighttpd.conf

   vi etc/lighttpd.conf

   找到 server.modules

删除 mod_fastcgi 前的注释

跟据你的需求修改下面定义

server.document-root = "/usr/local/lighttpd/htdocs/"

server.errorlog = "/usr/local/lighttpd/logs/lighttpd.error.log"

accesslog.filename = "/usr/local/lighttpd/logs/access.log"

注释 $HTTP["url"]

```
#$HTTP["url"] =~ "\.pdf$" {
#  server.range-requests = "disable"
#}
```

5. 运行lighttpd

```
/usr/local/lighttpd/sbin/lighttpd -f /usr/local/lighttpd/etc/lighttpd.conf
```

测试

curl http://ip/ 因为/www/pages/下没有HTML页面所以返回:

404 - Not Found

1.3.1. shell script

lighttpd script

例 39.1. /etc/init.d/lighttpd

```
#!/bin/bash
# lighttpd init file for web server
#
# chkconfig: - 100 100
# description: Security, speed, compliance, and flexibility--all of these describe LightTPD
which is rapidly redefining efficiency of a webserver;
#                                as it is designed and optimized for high performance
environments.
# author: Neo Chen<openunix@163.com>
#
# processname: $PROG
# config:
# pidfile: /var/run/lighttpd

# source function library
. /etc/init.d/functions

PREFIX=/usr/local/lighttpd
PROG=$PREFIX/sbin/lighttpd
OPTIONS="-f /usr/local/lighttpd/etc/lighttpd.conf"
USER=daemon
RETVAL=0
prog="lighttpd"

start() {
        echo -n $"Starting $prog: "
        if [ $UID -ne 0 ]; then
                RETVAL=1
                failure
        else
                daemon --user=$USER $PROG $OPTIONS
                RETVAL=$?
                [ $RETVAL -eq 0 ] && touch /var/lock/subsys/lighttpd
        fi;
        echo
```

```
        return $RETVAL
}

stop() {
        echo -n $"Stopping $prog: "
        if [ $UID -ne 0 ]; then
                RETVAL=1
                failure
        else
                killproc $PROG
                RETVAL=$?
                [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/lighttpd
        fi;
        echo
        return $RETVAL
}

reload(){
        echo -n $"Reloading $prog: "
        killproc $PROG -HUP
        RETVAL=$?
        echo
        return $RETVAL
}

restart(){
        stop
        start
}

condrestart(){
    [ -e /var/lock/subsys/lighttpd ] && restart
    return 0
}

case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart)
        restart
        ;;
  reload)
        reload
        ;;
  condrestart)
        condrestart
        ;;
  status)
        status lighttpd
        RETVAL=$?
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart|reload}"
        RETVAL=1
esac

exit $RETVAL
```

2. /etc/lighttpd/lighttpd.conf

2.1. max-worker / max-fds

max-worker 我一般设置为与处理器数目相同。

max-fds 最大连接数

```
server.max-worker = 24
server.max-fds = 4096
```

2.2. accesslog.filename

通过cronolog切割日志

```
#### accesslog module
#accesslog.filename          = "/www/logs/lighttpd.access.log"
accesslog.filename = "| /usr/local/sbin/cronolog /www/logs/%Y/%m/%d/access.log"
```

2.3. ETags

disable etags

```
static-file.exclude-extensions = ( ".php", ".pl", ".fcgi" )
static-file.etags = "disable"
```

2.4. server.tag

隐藏服务器信息

```
server.tag = "Apache"
```

测试结果Server: Apache

```
curl -I http://172.16.0.7/
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 4692
Date: Fri, 04 Nov 2011 12:33:19 GMT
Server: Apache
```

3. Module

```
server.modules              = (
#                                   "mod_rewrite",
#                                   "mod_redirect",
#                                   "mod_alias",
                                    "mod_access",
#                                   "mod_trigger_b4_dl",
#                                   "mod_auth",
#                                   "mod_status",
#                                   "mod_setenv",
#                                   "mod_fastcgi",
#                                   "mod_proxy",
#                                   "mod_simple_vhost",
#                                   "mod_evhost",
#                                   "mod_userdir",
#                                   "mod_cgi",
#                                   "mod_compress",
#                                   "mod_ssi",
#                                   "mod_usertrack",
#                                   "mod_expire",
#                                   "mod_secdownload",
#                                   "mod_rrdtool",
                                    "mod_accesslog" )
```

3.1. simple_vhost

```
$ sudo lighty-enable-mod simple-vhost
```

simple-vhost.default-host = "www.example.com"

create your virtual host directory

```
$ mkdir -p /var/www/www.example.com/html
```

create a test file

```
$ echo helloworld!!!> /var/www/www.example.com/html/index.html
```

3.2. ssl

启用 ssl 模块

```
$ sudo lighttpd-enable-mod ssl
[sudo] password for neo:
Available modules: auth cgi fastcgi proxy rrdtool simple-vhost ssi ssl status userdir
Already enabled modules: cgi fastcgi simple-vhost
Enabling ssl: ok
Run /etc/init.d/lighttpd force-reload to enable changes
```

创建 ssl 证书

```
$ sudo openssl req -new -x509 -keyout server.pem -out server.pem -days 365 -nodes
$ sudo chmod 400 server.pem
```

3.3. redirect

```
url.redirect                = ( "^/music/(.+)" => "http://www.example.org/$1" )
```

301重定向

```
RewriteCond %{HTTP_HOST} ^example\.org$ [NC]
RewriteRule ^(.*)$ http://www.example.org/$1 [R=301,L]
```

lighttpd 实现上面 apache功能

```
$HTTP["host"] =~ "^example\.org" {
    url.redirect = (
        "^/(.*)$" => "http://www.example.org/$1"
    )
}

$HTTP["host"] =~ "^example\.com$" {
  url.redirect = ( "^/(.*)" => "http://www.example.com/$1" )
}
```

3.4. rewrite

example 1

```
url.rewrite-once = ( "^/wiki/(.*)$" => "/wiki/awki.cgi/$1" )
$HTTP["url"] =~ "^/wiki" {
  $HTTP["url"] !~ "^/wiki/awki.cgi/" {
    url.access-deny = ("")
  }
}
```

example 2

```
$HTTP["host"] =~ "^.*\.(example.org)$" {
  url.rewrite-once = ( "^/(.*)" => "/index.php/$1" )
}
```

example 3

```
$HTTP["host"] =~ "^.*\.(example.org)$" {
  url.rewrite = (
        "^/(images|stylesheet).*" => "/$0",
        "^/(.*)" => "/index.php/$1"
  )
}
```

3.4.1. Lighttpd Rewrite QSA

```
# Apache
RewriteRule ^/index\.html$ /index.php [QSA]
RewriteRule ^/team_(.*)\.html$ /team.php?id=$1 [QSA]

#lighttpd
"^/index\.html(.*)"                      => "/index.php$1",
"^/team_(\w+)\.html\?(.*)"               => "/team.php?id=$1&$2",
```

ref: http://redmine.lighttpd.net/wiki/lighttpd/MigratingFromApache

```
url.rewrite = (
        "^/index\.html(.*)"                     => "/index.php$1",
        "^/index\.html"                         => "/index.php",
        "^/team_(.*)\.html"                     => "/team.php?id=$1",
        "^/team_(\w+)\.html\?(.*)"              => "/team.php?id=$1&$2"
)
```

3.5. alias

```
$HTTP["host"] =~ "^.*\.(example.org)$" {
    alias.url = (
        "/images" =>
"/home/neo/workspace/Development/photography/application/photography/images",
        "/stylesheet" =>
"/home/neo/workspace/Development/photography/application/photography/stylesheet"
    )
}
```

3.6. auth

enable auth

```
$ sudo lighttpd-enable-mod auth
```

/etc/lighttpd/conf-enabled/05-auth.conf

```
$ sudo vim  conf-enabled/05-auth.conf

auth.backend = "plain"
auth.backend.plain.userfile = "/etc/lighttpd/.secret"

auth.require = ( "/tmp/" =>
        (
        "method" => "basic",
        "realm" => "Password protected area",
        "require" => "user=neo"
        )
)
```

create a passwd file

```
$ sudo vim .secret
neo:chen

$ sudo chmod 400 .secret
$ sudo chown www-data /etc/lighttpd/.secret
```

$ sudo /etc/init.d/lighttpd reload

3.7. compress

创建cache目录

```
mkdir -p /var/cache/lighttpd/compress
```

配置lighttpd.conf文件

找到server.modules列表,去掉"mod_compress"注释,再打开compress module的注释

```
#### compress module
compress.cache-dir          = "/var/lighttpd/cache/compress/"
compress.filetype           = ("text/plain", "text/html")
```

Compressing Dynamic Content

php.ini

```
zlib.output_compression = On
zlib.output_handler = On
```

最后使用telnet测试

telnet www.bg7nyt.cn 80

```
GET /index.html HTTP/1.0
Host: 10.10.100.183
Accept-Encoding: gzip,deflate
```

看到乱码输出,而非HTML,表示配置成功.

例 39.2. lighttpd compress

```
$HTTP["host"] =~ "www\.example\.com$" {

        compress.cache-dir = "/www/compress/"
        compress.filetype = ("text/plain", "text/html", "application/x-javascript", "text/css",
"application/javascript", "text/javascript")

        $HTTP["url"] =~ "(\.png|\.css|\.js|\.jpg|\.gif)$" {
                expire.url = (""=>"access 30 seconds")
        }
}
```

3.8. expire

<access|modification> <number> <years|months|days|hours|minutes|seconds>

```
expire.url = ( "/images/" => "access 1 hours" )
```

Example to include all sub-directories:

```
$HTTP["url"] =~ "^/images/" {
        expire.url = ( "" => "access 1 hours" )
}
```

例 39.3. lighttpd expire

```
$HTTP["host"] =~ "www\.example\.com$" {
        $HTTP["url"] =~ "(\.png|\.css|\.js|\.jpg|\.gif)$" {
                expire.url = (""=>"access 30 seconds")
        }
}
```

3.9. status

```
$ sudo lighty-enable-mod status
$ sudo /etc/init.d/lighttpd force-reload
```

3.10. setenv

```
$HTTP["url"] =~ "^/(.*)" {
        setenv.add-response-header = ( "Cache-Control" => "no-store, no-cache, must-revalidate,
post-check=0, pre-check=0, max-age=-1" )
}

$HTTP["url"] =~ ".swf" {
       setenv.add-response-header  = ("Pragma" =>"no-cache","Expires" => "-1")
}

$HTTP["url"] =~ ".swf" {
       setenv.add-response-header  = ("Cache-Control" =>"max-age=0")
}

$HTTP["url"] =~ ".html" {
       setenv.add-response-header  = ("Cache-Control" =>"s-maxage=3600")
}

$HTTP["url"] =~ ".css" {
        setenv.add-response-header = (
      "Content-Encoding" => "gzip"
    )
}
```

3.10.1. Automatic Decompression

```
  $HTTP["url"] =~ "(README|ChangeLog|\.txt)\.gz$" {
    setenv.add-response-header  = ( "Content-Encoding" => "gzip")
    mimetype.assign = ("" => "text/plain" )
  }
```

3.11. fastcgi

3.11.1. enable fastcgi

enable fastcgi

```
$ sudo lighty-enable-mod fastcgi
```

3.11.1.1. spawn-fcgi

```
#### fastcgi module
## read fastcgi.txt for more info
## for PHP don't forget to set cgi.fix_pathinfo = 1 in the php.ini
fastcgi.server              = ( ".php" =>
                                ( "localhost" =>
                                  (
                                    "socket" => "/tmp/php-fastcgi.socket",
                                    "bin-path" => "/usr/local/bin/php-cgi",
                                    "max-procs" => 16,
                                    "bin-environment" => (
                                       "PHP_FCGI_CHILDREN" => "128",
                                       "PHP_FCGI_MAX_REQUESTS" => "1000"
                                    ),
                                    "broken-scriptfilename" => "enable"
                                  )
                                )
                              )

fastcgi.server    = ( ".php" =>
        ((
                "bin-path" => "/usr/bin/php-cgi",
                "socket" => "/tmp/php.socket",
                "max-procs" => 2,
                "idle-timeout" => 200,
                "bin-environment" => (
                        "PHP_FCGI_CHILDREN" => "10",
                        "PHP_FCGI_MAX_REQUESTS" => "10000"
                ),
                "bin-copy-environment" => (
```

```
                        "PATH", "SHELL", "USER"
                ),
                "broken-scriptfilename" => "enable"
        ))
)
```

3.11.1.2. php-fpm

```
fastcgi.server = ( ".php" =>
  ( "localhost" =>
    (
      "host" => "127.0.0.1",
      "port" => "9000"
    )
  )
)
```

3.11.2. PHP

3.11.2.1. 编译安装PHP

1. 下载PHP

```
cd /usr/local/src/
wget http://cn2.php.net/get/php-5.2.3.tar.bz2/from/cn.php.net/mirror
tar jxvf php-5.2.3.tar.bz2
cd php-5.2.3
```

2. configure

```
./configure --prefix=/usr/local/php-5.2.3 \
--with-config-file-path=/usr/local/php-5.2.3/etc \
--enable-fastcgi \
--enable-force-cgi-redirect \
--with-curl \
--with-gd \
--with-ldap \
--with-snmp \
--enable-zip \
--enable-exif \
--with-pdo-mysql \
--with-pdo-pgsql \

make
make test
make install
```

其它有用的模块

```
--enable-pcntl
```

3. 符号连接

```
ln -s /usr/local/php-5.2.3 /usr/local/php
ln -s /usr/local/php/bin/php /usr/local/bin/php
```

4. php.ini

```
cp php.ini-dist /usr/local/php/etc/php.ini
```

5. env

```
PHP_FCGI_CHILDREN=384
```

6. 使用 php -v FastCGI 安装情况

   php -v

   显示(cgi-fcgi)表示正确

```
# cd /usr/local/php/
# bin/php -v
PHP 5.2.2 (cgi-fcgi) (built: May 25 2007 15:50:28)
Copyright (c) 1997-2007 The PHP Group
Zend Engine v2.2.0, Copyright (c) 1998-2007 Zend Technologies
```

   (cgi-fcgi)不能正常工作

```
PHP 5.2.2 (cli) (built: May 25 2007 15:50:28)
Copyright (c) 1997-2007 The PHP Group
Zend Engine v2.2.0, Copyright (c) 1998-2007 Zend Technologies
```

   使用 php -m 查看PHP Modules

```
# bin/php -m
[PHP Modules]
cgi-fcgi
ctype
date
dom
filter
gd
hash
iconv
json
ldap
libxml
mssql
pcre
PDO
pdo_mysql
pdo_sqlite
posix
Reflection
session
SimpleXML
snmp
SPL
SQLite
standard
tokenizer
xml
xmlreader
xmlwriter
zip

[Zend Modules]
```

3.11.2.2. apt-get install

```
$ sudo apt-get install php5 php5-cli php5-cgi
```

[参考php安装]

找到 fastcgi.server 去掉注释

bin-path 改为PHP程序安装目录

```
fastcgi.server              = ( ".php" =>
                                ( "localhost" =>
                                  (
                                   "socket" => "/tmp/php-fastcgi.socket",
                                    "bin-path" => "/usr/local/php/bin/php"
                                  )
                                )
```

```
                                )
```

下面例子更复杂一些

1. /usr/local/lighttpd/etc/lighttpd.conf

```
include /usr/local/lighttpd/etc/php-fastcgi.conf
```

2. /usr/local/lighttpd/etc/php-fastcgi.conf

```
fastcgi.server = ( ".php" =>
        ( "localhost" =>
        ( "socket" => "/tmp/php-fastcgi.socket",
           "bin-path" => "/usr/local/php/bin/php",
           "min-procs" => 1,
           "max-procs" => 5,
           "max-load-per-proc" => 4,
           "idle-timeout" => 20
        )
        )
)
```

3. PHP FastCGI环境测试

echo "<?php phpinfo(); ?>" > /www/pages/index.php

curl http://127.0.0.1/index.php

3.11.3. Python

```
sudo apt-get install python
sudo apt-get install python-setuptools
```

3.11.3.1. Django

```
wget http://www.djangoproject.com/download/0.96/tarball/
tar zxvf Django-0.96.tar.gz
cd Django-0.96
python setup.py install
```

生成项目

```
django-admin.py startproject newtest
```

web server

```
cd newtest/
./manage.py runserver
```

helloworld.py

```
from django.http import HttpResponse

def index(request):
    return HttpResponse("Hello, Django.")
```

urls.py

```
from django.conf.urls.defaults import *

urlpatterns = patterns('',
    # Example:
    # (r'^newtest/', include('newtest.foo.urls')),
    (r'^$', 'newtest.helloworld.index'),

    # Uncomment this for admin:
#     (r'^admin/', include('django.contrib.admin.urls')),
)
```

启动Web Server

```
# ./manage.py runserver
Validating models...
0 errors found.

Django version 0.96, using settings 'newtest.settings'
Development server is running at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

curl http://127.0.0.1:8000/

3.11.3.2. Python Imaging Library

Debian/Ubuntu

```
sudo apt-get install libjpeg62-dev
sudo apt-get install python-imaging
```

采用源码安装

```
tar zxvf Imaging-1.1.6.tar.gz
cd Imaging-1.1.6/
```

sudo python setup.py install

decoder jpeg not available

首先确认jpeg库是否安装

find / -name jpeglib.h

然后修改头文件

Imaging-1.1.6/libImaging

修改Jpeg.h, #include "jpeglib.h" 改为

#include "/usr/include/jpeglib.h"

3.11.4. Perl

install fastcgi module

```
$ sudo apt-get install libfcgi-perl     libfcgi-procmanager-perl
```

3.11.4.1. Installing lighttpd and FastCGI for Catalyst

The examples also use a virtual host regexp that matches either www.myapp.com or myapp.com

```
$HTTP["host"] =~ "^(www.)?mysite.com"
```

Starting the FastCGI server

```
MyApp/script/myapp_fastcgi.pl -l /tmp/myapp.socket -n 5 -d
```

lighttpd.conf

```
server.document-root = "/var/www/MyApp/root"
```

$ sudo vim /etc/lighttpd/conf-available/10-fastcgi.conf

```
fastcgi.server = (
    "" => (
        "MyApp" => (
            "socket" => "/tmp/myapp.socket",
            "check-local" => "disable"
        )
    )
)
```

restart lighttpd

```
neo@master:~$ sudo /etc/init.d/lighttpd restart
 * Stopping web server lighttpd                    [ OK ]
 * Starting web server lighttpd                    [ OK ]
```

Testing

http://127.0.0.1/

More advanced configuration

例 39.4. fastcgi.conf

```
fastcgi.server = (
    "" => (
        "MyApp" => (
            "socket"        => "/tmp/myapp.socket",
            "check-local"   => "disable",
            "bin-path"      => "/var/www/MyApp/script/myapp_fastcgi.pl",
            "min-procs"     => 2,
            "max-procs"     => 5,
            "idle-timeout"  => 20
        )
    )
)
```

3.11.5. Ruby

3.12. user-agent

```
$HTTP["user-agent"] =~ "Googlebot|Sosospider+|eMule|Wget|^Java|^PHP|Ruby|Python" {
  url.rewrite = ( "^/(.*)" => "/crawler.html" )
}
```

```
$HTTP["user-agent"] =~ "Baiduspider+" {
    connection.delay-seconds = 10
}
```

---

4. 其他模块

4.1. mod_secdownload 防盗链

5. Example

5.1. s-maxage

s-maxage 头作用于反向代理服务器

例 39.5. Cache

```
$HTTP["url"] =~ "^/images/2010" {
        expire.url = ( "" => "access 15 minutes" )
}

$HTTP["host"] =~ "(img1|img2|img3)\.example\.com" {
    expire.url = ( "" => "access 15 minutes" )
    setenv.add-response-header  = ("Cache-Control" =>"s-maxage=3600")
}
```

第 40 章 Nginx

目录

1. Installing

1.1. Installing by apt-get under the debain/ubuntu

```
$ sudo apt-get install nginx
```

```
/etc/init.d/nginx start
```

1.2. CentOS

http://nginx.org/packages/centos/$releasever/$basearch/

$releasever 是版本号

$basearch 处理器架构

http://nginx.org/packages/centos/6/x86_64/

```
cat > /etc/yum.repos.d/nginx.repo <<EOF
[nginx]
name=nginx repo
baseurl=http://nginx.org/packages/centos/6/x86_64/
gpgcheck=0
enabled=1
EOF
```

i386

```
cat > /etc/yum.repos.d/nginx.repo <<EOF
[nginx]
name=nginx repo
baseurl=http://nginx.org/packages/centos/5/i386/
gpgcheck=0
enabled=1
EOF
```

```
yum search nginx
============================================= Matched: nginx
=============================================
nginx.x86_64 : high performance web server

yum install -y nginx
chkconfig nginx on
service nginx start
```

1.3. installing by source

```
cd /usr/local/src/
wget http://www.nginx.org/download/nginx-1.0.6.tar.gz

./configure --prefix=/usr/local/server/nginx \
--with-openssl=/usr/include \
--with-pcre=/usr/include/pcre/ \
--with-http_stub_status_module \
--without-http_memcached_module \
--without-http_fastcgi_module \
--without-http_rewrite_module \
--without-http_map_module \
--without-http_geo_module \
--without-http_autoindex_module
```

rpm 所使用的编译参数

```
nginx -V
nginx: nginx version: nginx/1.0.6
nginx: built by gcc 4.4.4 20100726 (Red Hat 4.4.4-13) (GCC)
nginx: TLS SNI support enabled
nginx: configure arguments: --prefix=/etc/nginx/ --sbin-path=/usr/sbin/nginx --conf-path=/etc/nginx/nginx.conf --error-log-path=/var/log/nginx/error.log --http-log-path=/var/log/nginx/access.log --pid-path=/var/run/nginx.pid --lock-path=/var/run/nginx.lock --http-client-body-temp-path=/var/cache/nginx/client_temp --http-proxy-temp-path=/var/cache/nginx/proxy_temp --http-fastcgi-temp-path=/var/cache/nginx/fastcgi_temp --http-uwsgi-temp-path=/var/cache/nginx/uwcgi_temp --http-scgi-temp-path=/var/cache/nginx/scgi_temp --user=nginx --group=nginx --with-http_ssl_module --with-http_realip_module --with-http_addition_module --with-http_sub_module --with-http_dav_module --with-http_flv_module --with-http_gzip_static_module --with-http_random_index_module --with-http_secure_link_module --with-http_stub_status_module --with-mail --with-mail_ssl_module --with-file-aio --with-ipv6
```

1.4. php-fpm

```
./configure --prefix=/srv/php-5.3.8 \
--with-config-file-path=/srv/php-5.3.8/etc \
--with-config-file-scan-dir=/srv/php-5.3.8/etc/conf.d \
--enable-fpm \
--with-fpm-user=www \
--with-fpm-group=www \
--with-pear \
--with-curl \
--with-gd \
--with-jpeg-dir \
--with-png-dir \
--with-freetype-dir \
--with-xpm-dir \
--with-iconv \
--with-mcrypt \
--with-mhash \
--with-zlib \
--with-xmlrpc \
--with-xsl \
--with-openssl \
--with-mysql=/srv/mysql-5.5.16-linux2.6-i686 \
--with-mysqli=/srv/mysql-5.5.16-linux2.6-i686/bin/mysql_config \
--with-pdo-mysql=/srv/mysql-5.5.16-linux2.6-i686 \
--with-sqlite=shared \
--with-pdo-sqlite=shared \
--disable-debug \
--enable-zip \
--enable-sockets \
--enable-soap \
--enable-mbstring \
--enable-magic-quotes \
--enable-inline-optimization \
--enable-gd-native-ttf \
--enable-xml \
--enable-ftp \
--enable-exif \
--enable-wddx \
--enable-bcmath \
--enable-calendar \
--enable-sqlite-utf8 \
--enable-shmop \
--enable-dba \
--enable-sysvsem \
--enable-sysvshm \
--enable-sysvmsg

make && make install
```

如果出现 fpm 编译错误，取消--with-mcrypt 可以编译成功。

```
# cp sapi/fpm/init.d.php-fpm /etc/init.d/php-fpm
# chmod 755 /etc/init.d/php-fpm
# ln -s /srv/php-5.3.5 /srv/php
# cp /srv/php/etc/php-fpm.conf.default /srv/php/etc/php-fpm.conf
# cp php.ini-production /srv/php/etc/php.ini
```

```
groupadd -g 80 www
adduser -o --home /www --uid 80 --gid 80 -c "Web User" www
```

php-fpm.conf

```
# grep -v ';' /srv/php-5.3.5/etc/php-fpm.conf | grep -v "^$"
[global]
pid = run/php-fpm.pid
error_log = log/php-fpm.log
[www]
listen = 127.0.0.1:9000

user = www
group = www
pm = dynamic
pm.max_children = 2048
pm.start_servers = 20
pm.min_spare_servers = 5
pm.max_spare_servers = 35

pm.max_requests = 500
```

```
chkconfig --add php-fpm
```

1.5. rotate log

1.5.1. log shell

```

# cat /srv/bin/rotatelog.sh

#!/bin/bash
# run this script at 0:00

#Nginx Log Path
log_dir="/var/log/nginx"
date_dir=`date +%Y/%m/%d/%H`

mkdir -p ${log_dir}/${date_dir} > /dev/null 2>&1
mv ${log_dir}/access.log ${log_dir}/${date_dir}/access.log
mv ${log_dir}/error.log ${log_dir}/${date_dir}/error.log

kill -USR1 `cat /var/run/nginx.pid`

gzip ${log_dir}/${date_dir}/access.log &
gzip ${log_dir}/${date_dir}/error.log &
```

1.5.2. /etc/logrotate.d/nginx

```

# cat /etc/logrotate.d/nginx
/var/log/nginx/*.log {
        daily
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                [ -f /var/run/nginx.pid ] && kill -USR1 `cat /var/run/nginx.pid`
        endscript
}
```

2. fastcgi

2.1. spawn-fcgi

config php fastcgi

```
sudo vim /etc/nginx/sites-available/default

        location ~ \.php$ {
                fastcgi_pass   127.0.0.1:9000;
                fastcgi_index  index.php;
                fastcgi_param  SCRIPT_FILENAME  /scripts$fastcgi_script_name;
                include fastcgi_params;
        }
```

Spawn-fcgi

We still need a script to start our fast cgi processes. We will extract one from Lighttpd. and then disable start script of lighttpd

```
$ sudo apt-get install lighttpd
$ sudo chmod -x /etc/init.d/lighttpd
```

```
$ sudo touch /usr/bin/php-fastcgi
$ sudo vim /usr/bin/php-fastcgi

#!/bin/sh
/usr/bin/spawn-fcgi -a 127.0.0.1 -p 9000 -u www-data -f /usr/bin/php5-cgi
```

fastcgi daemon

```
$ sudo touch /etc/init.d/nginx-fastcgi
$ sudo chmod +x /usr/bin/php-fastcgi
$ sudo vim /etc/init.d/nginx-fastcgi

This is also a new empty file, add the following and save:

#!/bin/bash
PHP_SCRIPT=/usr/bin/php-fastcgi
RETVAL=0
case "$1" in
start)
$PHP_SCRIPT
RETVAL=$?
;;
stop)
killall -9 php
RETVAL=$?
;;
restart)
killall -9 php
$PHP_SCRIPT
RETVAL=$?
;;
*)
echo "Usage: nginx-fastcgi {start|stop|restart}"
exit 1
;;
esac
exit $RETVAL

We need to change some permissions to make this all work.
```

```
$ sudo chmod +x /etc/init.d/nginx-fastcgi
```

create a test file

```
sudo vim /var/www/nginx-default/index.php
<?php echo phpinfo(); ?>
```

2.2. php5-fpm

```
sudo apt-get install php5-fpm
```

---

3. worker_processes

worker_processes = CPU 数量

4. events

```
events {
    worker_connections  4096;
}
```

5. 可用的全局变量

```
$args
$content_length
$content_type
$document_root
$document_uri
$host
$http_user_agent
$http_cookie
$limit_rate
$request_body_file
$request_method
$remote_addr
$remote_port
$remote_user
$request_filename
$request_uri
$query_string
$scheme
$server_protocol
$server_addr
$server_name
$server_port
$uri
```

6. http 配置

6.1. X-Forwarded-For

```
real_ip_header X-Forwarded-For;
```

6.2. server

6.2.1. VirtualHost (虚拟主机)

```
# cat /etc/nginx/conf.d/images.conf
server {
    listen       80;
    server_name  images.example.com;

    #charset koi8-r;
    access_log  /var/log/nginx/images.access.log  main;

    location / {
        root   /www/images;
        index  index.html index.htm;
    }

    #error_page  404              /404.html;

    # redirect server error pages to the static page /50x.html
    #
    error_page   500 502 503 504  /50x.html;
    location = /50x.html {
        root   /usr/share/nginx/html;
    }

    # proxy the PHP scripts to Apache listening on 127.0.0.1:80
    #
    #location ~ \.php$ {
    #    proxy_pass   http://127.0.0.1;
    #}

    # pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000
    #
    #location ~ \.php$ {
    #    root           html;
    #    fastcgi_pass   127.0.0.1:9000;
    #    fastcgi_index  index.php;
    #    fastcgi_param  SCRIPT_FILENAME  /scripts$fastcgi_script_name;
    #    include        fastcgi_params;
    #}

    # deny access to .htaccess files, if Apache's document root
    # concurs with nginx's one
    #
    #location ~ /\.ht {
    #    deny  all;
    #}
}
```

绑定多个域名

```
server_name  images.example.com img1.example.com img2.example.com;
```

使用通配符匹配

```
server_name  *.example.com
server_name  www.*;
```

正则匹配

```
server_name ~^(.+)\.example\.com$;
server_name ~^(www\.)?(.+)$;
```

6.2.2. location

```
    location / {
        root   /www;
        index  index.html index.htm;
    }
```

6.3. expires

```
#图片类资源缓存5天，并且不记录请求日志
location ~ .*\.(ico|gif|jpg|jpeg|png|bmp|swf)$
{
        expires      5d;
        access_log off;
}

#css/js 缓存一天，不记录请求日志
location ~ .*\.(js|css)?$
{
        expires      1d;
        access_log off;
}
```

```
location ~
.*\.(htm|html|gif|jpg|jpeg|png|bmp|swf|ioc|rar|zip|txt|flv|mid|doc|ppt|pdf|xls|mp3|wma)$
{
    expires      30d;
}
location ~ .*\.(js|css)?$
{
    expires      1h;
}
```

```
location ~* \.(js|css|jpg|jpeg|gif|png|swf)$ {
        if (-f $request_filename) {
           expires    1h;
           break;
        }
}

location ~ .*\.(gif|jpg|jpeg|png|bmp|swf|ico)$ {
    expires      30d;
    access_log   off;
}

location ~ .*\.(js|css)?$ {
    expires      30d;
    access_log   off;
}
```

6.4. access

```
#防止access文件被下载
location ~ /\.ht {
    deny  all;
}
```

```
location ~ ^/upload/.*\.php$
{
        deny all;
}

location ~ ^/static/images/.*\.php$
{
        deny all;
}
```

```
location ~ /\.ht {
    deny all;
}
```

```
location ~ .*\.(sqlite|sq3)$ {
    deny all;
}
```

6.5. autoindex

```
# vim /etc/nginx/sites-enabled/default

location  /  {
  autoindex  on;
}
```

```
# /etc/init.d/nginx reload
Reloading nginx configuration: nginx.
```

6.6. ssi

```
http {
  ssi  on;
}

location / {
  ssi on;
  ssi_silent_errors on;
  ssi_types text/shtml;
}
```

6.7. rewrite

```
Rewrite Flags
last - 基本上都用这个Flag。
break - 中止Rewirte，不在继续匹配
redirect - 返回临时重定向的HTTP状态302
permanent - 返回永久重定向的HTTP状态301

文件及目录匹配，其中:
-f和!-f用来判断是否存在文件
-d和!-d用来判断是否存在目录
-e和!-e用来判断是否存在文件或目录
-x和!-x用来判断文件是否可执行

正则表达式全部符号解释
~ 为区分大小写匹配
~* 为不区分大小写匹配
!~和!~* 分别为区分大小写不匹配及不区分大小写不匹配
(pattern) 匹配 pattern 并获取这一匹配。所获取的匹配可以从产生的 Matches 集合得到，在VBScript 中使用
SubMatches 集合，在JScript 中则使用 $0…$9 属性。要匹配圆括号字符，请使用 '\(' 或 '\)'。
^ 匹配输入字符串的开始位置。
$ 匹配输入字符串的结束位置。
```

```
server {
        listen 80;
        server_name www.example.com example.com ;
        if ($host = "example.com" )
        {
                rewrite ^/(.*)$ http://www.example.com/$1 permanent;
        }
        if ($host != "www.example.com" )
        {
                rewrite ^/(.*)$ http://www.example.com/$1 permanent;
        }
}
```

```
location ~* \.(js|css|jpg|jpeg|gif|png|swf)$ {
        if (!-f $request_filename){
                rewrite /(.*) http://images.example.com/$1;
        }
}
```

```
if ($host ~ '(.*)\.static\.example\.com' ) {
    set $subdomain $1;
    rewrite  "^/(.*)$"  /$subdomain/$1;
}
```

6.8. gzip

```
gzip  on;
gzip_min_length  1000;
gzip_buffers     4 8k;
gzip_types       text/plain application/x-javascript text/css text/html application/xml;


gzip on;
gzip_http_version 1.0;
gzip_disable "MSIE [1-6].";
gzip_types text/plain application/x-javascript text/css text/javascript;
```

6.9. Cache

```
add_header     Nginx-Cache     "HIT  from  www.example.com";
or
add_header     Nginx-Cache     "$upstream_cache_status  from  www.example.com";
```

6.10. stub_status

```
location /nginx_status {
        stub_status on;
        access_log  off;
        allow 127.0.0.1;
        deny all;
}
```

6.11. server_tokens

```
http {
...
server_tokens off;
...
}
```

---

7. Proxy

```
# cat /etc/nginx/nginx.conf

#user  nobody;
worker_processes  4;

#error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;

#pid        logs/nginx.pid;


events {
    worker_connections  40960;
        use epoll;
}


http {
    include       mime.types;
    default_type  application/octet-stream;

    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #                  '$status $body_bytes_sent "$http_referer" '
    #                  '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log  logs/access.log  main;

    access_log  /dev/null;

    sendfile        on;
    #tcp_nopush     on;

    #keepalive_timeout  0;
    keepalive_timeout  65;

    #gzip  on;

upstream backend{
#        server 172.16.0.6:80;
        server 10.0.0.68:80;
        server 10.0.0.69:80;
}


    server {
        listen       80;
        server_name  localhost;

        #charset koi8-r;

        #access_log  logs/host.access.log  main;

#        location / {
#            root   html;
#            index  index.html index.htm;
#        }

    access_log  /dev/null;
    error_log   /dev/null;


    location / {
#        proxy_pass $scheme://$host$request_uri;
#        proxy_set_header Host $http_host;

#        proxy_buffers 256 4k;
#        proxy_max_temp_file_size 0;

#        proxy_connect_timeout 30;

#        proxy_cache_valid 200 302 10m;
#        proxy_cache_valid 301 1h;
#        proxy_cache_valid any 1m;



         proxy_pass      http://backend;

         proxy_redirect          off;
         proxy_set_header        Host $host;
#         proxy_set_header        X-Real-IP $remote_addr;
#         proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
```

```
         client_max_body_size    10m;
         client_body_buffer_size 128k;
         proxy_connect_timeout   30;
         proxy_send_timeout      30;
         proxy_read_timeout      30;
         proxy_buffer_size       4k;
         proxy_buffers           256 4k;
         proxy_busy_buffers_size 64k;
         proxy_temp_file_write_size 64k;
        tcp_nodelay on;
    }


        #error_page  404              /404.html;

        # redirect server error pages to the static page /50x.html
        #
        error_page   500 502 503 504  /50x.html;
        location = /50x.html {
            root   html;
        }
    }

}
```

7.1. request_filename + proxy_pass

如果文件不存在，那么去指定的节点上寻找

```
    location / {
         root  /www;
         proxy_intercept_errors  on;
         if (!-f $request_filename) {
           proxy_pass http://172.16.1.1;
           break;
         }
     }
         location / {
         root  /www/images;
         proxy_intercept_errors  on;
         if (!-f $request_filename) {
           proxy_pass http://172.16.1.2;
           break;
         }
     }
```

第 41 章 Tomcat 安装与配置

目录

1. install java

解压安装

```
chmod +x jdk-6u1-linux-i586.bin
./jdk-6u1-linux-i586.bin
输入"yes"回车

mv jdk1.6.0_01 /usr/local/
ln -s /usr/local/jdk1.6.0_01/ /usr/local/java
```

/etc/profile.d/java.sh

例 41.1. /etc/profile.d/java.sh

```
##################################################
### Java environment
##################################################
export JAVA_HOME=/usr/local/java
export JRE_HOME=/usr/local/java/jre
export PATH=$PATH:/usr/local/java/bin:/usr/local/java/jre/bin
export CLASSPATH="./:/usr/local/java/lib:/usr/local/java/jre/lib:/usr/local/memcached/api/java"
export JAVA_OPTS="-Xms512m -Xmx1024m"
```

---

2. install tomcat

下载binary解压到/usr/local/

下载软件包

```
wget http://archive.apache.org/dist/tomcat/tomcat-6/v6.0.13/bin/apache-tomcat-6.0.13.tar.gz
wget http://archive.apache.org/dist/tomcat/tomcat-connectors/native/tomcat-native-1.1.10-
src.tar.gz
wget http://archive.apache.org/dist/tomcat/tomcat-connectors/jk/source/jk-1.2.23/tomcat-
connectors-1.2.23-src.tar.gz
```

```
tar zxvf apache-tomcat-6.0.13.tar.gz
mv apache-tomcat-6.0.13 /usr/local/
ln -s /usr/local/apache-tomcat-6.0.13/ /usr/local/tomcat
```

tomcat-native

```
tar zxvf tomcat-native-1.1.10-src.tar.gz
cd tomcat-native-1.1.10-src/jni/native
./configure --with-apr=/usr/local/apache/bin/apr-1-config --with-java-home=/usr/local/java/
make
make install
```

catalina.sh

```
CATALINA_OPTS="-Djava.library.path=/usr/local/apr/lib"
JAVA_OPTS="-Xss128k -Xms128m -Xmx1024m -XX:PermSize=128M -XX:MaxPermSize=256m -
XX:MaxNewSize=256m"
```

启动

```
startup.sh
```

2.1. tomcat-native

```

cd /usr/local/tomcat-6.0.18/bin
tar zxvf tomcat-native.tar.gz
cd tomcat-native-1.1.14-src/jni/native
./configure --with-apr=/usr/local/apr --with-java-home=/usr/java/jdk1.6.0_11
make && make install
```

3. 配置 Tomcat 服务器

3.1. server.xml

```
    <Connector port="80" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
```

性能调整

```
    <Connector port="80" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443"
               maxThreads="2048" />

        <Connector port="80" protocol="HTTP/1.1"
                                maxThreads="2048"
                                minSpareThreads="64"
                                maxSpareThreads="256"
                                acceptCount="128"
                                enableLookups="false"
                                redirectPort="8443"
                                debug="0"
                                connectionTimeout="20000"
                                disableUploadTimeout="true"
                                URIEncoding="UTF-8" />
```

3.1.1. compression

压缩传送数据

```
compression="on"
compressionMinSize="2048"
noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/plain,text/javascript,text/css"
```

3.1.2. useBodyEncodingForURI

如果你的站点编码非UTF-8,去掉URIEncoding="UTF-8"使用下面选项.

useBodyEncodingForURI="true"

3.1.3. HTTPS

```
   <Connector port="443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               SSLEngine="on"
               SSLCertificateFile="${catalina.base}/conf/localhost.crt"
```

```
                SSLCertificateKeyFile="${catalina.base}/conf/localhost.key" />
```

3.1.4. 隐藏Tomcat版本信息

在Connector中加入server="Neo App Srv 1.0"

```
vim $CATALINA_HOME/conf/server.xml

    <Connector port="80" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443"
                                maxThreads="8192"
                                minSpareThreads="64"
                                maxSpareThreads="128"
                                acceptCount="128"
                                enableLookups="false"
                server="Neo App Srv 1.0"/>
```

```
# curl -I http://localhost:8080/
HTTP/1.1 400 Bad Request
Transfer-Encoding: chunked
Date: Thu, 20 Oct 2011 09:51:55 GMT
Connection: close
Server: Neo App Srv 1.0
```

3.1.5. vhost

传统配置方式

```
      <Host name="www.example.com"  appBase="webapps"
            unpackWARs="true" autoDeploy="true"
            xmlValidation="false" xmlNamespaceAware="false">
                        <Context path="" docBase="/www/example/www" debug="0"
reloadable="false"/>
      </Host>
      <Host name="news.example.com"  appBase="webapps"
            unpackWARs="true" autoDeploy="true"
            xmlValidation="false" xmlNamespaceAware="false">
                        <Context path="" docBase="/www/example/news" debug="0"
reloadable="false"/>
      </Host>
```

建议配置方式

```
vim server.xml

<Engine name="Catalina" defaultHost="neo">
    <Host name="neo"    appBase="neoapps"/>
    <Host name="other" appBase="otherapps"/>
</Engine>
```

Configuring Your Contexts

```
mkdir $CATALINA_HOME/conf/Catalina/neo

cp $CATALINA_HOME/conf/Catalina/localhost/manager.xml $CATALINA_HOME/conf/Catalina/neo/ROOT.xml

or

cp $CATALINA_HOME/conf/Catalina/localhost/manager.xml $CATALINA_HOME/conf/Catalina/neo
```

Webapps Directory

```
mkdir $CATALINA_HOME/neo
```

3.1.6. access_log

```
<Host name="localhost" ...>
  ...
  <Valve className="org.apache.catalina.valves.AccessLogValve"
         prefix="localhost_access_log." suffix=".txt"
         pattern="common"/>
  ...
</Host>
```

3.2. tomcat-users.xml

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>

<role rolename="manager"/>
<user username="tomcat" password="QI0Ajp7" roles="manager"/>

</tomcat-users>
```

状态监控 http://localhost/manager/status

服务管理 http://localhost/manager/html/list

3.3. logging.properties

修改日志目录

```
1catalina.org.apache.juli.FileHandler.level = FINE
#1catalina.org.apache.juli.FileHandler.directory = ${catalina.base}/logs
1catalina.org.apache.juli.FileHandler.directory = /www/logs/tomcat
1catalina.org.apache.juli.FileHandler.prefix = catalina.
```

---

4. Connector

4.1. server.xml

vi conf/server.xml

```
<Connector port="8009"
           maxThreads="4096"
           minSpareThreads="100"
           maxSpareThreads="500"
           enableLookups="false"
           acceptCount="15000"
           connectionTimeout="30000"
           redirectPort="8443"
           disableUploadTimeout="true"
           URIEncoding="UTF-8"
           protocol="AJP/1.3"/>
```

4.2. mod_jk

mod_jk 安装

```
tar zxvf tomcat-connectors-1.2.23-src.tar.gz
cd tomcat-connectors-1.2.23-src/native/
./configure --with-apxs=/usr/local/apache/bin/apxs
make
make install
chmod 755 /usr/local/apache/modules/mod_jk.so
```

httpd.conf 尾部加入

```
Include conf/mod_jk.conf
```

配置workers.properties

apache/conf/workers.properties

```
# Define 1 real worker using ajp13
worker.list=worker1
# Set properties for worker1 (ajp13)
worker.worker1.type=ajp13
worker.worker1.host=127.0.0.1
worker.worker1.port=8009
worker.worker1.lbfactor=1
worker.worker1.cachesize=128
worker.worker1.cache_timeout=600
worker.worker1.socket_keepalive=1
worker.worker1.reclycle_timeout=300
```

mod_jk.conf

apache/conf/mod_jk.conf

```
[chenjingfeng@d3010 Includes]$ cat mod_jk.conf
<IfModule mod_jk.c>
# Load mod_jk module
LoadModule jk_module            modules/mod_jk.so
# Where to find workers.properties
JkWorkersFile           /usr/local/apache/conf/workers.properties
# Where to put jk logs
JkLogFile               /usr/local/apache/logs/mod_jk.log
# Set the jk log level [debug/error/info]
JkLogLevel              error
# Select the log format
JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
# JkOptions indicate to send SSL KEY SIZE,
JkOptions     +ForwardKeySize +ForwardURICompat -ForwardDirectories
# JkRequestLogFormat set the request format
JkRequestLogFormat     "%w %V %T"
JkShmFile     /usr/local/apache2/logs/mod_jk.shm
# Send jsp,servlet for context * to worker named worker1
JkMount  /status/* worker1
JkMount  /*.jsp worker1
JkMount  /*.jsps worker1
JkMount  /*.do worker1
JkMount  /*Servlet worker1
JkMount  /jk/* worker1
</IfModule>
```

分别测试apache,tomcat

4.3. mod_proxy_ajp

包含虚拟主机配置文件

vi conf/httpd.conf

```
# Virtual hosts
Include conf/extra/httpd-vhosts.conf
```

虚拟主机中配置ProxyPass,ProxyPassReverse

vi conf/extra/httpd-vhosts.conf

```
<VirtualHost *:80>
    ServerName netkiller.8800.org
    ProxyPass /images !
        ProxyPass /css !
        ProxyPass /js !
    ProxyPass /ajp ajp://localhost:8009/ajp
    ProxyPassReverse /ajp ajp://localhost:8009/ajp
</VirtualHost>
```

反向代理和均衡负载模块

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so

ProxyPass /admin balancer://tomcatcluster/admin lbmethod=byrequests stickysession=JSESSIONID
nofailover=Off timeout=5 maxattempts=3
ProxyPassReverse /admin balancer://tomcatcluster/admin

<Proxy balancer://tomcatcluster>
        BalancerMember ajp://localhost:8009 route=web1
        BalancerMember ajp://localhost:10009 smax=10 route=web2
        BalancerMember ajp://localhost:11009 route=web3
        BalancerMember ajp://localhost:12009 smax=10 route=web4
</Proxy>
```

4.4. RewriteEngine 连接 Tomcat

```
RewriteEngine On
```

```
RewriteRule ^/(.*) ajp://localhost:8009/ajp/$1 [P]
RewriteRule ^/(.*\.(jsp|do|sevlet)) ajp://localhost:8009/ajp/$1 [P]
```

4.5. Testing file

测试目录

```
[root@backup tomcat]# mkdir webapps/ajp
[root@backup tomcat]# mkdir webapps/jk
[root@backup tomcat]# vi webapps/ajp/index.jsp
[root@backup tomcat]# vi webapps/jk/index.jsp
```

测试文件

cat index.jsp

```
<%@ page contentType="text/html;charset=utf-8"%>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>apache+tomcat</title>
</head>

<body>
<%="It works!"%>
<%=new java.util.Date()%>
</body>
</html>
```

---

5. Init.d Script

5.1. Script 1

```
#!/bin/bash
################################################################
# Script for Apache and Tomcat
# File:/etc/rc.d/init.d/www
################################################################
# Setup environment for script execution
#

# chkconfig: - 91 35
# description: Starts and stops the apache and tomcat daemons \
#              used to provide Neo Chen
#
# pidfile: /var/run/www/apache.pid
# pidfile: /var/run/www/tomcat.pid
# config:  /etc/apache2/apache2.conf


#APACHE_HOME=/usr/local/apache
#TOMCAT_HOME=/usr/local/tomcat
#APACHE_USER=apache
#TOMCAT_USER=tomcat

APACHE_HOME=/usr/local/apache-evaluation
TOMCAT_HOME=/usr/local/apache-tomcat-evaluation
APACHE_USER=root
TOMCAT_USER=root

OPEN_FILES=20480

# Source function library.
if [ -f /etc/init.d/functions ] ; then
  . /etc/init.d/functions
elif [ -f /etc/rc.d/init.d/functions ] ; then
  . /etc/rc.d/init.d/functions
else
  exit 0
fi

if [ ! -d /var/run/www ] ; then
  mkdir /var/run/www
fi

if [ -f /var/lock/subsys/tomcat ] ; then
        echo " "
fi

start() {
        if [ `ulimit -n` != ${OPEN_FILES} ]; then
                ulimit -n ${OPEN_FILES}
        fi
        echo -en "\\033[1;32;1m"
        echo "Starting Tomcat $TOMCAT_HOME ..."
        echo -en "\\033[0;39;1m"
        if [ -s /var/run/www/tomcat.pid ]; then
                echo "tomcat (pid `cat /var/run/www/tomcat.pid`) already running"
        else
                su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh start > /dev/null"
                echo `pgrep java` > /var/run/www/tomcat.pid
                touch /var/lock/subsys/tomcat
        fi
        sleep 2
        echo -en "\\033[1;32;1m"
        echo "Starting Apache $APACHE_HOME ..."
        echo -en "\\033[0;39;1m"
        su - ${APACHE_USER} -c "$APACHE_HOME/bin/apachectl start"
        touch /var/lock/subsys/apache
}

stop() {
        echo -en "\\033[1;32;1m"
        echo "Shutting down Apache $APACHE_HOME ..."
        echo -en "\\033[0;39;1m"
        su - ${APACHE_USER} -c "$APACHE_HOME/bin/apachectl stop"
        sleep 2
        echo -en "\\033[1;32;1m"
        echo "Shutting down Tomcat $TOMCAT_HOME ..."
        echo -en "\\033[0;39;1m"
```

```
        su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh stop > /dev/null"
        rm -rf /var/run/www/tomcat.pid
        rm -f /var/lock/subsys/tomcat
        rm -f /var/lock/subsys/apache
}

restart() {
    stop
        if [ "`pgrep java`" = "" ]&& [ "`pgrep httpd`" = "" ]; then
                start
                exit 0
    else
                echo "Usage: $0 killall (^C)"
                echo -n "Waiting: "
    fi
    while true;
        do
                sleep 1
                if [ "`pgrep java`" = "" ] && [ "`pgrep httpd`" = "" ]; then
                        break
                else
                        echo -n "."
                        #echo -n "Enter your [y/n]: "; read ISKILL;
                fi
        done
        echo
    start
}

status() {
                ps -aux | grep -e tomcat -e apache

                echo -en "\\033[1;32;1m"
                echo ulimit open files: `ulimit -n`
                echo -en "\\033[0;39;1m"

                echo -en "\\033[1;32;1m"
                echo -en "httpd count:"
                ps axf|grep httpd|wc -l
                echo -en "\\033[0;39;1m"
}

killall() {
        if [ "`pgrep httpd`" != "" ]; then
                echo -en "\\033[1;32;1m"
                echo "kill Apache pid(`pgrep httpd`) ..."
                kill -9 `pgrep httpd`
                echo -en "\\033[0;39;1m"
        fi
        if [ "`pgrep java`" != "" ]; then
                echo -en "\\033[1;32;1m"
                echo "kill Tomcat pid(`pgrep java`) ..."
                kill -9 `pgrep java`
                echo -en "\\033[0;39;1m"
        fi
        rm -rf /var/run/www/tomcat.pid
        rm -f /var/lock/subsys/tomcat
        rm -f /var/lock/subsys/apache
}

# Determine and execute action based on command line parameter
case "$1" in
        start)
                start
                ;;
        stop)
                stop
                ;;
        restart)
                restart
                ;;
        status)
                status
                ;;
        killall)
                killall
                ;;
        *)
                echo -en "\\033[1;32;1m"
                echo "Usage: $1 {start|stop|restart|status|killall}"
                echo -en "\\033[0;39;1m"
                ;;
esac
echo -en "\\033[0;39;m"
exit 0
```

5.2. Shell Script 2

Apache,Tomcat 运行脚本

例 41.2. /etc/rc.d/init.d/www

```
#!/bin/bash
##############################################################
# Script for Apache and Tomcat
# File:/etc/rc.d/init.d/www
##############################################################
# Setup environment for script execution
#

# chkconfig: - 91 35
# description: Starts and stops the apache and tomcat daemons \
#              used to provide Neo Chen<openunix@163.com>
#
# pidfile: /var/run/www/apache.pid
# pidfile: /var/run/www/tomcat.pid
# config:  /etc/apache2/apache2.conf


#APACHE_HOME=/usr/local/apache
#TOMCAT_HOME=/usr/local/tomcat
#APACHE_USER=apache
#TOMCAT_USER=tomcat

APACHE_HOME=/usr/local/apache
TOMCAT_HOME=/usr/local/tomcat
APACHE_USER=root
TOMCAT_USER=root
WAIT_TIME=10
get_apache_pid(){
    APACHE_PID=`pgrep -o httpd`
    echo $APACHE_PID
}
get_tomcat_pid(){
    TOMCAT_PID=`ps axww | grep catalina.home | grep -v 'grep' | sed q | awk '{print $1}'`
    echo $TOMCAT_PID
}

#OPEN_FILS=40960

# Source function library.
#if [ -f /etc/init.d/functions ] ; then
#  . /etc/init.d/functions
#elif [ -f /etc/rc.d/init.d/functions ] ; then
#  . /etc/rc.d/init.d/functions
#else
#  exit 0
#fi

if [ ! -d /var/run/www ] ; then
  mkdir /var/run/www
fi

#if [ -f /var/lock/subsys/tomcat ] ; then
#fi

start() {
        #if [ `ulimit -n` -le  ${OPEN_FILES} ]; then
        #       ulimit -n ${OPEN_FILES}
        #fi
        echo -en "\\033[1;32;1m"
        echo "Starting Tomcat $TOMCAT_HOME ..."
        echo -en "\\033[0;39;1m"
        if [ -s /var/run/www/tomcat.pid ]; then
                echo "tomcat (pid `cat /var/run/www/tomcat.pid`) already running"
        else
                su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh start > /dev/null"
                echo `get_tomcat_pid` > /var/run/www/tomcat.pid
                touch /var/lock/subsys/tomcat
        fi
        sleep 2
        echo -en "\\033[1;32;1m"
        echo "Starting Apache $APACHE_HOME ..."
        echo -en "\\033[0;39;1m"
        su - ${APACHE_USER} -c "$APACHE_HOME/bin/apachectl start"
        touch /var/lock/subsys/apache
}

stop() {
        echo -en "\\033[1;32;1m"
        echo "Shutting down Apache $APACHE_HOME ..."
        echo -en "\\033[0;39;1m"
        su - ${APACHE_USER} -c "$APACHE_HOME/bin/apachectl stop"
        sleep 2
        echo -en "\\033[1;32;1m"
        echo "Shutting down Tomcat $TOMCAT_HOME ..."
        echo -en "\\033[0;39;1m"
        su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh stop > /dev/null"
        rm -rf /var/run/www/tomcat.pid
        rm -f /var/lock/subsys/tomcat
        rm -f /var/lock/subsys/apache
}

restart() {
    stop
    sleep 2
    if [ -z `get_tomcat_pid` ]&& [ -z `get_apache_pid` ]; then
                start
                exit 0
    else
                echo "Usage: $0 killall (^C)"
                echo -n "Waiting: "
    fi
    while true;
        do
                sleep 1
                if [ -z `get_tomcat_pid` ] && [ -z `get_apache_pid` ]; then
```

```
                        break
                else
                        echo -n "."
                fi
        done
        echo
    start
}

k9restart() {
    ISEXIT='false'
    stop
    for i in `seq 1 ${WAIT_TIME}`;
    do
                if [ -z `get_tomcat_pid` ] && [ -z `get_apache_pid` ]; then
                ISEXIT='true'
                break
                else
                        sleep 1
                fi
        done

        if [ $ISEXIT == 'false' ]; then
            while true;
                do
                        if [ -z `get_tomcat_pid` ] && [ -z `get_apache_pid` ]; then
                                ISEXIT='true'
                        break
                        fi

                        if [ -n `get_apache_pid` ]; then
                                kill -9 `pgrep httpd`
                        fi
                        if [ -n `get_tomcat_pid` ]; then
                                kill -9 `get_tomcat_pid`
                        fi
                done
                rm -rf /var/run/www/tomcat.pid
                rm -f /var/lock/subsys/tomcat
                rm -f /var/lock/subsys/apache
        fi

        echo

        if [ $ISEXIT == 'true' ]; then
                start
        fi
}

status() {
                #ps -aux | grep -e tomcat -e apache

                echo -en "\\033[1;32;1m"
                echo ulimit open files: `ulimit -n`
                echo -en "\\033[0;39;1m"

                echo -en "\\033[1;32;1m"
                echo -en "httpd count:"
                let hc=`ps axf|grep httpd|wc -l`-1
                echo $hc
                echo -en "apache count:"
                netstat -alp | grep '*:http' | wc -l
                echo -en "tomcat count:"
                netstat -alp | grep '*:webcache' | wc -l
                echo -en "dbconn count:"
                netstat -a | grep ':3433' | wc -l
                echo -en "\\033[0;39;1m"
}

kall() {
        if [ `get_apache_pid` ]; then
                echo -en "\\033[1;32;1m"
                echo "kill Apache pid(`pgrep httpd`) ..."
                kill `pgrep httpd`
                echo -en "\\033[0;39;1m"
        fi
        if [ `get_tomcat_pid` ]; then
                echo -en "\\033[1;32;1m"
                echo "kill Tomcat pid(`pgrep java`) ..."
                kill `pgrep java`
                echo -en "\\033[0;39;1m"
        fi
        rm -rf /var/run/www/tomcat.pid
        rm -f /var/lock/subsys/tomcat
        rm -f /var/lock/subsys/apache
}

reload() {
        killall -HUP httpd
}

tomcat_restart() {
    su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh stop > /dev/null"
    rm -rf /var/run/www/tomcat.pid
    rm -f /var/lock/subsys/tomcat
    sleep 2
    if [ -z `get_tomcat_pid` ]; then
        su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh start > /dev/null"
        exit 0
    else
        echo "Usage: $0 killall (^C)"
        echo -n "Waiting: "
    fi
    while true;
    do
```

```
                sleep 1
                if [ -z `get_tomcat_pid` ]; then
                        echo
                        break
                else
                        echo -n "."
                        #echo -n "Enter your [y/n]: "; read ISKILL;
                fi
    done
    su - ${TOMCAT_USER} -c "$TOMCAT_HOME/bin/catalina.sh start > /dev/null"
    echo `get_tomcat_pid` > /var/run/www/tomcat.pid
    touch /var/lock/subsys/tomcat
}


# Determine and execute action based on command line parameter
case $1 in
    apache)
        case "$2" in
            reload)
                reload
                ;;
            *)
                su - ${APACHE_USER} -c "${APACHE_HOME}/bin/apachectl $2"
                ;;
        esac
        ;;
    tomcat)
        case "$2" in
            restart)
                tomcat_restart
                ;;
            *)
                su - ${TOMCAT_USER} -c "${TOMCAT_HOME}/bin/catalina.sh $2"
                ;;
        esac
        ;;
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        restart
        ;;
    status)
        status
        ;;
    killall)
        kall
        ;;
    k9restart)
        k9restart >/dev/null
        ;;
    *)
        echo -en "\\033[1;32;1m"
        echo "Usage: $0 {start|stop|restart|status|killall|k9restart}"
        echo "Usage: $0 apache {start|restart|graceful|graceful-stop|stop|reload}"
        echo "Usage: $0 tomcat {debug|run|start|restart|stop|version}"
        echo -en "\\033[0;39;1m"
        ;;
esac
echo -en "\\033[0;39;m"
exit 0
```

```
chmod 700 /etc/init.d/www
```

第 42 章 Resin

目录

http://www.caucho.com

1. 安装Resin

JRE

```
$ sudo apt-get install sun-java6-jre
```

下载Resin

注意: Resin Pro 与 Resin 前者要Licence

1.1. 直接使用

简易安装，直接解压缩后即可使用

```
$ wget http://www.caucho.com/download/resin-4.0.1.tar.gz
$ tar zxvf resin-4.0.1.tar.gz
$ sudo mv resin-4.0.1 ..
$ cd ..
$ sudo ln -s resin-4.0.1 resin
```

```

```

1.2. Debian/Ubuntu

```
$ wget http://www.caucho.com/download/resin_4.0.1-i386.deb
```

安装 Resin

```
$ sudo dpkg -i resin_4.0.1-i386.deb
```

1.3. 源码安装Resin

源码安装

```
$ cd /usr/local/src/
$ wget http://www.caucho.com/download/resin-4.0.1.tar.gz
$ tar zxvf resin-4.0.1.tar.gz
$ ./configure --prefix=/usr/local/resin-4.0.1 \
--with-apxs=/usr/local/httpd/bin/apxs \
--with-java-home=/usr/local/java \
--enable-64bit \
--enable-lfs \
--enable-ssl \
--enable-debug
$ make && make install
$ cd ..
$ sudo ln -s resin-4.0.1 resin
```

设置 resin 以服务的形式开机自启动

```
$ sudo cp /usr/local/resin/contrib/init.resin /etc/init.d/resin
$ sudo chmod 755 /etc/init.d/resin
$ sudo update-rc.d resin defaults 99
```

2. Compiling mod_caucho.so

```
unix> ./configure --with-apxs=/usr/local/apache/bin/apxs
unix> make && make install
```

```
#
# mod_caucho Resin Configuration
#
LoadModule caucho_module /usr/local/apache/modules/mod_caucho.so
ResinConfigServer localhost 6802
CauchoConfigCacheDirectory /tmp
CauchoStatus yes
<Location /caucho-status>
  SetHandler caucho-status
</Location>
```

```
<IfModule mod_caucho.c>
ResinConfigServer localhost 6802
<Location /caucho-status>
SetHandler caucho-status
</Location>
</IfModule>

AddHandler caucho-request jsp
<Location /servlet/*>
SetHandler caucho-request
</Location>


<IfModule mod_caucho.c>
        <LocationMatch (.*?)\.action>
                SetHandler caucho-request
        </LocationMatch>
        <LocationMatch (.*?)\.jsp>
                SetHandler caucho-request
        </LocationMatch>
        <LocationMatch (.*?)\.do>
                SetHandler caucho-request
        </LocationMatch>
</IfModule>
```

3. resin.conf

3.1. Maximum number of threads

Maximum number of threads.

```
<thread-max>4096</thread-max>
```

thread-max数值需要使用ab命令做压力测试，逐步调整。

3.2. Configures the keepalive

```
      <!-- Configures the keepalive -->
      <keepalive-max>128</keepalive-max>
      <keepalive-timeout>15s</keepalive-timeout>
```

3.3. ssl

```
<http address="*" port="443">
  <openssl>
  <certificate-file>/srv/keys/example.com/star.example.com.crt</certificate-file>
  <certificate-key-file>/srv/keys/example.com/star.example.com.key</certificate-key-file>
  <password>4fff74da-aea4-a9fc-4b5f-e6d497588726</password>
  </openssl>
</http>
```

自颁发证书，首先是使用keytool工具安装证书

```
生成证书:
keytool -genkeypair -keyalg RSA -keysize 2048 SHA1withRSA -validity 3650  -alias neo -keystore
server.keystore -storepass password -dname "CN=www.example.com, OU=test, O=example.com, L=SZ,
ST=GD, C=CN"

导出证书
-keytool -exportcert -alias neo -keystore server.keystore -storepass password  -file server.cer
-rfc

打印证书
Keytool -printcert -file server.cer

导出证书签发申请
Keytool -certreg -aias neo -keystore server.keystore -storepass password -file ins.csr -v

导入证书
Keytool -importcert -trustcacerts -alias neo -file server.cer -keystore server.keystore -
storepass password

查看数字证书
Keytool -list

当成功的导入了证书以后就要容器中进行配置才可以使用
首先是要把证书中的那个 server.keystore 和 server.cer这两个文件放入到Resin服务器的keys这个文件夹中 如果没有的
话 就手动的建立这个文件夹
然后去 config 文件夹下配置你的配置文件
我在resin 这个容器中的配置如下
```

```
<http address="*" port="443">
    <jsse-ssl>
       <key-store-file>keys/server.keystore</key-store-file>
       <password>password</password>
    </jsse-ssl>
</http>
```

---

4. virtual hosts

4.1. explicit host

例 42.1. explicit host in resin.conf

```
<resin xmlns="http://caucho.com/ns/resin">
<cluster id="">

<host host-name="www.foo.com">
  <host-alias>foo.com</host-alias>
  <host-alias>web.foo.com</host-alias>

  <root-directory>/opt/www/www.foo.com</root-directory>

  <web-app id="/" document-directory="webapps/ROOT">

  </web-app>
  ...
</host>

</cluster>
</resin>
```

4.2. regexp host

例 42.2. regexp host in resin.conf

```
<resin xmlns="http://caucho.com/ns/resin">
<cluster id="">

<host regexp="([^.]+)\.foo\.com">
  <host-name>${host.regexp[1]}.foo.com</host-name>

  <root-directory>/var/www/hosts/www.${host.regexp[1]}.com</root-directory>

  ...
</host>

</cluster>
</resin>
```

4.3. host-alias

例 42.3. host-alias in the resin.conf

```
<resin xmlns="http://caucho.com">
<cluster id="">
```

```
  <host id="www.foo.com" root-directory="/var/www/foo.com">
    <host-alias>foo.com</host-alias>

    <web-app id=""/>
  </host>

</cluster>
</resin>
```

例 42.4. host-alias in a /var/www/hosts/foo/host.xml

```
<host xmlns="http://caucho.com">

  <host-name>www.foo.com</host-name>
  <host-alias>foo.com</host-alias>

  <web-app id="" root-directory="htdocs"/>

</host>
```

例 42.5. host-alias-regexp in the resin.conf

```
<resin xmlns="http://caucho.com">
<cluster id="">

  <host id="www.foo.com" root-directory="/var/www/foo.com">
    <host-alias-regexp>.*foo.com</host-alias-regexp>

    <web-app id=""/>
  </host>

</cluster>
</resin>
```

4.4. configures a deployment directory for virtual hosts

```
<resin xmlns="http://caucho.com/ns/resin">
  <cluster id="app-tier">
    <root-directory>/var/www</root-directory>

    <host-deploy path="hosts">
      <host-default>
        <resin:import path="host.xml" optional="true"/>

        <web-app-deploy path="webapps"/>
      </host-default>
    </host-deploy>
  </cluster>
</resin>
```

$RESIN_HOME/hosts其下的任何目录将对应一个虚拟主机。在$RESIN_HOME/hosts下也可以放置jar文件，其会被展开变成一个虚拟主机。

```
$RESIN_HOME/hosts/www.example.com
$RESIN_HOME/hosts/www.example.net
$RESIN_HOME/hosts/www.example.org
```

4.5. Resources

例 42.6. shared database in host

```
<resin xmlns="http://caucho.com/ns/resin">
  <cluster id="app-tier">
     <server id="a" .../>

     <host id="www.foo.com">
        <database jndi-name="jdbc/test">
            <driver type="org.postgresql.Driver">
                <url>jdbc:postgresql://localhost/test</url>
                <user>caucho</user>
            </driver>
        </database>

        <web-app-default path="webapps"/>
    </host>
  </cluster>
</resin>
```

Oracle JDBC

```
<database>
        <jndi-name>jdbc/test</jndi-name>
        <driver type="oracle.jdbc.pool.OracleConnectionPoolDataSource">
        <url>jdbc:oracle:thin:@172.16.0.1:1521:database</url>
        <user>user</user>
        <password>password</password>
        </driver>
        <prepared-statement-cache-size>8</prepared-statement-cache-size>
        <max-connections>1024</max-connections>
        <max-idle-time>20s</max-idle-time>
</database>
```

例 42.7. rewrite-dispatch

```
<resin xmlns="http://caucho.com/ns/resin">
  <cluster id="app-tier">

    <host host-name="www.foo.com">
      <rewrite-dispatch>
        <redirect regexp="^/foo" target="/index.php?foo="/>
      </rewrite-dispatch>
    </host>

  </cluster>
</resin>
```

5. FAQ

5.1. java.lang.OutOfMemoryError: PermGen space

```
vim /usr/local/resin/conf/resin.conf

<jvm-arg>-XX:PermSize=128M</jvm-arg>
<jvm-arg>-XX:MaxPermSize=512m</jvm-arg>
```

第 43 章 Application Server

目录

1. Zope

参考Python安装

1. 下载 Zope-3

```
wget http://www.zope.org/Products/Zope3/3.3.1/Zope-3.3.1.tgz
tar zxvf Zope-3.3.1.tgz
cd cd Zope-3.3.1
```

2. configure

```
./configure --prefix=/usr/local/Zope --with-python=/usr/local/python2.4/bin/python

make
make check
make install
```

3. 创建一个Zope实例

```
cd /usr/local/Zope
./bin/mkzopeinstance -u neo:chen -d /usr/local/Zope/webapps
cd webapps
./bin/runzope
```

4. 测试

```
http://netkiller.8800.org:8080/
```

2. JBoss - JBoss Enterprise Middleware

参考Java安装

1. 下载安装 JBoss

```
cd /usr/local/src/
wget http://nchc.dl.sourceforge.net/sourceforge/jboss/jboss-5.0.0.Beta2.zip
unzip jboss-5.0.0.Beta2.zip
mv jboss-5.0.0.Beta2 ..
cd ..
ln -s jboss-5.0.0.Beta2 jboss
```

2. 运行 Jboss

```
cd jboss/bin
chmod +x *.sh
./run.sh
```

第 44 章 Search Engine

目录

1. Solr

http://lucene.apache.org/solr/

java 采用apt-get安装

例 44.1. /etc/profile.d/java.sh

```
##################################################
### Java environment by neo
##################################################
export JAVA_HOME=/usr
export JRE_HOME=/usr
export PATH=$PATH:/usr/local/apache-tomcat/bin/:/usr/local/jetty-6.1.18/bin
export CLASSPATH="./:/usr/share/java/:/usr/local/apache-solr/example/multicore/lib"
```

```
export JAVA_OPTS="-Xms128m -Xmx1024m"
```

1.1. Embedded Jetty

```
wget http://apache.freelamp.com/lucene/solr/1.3.0/apache-solr-1.3.0.tgz
tar zxvf apache-solr-1.3.0.tgz
ln -s apache-solr-1.3.0 ../apache-solr
cd ../apache-solr/example/
java -jar start.jar
```

multicore: java -Dsolr.solr.home=multicore -jar start.jar

1.2. Jetty

http://jetty.mortbay.org/jetty/

过程 44.1. apt-get install

1. install

```
$ sudo apt-get install libxpp3-java
$ sudo apt-get install solr-jetty
```

2. firewall

```
$ sudo ufw allow 8280
```

3. Testing.

   http://172.16.0.1:8280/

   http://172.16.0.1:8280/admin/ (user:admin, passwd:admin)

过程 44.2. source codes install

- download

```
wget http://dist.codehaus.org/jetty/jetty-6.1.18/jetty-6.1.18.zip
```

1.3. Tomcat

http://tomcat.apache.org/

1. download

```
cd /usr/local/src

wget http://apache.etoak.com/tomcat/tomcat-6/v6.0.20/bin/apache-tomcat-6.0.20.tar.gz
wget http://apache.freelamp.com/lucene/solr/1.3.0/apache-solr-1.3.0.tgz

tar zxvf apache-tomcat-6.0.20.tar.gz
ln -s apache-tomcat-6.0.20 ../apache-tomcat

tar zxvf apache-solr-1.3.0.tgz
ln -s apache-solr-1.3.0 ../apache-solr
```

2. solr.xml

```
vim /usr/local/apache-tomcat/conf/Catalina/localhost/solr.xml

<Context docBase="/usr/local/apache-solr/dist/apache-solr-1.3.0.war" debug="0"
crossContext="true" >
   <Environment name="solr/home" type="java.lang.String" value="/usr/local/apache-
solr/example/solr" override="true" />
</Context>
```

1.4. solr-php-client

http://code.google.com/p/solr-php-client/

```
wget http://solr-php-client.googlecode.com/files/SolrPhpClient.2009-03-11.tgz
tar zxvf SolrPhpClient.2009-03-11.tgz
sudo mv SolrPhpClient/Apache /usr/share/php/
```

1.5. multicore

solr.xml

```
vim /usr/local/apache-solr/example/multicore/solr.xml

<?xml version="1.0" encoding="UTF-8" ?>
<solr persistent="false">
  <cores adminPath="/admin/cores">
    <core name="core0" instanceDir="core0" />
    <core name="core1" instanceDir="core1" />

    <core name="article" instanceDir="article" />

  </cores>
</solr>
```

core directory and config file

```
mkdir -p article/conf

vim article/conf/solrconfig.xml

<?xml version="1.0" encoding="UTF-8" ?>
<config>
  <updateHandler class="solr.DirectUpdateHandler2" />
  <requestDispatcher handleSelect="true" >
    <requestParsers enableRemoteStreaming="false" multipartUploadLimitInKB="2048" />
  </requestDispatcher>
  <requestHandler name="standard" class="solr.StandardRequestHandler" default="true" />
  <requestHandler name="/update" class="solr.XmlUpdateRequestHandler" />
  <requestHandler name="/admin/" class="org.apache.solr.handler.admin.AdminHandlers" />
  <admin>
    <defaultQuery>solr</defaultQuery>
  </admin>
</config>

vim article/conf/schema.xml

<?xml version="1.0" ?>
<schema name="example core zero" version="1.1">
  <types>
   <fieldType name="sint" class="solr.SortableIntField" sortMissingLast="true"
```

```
omitNorms="true"/>
   <fieldtype name="string"  class="solr.StrField" sortMissingLast="true" omitNorms="true"/>
   <fieldType name="date" class="solr.DateField" sortMissingLast="true" omitNorms="true"/>
   <fieldType name="text" class="solr.TextField" positionIncrementGap="100" />
  </types>
 <fields>
  <!-- general -->
  <field name="id"      type="sint"   indexed="true"  stored="true"  multiValued="false"
required="true"/>
  <field name="type"    type="string"   indexed="true"  stored="true"  multiValued="false" />
  <field name="name"    type="string"   indexed="true"  stored="true"  multiValued="false" />
  <field name="title"   type="string"   indexed="true"  stored="true"  multiValued="false" />
  <field name="content"   type="text"   indexed="true"  stored="true"  multiValued="false" />
  <field name="timestamp" type="date" indexed="true" stored="true" default="NOW"/>
 </fields>
 <!-- field to use to determine and enforce document uniqueness. -->
 <uniqueKey>id</uniqueKey>
 <!-- field for the QueryParser to use when an explicit fieldname is absent -->
 <defaultSearchField>content</defaultSearchField>
 <!-- SolrQueryParser configuration: defaultOperator="AND|OR" -->
 <solrQueryParser defaultOperator="OR"/>
        <copyField source="title" dest="content"/>
        <copyField source="name" dest="content"/>
</schema>
```

commit datas

```
vim test.xml

<add>
        <doc>
          <field name="id">1</field>
          <field name="name">Hello world</field>
        </doc>

        <doc>
          <field name="id">2</field>
          <field name="title">Title Hello world</field>
        </doc>

        <doc>
          <field name="id">3</field>
          <field name="name">Hello world 1</field>
          <field name="content">Content 1</field>
        </doc>

        <doc>
          <field name="id">4</field>
          <field name="name">Name Neo</field>
        </doc>

        <doc>
          <field name="id">5</field>
          <field name="name">Last Chan</field>
        </doc>
</add>


java -Durl=http://localhost:8983/solr/article/update -Dcommit=yes -jar ../exampledocs/post.jar
test.xml
```

1.6. 中文分词

1.6.1. ChineseTokenizerFactory

```
<fieldType name="text" class="solr.TextField" >
    <analyzer>
        <tokenizer class="org.apache.solr.analysis.ChineseTokenizerFactory"/>
    </analyzer>
</fieldType>
```

1.6.2. CJK

```
<fieldType name="text" class="solr.TextField" positionIncrementGap="100">
        <analyzer>
        <tokenizer class="solr.CJKTokenizerFactory"/>
        </analyzer>
</fieldType>
```

1.6.3. mmseg4j

http://code.google.com/p/mmseg4j/

install

```
$ cd /usr/local/src/
$ wget http://mmseg4j.googlecode.com/files/mmseg4j-1.7.2.zip
$ unzip mmseg4j-1.7.2.zip
$ mkdir /usr/local/apache-solr/example/multicore/lib
$ cp /usr/local/src/mmseg4j-1.7.2/mmseg4j-all-1.7.2.jar /usr/local/apache-solr/example/multicore/lib
$ cd mmseg4j-1.7.2/
```

test

```
$ java -Dmmseg.dic.path=/usr/local/apache-solr/example/solr -jar mmseg4j-all-1.7.2.jar 这里是字符串
$ java -Dmmseg.dic.path=/usr/local/apache-solr/example/solr -cp .:mmseg4j-all-1.7.2.jar com.chenlb.mmseg4j.example.Simple 这里是字符串
$ java -Dmmseg.dic.path=/usr/local/apache-solr/example/solr -cp .:mmseg4j-all-1.7.2.jar com.chenlb.mmseg4j.example.MaxWord 这里是字符串
```

mmseg4j 在 solr 中主要支持两个参数：mode、dicPath。mode 表示是什么模式分词（有效值：simplex、complex、max-word，如果输入了无效的默认用 max-word。）。dicPath 是词库目录可以是绝对目录，也可以是相对目录（是相对 solr.home 目录下的，dic 就会在 solr.home/dic 目录下找词库文件），如果不指定就是默认在 CWD/data 目录（程序运行当前目录的data子目录）下找。

分词例子

```
<fieldtype name="textComplex" class="solr.TextField">
        <analyzer>
                <tokenizer class="com.chenlb.mmseg4j.solr.MMSegTokenizerFactory"
                        mode="complex" dicPath="dic">
                </tokenizer>
        </analyzer>
</fieldtype>

<fieldtype name="textMaxWord" class="solr.TextField">
        <analyzer>
                <tokenizer class="com.chenlb.mmseg4j.solr.MMSegTokenizerFactory"
                        mode="max-word" dicPath="dic">
                </tokenizer>
        </analyzer>
</fieldtype>

<fieldtype name="textSimple" class="solr.TextField">
        <analyzer>
                <tokenizer class="com.chenlb.mmseg4j.solr.MMSegTokenizerFactory"
                        mode="simple" dicPath="/usr/local/apache-solr/example/solr/my_dic">
                </tokenizer>
        </analyzer>
</fieldtype>
```

添加到schema.xml

```
<fieldType name="text" class="solr.TextField" positionIncrementGap="100" >
    <analyzer>
        <tokenizer class="com.chenlb.mmseg4j.solr.MMSegTokenizerFactory" mode="complex" dicPath="dic"/>
        <filter class="solr.LowerCaseFilterFactory"/>
    </analyzer>
</fieldType>
```

http://localhost:8080/solr/admin/analysis.jsp 在 Field 的下拉菜单选择 name，然后在应用输入 complex。可以看 mmseg4j 的分词的结果.

1.6.4. 中文分词“庖丁解牛” Paoding Analysis

```
$ cd /usr/local/src/
$ mkdir paoding-analysis-2.0.4-beta
$ cd paoding-analysis-2.0.4-beta/
$ wget http://paoding.googlecode.com/files/paoding-analysis-2.0.4-beta.zip
$ unzip paoding-analysis-2.0.4-beta.zip
$ cp paoding-analysis.jar /usr/local/apache-solr/example/multicore/lib/
```

ChineseTokenizerFactory

```

```

---

2. Nutch

http://lucene.apache.org/nutch/

How to Setup Nutch and Hadoop

http://wiki.apache.org/nutch/NutchHadoopTutorial

1. 下载

```
$ cd /usr/local/src/
$ wget http://apache.etoak.com/lucene/nutch/nutch-1.0.tar.gz
$ tar zxvf nutch-1.0.tar.gz
$ sudo cp -r nutch-1.0 ..
$ cd ..
$ sudo ln -s nutch-1.0 apache-nutch
```

2. 创建文件myurl

```
$ cd apache-nutch
$ mkdir urls
$ vim urls/myurl
http://netkiller.8800.org/
```

3. 配置文件 crawl-urlfilter.txt

   编辑conf/crawl-urlfilter.txt文件，修改MY.DOMAIN.NAME部分，把它替换为你想要抓取的域名

```
$ cp conf/crawl-urlfilter.txt conf/crawl-urlfilter.txt.old
$ vim conf/crawl-urlfilter.txt

# accept hosts in MY.DOMAIN.NAME
+^http://([a-z0-9]*\.)*MY.DOMAIN.NAME/
修改为:
# accept hosts in MY.DOMAIN.NAME
+^http://([a-z0-9]*\.)*netkiller.8800.org/
```

4. http.agent.name

```
$ vim conf/nutch-site.xml
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>

<!-- Put site-specific property overrides in this file. -->

<configuration>

<property>
  <name>http.agent.name</name>
  <value>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1) Gecko/20090624
Firefox/3.5</value>
  <description>HTTP 'User-Agent' request header. MUST NOT be empty -
  please set this to a single word uniquely related to your organization.

  NOTE: You should also check other related properties:

    http.robots.agents
    http.agent.description
    http.agent.url
    http.agent.email
```

```
    http.agent.version

  and set their values appropriately.

  </description>
</property>

<property>
  <name>http.agent.description</name>
  <value></value>
  <description>Further description of our bot- this text is used in
  the User-Agent header.  It appears in parenthesis after the agent name.
  </description>
</property>

<property>
  <name>http.agent.url</name>
  <value>http://netkiller.8800.org/robot.html</value>
  <description>A URL to advertise in the User-Agent header.  This will
   appear in parenthesis after the agent name. Custom dictates that this
   should be a URL of a page explaining the purpose and behavior of this
   crawler.
  </description>
</property>

<property>
  <name>http.agent.email</name>
  <value>openunix@163.com</value>
  <description>An email address to advertise in the HTTP 'From' request
   header and User-Agent header. A good practice is to mangle this
   address (e.g. 'info at example dot com') to avoid spamming.
  </description>
</property>

</configuration>
```

5. 运行以下命令行开始工作

$ bin/nutch crawl urls -dir crawl -depth 3 -threads 5

```
bin/nutch crawl <your_url> -dir <your_dir> -depth 2 -threads 4 >&logs/logs1.log

urls 存放需要爬行的url文件的目录，即目录/nutch/urls。
-dir  dirnames          设置保存所抓取网页的目录.
-depth  depth           表明抓取网页的层次深度
-delay  delay           表明访问不同主机的延时，单位为“秒”
-threads  threads       表明需要启动的线程数
-topN 50        topN    一个网站保存的最大页面数。


$ nohup bin/nutch crawl /usr/local/apache-nutch/urls -dir /usr/local/apache-nutch/crawl -
depth 5 -threads 50 -topN 50 > /tmp/nutch.log &
```

6. depoly

```
$ cd /usr/local/apache-tomcat/conf/Catalina/localhost
$ vim nutch.xml
<Context docBase="/usr/local/apache-nutch/nutch-1.0.war" debug="0" crossContext="true" >
</Context>
```

searcher.dir

```
$ vim /usr/local/apache-tomcat/webapps/nutch/WEB-INF/classes/nutch-site.xml

<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>

<!-- Put site-specific property overrides in this file. -->

<configuration>
    <property>
        <name>searcher.dir</name>
        <value>/usr/local/apache-nutch/crawl</value>
    </property>
</configuration>
```

test

http://172.16.0.1:8080/nutch/

3. Lucene

http://lucene.apache.org/

4. MG4J

http://mg4j.dsi.unimi.it/

5. PhpDig

http://www.phpdig.net/

PhpDig is a web spider and search engine written in PHP, using a MySQL database and flat file support. PhpDig builds a glossary with words found in indexed pages. On a search query, it displays a result page containing the search keys, ranked by occurrence.

6. Sphinx

http://sphinxsearch.com/

```
sudo apt-get install sphinxsearch
```

/etc/sphinxsearch/sphinx.conf

```
sudo cp /etc/sphinxsearch/sphinx-min.conf.dist /etc/sphinxsearch/sphinx.conf
```

创建测试数据库并导入测试数据

```
$ wget http://sphinxsearch.googlecode.com/svn/trunk/example.sql
$ mysql -h localhost -uroot -p < example.sql
$ mysql -h localhost -uroot -p
CREATE USER 'test'@'localhost' IDENTIFIED BY  '';
GRANT SELECT ON test.* TO 'test'@'localhost';
FLUSH PRIVILEGES;
mysql> quit


$ echo "select * from documents" | mysql -utest -p test
Enter password:
id      group_id        group_id2       date_added      title   content
1       1       5       2011-02-12 15:29:34     test one        this is my test document number
one. also checking search within phrases.
2       1       6       2011-02-12 15:29:34     test two        this is my test document number
two
3       2       7       2011-02-12 15:29:34     another doc     this is another group
4       2       8       2011-02-12 15:29:34     doc number four this is to test groups
```

创建索引

sudo indexer <index>

```
$ sudo indexer test1

Sphinx 0.9.8.1-release (r1533)
Copyright (c) 2001-2008, Andrew Aksyonoff

using config file '/etc/sphinxsearch/sphinx.conf'...
indexing index 'test1'...
collected 4 docs, 0.0 MB
sorted 0.0 Mhits, 100.0% done
total 4 docs, 193 bytes
total 0.012 sec, 16531.05 bytes/sec, 342.61 docs/sec
```

```
$ sudo /etc/init.d/sphinxsearch start
Starting sphinx: Sphinx 0.9.8.1-release (r1533)
Copyright (c) 2001-2008, Andrew Aksyonoff

using config file '/etc/sphinxsearch/sphinx.conf'...
creating server socket on 0.0.0.0:3312
sphinx.
```

测试

search "keyword"

```
$ search test
Sphinx 0.9.8.1-release (r1533)
Copyright (c) 2001-2008, Andrew Aksyonoff

using config file '/etc/sphinxsearch/sphinx.conf'...
index 'test1': query 'test ': returned 3 matches of 3 total in 0.000 sec

displaying matches:
1. document=1, weight=2, group_id=1, date_added=Sat Feb 12 15:29:34 2011
        id=1
        group_id=1
        group_id2=5
        date_added=2011-02-12 15:29:34
        title=test one
        content=this is my test document number one. also checking search within phrases.
2. document=2, weight=2, group_id=1, date_added=Sat Feb 12 15:29:34 2011
        id=2
        group_id=1
        group_id2=6
        date_added=2011-02-12 15:29:34
        title=test two
        content=this is my test document number two
3. document=4, weight=1, group_id=2, date_added=Sat Feb 12 15:29:34 2011
        id=4
        group_id=2
        group_id2=8
        date_added=2011-02-12 15:29:34
        title=doc number four
        content=this is to test groups

words:
1. 'test': 3 documents, 5 hits
```

```
wget http://sphinxsearch.googlecode.com/svn/trunk/api/sphinxapi.php
wget http://sphinxsearch.googlecode.com/svn/trunk/api/test.php
php test.php test
```

---

7. Mahout

http://mahout.apache.org/

第 45 章 Web Server Optimization

目录

系统配置

1. Intel(R) Xeon(TM) CPU 3.00GHz
2. Memory 4G
3. Ethernet adapter 1000M

1. ulimit

查看 ulimit

```
ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
file size               (blocks, -f) unlimited
pending signals                 (-i) 1024
max locked memory       (kbytes, -l) 32
max memory size         (kbytes, -m) unlimited
```

```
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
stack size               (kbytes, -s) 2048
cpu time                (seconds, -t) unlimited
max user processes              (-u) 77824
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

1.1. open files

对于linux系统，所有设备都以映射为设备文件的方式存在，包括硬件（键盘，鼠标，打印机，显示器，串口，并口，USB，硬盘，内存，网卡，声卡，显卡，等等....），还有软件(管道，socket)，访问这些资源，就相当与打开一个文件，

所以"open files"文件数限制很重要，默认值根本不能满足我们。

查看文件打开数

```
$ cat /proc/sys/fs/file-nr

3200    0        197957
已分配文件句柄的数目       已使用文件句柄的数目       文件句柄的最大数目

查看所有进程的文件打开数
     lsof |wc -l
查看某个进程打开的文件数
         lsof -p pid |wc -l
```

临时更改

```
# ulimit -n 65536
or
# ulimit -SHn 65536
or
# echo "65535" > /proc/sys/fs/file-max
```

永久更改

/etc/security/limits.conf

```
nobody           soft    nofile          40960
root             soft    nofile          40960
nobody           hard    nofile          40960
root             hard    nofile          40960
daemon           soft    nofile          40960
daemon           hard    nofile          40960
```

更省事的方法

```
*          soft    nofile          40960
*          hard    nofile          40960
```

最大线程数限制 threads-max

查看当前值

```
# cat /proc/sys/kernel/threads-max
32624
```

设置

有多种方法加大Linux的threads数，下买是临时更改

```
1、sysctl -w kernel.threads-max=65536
2、echo 65536 > /proc/sys/kernel/threads-max
```

永久修改

```
编辑/etc/sysctl.conf
增加
kernel.threads-max = 65536
#sysctl -p 马上生效
```

以上数值仅供参考，随着计算机发展，上面的值已经不太适合，当前流行的服务器。

---

2. Memcached

2.1. 编译安装

http://www.monkey.org/~provos/libevent/

```
cd /usr/local/src/
wget http://www.monkey.org/~provos/libevent-1.4.13-stable.tar.gz
tar zxf libevent-1.4.13-stable.tar.gz
cd libevent-1.4.13-stable
./configure --prefix=/usr/local/libevent-1.4.13-stable
make
make install
make verify

ln -s /usr/local/libevent-1.4.13-stable /usr/local/libevent
ln -s /usr/local/libevent/lib/* /usr/lib/
ln -s /usr/local/libevent/include/* /usr/include/
ln -s /usr/local/libevent/lib/* /usr/local/lib/
ln -s /usr/local/libevent/include/* /usr/local/include/
```

http://www.danga.com/memcached/

```
cd /usr/local/src/
wget http://memcached.googlecode.com/files/memcached-1.4.5.tar.gz
tar zxf memcached-1.4.5.tar.gz
cd memcached-1.4.5
./configure --prefix=/usr/local/memcached-1.4.5 --with-libevent=/usr/local/libevent
make
make install

ln -s /usr/local/memcached-1.4.5/ /usr/local/memcached
ln -s /usr/local/memcached/bin/memcached /usr/sbin/memcached
```

/usr/local/memcached/bin/memcached -d -m 2048 -l 127.0.0.1 -p 11211 -u root -c 15000 -P /tmp/memcached.pid

例 45.1. /etc/init.d/memcached

```
#!/bin/bash
# memcached init file for memcached
#
# chkconfig: - 100 100
# description: a distributed memory object caching system
# author: Neo Chen<openunix@163.com>
#
# processname: /usr/sbin/memcached
# config:
# pidfile: /var/run/memcached

# source function library
. /etc/init.d/functions

OPTIONS="-d -m 2048 -l 127.0.0.1 -p 11211 -u root -c 4096 -P /var/run/memcached"
USER=daemon
RETVAL=0
prog="memcached"

start() {
        echo -n $"Starting $prog: "
        if [ $UID -ne 0 ]; then
                RETVAL=1
                failure
        else
                daemon --user=$USER /usr/sbin/memcached $OPTIONS
                RETVAL=$?
                [ $RETVAL -eq 0 ] && touch /var/lock/subsys/memcached
        fi;
```

```
        echo
        return $RETVAL
}

stop() {
        echo -n $"Stopping $prog: "
        if [ $UID -ne 0 ]; then
                RETVAL=1
                failure
        else
                killproc /usr/sbin/memcached
                RETVAL=$?
                [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/memcached
        fi;
        echo
        return $RETVAL
}

reload(){
        echo -n $"Reloading $prog: "
        killproc /usr/sbin/memcached -HUP
        RETVAL=$?
        echo
        return $RETVAL
}

restart(){
        stop
        start
}

condrestart(){
    [ -e /var/lock/subsys/memcached ] && restart
    return 0
}

case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart)
        restart
        ;;
#  reload)
#       reload
#        ;;
  condrestart)
        condrestart
        ;;
  status)
        status memcached
        RETVAL=$?
        ;;
  *)
        echo $"Usage: $0 {start|stop|status|restart|condrestart}"
        RETVAL=1
esac

exit $RETVAL
```

/etc/init.d/memcached

```
chmod +x /etc/init.d/memcached
```

flush_all指令清空memcache中的数据

```
$ telnet 172.16.3.51 11511
Trying 172.16.3.51...
Connected to 172.16.3.51.
Escape character is '^]'.
flush_all
OK
quit
Connection closed by foreign host.
```

2.2. debian/ubuntu

```
$ sudo apt-get install memcache
```

/etc/memcached.conf

```
$ cat /etc/memcached.conf
# memcached default config file
# 2003 - Jay Bonci <jaybonci@debian.org>
# This configuration file is read by the start-memcached script provided as
# part of the Debian GNU/Linux distribution.

# Run memcached as a daemon. This command is implied, and is not needed for the
# daemon to run. See the README.Debian that comes with this package for more
# information.
-d

# Log memcached's output to /var/log/memcached
logfile /var/log/memcached.log

# Be verbose
# -v

# Be even more verbose (print client commands as well)
# -vv

# Start with a cap of 64 megs of memory. It's reasonable, and the daemon default
# Note that the daemon will grow to this size, but does not start out holding this much
# memory
-m 64

# Default connection port is 11211
-p 11211

# Run the daemon as root. The start-memcached will default to running as root if no
# -u command is present in this config file
-u nobody

# Specify which IP address to listen on. The default is to listen on all IP addresses
# This parameter is one of the only security measures that memcached has, so make sure
# it's listening on a firewalled interface.
-l 127.0.0.1

# Limit the number of simultaneous incoming connections. The daemon default is 1024
# -c 1024

# Lock down all paged memory. Consult with the README and homepage before you do this
# -k

# Return error when memory is exhausted (rather than removing items)
# -M

# Maximize core file limit
# -r
```

restart

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

3. khttpd

homepage: http://www.fenrus.demon.nl

4. php.ini

4.1. Resource Limits

Resource Limits

```
;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;

max_execution_time = 30     ; Maximum execution time of each script, in seconds
max_input_time = 60 ; Maximum amount of time each script may spend parsing request data
;max_input_nesting_level = 64 ; Maximum input variable nesting level
memory_limit = 512M      ; Maximum amount of memory a script may consume (16MB)
```

4.2. File Uploads

```
;;;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
upload_max_filesize = 5M
```

4.3. Session Shared

编辑 php.ini 在 [Session]位置添加。

```
extension=memcache.so
memcache.allow_failover = 1
memcache.max_failover_attempts = 20
memcache.chunk_size = 8192
memcache.default_port = 11211

session.save_handler = memcache
session.save_path = "udp://172.16.0.10:11211,tcp://172.16.0.11:11211"
```

4.4. PATHINFO

```
cgi.fix_pathinfo=1
```

5. APC Cache (php-apc - APC (Alternative PHP Cache) module for PHP 5)

```
$ apt-cache search php-apc
php-apc - APC (Alternative PHP Cache) module for PHP 5

$ sudo apt-get install php-apc
```

apc cache 状态监控

http://pecl.php.net/package/APC

下载解包找到apc.php,放到web服务器上

6. Zend Optimizer

http://www.zend.com/

```
tar zxvf ZendOptimizer-3.2.8-linux-glibc21-i386.tar.gz
cd ZendOptimizer-3.2.8-linux-glibc21-i386
./install
```

过程 45.1. 安装 Zend Optimizer

1. 欢迎界面

```
                    Zend Optimizer 3.2.8
Welcome to the Zend Optimizer 3.2.8 Installation!

For more information regarding this procedure, please see the
Zend Optimizer Installation Guide.

                          <  OK  >
```

单击 < OK > 按钮

2. LICENSE

Page Down / Page Up 阅读

```
                          Zend Optimizer 3.2.8
ZEND LICENSE AGREEMENT
Zend Optimizer

ZEND TECHNOLOGIES LTD. ("ZEND") SOFTWARE LICENSE AGREEMENT ("AGREEMENT")

IMPORTANT: READ THESE TERMS CAREFULLY BEFORE INSTALLING THE SOFTWARE KNOWN
AS THE "ZEND OPTIMIZER," AS INSTALLED BY THIS INSTALLATION PROCESS, IN
MACHINE-EXECUTABLE FORM ONLY, AND ANY RELATED DOCUMENTATION (COLLECTIVELY,
THE "SOFTWARE") BY INSTALLING, OR OTHERWISE USING THIS SOFTWARE, YOU (THE
"LICENSEE") ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, AND THAT YOU
AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ALL
OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU ARE NOT AN AUTHORIZED
USER OF THE SOFTWARE AND IT IS YOUR RESPONSIBILITY TO EXIT THIS
INSTALLATION PROGRAM WITHOUT INSTALLING THE SOFTWARE, OR TO DELETE THE
SOFTWARE FROM YOUR COMPUTER.

1. License. Subject to the terms and conditions of this Agreement,
including, without limitation, Section 2 hereof, Zend hereby grants to
Licensee, during the Term (as defined below), a limited, a non-exclusive
license (the "License") to: (i) install and operate the Software on a
computer or a computer network owned or operated by Licensee; (ii) make
copies of the Software; and (iii) sublicense and distribute a limited,
non-exclusive sublicense to install, use and sublicense such copies of the
Software, provided that any sub-license granted hereunder shall be subject
to the limitations and restrictions set forth in this Agreement.

2. Restrictions. Except as otherwise expressly set forth herein, Licensee
or any of its sub-licensees shall not: (a) translate or decompile, or
create or attempt to create, by reverse engineering or otherwise, the
source code form from the object code supplied hereunder; (b) modify,
adapt, translate or create a derivative work from the Software; (c) remove
any proprietary notices, labels, or marks on the Software.
```

```
3. Termination. This Agreement and the License hereunder shall be in
effect from and after the date Licensee installs the Software on a
computer in accordance with the terms and conditions hereof and shall
continue perpetually unless terminated in accordance with this Section 3.
This Agreement shall be automatically terminated upon any breach by
Licensee of any term or condition of this Agreement. Such period shall be
                                                                  ( 21%)
                              < EXIT >
```

单击 < EXIT > 按钮

3. 是否接受LICENSE?

```
                    Zend Optimizer 3.2.8

IMPORTANT:
BY SELECTING THE 'YES' OPTION BELOW, DOWNLOADING, INSTALLING, OR
OTHERWISE USING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THE
LICENSE AGREEMENT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS AND
CONDITIONS.
IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF SUCH AGREEMENT,
YOU ARE NOT AN AUTHORIZED USER OF THE SOFTWARE AND IT IS YOUR
RESPONSIBILITY TO EXIT THIS DOWNLOADING/INSTALLATION PROCESS WITHOUT
DOWNLOADING OR INSTALLING THE SOFTWARE BY SELECTING THE 'NO' OPTION BELOW,
AND TO DELETE THE SOFTWARE FROM YOUR COMPUTER.

Do you accept the terms of this license?

                  < Yes >          < No  >
```

单击 < Yes > 按钮

4. Zend Optimizer 安装路径

```
                  Zend Optimizer 3.2.8

Please specify the location for installing Zend Optimizer:

 /usr/local/Zend

                 <  OK  >        <Cancel>
```

单击 < OK > 按钮

建议安装在/usr/local/Zend_3.2.8

5. php.ini 安装路径

```
          Zend Optimizer 3.2.8

Enter the location of your php.ini file

 /usr/local/php/etc

           <  OK  >    <Cancel>
```

输入php.ini安装路径

单击 < OK > 按钮

6. 是否使用了Apache?

```
┌──────── Zend Optimizer 3.2.8 ────────┐
│ Are you using Apache Web server?     │
│──────────────────────────────────────│
│         < Yes >    < No  >           │
└──────────────────────────────────────┘
```

我的环境是 lighttpd 所以选择 No

单击 < Yes > 按钮

7. 提示信息

```
┌──────────────────────────────────── Zend Optimizer 3.2.8
──────────────────────────────────────┐
│
│ The following configuration changes have been made:
│
│
│ - The php.ini file has been relocated from /usr/local/php/etc to
/usr/local/Zend_3.2.8/etc │
│
│ - A symbolic link for the php.ini file has been created in /usr/local/php/etc.
│
│
│ - The original php.ini was backed up to
│  /usr/local/php/etc/php.ini-zend_optimizer.bak
│
│
│
├──────────────────────────────────────────────────────────────────────────────────────────────────────────┤
│                                                  <  OK  >
└──────────────────────────────────────────────────────────────────────────────────────────────────────────┘
```

单击 < OK > 按钮

8. 安装完成

```
┌──────────────────────────── Zend Optimizer 3.2.8 ────────────────────────────┐ │
│ The installation has completed successfully.                                 │ │
│ Zend Optimizer is now ready for use.                                         │ │
│ You must restart your Web server for the modifications to take effect.       │ │
│──────────────────────────────────────────────────────────────────────────────│ │
│                                    <  OK  >                                  │ │
└──────────────────────────────────────────────────────────────────────────────┘ │
```

单击 < OK > 按钮

---

7. eaccelerator

```
tar jxvf eaccelerator-0.9.5.3.tar.bz2
cd eaccelerator-0.9.5.3/
/opt/php/bin/phpize
./configure  --enable-eaccelerator=shared --with-php-config=/opt/php/bin/php-config
make
make install
```

第 46 章 varnish - a state-of-the-art, high-performance HTTP accelerator

目录

1. Varnish Install

http://varnish.projects.linpro.no/

1. install

```
$ sudo apt-get install varnish
```

2. /etc/default/varnish

```
$ sudo vim /etc/default/varnish
DAEMON_OPTS="-a :80 \
             -T localhost:6082 \
             -f /etc/varnish/default.vcl \
             -s file,/var/lib/varnish/$INSTANCE/varnish_storage.bin,1G"
```

3. /etc/varnish/default.vcl

```
$ sudo vim /etc/varnish/default.vcl
```

```
backend default {
        .host = "127.0.0.1";
        .port = "8080";
}
```

4. reload

```
$ sudo /etc/init.d/varnish force-reload
 * Stopping HTTP accelerator                                [ OK ]
 * Starting HTTP accelerator
```

上一页 上一级 下一页

7. eaccelerator 起始页 2. varnish utility

2. varnish utility

2.1. status

```
$ varnishstat
or
$ varnishstat -n /var/lib/varnish/atom-netkiller/
```

HTTP Head

```
$ curl -I http://bg7nyt.mooo.com/
HTTP/1.1 404 Not Found
X-Powered-By: PHP/5.2.6-3ubuntu4.2
Content-type: text/html
Server: lighttpd/1.4.19
Content-Length: 539
Date: Wed, 23 Sep 2009 00:05:11 GMT
X-Varnish: 938430316
Age: 0
Via: 1.1 varnish
Connection: keep-alive
```

test gzip,defalte

```
$ curl -H Accept-Encoding:gzip,defalte -I http://bg7nyt.mooo.com/
HTTP/1.1 200 OK
X-Powered-By: PHP/5.2.6-3ubuntu4.2
Content-Encoding: gzip
Vary: Accept-Encoding
Content-type: text/html
Server: lighttpd/1.4.19
Date: Wed, 23 Sep 2009 00:08:51 GMT
X-Varnish: 938430335
Age: 0
Via: 1.1 varnish
Connection: keep-alive
```

2.2. varnishadm

help messages

```
$ varnishadm -T 127.0.0.1:6082 help
help [command]
ping [timestamp]
status
start
stop
stats
vcl.load <configname> <filename>
vcl.inline <configname> <quoted_VCLstring>
vcl.use <configname>
vcl.discard <configname>
vcl.list
vcl.show <configname>
param.show [-l] [<param>]
param.set <param> <value>
quit
purge.url <regexp>
purge.hash <regexp>
purge <field> <operator> <arg> [&& <field> <oper> <arg>]...
purge.list
```

2.2.1. 清除缓存

通过Varnish管理端口，使用正则表达式批量清除缓存：

清除所有缓存

```
/usr/local/varnish/bin/varnishadm -T 127.0.0.1:6082 url.purge *$
```

http://bg7nyt.mooo.com/zh-cn/technology/news.html 清除类/zh-cn/下所有缓存

```
/usr/local/varnish/bin/varnishadm -T 127.0.0.1:6082 url.purge /zh-cn/
```

```
/usr/local/varnish/bin/varnishadm -T 127.0.0.1:3500 url.purge w*$
```

2.3. varnishtop

```
varnishtop -i rxurl
varnishtop -i txurl
varnishtop -i RxHeader -I Accept-Encoding
```

2.4. varnishhist

2.5. varnishsizes

---

3. log file

log file

```
$ sudo vim  /etc/default/varnishlog
VARNISHLOG_ENABLED=1
$ sudo /etc/init.d/varnishlog start
 * Starting HTTP accelerator log deamon    [ OK ]

$ sudo vim  /etc/default/varnishncsa
VARNISHNCSA_ENABLED=1
$ sudo /etc/init.d/varnishncsa start
 * Starting HTTP accelerator log deamon    [ OK ]
```

4. Varnish Configuration Language - VCL

Varnish配置文件VCL中的函数详解

内置的例程

```
vcl_recv
有请求到达后成功接收并分析时被调用，一般以以下几个关键字结束。
error code [reason] 返回code给客户端，并放弃处理该请求
pass 进入pass模式，把控制权交给vcl_pass
pipe 进入pipe模式，把控制权交给vcl_pipe
lookup 在缓存里查找被请求的对象，根据查找结果把控制权交给vcl_hit或vcl_miss

vcl_pipe
进入pipe模式时被调用。请求被直接发送到backend，后端和客户端之间的后继数据不进行处理，只是简单传递，直到一方关闭连接。一般以以下几个关键字结束。
error code [reason]
pipe

vcl_pass
进入pass模式时被调用。请求被送到后端，后端应答数据送给客户端，但不进入缓存。同一连接的后继请求正常处理。一般以以下几个关键字结束。
error code [reason]
pass

vcl_hash
目前不使用

vcl_hit
在lookup以后如果在cache中找到请求的内容事调用。一般以以下几个关键字结束。
error code [reason]
pass
deliver 将找到的内容发送给客户端，把控制权交给vcl_deliver.

vcl_miss
lookup后但没有找到缓存内容时调用，可以用于判断是否需要从后端服务器取内容。一般以以下几个关键字结束。
error code [reason]
pass
fetch 从后端取得请求的内容，把控制权交给vcl_fetch.


vcl_fetch
从后端取得内容后调用。一般以以下几个关键字结束。
error code [reason]
pass
insert 将取到的内容插入缓存，然后发送给客户端，把控制权交给vcl_deliver


vcl_deliver
缓存内容发动给客户端前调用。一般以以下几个关键字结束。
error code [reason]
deliver 内容发送给客户端

vcl_timeout
在缓存内容到期前调用。一般以以下几个关键字结束。
fetch 从后端取得该内容
discard 丢弃该内容



vcl_discard
由于到期或者空间不足而丢弃缓存内容时调用。一般以以下几个关键字结束。
discard 丢弃
keep 继续保留在缓存里

如果这些内置例程没有被定义，则执行缺省动作


一些内置的变量
now 当前时间，标准时间点（1970？）到现在的秒数

backend.host 后端的IP或主机名
backend.port 后端的服务名或端口

请求到达后有效的变量
client.ip 客户端IP
```

```
server.ip 服务端IP
req.request 请求类型，比如GET或者HEAD或者POST
req.url 请求的URL
req.proto 请求的HTTP版本号
req.backend 请求对应的后端
req.http.header 对应的HTTP头

往后段的请求时有效的变量
bereq.request 比如GET或HEAD
bereq.url URL
bereq.proto 协议版本
bereq.http.header HTTP头

从cache或后端取到内容后有效的变量
obj.proto HTTP协议版本
obj.status HTTP状态代码
obj.response HTTP状态信息
obj.valid 是否有效的HTTP应答
obj.cacheable 是否可以缓存的内容，也就是说如果HTTP返回是200、203、300、301、302、404、410并且有非0的生存期，则为可缓存
obj.ttl 生存期，秒
obj.lastuse 上一次请求到现在间隔秒数

对客户端应答时有效的变量
resp.proto response的HTTP版本
resp.status 回给客户端的HTTP状态代码
resp.response 回给客户端的HTTP状态信息
resp.http.header HTTP头
```

---

5. example

例 46.1. default.vcl

```
neo@netkiller:/etc/varnish$ cat default.vcl
# This is a basic VCL configuration file for varnish.  See the vcl(7)
# man page for details on VCL syntax and semantics.
#
# Default backend definition.  Set this to point to your content
# server.
#
backend default {
    .host = "127.0.0.1";
    .port = "8080";
}
#
# Below is a commented-out copy of the default VCL logic.  If you
# redefine any of these subroutines, the built-in logic will be
# appended to your code.
#
sub vcl_recv {
    if (req.http.x-forwarded-for) {
        set req.http.X-Forwarded-For =
            req.http.X-Forwarded-For ", " client.ip;
    } else {
        set req.http.X-Forwarded-For = client.ip;
    }
    if (req.request != "GET" &&
      req.request != "HEAD" &&
      req.request != "PUT" &&
      req.request != "POST" &&
      req.request != "TRACE" &&
      req.request != "OPTIONS" &&
      req.request != "DELETE") {
        /* Non-RFC2616 or CONNECT which is weird. */
        return (pipe);
    }
    if (req.request != "GET" && req.request != "HEAD") {
        /* We only deal with GET and HEAD by default */
        return (pass);
    }
    if (req.http.Authorization || req.http.Cookie) {
        /* Not cacheable by default */
/*        return (pass);*/
        return (lookup);
    }
    return (lookup);
}

sub vcl_pipe {
    # Note that only the first request to the backend will have
    # X-Forwarded-For set.  If you use X-Forwarded-For and want to
    # have it set for all requests, make sure to have:
    # set req.http.connection = "close";
    # here.  It is not set by default as it might break some broken web
    # applications, like IIS with NTLM authentication.
    return (pipe);
}

sub vcl_pass {
    return (pass);
}

sub vcl_hash {
    set req.hash += req.url;
    if (req.http.host) {
        set req.hash += req.http.host;
    } else {
        set req.hash += server.ip;
    }
    return (hash);
}

sub vcl_hit {
    if (!obj.cacheable) {
        return (pass);
    }
    return (deliver);
}
```

```
sub vcl_miss {
    return (fetch);
}

sub vcl_fetch {
    if (!beresp.cacheable) {
        return (pass);
    }
    if (beresp.http.Set-Cookie) {
#         return (pass);
        return (deliver);
    }
    return (deliver);
}

sub vcl_deliver {
    return (deliver);
}
#
# sub vcl_error {
#     set obj.http.Content-Type = "text/html; charset=utf-8";
#     synthetic {"
# <?xml version="1.0" encoding="utf-8"?>
# <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
#  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
# <html>
#   <head>
#     <title>"} obj.status " " obj.response {"</title>
#   </head>
#   <body>
#     <h1>Error "} obj.status " " obj.response {"</h1>
#     <p>"} obj.response {"</p>
#     <h3>Guru Meditation:</h3>
#     <p>XID: "} req.xid {"</p>
#     <hr>
#     <p>Varnish cache server</p>
#   </body>
# </html>
# "};
#     return (deliver);
# }
```

第 47 章 Traffic Server

目录

1. Install

```
yum install gcc gcc-c++ make autoconf -y
yum -y install  tcl lzma tcl-devel expat expat-devel pcre-devel perl perl-devel
```

```
cd /usr/local/src/
wget http://mirror.bjtu.edu.cn/apache//trafficserver/trafficserver-3.0.1.tar.bz2
tar -xvjf trafficserver-3.0.1.tar.bz2
```

```
cd trafficserver-3.0.1
./configure --prefix=/srv/trafficserver-3.0.1 && make && make install
```

2.

```
修改配置
vi records.config
  CONFIG proxy.config.proxy_name STRING cache1                    ### 修改成cache的server name即可
  CONFIG proxy.config.cluster.ethernet_interface STRING eth0     ### 修改成需要侦听的interface名称,
默认是 null
  CONFIG proxy.config.admin.user_id STRING nobody                 ### 用来运行 traffic server 的用
户,默认是nobody
  CONFIG proxy.config.http.server_port INT 80                     ### traffic server 侦听的端口,默
认是8080

vi cache.config
dest_domain=www.xiu.com scheme=http     revalidate=2h

vi remap.conf
map http://www.xiu.com  http://10.0.0.51  #前一个是用户访问的地址,后一个是源站点的IP,或者域名

配置变更应用生效
/srv/ts/bin/traffic_line -x

启动服务

/srv/ts/bin/trafficserver start


./traffic_shell
show
show:cache
show:cache-stats
show:proxy-stats

./logstats -i www.xiu.com

如果服务器down掉,默认会生成core文件,在/ts
使用

ts/bin/traffic_server -c core.1234
```

第 48 章 Cherokee

目录

1. Installing Cherokee

```
apt-get install cherokee
```

Cherokee can be configured through a web-based control panel which we can start as follows:

```
cherokee-admin -b
```

cherokee script

```
/etc/init.d/cherokee restart
```

第 49 章 Jetty

第 50 章 Other Web Server

目录

1. Python SimpleHTTPServer

```
python -m SimpleHTTPServer &
```

```
curl http://localhost:8000/
```

部分 IV. Backup, Recovery, and Archiving Solutions

File Transfer, Synchronize, Storage

目录

第 51 章 Logical Volume Manager (LVM)

目录

vg,lv命名规则，建议采用：

1. /dev/vg00/lvol00

2. /dev/VolGroup00/LogVol00

lvm 创建流程 pvcreate - vgcreate - lvcreate

```
# pvcreate /dev/sdb4
  Physical volume "/dev/sdb4" successfully created

# vgcreate vg1 /dev/sdb4
  Volume group "vg1" successfully created

# lvcreate -l 10239 -n lv0 vg1
  Logical volume "lv0" created
```

1. 物理卷管理（physical volume）

1.1. pvcreate

将整个硬盘划为物理卷

```
# pvcreate /dev/hdb
```

将单个分区创建为物理卷的命令为：

```
# pvcreate /dev/hda5
```

实例

```
# pvcreate /dev/sdb4
  Physical volume "/dev/sdb4" successfully created
```

1.2. pvdisplay

```
# pvdisplay
  --- Physical volume ---
  PV Name               /dev/sdb4
  VG Name               vg1
  PV Size               1.02 TiB / not usable 4.90 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              267301
  Free PE               257062
  Allocated PE          10239
  PV UUID               g2xLQ8-7tgm-iNZc-8dVq-vo3z-CFJp-LryYAs
```

1.3. pvs

```
# pvs
  PV         VG   Fmt  Attr PSize PFree
  /dev/sdb4  vg1  lvm2 a-   1.02t 1004.15g
```

2. 卷组管理（Volume Group）

2.1. vgcreate

```
# vgcreate vg1 /dev/sdb4
  Volume group "vg1" successfully created
```

2.2. vgdisplay

```
# vgdisplay
  --- Volume group ---
  VG Name               vg1
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  2
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               1.02 TiB
  PE Size               4.00 MiB
  Total PE              267301
  Alloc PE / Size       10239 / 40.00 GiB
  Free  PE / Size       257062 / 1004.15 GiB
  VG UUID               Kxd02t-mFtJ-nThA-Lciy-zI2A-Dwzq-2nJoVh
```

2.3. vgs

```
# vgs
  VG   #PV #LV #SN Attr   VSize VFree
  vg1    1   1   0 wz--n- 1.02t 1004.15g
```

2.4. vgchange

激活卷组

```
# vgchange -a y vg1
```

2.5. vgextend

```
vgextend vg1 /dev/sdb3
```

```
# vgdisplay
  --- Volume group ---
  VG Name               vg1
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  2
  VG Access             read/write
  VG Status             resizable
```

```
  MAX LV                0
  Cur LV                1
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               1.02 TiB
  PE Size               4.00 MiB
  Total PE              267301
  Alloc PE / Size       10239 / 40.00 GiB
  Free  PE / Size       257062 / 1004.15 GiB
  VG UUID               Kxd02t-mFtJ-nThA-Lciy-zI2A-Dwzq-2nJoVh

# vgs
  VG   #PV #LV #SN Attr   VSize VFree
  vg1    1   1   0 wz--n- 1.02t 1004.15g

# vgextend vg1 /dev/sdb3
  No physical volume label read from /dev/sdb3
  Physical volume "/dev/sdb3" successfully created
  Volume group "vg1" successfully extended

# vgdisplay
  --- Volume group ---
  VG Name               vg1
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  3
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               0
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               1.51 TiB
  PE Size               4.00 MiB
  Total PE              395303
  Alloc PE / Size       10239 / 40.00 GiB
  Free  PE / Size       385064 / 1.47 TiB
  VG UUID               Kxd02t-mFtJ-nThA-Lciy-zI2A-Dwzq-2nJoVh

# vgs
  VG   #PV #LV #SN Attr   VSize VFree
  vg1    2   1   0 wz--n- 1.51t 1.47t

  # pvdisplay
  --- Physical volume ---
  PV Name               /dev/sdb4
  VG Name               vg1
  PV Size               1.02 TiB / not usable 4.90 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              267301
  Free PE               257062
  Allocated PE          10239
  PV UUID               g2xLQ8-7tgm-iNZc-8dVq-vo3z-CFJp-LryYAs

  --- Physical volume ---
  PV Name               /dev/sdb3
  VG Name               vg1
  PV Size               500.01 GiB / not usable 1.12 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              128002
  Free PE               128002
  Allocated PE          0
  PV UUID               77RRJm-e4iz-Zfos-ZYHT-XEBa-AZ7D-Yd7fdU
```

2.6. vgreduce

```
# vgreduce vg1 /dev/sdb3
  Removed "/dev/sdb3" from volume group "vg1"

# pvdisplay
  --- Physical volume ---
  PV Name               /dev/sdb4
  VG Name               vg1
  PV Size               1.02 TiB / not usable 4.90 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              267301
  Free PE               257062
  Allocated PE          10239
  PV UUID               g2xLQ8-7tgm-iNZc-8dVq-vo3z-CFJp-LryYAs

  "/dev/sdb3" is a new physical volume of "500.01 GiB"
  --- NEW Physical volume ---
  PV Name               /dev/sdb3
  VG Name
  PV Size               500.01 GiB
  Allocatable           NO
  PE Size               0
  Total PE              0
  Free PE               0
  Allocated PE          0
```

```
  PV UUID               77RRJm-e4iz-Zfos-ZYHT-XEBa-AZ7D-Yd7fdU
```

3. 逻辑卷管理（logical volume）

3.1. lvcreate

创建1000M逻辑卷

```
# lvcreate -l 1000 -n lv0 vg1
  Logical volume "lv0" created

# ls /dev/vg1/lv0
```

使用-L参数

```
# lvcreate -L 100G -n lv3 vg1
  Logical volume "lv3" created
```

3.1.1. snapshot

```
# lvcreate --size 16m --snapshot --name snap0 /dev/vg1/lv0
  Logical volume "snap0" created

# find /dev/vg1/
/dev/vg1/
/dev/vg1/snap0
/dev/vg1/lv3
/dev/vg1/lv1
/dev/vg1/lv0
```

3.2. lvdisplay

```
# lvdisplay
  --- Logical volume ---
  LV Name                /dev/vg1/lv0
  VG Name                vg1
  LV UUID                DyvPgz-VFjs-gu58-mxNX-ybCm-tcUP-kKk90y
  LV Write Access        read/write
  LV Status              available
  # open                 0
  LV Size                40.00 GiB
  Current LE             10239
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:0

  --- Logical volume ---
  LV Name                /dev/vg1/lv1
  VG Name                vg1
  LV UUID                8Nbuio-w2CH-euVD-9LNB-3Dcd-frS0-Cm3EBD
  LV Write Access        read/write
  LV Status              available
  # open                 0
  LV Size                3.91 GiB
  Current LE             1000
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:1
```

3.3. lvremove

```
# lvcreate -l 1000 -n lv1 vg1
  Logical volume "lv1" created

# lvdisplay
  --- Logical volume ---
  LV Name                /dev/vg1/lv0
  VG Name                vg1
  LV UUID                DyvPgz-VFjs-gu58-mxNX-ybCm-tcUP-kKk90y
  LV Write Access        read/write
  LV Status              available
  # open                 0
  LV Size                40.00 GiB
  Current LE             10239
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:0

  --- Logical volume ---
  LV Name                /dev/vg1/lv1
  VG Name                vg1
  LV UUID                8Nbuio-w2CH-euVD-9LNB-3Dcd-frS0-Cm3EBD
  LV Write Access        read/write
  LV Status              available
  # open                 0
  LV Size                3.91 GiB
  Current LE             1000
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:1


# lvremove /dev/vg1/lv1
Do you really want to remove active logical volume lv1? [y/n]: y
  Logical volume "lv1" successfully removed

# lvdisplay
  --- Logical volume ---
  LV Name                /dev/vg1/lv0
  VG Name                vg1
  LV UUID                DyvPgz-VFjs-gu58-mxNX-ybCm-tcUP-kKk90y
  LV Write Access        read/write
  LV Status              available
  # open                 0
  LV Size                40.00 GiB
  Current LE             10239
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:0
```

3.3.1. snapshot

```
# lvremove /dev/vg1/snap0
Do you really want to remove active logical volume snap0? [y/n]: y
  Logical volume "snap0" successfully removed
```

---

4. Format

```
# mkfs.ext4 /dev/vg1/lv0
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
2621440 inodes, 10484736 blocks
524236 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
320 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 24 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

5. mount

5.1. lv

```
# mkdir /mnt/lv0
# mount /dev/vg1/lv0 /mnt/lv0
```

5.2. snapshot

```
# find /dev/vg1/
/dev/vg1/
/dev/vg1/snap0
/dev/vg1/lv3
/dev/vg1/lv1
/dev/vg1/lv0

# mkdir /mnt/snap0
# mount /dev/vg1/snap0 /mnt/snap0
```

6. snapshot backup

dump + restore

```
1.挂载备份源www
mount /dev/vg1/www /www

2.创建快照
lvcreate -L 16m -p r -s -n www-backup /dev/vg1/www

3.挂载快照
mkdir /mnt/www-backup
mount -o ro /dev/vg1/www-backup /mnt/www-backup

4.备份快照
dump -0u -f /tmp/www-backup.dump /mnt/www-backup

5.删除快照
umount /mnt/www-backup
lvremove /dev/vg1/www-backup

6.重做www
umount /www
mkfs.ext4 /dev/vg1/www
mount /dev/vg1/www /www

7.恢复快照
cd /www
restore -rf /tmp/www-backup.dump
```

dd

```
# mount -o remount,ro /dev/VolGroup00/LogVol01
# lvcreate -L500M -s -n backup /dev/VolGroup00/LogVol01
# dd if=/dev/VolGroup00/backup of=/mnt/VolGroup01/LogVol01/
# mount -o remount,rw /dev/VolGroup00/LogVol01
# umount /mnt/VolGroup01/LogVol01
# lvremove /dev/VolGroup00/backup
```

第 52 章 Download Tools

目录

1. wget - retrieves files from the web

wget各种选项分类列表

```
* 启动
-V, -version 显示wget的版本后退出
-h, -help 打印语法帮助
-b, -background 启动后转入后台执行
-e, -execute=COMMAND 执行`.wgetrc'格式的命令, wgetrc格式参见/etc/wgetrc或~/.wgetrc
* 记录和输入文件
-o, -output-file=FILE 把记录写到FILE文件中
-a, -append-output=FILE 把记录追加到FILE文件中
-d, -debug 打印调试输出
-q, -quiet 安静模式(没有输出)
-v, -verbose 冗长模式(这是缺省设置)
-nv, -non-verbose 关掉冗长模式, 但不是安静模式
-i, -input-file=FILE 下载在FILE文件中出现的URLs
-F, -force-html 把输入文件当作HTML格式文件对待
-B, -base=URL 将URL作为在-F -i参数指定的文件中出现的相对链接的前缀
-sslcertfile=FILE 可选客户端证书
-sslcertkey=KEYFILE 可选客户端证书的KEYFILE
-egd-file=FILE 指定EGD socket的文件名
* 下载
-bind-address=ADDRESS 指定本地使用地址(主机名或IP, 当本地有多个IP或名字时使用)
-t, -tries=NUMBER 设定最大尝试链接次数(0 表示无限制).
-O -output-document=FILE 把文档写到FILE文件中
-nc, -no-clobber 不要覆盖存在的文件或使用.#前缀
-c, -continue 接着下载没下载完的文件
-progress=TYPE 设定进程条标记
-N, -timestamping 不要重新下载文件除非比本地文件新
-S, -server-response 打印服务器的回应
-spider 不下载任何东西
-T, -timeout=SECONDS 设定响应超时的秒数
-w, -wait=SECONDS 两次尝试之间间隔SECONDS秒
-waitretry=SECONDS 在重新链接之间等待1…SECONDS秒
-random-wait 在下载之间等待0…2*WAIT秒
-Y, -proxy=on/off 打开或关闭代理
-Q, -quota=NUMBER 设置下载的容量限制
-limit-rate=RATE 限定下载输率
* 目录
-nd -no-directories 不创建目录
-x, -force-directories 强制创建目录
-nH, -no-host-directories 不创建主机目录
-P, -directory-prefix=PREFIX 将文件保存到目录 PREFIX/…
-cut-dirs=NUMBER 忽略 NUMBER层远程目录
* HTTP 选项
-http-user=USER 设定HTTP用户名为 USER.
-http-passwd=PASS 设定http密码为 PASS.
-C, -cache=on/off 允许/不允许服务器端的数据缓存 (一般情况下允许).
-E, -html-extension 将所有text/html文档以.html扩展名保存
-ignore-length 忽略 `Content-Length'头域
-header=STRING 在headers中插入字符串 STRING
```

```
–proxy-user=USER 设定代理的用户名为 USER
–proxy-passwd=PASS 设定代理的密码为 PASS
–referer=URL 在HTTP请求中包含 `Referer: URL’头
-s, –save-headers 保存HTTP头到文件
-U, –user-agent=AGENT 设定代理的名称为 AGENT而不是 Wget/VERSION.
–no-http-keep-alive 关闭 HTTP活动链接 (永远链接).
–cookies=off 不使用 cookies.
–load-cookies=FILE 在开始会话前从文件 FILE中加载cookie
–save-cookies=FILE 在会话结束后将 cookies保存到 FILE文件中
* FTP 选项
-nr, –dont-remove-listing 不移走 `.listing’文件
-g, –glob=on/off 打开或关闭文件名的 globbing机制
–passive-ftp 使用被动传输模式 (缺省值).
–active-ftp 使用主动传输模式
–retr-symlinks 在递归的时候，将链接指向文件(而不是目录)
* 递归下载
-r, –recursive 递归下载——慎用!
-l, –level=NUMBER 最大递归深度 (inf 或 0 代表无穷).
–delete-after 在现在完毕后局部删除文件
-k, –convert-links 转换非相对链接为相对链接
-K, –backup-converted 在转换文件X之前，将之备份为 X.orig
-m, –mirror 等价于 -r -N -l inf -nr.
-p, –page-requisites 下载显示HTML文件的所有图片
* 递归下载中的包含和不包含(accept/reject)
-A, –accept=LIST 分号分隔的被接受扩展名的列表
-R, –reject=LIST 分号分隔的不被接受的扩展名的列表
-D, –domains=LIST 分号分隔的被接受域的列表
–exclude-domains=LIST 分号分隔的不被接受的域的列表
–follow-ftp 跟踪HTML文档中的FTP链接
–follow-tags=LIST 分号分隔的被跟踪的HTML标签的列表
-G, –ignore-tags=LIST 分号分隔的被忽略的HTML标签的列表
-H, –span-hosts 当递归时转到外部主机
-L, –relative 仅仅跟踪相对链接
-I, –include-directories=LIST 允许目录的列表
-X, –exclude-directories=LIST 不被包含目录的列表
-np, –no-parent 不要追溯到父目录
```

```
setlocal ENABLEDELAYEDEXPANSION
for /l %%i in (1001,1,1162) do for /l %%j in (101,1,112) do @(
                          set s=%%i
                          set t=%%j
                          wget -O !s:~1,3!!t:~1,2!.jpg
hxxp://www.sergeaura.net/TGP/!s:~1,3!/images/!t:~1,2!.jpg)
endlocal
```

-np 的作用是不遍历父目录

-nd 不重新创建目录结构。

--accept=iso 仅下载所有扩展名为 iso 的文件

-i filename.txt 此命令常用于批量下载的情形，把所有需要下载文件的地址放到 filename.txt 中，然后 wget 就会自动为你下载所有文件了。

-c 选项的作用为断点续传。

$ wget -m -k (-H) http://www.example.com/ 该命令可用来镜像一个网站，wget 将对链接进行转换。如果网站中的图像是放在另外的站点，那么可以使用 -H 选项。

1.1. 下载所有图片

```
wget --reject=htm,html,txt --accept=jpg,gif -p -m -H http://www.example.com
wget --domains=example.com --reject=htm,html,txt --accept=jpg,gif -p -m -H
http://www.example.com
```

1.2. mirror

```
wget -m -e robots=off http://www.example.com/

wget -m -e robots=off -U "Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1.6)
Gecko/20091201 Firefox/3.5.6” "http://www.example.com/"
```

1.3. reject

```
wget -m --reject=gif http://target.web.site/subdirectory
```

1.4. ftp 下载

```
wget -q -c -m -P /backup/logs/cdn -nH  ftp://user:passwd@localhost/
```

---

2. axel - A light download accelerator - Console version

axel

```
sudo apt-get install axel
```

第 53 章 FTP (File Transfer Protocol)

目录

参考http://netkiller.8800.org/article/ftpserver/

1. lftp

1.1. pget

多线程下载

```
lftp -c 'pget http://url.example.com/file.ext' # 默认5个线程
lftp -c 'pget -n 10 http://url.example.com/file.ext'
```

1.2. lftp 批处理

```
lftp $HOSTADDR<<FTPCMD
cd $REMOTEPATH
lcd $DESTPATH
nlist > $DYNAFILE
quit
FTPCMD
```

上一页 上一级 下一页

2. axel - A light download accelerator - Console version

起始页

2. ncftp

2. ncftp

```
sudo apt-get install ncftp
ncftp ftp://neo@127.0.0.1
```

2.1. batch command

batch ftp command

```
neo@netkiller:~$ cat upload
#!/bin/bash

ncftp ftp://netkiller:******@netkiller.hikz.com/www/book/linux <<END_SCRIPT
put /home/neo/workspace/Development/public_html/book/linux/*.html
```

2.2. ncftpget

```
  ncftpget ftp.freebsd.org . /pub/FreeBSD/README.TXT /pub/FreeBSD/index.html
  ncftpget ftp.gnu.org /tmp '/pub/gnu/README.*'
  ncftpget ftp://ftp.freebsd.org/pub/FreeBSD/README.TXT
  ncftpget -R ftp.ncftp.com /tmp /ncftp  (ncftp is a directory)
  ncftpget -u gleason -p my.password Bozo.probe.net . '/home/mjg/.*rc'
  ncftpget -u gleason Bozo.probe.net . /home/mjg/foo.txt  (prompt for password)
  ncftpget -f Bozo.cfg '/home/mjg/.*rc'
  ncftpget -c ftp.freebsd.org /pub/FreeBSD/README.TXT | /usr/bin/more
  ncftpget -c ftp://ftp.freebsd.org/pub/FreeBSD/README.TXT | /usr/bin/more
  ncftpget -a -d /tmp/debug.log -t 60 ftp.wustl.edu . '/pub/README*'
```

2.3. ncftpput

```
$ ncftpput -R -u netkiller -p password netkiller.hikz.com /home/netkiller/www ~/public_html/*
```

3. FileZilla

http://filezilla-project.org/

4. vsftpd - The Very Secure FTP Daemon

```
$ sudo apt-get install vsftpd
```

test

```
[08:25:37 jobs:0] $ ncftp ftp://127.0.0.1
NcFTP 3.2.1 (Jul 29, 2007) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 127.0.0.1...
(vsFTPd 2.0.7)
Logging in...
Login successful.
Logged in to 127.0.0.1.
Current remote directory is /.
ncftp / >
```

enable local user

```
$ sudo vim /etc/vsftpd.conf

# Uncomment this to allow local users to log in.
local_enable=YES
chroot_local_user=YES

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

testing for local user

```
$ ncftp ftp://neo@127.0.0.1/
NcFTP 3.2.1 (Jul 29, 2007) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 127.0.0.1...
(vsFTPd 2.0.7)
Logging in...
Password requested by 127.0.0.1 for user "neo".

    Please specify the password.

Password: *******

Login successful.
Logged in to 127.0.0.1.
Current remote directory is /home/neo.
ncftp /home/neo >
```

4.1. chroot

4.1.1. local user

chroot 所有本地用户

```
chroot_local_user=YES
```

4.1.2. /etc/vsftpd/chroot_list

受限用户用户添加到文件vsftpd.chroot_list

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
```

注意：每行一个用户名

4.2. test

```
adduser -o --home /www --shell /sbin/nologin --uid 99 --gid 99 --group nobody www
echo "www:chen" | chpasswd
echo www > /etc/vsftpd/chroot_list
ncftp ftp://www:chen@172.16.0.1
```

---

6. Pure-FTPd + LDAP + MySQL + PGSQL + Virtual-Users + Quota

参考 http://netkiller.sourceforge.net/pureftpd/

第 54 章 File Synchronize

目录

1. 跨服务器文件传输

1.1. scp - secure copy (remote file copy program)

限速1M

```
# scp -l 1000 /www/index.html root@172.16.0.1:/www
```

1.2. nc - TCP/IP swiss army knife

tar 通过nc发送到另一端

```
# Server
$ tar cf - win98 | nc -l -p 5555

# Backup Machine
nc server_ip/server_doman_name 5555 | tar xf -
```

---

2. rsync - fast remote file copy program (like rcp)

rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2 and is currently being maintained by Wayne Davison.

2.1. 安装Rsync与配置守护进程

2.1.1. install with source

过程 54.1. rsync

1. 安装rsync

   在AS3 第二张CD上找到rsync-2.5.6-20.i386.rpm

```
[root@linuxas3 root]# cd /mnt
[root@linuxas3 mnt]# mount cdrom
[root@linuxas3 mnt]# cd cdrom/RedHat/RPMS
[root@linuxas3 RPMS]# rpm -ivh rsync-2.5.6-20.i386.rpm
```

2. 配置/etc/rsyncd.conf

   在rh9,as3系统上rsync安装后,并没有创建rsyncd.conf文档，要自己创建rsyncd.conf文档

```
[root@linuxas3 root]# vi /etc/rsyncd.conf

uid=nobody
gid=nobody
max connections=5
use chroot=no
log file=/var/log/rsyncd.log
pid file=/var/run/rsyncd.pid
lock file=/var/run/rsyncd.lock
#auth users=root
secrets file=/etc/rsyncd.passwd

[postfix]
path=/var/mail
comment = backup mail
ignore errors
read only = yes
list = no
auth users = postfix

[netkiller]
path=/home/netkiller/web
comment = backup 9812.net
ignore errors
read only = yes
list = no
auth users = netkiller

[pgsqldb]
path=/var/lib/pgsql
comment = backup postgresql database
ignore errors
read only = yes
list = no
```

a. 选项说明

```
uid = nobody
gid = nobody
use chroot = no         # 不使用chroot
max connections = 4     # 最大连接数为4
pid file = /var/run/rsyncd.pid            #进程ID文件
lock file = /var/run/rsync.lock
log file = /var/log/rsyncd.log     # 日志记录文件
secrets file = /etc/rsyncd.pwd     # 认证文件名,主要保存用户密码，权限建议设为600，所有者root

[module]            # 这里是认证的模块名，在client端需要指定
path = /var/mail    # 需要做镜像的目录
comment = backup xxxx # 注释
ignore errors         # 可以忽略一些无关的IO错误
read only = yes       # 只读
list = no             # 不允许列文件
auth users = postfix  # 认证的用户名，如果没有这行，则表明是匿名

[other]
path = /path/to...
comment = xxxxx
```

b. 密码文件

在server端生成一个密码文件/etc/rsyncd.pwd

```
[root@linuxas3 root]# echo postfix:xxx >>/etc/rsyncd.pwd
[root@linuxas3 root]# echo netkiller:xxx >>/etc/rsyncd.pwd
[root@linuxas3 root]# chmod 600 /etc/rsyncd.pwd
```

c. 启动rsync daemon

```
[root@linuxas3 root]# rsync --daemon
```

3. 添加到启动文件

```
echo "rsync --daemon" >> /etc/rc.d/rc.local                                    [  OK  ]
```

cat /etc/rc.d/rc.local 确认一下

4. 测试

```
[root@linux docbook]#  rsync rsync://netkiller.8800.org/netkiller
[root@linux tmp]# rsync rsync://netkiller@netkiller.8800.org/netkiller
Password:

[chen@linux temp]$  rsync -vzrtopg --progress --delete postfix@netkiller.8800.org::postfix
/tmp
Password:
```

2.1.2. install with aptitude

过程 54.2. installation setp by setp

1. installation

```
$ sudo apt-get install rsync
```

2. enable

```
$ sudo vim /etc/default/rsync

RSYNC_ENABLE=true
```

3. config /etc/rsyncd.conf

```
$ sudo vim /etc/rsyncd.conf

uid=nobody
gid=nobody
max connections=5
use chroot=no
pid file=/var/run/rsyncd.pid
lock file=/var/run/rsyncd.lock
log file=/var/log/rsyncd.log
#auth users=root
secrets file=/etc/rsyncd.secrets

[neo]
path=/home/neo/www
comment = backup neo
ignore errors
read only = yes
list = no
auth users = neo

[netkiller]
path=/home/netkiller/public_html
comment = backup netkiller
ignore errors
read only = yes
list = no
auth users = netkiller

[mirror]
path=/var/www/netkiller.8800.org/html/
comment = mirror netkiller.8800.org
exclude = .svn
ignore errors
read only = yes
list = yes

[music]
path=/var/music
comment = backup music database
ignore errors
read only = yes
list = no

[pgsqldb]
path=/var/lib/pgsql
comment = backup postgresql database
ignore errors
read only = yes
list = no
auth users = neo,netkiller
```

4. /etc/rsyncd.secrets

```
$ sudo vim  /etc/rsyncd.secrets

neo:123456
netkiller:123456
```

```
$ sudo chmod 600 /etc/rsyncd.secrets
```

5. start

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

6. test

```
$ rsync -vzrtopg --progress --delete neo@localhost::neo /tmp/test1/
$ rsync -vzrtopg --progress --delete localhost::music /tmp/test2/
```

7. firewall

```
$ sudo ufw allow rsync
```

2.1.3. xinetd

```
yum install xinetd
```

```
cat /etc/xinetd.d/rsync
# default: off
# description: The rsync server is a good addition to an ftp server, as it \
#       allows crc checksumming etc.
service rsync
{
        disable = yes
        flags           = IPv6
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/bin/rsync
        server_args     = --daemon
        log_on_failure  += USERID
}
```

```
chkconfig xinetd on
/etc/init.d/xinetd restart
```

2.2. rsyncd.conf

```
# Minimal configuration file for rsync daemon
# See rsync(1) and rsyncd.conf(5) man pages for help

# This line is required by the /etc/init.d/rsyncd script
pid file = /var/run/rsyncd.pid
port = 873
address = 192.168.1.171
#uid = nobody
#gid = nobody
uid = root
gid = root

use chroot = yes
read only = yes


#limit access to private LANs
hosts allow=192.168.1.0/255.255.255.0 10.0.1.0/255.255.255.0
hosts deny=*

max connections = 5
motd file = /etc/rsyncd/rsyncd.motd

#This will give you a separate log file
#log file = /var/log/rsync.log

#This will log every file transferred - up to 85,000+ per user, per sync
#transfer logging = yes

log format = %t %a %m %f %b
syslog facility = local3
timeout = 300

[home]
path = /home
list=yes
ignore errors
auth users = linux
secrets file = /etc/rsyncd/rsyncd.secrets
comment = linuxsir home
exclude =   beinan/  samba/

[beinan]
path = /opt
list=no
ignore errors
comment = optdir
auth users = beinan
secrets file = /etc/rsyncd/rsyncd.secrets

[www]
path = /www/
ignore errors
read only = true
list = false
hosts allow = 172.16.1.1
hosts deny = 0.0.0.0/32
auth users = backup
secrets file = /etc/backserver.pas


[web_user1]
path = /home/web_user1/
ignore errors
read only = true
list = false
hosts allow = 202.99.11.121
```

```
hosts deny = 0.0.0.0/32
uid = web_user1
gid = web_user1
auth users = backup
secrets file = /etc/backserver.pas


[pub]
        comment = Random things available for download
        path = /path/to/my/public/share
        read only = yes
        list = yes
        uid = nobody
        gid = nobody
        auth users = pub
        secrets file = /etc/rsyncd.secrets
```

2.3. upload

```
$ rsync -v -u -a --delete --rsh=ssh --stats localfile username@hostname:/home/username/
```

for example:

I want to copy local workspace of eclipse directory to another computer.

```
$ rsync -v -u -a --delete --rsh=ssh --stats workspace neo@192.168.245.131:/home/neo/
```

2.4. download

```
$ rsync -v -u -a --delete --rsh=ssh --stats neo@192.168.245.131:/home/neo/* /tmp/
```

2.5. mirror

rsync使用方法

rsync rsync://认证用户@主机/模块

```
rsync -vzrtopg --progress --delete 认证用户@主机::模块 /mirror目录
```

2.6. step by step to learn rsync

1. transfer file from src to dest directory

```
neo@netkiller:/tmp$ mkdir rsync
neo@netkiller:/tmp$ cd rsync/
neo@netkiller:/tmp/rsync$ ls
neo@netkiller:/tmp/rsync$ mkdir src dest
neo@netkiller:/tmp/rsync$ echo file1 > src/file1
neo@netkiller:/tmp/rsync$ echo file2 > src/file2
neo@netkiller:/tmp/rsync$ echo file3 > src/file3
```

2. skipping directory

```
neo@netkiller:/tmp/rsync$ mkdir src/dir1
neo@netkiller:/tmp/rsync$ mkdir src/dir2
neo@netkiller:/tmp/rsync$ rsync src/* dest/
skipping directory src/dir1
skipping directory src/dir2
```

3. recurse into directories

```
neo@netkiller:/tmp/rsync$ rsync -r src/* dest/
neo@netkiller:/tmp/rsync$ ls dest/
dir1  dir2  file1  file2  file3
```

4. backup

```
neo@netkiller:/tmp/rsync$ rsync -r --backup --suffix=.2008-11-21 src/* dest/
neo@netkiller:/tmp/rsync$ ls dest/
dir1  dir2  file1  file1.2008-11-21  file2  file2.2008-11-21  file3  file3.2008-11-21
neo@netkiller:/tmp/rsync$
```

backup-dir

```
neo@netkiller:/tmp/rsync$ rsync -r --backup --suffix=.2008-11-21 --backup-dir mybackup
src/* dest/
neo@netkiller:/tmp/rsync$ ls dest/
dir1  dir2  file1  file1.2008-11-21  file2  file2.2008-11-21  file3  file3.2008-11-21
mybackup
neo@netkiller:/tmp/rsync$ ls dest/mybackup/
file1.2008-11-21  file2.2008-11-21  file3.2008-11-21
```

```
rsync -r --backup --suffix=.2008-11-21 --backup-dir ../mybackup src/* dest/
neo@netkiller:/tmp/rsync$ ls
dest  mybackup  src
neo@netkiller:/tmp/rsync$ ls src/
dir1  dir2  file1  file2  file3
```

5. update

```
neo@netkiller:/tmp/rsync$ rm -rf dest/*
neo@netkiller:/tmp/rsync$ rsync -r -u src/* dest/
neo@netkiller:/tmp/rsync$ echo netkiller>>src/file2
neo@netkiller:/tmp/rsync$ rsync -v -r -u src/* dest/
building file list ... done
file2

sent 166 bytes  received 42 bytes  416.00 bytes/sec
total size is 38  speedup is 0.18
```

update by time and size

```
neo@netkiller:/tmp/rsync$ echo Hi>src/dir1/file1.1
neo@netkiller:/tmp/rsync$ rsync -v -r -u src/* dest/
building file list ... done
dir1/file1.1

sent 166 bytes  received 42 bytes  416.00 bytes/sec
total size is 41  speedup is 0.20
```

6. --archive

```
rsync -a src/ dest/
```

7. --compress

```
rsync -a -z src/ dest/
```

8. --delete

src

```
svn@netkiller:~$ ls src/
dir1  dir2  file1  file2  file3
```

dest

```
neo@netkiller:~$ rsync -v -u -a --delete -e ssh svnroot@127.0.0.1:/home/svnroot/src
/tmp/dest
svnroot@127.0.0.1's password:
receiving file list ... done
created directory /tmp/dest
src/
src/file1
src/file2
src/file3
src/dir1/
src/dir2/

sent 104 bytes  received 309 bytes  118.00 bytes/sec
total size is 0  speedup is 0.00
```

src

```
svn@netkiller:~$ rm -rf src/file2
svn@netkiller:~$ rm -rf src/dir2
```

dest

```
neo@netkiller:~$ rsync -v -u -a --delete -e ssh svnroot@127.0.0.1:/home/svnroot/src
/tmp/dest
svnroot@127.0.0.1's password:
receiving file list ... done
deleting src/dir2/
deleting src/file2
src/

sent 26 bytes  received 144 bytes  68.00 bytes/sec
total size is 0  speedup is 0.00
```

2.7. rsync examples

http://samba.anu.edu.au/rsync/examples.html

例 54.1. examples

2.7.1. backup to a central backup server with 7 day incremental

例 54.2. backup to a central backup server with 7 day incremental

```
#!/bin/sh

# This script does personal backups to a rsync backup server. You will end up
# with a 7 day rotating incremental backup. The incrementals will go
# into subdirectories named after the day of the week, and the current
# full backup goes into a directory called "current"
# tridge@linuxcare.com

# directory to backup
BDIR=/home/$USER

# excludes file - this contains a wildcard pattern per line of files to exclude
EXCLUDES=$HOME/cron/excludes

# the name of the backup machine
```

```
BSERVER=owl

# your password on the backup server
export RSYNC_PASSWORD=XXXXXX


#######################################################################

BACKUPDIR=`date +%A`
OPTS="--force --ignore-errors --delete-excluded --exclude-from=$EXCLUDES
      --delete --backup --backup-dir=/$BACKUPDIR -a"

export PATH=$PATH:/bin:/usr/bin:/usr/local/bin

# the following line clears the last weeks incremental directory
[ -d $HOME/emptydir ] || mkdir $HOME/emptydir
rsync --delete -a $HOME/emptydir/ $BSERVER::$USER/$BACKUPDIR/
rmdir $HOME/emptydir

# now the actual transfer
rsync $OPTS $BDIR $BSERVER::$USER/current
```

2.7.2. backup to a spare disk

例 54.3. backup to a spare disk

```
I do local backups on several of my machines using rsync. I have an
extra disk installed that can hold all the contents of the main
disk. I then have a nightly cron job that backs up the main disk to
the backup. This is the script I use on one of those machines.

    #!/bin/sh

    export PATH=/usr/local/bin:/usr/bin:/bin

    LIST="rootfs usr data data2"

    for d in $LIST; do
        mount /backup/$d
        rsync -ax --exclude fstab --delete /$d/ /backup/$d/
        umount /backup/$d
    done

    DAY=`date "+%A"`

    rsync -a --delete /usr/local/apache /data2/backups/$DAY
    rsync -a --delete /data/solid /data2/backups/$DAY


The first part does the backup on the spare disk.  The second part
backs up the critical parts to daily directories.  I also backup the
critical parts using a rsync over ssh to a remote machine.
```

2.7.3. mirroring vger CVS tree

例 54.4. mirroring vger CVS tree

```
The vger.rutgers.edu cvs tree is mirrored onto cvs.samba.org via
anonymous rsync using the following script.

    #!/bin/bash

    cd /var/www/cvs/vger/
    PATH=/usr/local/bin:/usr/freeware/bin:/usr/bin:/bin

    RUN=`lps x | grep rsync | grep -v grep | wc -l`
    if [ "$RUN" -gt 0 ]; then
            echo already running
            exit 1
    fi

    rsync -az vger.rutgers.edu::cvs/CVSROOT/ChangeLog $HOME/ChangeLog

    sum1=`sum $HOME/ChangeLog`
```

```
    sum2=`sum /var/www/cvs/vger/CVSROOT/ChangeLog`

    if [ "$sum1" = "$sum2" ]; then
            echo nothing to do
            exit 0
    fi

    rsync -az --delete --force vger.rutgers.edu::cvs/ /var/www/cvs/vger/
    exit 0

Note in particular the initial rsync of the ChangeLog to determine if
anything has changed. This could be omitted but it would mean that the
rsyncd on vger would have to build a complete listing of the cvs area
at each run. As most of the time nothing will have changed I wanted to
save the time on vger by only doing a full rsync if the ChangeLog has
changed. This helped quite a lot because vger is low on memory and
generally quite heavily loaded, so doing a listing on such a large
tree every hour would have been excessive.
```

2.7.4. automated backup at home

例 54.5. automated backup at home

```
I use rsync to backup my wifes home directory across a modem link each
night. The cron job looks like this

    #!/bin/sh
    cd ~susan
    {
    echo
    date
    dest=~/backup/`date +%A`
    mkdir $dest.new
    find . -xdev -type f \( -mtime 0 -or -mtime 1 \) -exec cp -aPv "{}"
    $dest.new \;
    cnt=`find $dest.new -type f | wc -l`
    if [ $cnt -gt 0 ]; then
      rm -rf $dest
      mv $dest.new $dest
    fi
    rm -rf $dest.new
    rsync -Cavze ssh . samba:backup
    } >> ~/backup/backup.log 2>&1


note that most of this script isn't anything to do with rsync, it just
creates a daily backup of Susans work in a ~susan/backup/ directory so
she can retrieve any version from the last week. The last line does
the rsync of her directory across the modem link to the host
samba. Note that I am using the -C option which allows me to add
entries to .cvsignore for stuff that doesn't need to be backed up.
```

2.7.5. Fancy footwork with remote file lists

例 54.6. Fancy footwork with remote file lists

```
One little known feature of rsync is the fact that when run over a
remote shell (such as rsh or ssh) you can give any shell command as
the remote file list. The shell command is expanded by your remote
shell before rsync is called. For example, see if you can work out
what this does:

        rsync -avR remote:'`find /home -name "*.[ch]"`' /tmp/

note that that is backquotes enclosed by quotes (some browsers don't
show that correctly).
```

2.8. rsync for windows

http://www.rsync.net/resources/howto/windows_rsync.html

2.9. 多进程 rsync 脚本

```
#!/usr/bin/perl

my $path = "/data";           #本地目录
my $ip="172.16.xxx.xxx";     #远程目录
my $maxchild=5;               #同时并发的个数

open FILE,"ls $path|";
while()
{

        chomp;
        my $filename = $_;
        my $i = 1;
        while($i<=1){
                my $un = `ps -ef |grep rsync|grep -v grep |grep avl|wc -l`;
                $i =$i+1;
                if( $un < $maxchild){
                        system("rsync -avl --size-only $path/$_   $ip:$path &") ;
                }else{
                        sleep 5;
                        $i = 1;
                }
        }
}
```

2.10. 数度限制

限制为 100k Bytes/s

```
rsync -auvzP--bwlimit=100 /www/* root@172.16.0.1/www
```

3. tsync

homepage: http://tsyncd.sourceforge.net/

4. Unison File Synchronizer

If you are looking for a tool to sync your laptop with your workstation, you better have a look at Unison.

homepage: http://www.cis.upenn.edu/~bcpierce/unison/

installation

```
$ sudo apt-get install unison
```

4.1. local

dir to dir

```
unison dir1 dir2
```

4.2. remote

ssh

```
unison dir1 ssh://username@remotehostname(ip)//absolute/path/to/dir2
```

socket

target host

```
# unison -socket NNNN
```

source host

```
# unison dir1 socket://remotehost(ip):port//absolute/path/to/dir2
```

4.3. config

create a config file under '.unison' directory.

```
vim ~/.unison/config.prf

root = /var/www
root = ssh://netkiller@netkiller.8800.org//var/www
force = /var/www
ignore = Path templates_compiled
ignore = Name tmp/*.pdf
auto = true
log = true
```

```
logfile = /home/netkiller/.unison/netkiller.8800.org.log
```

5. csync2 - cluster synchronization tool

homepage: http://oss.linbit.com/

5.1. server

过程 54.3. Install and setup csync2 on Ubuntu

1. installation

```
$ sudo apt-get install csync2 sqlite3 openssl xinetd
```

The following line will be added to your /etc/inetd.conf file:

```
$ cat /etc/inetd.conf
csync2          stream  tcp     nowait  root    /usr/sbin/csync2        csync2 -i
```

If you are indeed using xinetd, you will have to convert the above into /etc/xinetd.conf format, and add it manually.

```
service csync2
{
        disable = no
        protocol = tcp
        socket_type = stream
        wait = no
        user = root
        server = /usr/sbin/csync2
        server_args = -i
}
```

/etc/services

```
$ cat /etc/services |grep csync2
csync2          30865/tcp                       # cluster synchronization tool
```

2. create a self-signed SSL certificate for csync2

```
sudo openssl genrsa -out /etc/csync2_ssl_key.pem 1024
sudo openssl req -new -key /etc/csync2_ssl_key.pem -out /etc/csync2_ssl_cert.csr
sudo openssl x509 -req -days 600 -in /etc/csync2_ssl_cert.csr -signkey
/etc/csync2_ssl_key.pem -out /etc/csync2_ssl_cert.pem
```

```
$ sudo csync2 -k /etc/csync2_ssl_cert.key
```

3. After having done everything, we are now going to configure Csync2 so that we can determine which files are going to be synchronized.

For this example, we are going to synchronize /etc/apache2 and /etc/mysql. For that we open /etc/csync2.cfg and we configure it like this:

```
$ sudo vim /etc/csync2.cfg
# please see the REAMDE file how to configure csync2

group testing #group name, we can have multiple groups
{
    host master; #master server
    host (slave); #slave server
    #host (node1);

    key /etc/csync2_ssl_cert.key;

    include /etc/apache2/;
    include /home/neo;

    backup-directory /var/backups/csync2;
    backup-generations 3;
    auto none; #no automatic sync
}
```

4. hosts

```
$ sudo vim /etc/hosts
192.168.245.131 slave
```

5. restart

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

5.2. node

过程 54.4. node

1. login to slave node

```
neo@slave:~$ sudo vim /etc/hosts
192.168.245.129 master
```

2. install

```
$ sudo apt-get install csync2 xinetd
```

3. copy config file from master

```
neo@slave:~$  sudo scp root@master:/etc/csync2* /etc/
```

4. restart

```
neo@slave:~$ sudo /etc/init.d/xinetd restart
```

5.3. test

过程 54.5. testing

1. master

```
neo@master:/etc/apache2$ sudo touch test.master
neo@master:/etc/apache2$ sudo csync2 -x
```

2. node

```
neo@slave:/etc/apache2$ ls test.master -l
-rw-r--r-- 1 root root 0 2008-10-31 06:37 test.master
```

5.4. Advanced Configuration

例 54.7. /etc/csync2.cfg

```
$ sudo cat /etc/csync2.cfg

# please see the REAMDE file how to configure csync2
# group name, we can have multiple groups

group www {
    host master;
    host (slave);

    key /etc/csync2_ssl_cert.key;

    include /etc/apache2/;
    include /etc/csync2.cfg;
    include /var/www;
    include %homedir%/neo;
    exclude %homedir%/neo/temp;
    exclude *~ .*;

action
{
        pattern /etc/apache2/httpd.conf;
        pattern /etc/apache2/sites-available/*;
        exec "/usr/sbin/apache2ctl graceful";
        logfile "/var/log/csync2_action.log";
        do-local;
}

    backup-directory /var/backups/csync2;
    backup-generations 3;
    auto none;
}

prefix homedir
{
        on *: /home;
}
```

5.5. 编译安装

过程 54.6.

-
```
# yum install byacc -y
```

```
# tar zxvf librsync-0.9.7.tar.gz
# cd librsync-0.9.7
./configure --prefix=/usr/local/librsync-0.9.7
# make && make install
```

```
# www.sqlite.org
# wget http://www.sqlite.org/sqlite-3.7.2.tar.gz
# tar zxvf sqlite-3.7.2.tar.gz
```

```
# www.gnu.org/software/gnutls/
# wget http://ftp.gnu.org/pub/gnu/gnutls/gnutls-2.10.1.tar.bz2
# tar jxvf gnutls-2.10.1.tar.bz2
```

```
# wget http://oss.linbit.com/csync2/csync2-1.34.tar.gz
# tar csync2-1.34.tar.gz
# ./configure --prefix=/usr/local/csync2-1.34 --with-librsync-
source=/usr/local/src/librsync-0.9.7.tar.gz --with-libsqlite-source=/usr/local/src/sqlite-
3.7.2.tar.gz --disable-gnutls
```

---

6. synctool

synctool 是一个集群管理工具，用来在集群中的所有节点间进行保证配置文件的同步。节点可以是一个逻辑组和类的一部分，它们可能需要部分的配置文件。synctool 守护进程可以根据配置更改而对应用进行重启，还包括执行一些其他的管理任务。 新版本增加了一个新的工具 synctool-scp ，你可以使用这个工具来将文件复制到集群中的所有节点。

第 55 章 File Share

目录

1. NFSv4

1.1. Installation

1.1.1. NFSv4 server

```
sudo apt-get install nfs-kernel-server
```

Configuration

```
vim /etc/exports
/www     *(ro,sync,no_root_squash)
/home    *(rw,sync,no_root_squash)
/export       192.168.1.0/24(rw,fsid=0,insecure,no_subtree_check,async)
/export/users 192.168.1.0/24(rw,nohide,insecure,no_subtree_check,async)
```

To start the NFS server

```
sudo /etc/init.d/nfs-kernel-server start
```

1.1.2. NFSv4 client

```
sudo apt-get install nfs-common
```

NFSv3

```
sudo mount example.hostname.com:/www /www
```

NFSv4

```
# mount -t nfs4 -o proto=tcp,port=2049 nfs-server:/ /mnt
# mount -t nfs4 -o proto=tcp,port=2049 nfs-server:/users /home/users
```

NFS Client Configuration

```
vim /etc/fstab
example.hostname.com:/ubuntu /local/ubuntu nfs rsize=8192,wsize=8192,timeo=14,intr
```

1.2. exports

1.2.1. Permission

```
/etc/exports为:

/tmp     *(rw,no_root_squash)

/home/public 192.168.0.*(rw)   *(ro)

/home/test  192.168.0.100(rw)
```

```
/home/linux  *.example.com(rw,all_squash,anonuid=40,anongid=40)
```

1.2.2. Parameters

General Options

```
ro                          只读访问
rw                          读写访问
rsize                                   同时传输(读 )的数据块大小
wsize                                   同时传输(写)的数据块大小

sync                        所有数据在请求时写入共享
async                       NFS在写入数据前可以相应请求

secure                      NFS通过1024以下的安全TCP/IP端口发送
insecure                    NFS通过1024以上的端口发送
wdelay                      如果多个用户要写入NFS目录，则归组写入（默认）
no_wdelay                   如果多个用户要写入NFS目录，则立即写入，当使用async时，无需此设置。
hide                        在NFS共享目录中不共享其子目录
no_hide                     共享NFS目录的子目录
subtree_check               如果共享/usr/bin之类的子目录时，强制NFS检查父目录的权限（默认）
no_subtree_check            和上面相对，不检查父目录权限
```

User ID Mapping

```
all_squash                  共享文件的UID和GID映射匿名用户anonymous，适合公用目录。
no_all_squash               保留共享文件的UID和GID（默认）
root_squash                 root用户的所有请求映射成如anonymous用户一样的权限（默认）
no_root_squas               root用户具有根目录的完全管理访问权限
anonuid=xxx                 指定NFS服务器/etc/passwd文件中匿名用户的UID
anongid=xxx                 指定NFS服务器/etc/passwd文件中匿名用户的GID
```

1.2.3. 实例参考

只读挂载

```
172.16.2.5:/   /www/images   nfs4       ro,rsize=8192,wsize=8192,timeo=15,intr,noac
```

---

2. Samba

2.1. install

环境 ubuntu 8.10

```
$ sudo apt-get install samba
```

查看Samba 服务器的端口

```
neo@shenzhen:~$ sudo netstat -tlnp |grep smb
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      4480/smbd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      4480/smbd
neo@shenzhen:~$
```

防火墙

```
neo@shenzhen:~$ iptables -L
```

iptables -L

2.2. smb.conf

security = share|user 共享|用户模式

```
comment = 描述
valid users = '%S'登录用户, 'neo'允许neo访问
read only = 'No'读写模式, 'Yes'只读模式
browseable = 'No'不显示, 'Yes'显示
```

2.2.1. Security consideration

```
[global]
interfaces = lo, eth0
bind interfaces only = true
```

2.3. by Example

Backup the /etc/samba/smb.conf file:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.original
```

2.3.1. share

security = share

```
[tmp]
   comment = test
   writable = yes
   locking = yes
   path = /tmp
   public = yes

[neo]
   comment = neo
   writable = yes
   locking = yes
   path = /home/neo/
   public = yes

[htdocs]
   comment = neo
   writable = yes
   locking = yes
   path = /opt/lampp/htdocs
   public = yes
```

2.3.2. user

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.original
```

```
security = user
```

add user

```
sudo useradd -s /bin/true neo
sudo smbpasswd -L -a neo
```

enable

```
sudo smbpasswd -L -e neo
```

del user

```
sudo smbpasswd -L -x neo
```

2.3.3. test

测试配置文件是否正确

```
$ testparm
```

查看共享目录

```
$ smbclient -L localhost -N

Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.3.2]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        developer       Disk      Development
        IPC$            IPC       IPC Service (ubuntu server (Samba, Ubuntu))
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.3.2]

        Server               Comment
        ---------            -------
        PRINTSERVER
        UBUNTU               ubuntu server (Samba, Ubuntu)
```

```
        Workgroup            Master
        ---------            -------
        WORKGROUP            PRINTSERVER
```

Windows 访问测试

```
C:\>net view \\192.168.3.40
在 \\192.168.3.40 的共享资源

ubuntu server (Samba, Ubuntu)

共享名       类型   使用为   注释

-------------------------------------------------------------
developer  Disk  Development
命令运行完毕，但发生一个或多个错误。
```

2.4. nmblookup - NetBIOS over TCP/IP client used to lookup NetBIOS names

```
$ nmblookup -A 172.16.0.5
Looking up status of 172.16.0.5
        USER            <00> -         B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        USER            <20> -         B <ACTIVE>
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>
        WORKGROUP       <1d> -         B <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>

        MAC Address = 00-25-64-A7-18-97
```

2.5. smbfs/smbmount/smbumount

```
sudo apt-get install smbfs
```

smbmount

```
$ sudo mkdir /mnt/winfs
$ sudo smbmount //172.16.0.92/tmp /mnt/winfs
$ ls /mnt/winfs/
```

使用neo帐号登录

```
$ sudo smbmount //172.16.0.92/tmp /mnt/winfs -o username=neo
```

mount

```
$ mount -t smbfs -o username=jwhittal \\\\172.16.1.3\\c$ /mnt/thumb
```

linux 不再使用smbfs, 替换为 cifs

```
$ mount -t cifs //192.168.0.2/ /mnt/
```

2.6. smbclient - ftp-like client to access SMB/CIFS resources on servers

```
$ sudo apt-get install smbclient
```

2.6.1. 显示共享目录

$ smbclient -L 172.16.1.3

```
neo@netkiller:~$ smbclient -L 172.16.0.1
Enter neo's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.0]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (netkiller server (Samba, Ubuntu))
        www             Disk      www diretcory
        print$          Disk      Printer Drivers
        neo             Disk      Home Directories
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.0]

        Server               Comment
        ---------            -------
        DEBIAN               debian server
        NETKILLER            netkiller server (Samba, Ubuntu)

        Workgroup            Master
        ---------            -------
        WORKGROUP            DEBIAN
```

2.6.2. 访问共享资源

访问developer共享目录

```
$ smbclient //localhost/developer

Enter neo's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.3.2]
Server not using user level security and no password supplied.
smb: \> ls
  .                                   D        0  Thu Oct 29 02:05:37 2009
  ..                                  D        0  Thu Oct 22 05:27:16 2009
  ofcard.php                       1104  Tue Oct 27 02:00:49 2009
  index.html                        580  Thu Oct 29 02:05:37 2009
  webapps                             D        0  Wed Oct 28 06:04:08 2009
  ecmall                              D        0  Thu Oct 22 00:00:12 2009
  doc                                 D        0  Wed Oct 28 06:04:09 2009
  supersite                           D        0  Thu Oct 22 03:35:08 2009
  empire                              D        0  Thu Oct 22 02:56:12 2009
  discuz                              D        0  Wed Oct 21 22:04:29 2009
  resin-data                          D        0  Wed Oct 28 06:21:02 2009
  phpMyAdmin                          D        0  Sat Oct 24 09:02:29 2009
  empirecms6                          D        0  Thu Oct 22 04:12:44 2009
  ecshop                              D        0  Wed Oct 21 21:56:40 2009
  watchdog-data                       D        0  Wed Oct 28 06:07:19 2009
  ucenter                             D        0  Wed Oct 21 22:41:58 2009
  ecshop.old                          D        0  Fri Oct 23 11:35:39 2009
  magento                             D        0  Tue Oct  6 19:19:54 2009
  weberp                              D        0  Fri Oct 23 05:21:33 2009

                61335 blocks of size 131072. 41655 blocks available
smb: \>
```

2.6.3. 用户登录

使用用户Neo登录

```
$ smbclient //localhost/developer -U neo

Enter neo's password:
Domain=[UBUNTU] OS=[Unix] Server=[Samba 3.3.2]
smb: \> ls
  .                                   D        0  Thu Oct 29 03:13:31 2009
  ..                                  D        0  Thu Oct 22 05:27:16 2009
  ofcard.php                       1104  Tue Oct 27 02:00:49 2009
  index.html                        676  Thu Oct 29 03:13:31 2009
  webapps                             D        0  Wed Oct 28 06:04:08 2009
  ecmall                              D        0  Thu Oct 22 00:00:12 2009
  doc                                 D        0  Wed Oct 28 06:04:09 2009
  supersite                           D        0  Thu Oct 22 03:35:08 2009
  empire                              D        0  Thu Oct 22 02:56:12 2009
  discuz                              D        0  Wed Oct 21 22:04:29 2009
  resin-data                          D        0  Wed Oct 28 06:21:02 2009
  phpMyAdmin                          D        0  Sat Oct 24 09:02:29 2009
  empirecms6                          D        0  Thu Oct 22 04:12:44 2009
  ecshop                              D        0  Wed Oct 21 21:56:40 2009
  watchdog-data                       D        0  Wed Oct 28 06:07:19 2009
  ucenter                             D        0  Wed Oct 21 22:41:58 2009
  ecshop.old                          D        0  Fri Oct 23 11:35:39 2009
  magento                             D        0  Tue Oct  6 19:19:54 2009
  weberp                              D        0  Fri Oct 23 05:21:33 2009

                61335 blocks of size 131072. 41654 blocks available
```

```
smb: \> quit
```

2.7. smbtar - shell script for backing up SMB/CIFS shares directly to UNIX tape drives

2.8. FAQ

2.8.1. smbd/service.c:make_connection_snum(1013)

```
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:08, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:08, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:11, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:13, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:13, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:13, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
[2010/05/17 17:26:13, 0] smbd/service.c:make_connection_snum(1013)
  '/www' does not exist or permission denied when connecting to [www] Error was Permission
denied
```

关闭 SELinux

第 56 章 Distributed Filesystem

目录

1. DRBD (Distributed Replicated Block Device)

Homepage: http://www.drbd.org/

实验环境需要两台电脑，如果你没有，建议你使用VMware，并且为每一个虚拟机添加两块硬盘。

实验环境

1. master: 192.168.0.1 DRBD:/dev/sdb
2. slave: 192.168.0.2 DRBD:/dev/sdb

1.1. disk and partition

Each of the following steps must be completed on both nodes

show all of disk and partition

```
neo@master:~$ sudo sfdisk -s
/dev/sda:   8388608
/dev/sdb:   2097152
total: 10485760 blocks
```

create a new partition on the disk /dev/sdb

```
$ sudo cfdisk /dev/sdb
```

you must have extended partition

check partition

```
neo@master:~$ sudo fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x000301bd
```

```
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         993     7976241   83  Linux
/dev/sda2             994        1044      409657+   5  Extended
/dev/sda5             994        1044      409626   82  Linux swap / Solaris

Disk /dev/sdb: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1         261     2096451    5  Extended
/dev/sdb5               1         261     2096419+  83  Linux
```

format /dev/sdb1

```
neo@master:~$ sudo mkfs.ext3 /dev/sdb1
```

you also can using other file system

reiserfs

```
neo@master:~$ sudo mkfs.reiserfs /dev/sdb1
```

I suggest you using reiserfs.

1.2. Installation

Each of the following steps must be completed on both nodes

search drbd8-utils package

```
neo@master:~$ apt-cache search drbd
drbd8-utils - RAID 1 over tcp/ip for Linux utilities
drbd0.7-module-source - RAID 1 over tcp/ip for Linux module source
drbd0.7-utils - RAID 1 over tcp/ip for Linux utilities
drbdlinks - Manages symlinks into a shared DRBD partition
```

installation

```
neo@master:~$ sudo apt-get install drbd8-utils
```

to add modules from the Linux Kernel

```
neo@master:~$ sudo modprobe drbd
neo@master:~$ lsmod |grep drbd
drbd                  213000  0
cn                      9632  1 drbd
```

1.3. configure

Each of the following steps must be completed on both nodes

backup configure file

```
neo@master:~$ sudo cp /etc/drbd.conf /etc/drbd.conf.old
```

edit /etc/drbd.conf

```
global {
  usage-count yes;
}
common {
  protocol C;
}
resource r0 {
  on master {
    device    /dev/drbd0;
    disk      /dev/sdb5;
    address   192.168.0.1:7789;
    meta-disk internal;
  }
  on slave {
    device    /dev/drbd0;
    disk      /dev/sdb5;
    address   10.1.1.32:7789;
    meta-disk internal;
  }
}
```

1.4. Starting

Each of the following steps must be completed on both nodes.

```
neo@master:~$ sudo drbdadm create-md r0
neo@master:~$ sudo drbdadm attach r0
neo@master:~$ sudo drbdadm connect r0
neo@master:~$ sudo drbdadm -- --overwrite-data-of-peer primary r0

neo@slave:~$ sudo drbdadm create-md r0
neo@slave:~$ sudo drbdadm attach r0
neo@slave:~$ sudo drbdadm connect r0
```

master

```
neo@master:~$ sudo drbdadm create-md r0
v08 Magic number not found
md_offset 2146725888
al_offset 2146693120
bm_offset 2146627584

Found some data
 ==> This might destroy existing data! <==

Do you want to proceed?
[need to type 'yes' to confirm] yes

v07 Magic number not found
v07 Magic number not found
v08 Magic number not found
Writing meta data...
initialising activity log
NOT initialized bitmap
New drbd meta data block sucessfully created.
success
```

slave

```
neo@slave:~# sudo drbdadm create-md r0
v08 Magic number not found
md_offset 2146725888
al_offset 2146693120
bm_offset 2146627584

Found some data
 ==> This might destroy existing data! <==

Do you want to proceed?
[need to type 'yes' to confirm] yes

v07 Magic number not found
v07 Magic number not found
v08 Magic number not found
Writing meta data...
initialising activity log
NOT initialized bitmap
New drbd meta data block sucessfully created.
success
```

status

```
neo@master:~$ cat /proc/drbd
version: 8.0.11 (api:86/proto:86)
GIT-hash: b3fe2bdfd3b9f7c2f923186883eb9e2a0d3a5b1b build by phil@mescal, 2008-02-12 11:56:43
 0: cs:StandAlone st:Primary/Unknown ds:UpToDate/DUnknown   r---
    ns:0 nr:0 dw:0 dr:0 al:0 bm:0 lo:0 pe:0 ua:0 ap:0
        resync: used:0/31 hits:0 misses:0 starving:0 dirty:0 changed:0
        act_log: used:0/127 hits:0 misses:0 starving:0 dirty:0 changed:0
 1: cs:Connected st:Secondary/Secondary ds:Diskless/Inconsistent C r---
    ns:0 nr:0 dw:0 dr:0 al:0 bm:0 lo:0 pe:0 ua:0 ap:0
```

1.5. Using

master

```
neo@master:~$ sudo drbdadm primary all
neo@master:~$ sudo mkfs.reiserfs /dev/drbd0
neo@master:~$ sudo mkdir /mnt/drbd0
neo@master:~$ sudo mount /dev/drbd0 /mnt/drbd0/
neo@master:~$ sudo touch /mnt/drbd0/helloworld.tmp
neo@master:~$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda1             7.6G  1.3G  6.0G  18% /
varrun                125M  216K  125M   1% /var/run
varlock               125M  8.0K  125M   1% /var/lock
udev                  125M   60K  125M   1% /dev
devshm                125M     0  125M   0% /dev/shm
/dev/drbd0            2.0G   33M  2.0G   2% /mnt/drbd0
neo@master:~$ sudo dd if=/dev/zero of=/mnt/drbd0/tempfile1.tmp bs=104857600 count=1
1+0 records in
1+0 records out
104857600 bytes (105 MB) copied, 0.564911 s, 186 MB/s
neo@master:~$ sudo umount /mnt/drbd0/
neo@master:~$ sudo drbdadm secondary all
```

slave

```
neo@slave:~$ sudo drbdadm primary all
neo@slave:~$ sudo mkdir /mnt/drbd0
neo@slave:~$ sudo mount /dev/drbd0 /mnt/drbd0/
neo@slave:~$ ls /mnt/drbd0/
helloworld.tmp  tempfile1.tmp
```

---

2. Network Block Device protocol

2.1. nbd-server - Network Block Device protocol - server

```
apt-get install nbd-server

# modprobe nbd
# mkdir -p /home/exported
# dd if=/dev/zero of=/home/exported/trial.img count=256 bs=1024k
# mkfs.ext3 /home/exported/trial.img

# nbd-server 1234 /home/exported/trial.img

# touch /root/empty
# nbd-server 1234 /home/exported/trial.img -C /root/empty
```

2.2. nbd-client - Network Block Device protocol - client

```
# apt-get install nbd-client


# nbd-client mine.my.flat 1234 /dev/nbd0
Negotiation: ..size = 262144KB
bs=1024, sz=262144

# mkdir /mnt/remote
# mount /dev/nbd0 /mnt/remote
# for i in $(seq 1 100) ; do echo $i > /mnt/remote/$i; done

# umount /mnt/remote

root@vain:~#  nbd-client 127.0.0.1 1234 /dev/nbd0
root@vain:~# mkdir /tmp/foo
root@vain:~#  mount /dev/nbd0 /tmp/foo
root@vain:~#  ls /tmp/foo/
1    14  2   25  30  36  41  47  52  58  63  69  74  8   85  90  96
10   15  20  26  31  37  42  48  53  59  64  7   75  80  86  91  97
100  16  21  27  32  38  43  49  54  6   65  70  76  81  87  92  98
11   17  22  28  33  39  44  5   55  60  66  71  77  82  88  93  99
12   18  23  29  34  4   45  50  56  61  67  72  78  83  89  94
13   19  24  3   35  40  46  51  57  62  68  73  79  84  9   95  lost+found
```

3. GridFS

http://www.mongodb.org/display/DOCS/GridFS

GridFS 类似 MogileFS

3.1. nginx-gridfs

http://github.com/mdirolf/nginx-gridfs

4. Moose File System

http://www.moosefs.org/

4.1. Master server installation

```
groupadd mfs
useradd -g mfs mfs
cd /usr/local/src
wget
http://pro.hit.gemius.pl/hitredir/id=nXCV9nrckU2Et.zoR5kxdXZJLQq1fqbG4AIiq5K95Gz.07/url=moosefs.org/
1.6.19.tar.gz
tar zxvf mfs-1.6.19.tar.gz
cd mfs-1.6.19
./configure --prefix=/srv/mfs \
--with-default-user=mfs \
--with-default-group=mfs \
--disable-mfschunkserver \
--disable-mfsmount

make
make install
```

```
cd /srv/mfs/etc/
cp /srv/mfs/var/mfs/metadata.mfs.empty /srv/mfs/var/mfs/metadata.mfs

cp mfsexports.cfg.dist mfsexports.cfg
cp mfsmaster.cfg.dist mfsmaster.cfg
cp mfsmetalogger.cfg.dist mfsmetalogger.cfg
vim mfsmaster.cfg
```

```
WORKING_USER = mfs
WORKING_GROUP = mfs
SYSLOG_IDENT = mfsmaster
LOCK_MEMORY = 0
NICE_LEVEL = -19

EXPORTS_FILENAME = /srv/mfs/etc/mfsexports.cfg

DATA_PATH = /srv/mfs/var/mfs

BACK_LOGS = 50

REPLICATIONS_DELAY_INIT = 300
REPLICATIONS_DELAY_DISCONNECT = 3600

MATOML_LISTEN_HOST = *
MATOML_LISTEN_PORT = 9419

MATOCS_LISTEN_HOST = *
MATOCS_LISTEN_PORT = 9420

MATOCU_LISTEN_HOST = *
MATOCU_LISTEN_PORT = 9421

CHUNKS_LOOP_TIME = 300
CHUNKS_DEL_LIMIT = 100
CHUNKS_WRITE_REP_LIMIT = 1
CHUNKS_READ_REP_LIMIT = 5

REJECT_OLD_CLIENTS = 0

# deprecated, to be removed in MooseFS 1.7
# LOCK_FILE = /srv/mfs/var/run/mfs/mfsmaster.lock
```

```
echo "192.168.3.10        mfsmaster" >> /etc/hosts
```

```
# /srv/mfs/sbin/mfsmaster start
working directory: /srv/mfs/var/mfs
lockfile created and locked
initializing mfsmaster modules ...
loading sessions ... ok
sessions file has been loaded
exports file has been loaded
loading metadata ...
create new empty filesystemmetadata file has been loaded
no charts data file - initializing empty charts
master <-> metaloggers module: listen on *:9419
master <-> chunkservers module: listen on *:9420
main master server module: listen on *:9421
mfsmaster daemon initialized properly
```

```
# /srv/mfs/sbin/mfscgiserv
starting simple cgi server (host: any , port: 9425 , rootpath: /srv/mfs/share/mfscgi)
```

http://192.168.3.10:9425/

4.2. Backup server (metalogger) installation

```
groupadd mfs
useradd -g mfs mfs
cd /usr/local/src
wget
http://pro.hit.gemius.pl/hitredir/id=nXCV9nrckU2Et.zoR5kxdXZJLQq1fqbG4AIiq5K95Gz.07/url=moosefs.org/
1.6.19.tar.gz
tar zxvf mfs-1.6.19.tar.gz
cd mfs-1.6.19
./configure --prefix=/srv/mfs \
--with-default-user=mfs \
--with-default-group=mfs \
--disable-mfschunkserver \
--disable-mfsmount

make
make install

cd /srv/mfs/etc/
cp mfsmetalogger.cfg.dist mfsmetalogger.cfg
vim mfsmetalogger.cfg
```

```
WORKING_USER = mfs
WORKING_GROUP = mfs
SYSLOG_IDENT = mfsmetalogger
LOCK_MEMORY = 0
NICE_LEVEL = -19

DATA_PATH = /srv/mfs/var/mfs

BACK_LOGS = 50
META_DOWNLOAD_FREQ = 24

MASTER_RECONNECTION_DELAY = 5

MASTER_HOST = mfsmaster
MASTER_PORT = 9419

MASTER_TIMEOUT = 60

# deprecated, to be removed in MooseFS 1.7
# LOCK_FILE = /srv/mfs/var/run/mfs/mfsmetalogger.lock
```

```
echo "192.168.3.10        mfsmaster" >> /etc/hosts
```

```
# /srv/mfs/sbin/mfsmetalogger start
working directory: /srv/mfs/var/mfs
lockfile created and locked
initializing mfsmetalogger modules ...
mfsmetalogger daemon initialized properly
```

4.3. Chunk servers installation

```
groupadd mfs
useradd -g mfs mfs
cd /usr/local/src
wget
http://pro.hit.gemius.pl/hitredir/id=nXCV9nrckU2Et.zoR5kxdXZJLQq1fqbG4AIiq5K95Gz.07/url=moosefs.org/
```

```
1.6.19.tar.gz
tar zxvf mfs-1.6.19.tar.gz
cd mfs-1.6.19

./configure --prefix=/srv/mfs \
--with-default-user=mfs \
--with-default-group=mfs \
--disable-mfsmaster \
--disable-mfsmount

make
make install

cd /srv/mfs/etc/
cp mfschunkserver.cfg.dist mfschunkserver.cfg
cp mfshdd.cfg.dist mfshdd.cfg
vim mfschunkserver.cfg
```

```
WORKING_USER = mfs
WORKING_GROUP = mfs
SYSLOG_IDENT = mfschunkserver
LOCK_MEMORY = 0
NICE_LEVEL = -19

DATA_PATH = /srv/mfs/var/mfs

MASTER_RECONNECTION_DELAY = 5

BIND_HOST = *
MASTER_HOST = mfsmaster
MASTER_PORT = 9420

MASTER_TIMEOUT = 60

CSSERV_LISTEN_HOST = *
CSSERV_LISTEN_PORT = 9422
CSSERV_TIMEOUT = 5

HDD_CONF_FILENAME = /srv/mfs/etc/mfshdd.cfg
HDD_TEST_FREQ = 10

# deprecated, to be removed in MooseFS 1.7
# LOCK_FILE = /srv/mfs/var/run/mfs/mfschunkserver.lock
# BACK_LOGS = 50
```

```
cat >> /srv/mfs/etc/mfshdd.cfg <<EOF
/mnt/mfschunks
EOF

chown -R mfs:mfs /mnt/mfschunks
```

```
echo "192.168.3.10        mfsmaster" >> /etc/hosts
```

```
# /srv/mfs/sbin/mfschunkserver start
working directory: /srv/mfs/var/mfs
lockfile created and locked
initializing mfschunkserver modules ...
hdd space manager: scanning folder /mnt/mfschunks/ ...
hdd space manager: scanning complete
hdd space manager: /mnt/mfschunks/: 0 chunks found
hdd space manager: scanning complete
main server module: listen on *:9422
no charts data file - initializing empty charts
mfschunkserver daemon initialized properly
```

http://192.168.3.10:9425/mfs.cgi?sections=CS

http://192.168.3.10:9425/mfs.cgi?sections=HD

4.4. Users' computers installation

```
yum install fuse-devel

cd /usr/local/src
wget
http://pro.hit.gemius.pl/hitredir/id=nXCV9nrckU2Et.zoR5kxdXZJLQq1fqbG4AIiq5K95Gz.07/url=moosefs.org/
1.6.19.tar.gz
tar zxvf mfs-1.6.19.tar.gz
cd mfs-1.6.19
./configure --prefix=/srv/mfs \
 --with-default-user=mfs \
--with-default-group=mfs \
```

```
--disable-mfsmaster \
--disable-mfschunkserver

make
make install
```

mount

```
mkdir -p /mnt/mfs
modprobe fuse
/srv/mfs/bin/mfsmount /mnt/mfs -H 192.168.3.10
```

```
# df /mnt/mfs
Filesystem           1K-blocks      Used Available Use% Mounted on
mfs#192.168.3.10:9421
                       6085120         0   6085120   0% /mnt/mfs
```

umount

```
umount /mnt/mfs
```

4.5. Testing MFS

mfs client

```
[root@dev4 ~]# mkdir -p /mnt/mfs/neo
[root@dev4 ~]# touch test /mnt/mfs/
[root@dev4 ~]# touch /mnt/mfs/neo/test
[root@dev4 ~]# touch /mnt/mfs/helloworld
```

write testing

```
# time dd if=/dev/zero of=sometestfile bs=1024 count=100000
```

mfs chunk server

```
# ls /mnt/mfschunks/
00  07  0E  15  1C  23  2A  31  38  3F  46  4D  54  5B  62  69  70  77  7E  85  8C  93  9A  A1
A8  AF  B6  BD  C4  CB  D2  D9  E0  E7  EE  F5  FC
01  08  0F  16  1D  24  2B  32  39  40  47  4E  55  5C  63  6A  71  78  7F  86  8D  94  9B  A2
A9  B0  B7  BE  C5  CC  D3  DA  E1  E8  EF  F6  FD
02  09  10  17  1E  25  2C  33  3A  41  48  4F  56  5D  64  6B  72  79  80  87  8E  95  9C  A3
AA  B1  B8  BF  C6  CD  D4  DB  E2  E9  F0  F7  FE
03  0A  11  18  1F  26  2D  34  3B  42  49  50  57  5E  65  6C  73  7A  81  88  8F  96  9D  A4
AB  B2  B9  C0  C7  CE  D5  DC  E3  EA  F1  F8  FF
04  0B  12  19  20  27  2E  35  3C  43  4A  51  58  5F  66  6D  74  7B  82  89  90  97  9E  A5
AC  B3  BA  C1  C8  CF  D6  DD  E4  EB  F2  F9
05  0C  13  1A  21  28  2F  36  3D  44  4B  52  59  60  67  6E  75  7C  83  8A  91  98  9F  A6
AD  B4  BB  C2  C9  D0  D7  DE  E5  EC  F3  FA
06  0D  14  1B  22  29  30  37  3E  45  4C  53  5A  61  68  6F  76  7D  84  8B  92  99  A0  A7
AE  B5  BC  C3  CA  D1  D8  DF  E6  ED  F4  FB
```

5. GlusterFS

http://www.gluster.org/

```
$ apt-cache search glusterfs
glusterfs-client - clustered file-system (client package)
glusterfs-dbg - GlusterFS debugging symbols
glusterfs-examples - example files for the glusterfs server and client
glusterfs-server - clustered file-system (server package)
libglusterfs-dev - GlusterFS development libraries and headers (development files)
libglusterfs0 - GlusterFS libraries and translator modules
```

5.1. glusterfs-server

```
$ sudo apt-get install glusterfs-server
$ sudo cp /etc/glusterfs/glusterfsd.vol /etc/glusterfs/glusterfsd.vol.orig
```

```
$ cat /etc/glusterfs/glusterfsd.vol
### file: server-volume.vol.sample

#######################################
###  GlusterFS Server Volume File  ##
#######################################

#### CONFIG FILE RULES:
### "#" is comment character.
### - Config file is case sensitive
### - Options within a volume block can be in any order.
### - Spaces or tabs are used as delimitter within a line.
### - Multiple values to options will be : delimitted.
### - Each option should end within a line.
### - Missing or commented fields will assume default values.
### - Blank/commented lines are allowed.
### - Sub-volumes should already be defined above before referring.

### Export volume "brick" with the contents of "/home/export" directory.
volume brick
  type storage/posix                   # POSIX FS translator
  option directory /home/export        # Export this directory
end-volume

### Add network serving capability to above brick.
volume server
  type protocol/server
  option transport-type tcp
# option transport-type unix
# option transport-type ib-sdp
# option transport.socket.bind-address 192.168.1.10     # Default is to listen on all interfaces
# option transport.socket.listen-port 6996              # Default is 6996

# option transport-type ib-verbs
# option transport.ib-verbs.bind-address 192.168.1.10     # Default is to listen on all
interfaces
# option transport.ib-verbs.listen-port 6996              # Default is 6996
# option transport.ib-verbs.work-request-send-size  131072
# option transport.ib-verbs.work-request-send-count 64
# option transport.ib-verbs.work-request-recv-size  131072
# option transport.ib-verbs.work-request-recv-count 64

# option client-volume-filename /etc/glusterfs/glusterfs-client.vol
  subvolumes brick
# NOTE: Access to any volume through protocol/server is denied by
# default. You need to explicitly grant access through # "auth"
# option.
  option auth.addr.brick.allow * # Allow access to "brick" volume
end-volume
```

```
$ sudo mkdir /home/export
$ sudo /etc/init.d/glusterfs-server start
$ sudo /etc/init.d/glusterfs-server status
 * GlusterFS server is running.
```

5.2. glusterfs-client

```
$ sudo apt-get install glusterfs-client
$ sudo cp /etc/glusterfs/glusterfs.vol /etc/glusterfs/glusterfs.vol.orig
```

```
# cat /etc/glusterfs/glusterfs.vol
### file: client-volume.vol.sample

######################################
###  GlusterFS Client Volume File  ##
######################################

#### CONFIG FILE RULES:
### "#" is comment character.
### - Config file is case sensitive
### - Options within a volume block can be in any order.
### - Spaces or tabs are used as delimitter within a line.
### - Each option should end within a line.
### - Missing or commented fields will assume default values.
### - Blank/commented lines are allowed.
### - Sub-volumes should already be defined above before referring.

### Add client feature and attach to remote subvolume
volume client
  type protocol/client
  option transport-type tcp
# option transport-type unix
# option transport-type ib-sdp
  option remote-host 192.168.80.1         # IP address of the remote brick
# option transport.socket.remote-port 6996              # default server port is 6996

# option transport-type ib-verbs
# option transport.ib-verbs.remote-port 6996              # default server port is 6996
# option transport.ib-verbs.work-request-send-size  1048576
# option transport.ib-verbs.work-request-send-count 16
# option transport.ib-verbs.work-request-recv-size  1048576
# option transport.ib-verbs.work-request-recv-count 16

# option transport-timeout 30          # seconds to wait for a reply
                                       # from server for each request
  option remote-subvolume brick        # name of the remote volume
end-volume

### Add readahead feature
#volume readahead
#  type performance/read-ahead
#  option page-size 1MB     # unit in bytes
#  option page-count 2       # cache per file  = (page-count x page-size)
#  subvolumes client
#end-volume

### Add IO-Cache feature
#volume iocache
#  type performance/io-cache
#  option page-size 256KB
#  option page-count 2
#  subvolumes readahead
#end-volume

### Add writeback feature
#volume writeback
#  type performance/write-behind
#  option aggregate-size 1MB
#  option window-size 2MB
#  option flush-behind off
#  subvolumes iocache
#end-volume
```

```
mkdir /mnt/glusterfs

glusterfs -f /etc/glusterfs/glusterfs.vol /mnt/glusterfs
or
mount -t glusterfs /etc/glusterfs/glusterfs.vol /mnt/glusterfs
```

fstab

```
/etc/glusterfs/glusterfs.vol  /mnt/glusterfs  glusterfs  defaults  0  0
```

5.3. Testing

client

```
touch /mnt/glusterfs/test1
touch /mnt/glusterfs/test2
```

server

```
# ll /mnt/glusterfs
total 0
-rw-r--r-- 1 root root 0 Jun 16 11:57 test1
-rw-r--r-- 1 root root 0 Jun 16 11:57 test2
```

5.4. RAID

http://www.gluster.com/community/documentation/index.php/GlusterFS_User_Guide

http://www.gluster.com/community/documentation/index.php/Storage_Server_Installation_and_Configuration

ref:http://www.howtoforge.com/high-availability-storage-cluster-with-glusterfs-on-ubuntu-p2

5.4.1. Mirror

例 56.1. Mirror

```
glusterfs-volgen --name store1 --raid 1 gluster1:/home/export gluster2:/home/export
```

5.4.2. Strip

例 56.2. Strip

```
glusterfs-volgen --name store1 --raid 0 gluster1:/home/export gluster2:/home/export
```

5.5. Filesystem Administration

```
# /etc/init.d/glusterd start

gluster peer probe gluster1
gluster peer probe gluster2

# gluster peer status
Number of Peers: 3

Hostname: gluster1
Uuid: 195c5908-750f-4051-accc-697ab72fa3f2
State: Probe Sent to Peer (Connected)

Hostname: gluster2
Uuid: 5f9887a9-da15-443f-aab1-5d9952247507
State: Probe Sent to Peer (Connected)

# gluster peer detach gluster3
Detach successful
```

To create a new volume

```
gluster volume create test-volume gluster1:/exp3 gluster2:/exp4
```

6. Lustre

6. Lustre

7. Hadoop - HDFS

http://hadoop.apache.org/

java

```
$ sudo apt-get install openjdk-6-jre-headless

$ sudo vim /etc/profile.d/java.sh
##################################################
### Java environment by neo
##################################################
export JAVA_HOME=/usr
export JRE_HOME=/usr
export PATH=$PATH:/usr/local/apache-tomcat/bin/:/usr/local/jetty-6.1.18/bin:/usr/local/apache-
nutch/bin
export CLASSPATH="./:/usr/share/java/:/usr/local/apache-solr/example/multicore/lib"
export JAVA_OPTS="-Xms128m -Xmx1024m"
```

过程 56.1. Master configure

1. Download and Installing Software

```
$ cd /usr/local/src/
$ wget http://apache.etoak.com/hadoop/core/hadoop-0.20.0/hadoop-0.20.0.tar.gz
$ tar zxvf hadoop-0.20.0.tar.gz
$ sudo cp -r hadoop-0.20.0 ..
$ sudo ln -s hadoop-0.20.0 hadoop
$ cd hadoop
```

2. Configuration

   hadoop-env.sh

```
$ vim conf/hadoop-env.sh
export JAVA_HOME=/usr
```

   conf/core-site.xml

```
$ vim conf/core-site.xml

<configuration>
  <property>
    <name>fs.default.name</name>
    <value>hdfs://localhost:9000</value>
  </property>
</configuration>
```

   conf/hdfs-site.xml

```
$ vim conf/hdfs-site.xml

<configuration>
  <property>
    <name>dfs.replication</name>
    <value>1</value>
  </property>
</configuration>
```

conf/mapred-site.xml

```
$ vim conf/mapred-site.xml

<configuration>
  <property>
    <name>mapred.job.tracker</name>
    <value>localhost:9001</value>
  </property>
</configuration>
```

3. Setup passphraseless ssh

```
Now check that you can ssh to the localhost without a passphrase:
$ ssh localhost

If you cannot ssh to localhost without a passphrase, execute the following commands:
$ ssh-keygen -t dsa -P '' -f ~/.ssh/id_dsa
$ cat ~/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys
```

4. Execution

```
 Format a new distributed-filesystem:
$ bin/hadoop namenode -format

Start the hadoop daemons:
$ bin/start-all.sh

When you're done, stop the daemons with:
$ bin/stop-all.sh
```

5. Monitor

Browse the web interface for the NameNode and the JobTracker; by default they are available at:

- NameNode - http://localhost:50070/
- JobTracker - http://localhost:50030/

6. Test

```
$ bin/hadoop dfs -mkdir test
$ echo helloworld > testfile
$ bin/hadoop dfs -copyFromLocal testfile test/
$ bin/hadoop dfs -ls
Found 1 items
drwxr-xr-x   - neo supergroup          0 2009-07-10 14:18 /user/neo/test

$ bin/hadoop dfs -ls test

$ bin/hadoop dfs –cat test/file
```

过程 56.2. slave config

1. SSH

```
$ scp neo@master:~/.ssh/id_dsa.pub .ssh/master.pub
$ cat .ssh/master.pub >> .ssh/authorized_keys
```

2. Hadoop

```
$ scp neo@master:/usr/local/hadoop /usr/local/hadoop
```

---

8. MogileFS

http://www.danga.com/mogilefs/

9. Ceph

http://ceph.newdream.net/

10. Kosmos distributed file system (KFS)

http://kosmosfs.sourceforge.net/

11. Coda

12. OpenAFS

http://www.openafs.org/

13. fam & imon

第 57 章 inotify

目录

$ ls -ld /proc/sys/fs/inotify/*

1. inotify-tools

Installation

ubuntu

```
sudo apt-get install inotify-tools
```

centos

```
yum install inotify-tools
```

inotifywait -r -m $HOME

监控登录过程

```
neo@master:~$ inotifywait -r  -m $HOME
Setting up watches.  Beware: since -r was given, this may take a while!
Watches established.
/home/neo/ OPEN .profile
/home/neo/ ACCESS .profile
/home/neo/ CLOSE_NOWRITE,CLOSE .profile
/home/neo/ OPEN .bashrc
/home/neo/ ACCESS .bashrc
/home/neo/ CLOSE_NOWRITE,CLOSE .bashrc
/home/neo/ OPEN .bash_history
/home/neo/ ACCESS .bash_history
/home/neo/ CLOSE_NOWRITE,CLOSE .bash_history
/home/neo/ OPEN .bash_history
/home/neo/ ACCESS .bash_history
/home/neo/ CLOSE_NOWRITE,CLOSE .bash_history
```

create a new file helloworld.txt

```
/home/neo/ CREATE helloworld.txt
/home/neo/ OPEN helloworld.txt
/home/neo/ MODIFY helloworld.txt
/home/neo/ CLOSE_WRITE,CLOSE helloworld.txt
```

cat a file using cat helloworld.txt

```
/home/neo/ OPEN,ISDIR
/home/neo/ CLOSE_NOWRITE,CLOSE,ISDIR
/home/neo/ OPEN,ISDIR
/home/neo/ CLOSE_NOWRITE,CLOSE,ISDIR
/home/neo/ OPEN helloworld.txt
/home/neo/ ACCESS helloworld.txt
/home/neo/ CLOSE_NOWRITE,CLOSE helloworld.txt
```

delete a file helloworld.txt

```
/home/neo/ OPEN,ISDIR
/home/neo/ CLOSE_NOWRITE,CLOSE,ISDIR
/home/neo/ OPEN,ISDIR
/home/neo/ CLOSE_NOWRITE,CLOSE,ISDIR
/home/neo/ DELETE helloworld.txt
```

---

2. Incron - cron-like daemon which handles filesystem events

3. inotify-tools + rsync

1. -m 是保持一直监听
2. -r 是递归查看目录
3. -q 是打印出事件～
4. -e create,move,delete,modify 监听 创建 移动 删除 写入 事件

```
inotifywait -mrq --event create,delete,modify,move --format '%w %e' /your_path | while read w
e; do
    if [ "$e" = "IGNORED" ]; then
        continue
    fi
    rsync -az --delete $w username@your_ip:$w
done
```

```
#!/bin/sh
# A slightly complex but actually useful example
inotifywait -mrq --timefmt '%d/%m/%y %H:%M' --format '%T %f' \
-e close_write /home/billy | while read date time file; do
    rsync /home/billy/${file} rsync://billy@example.com/backup/${file} && \
    echo "At ${time} on ${date}, file ${file} was backed up via rsync"
done
```

```
[root@development ~]# cat inotify-rsync
#!/bin/bash
# $Id$ #
# Author neo<openunix@163.com> #

# monitor path
monitor_path=cms
#inotifywait path
INOTIFYWAIT=inotifywait

# rsync image file
function images {
        local file=$1
        rsync -az --delete $file /tmp/images/$file
#       rsync ${file} ${rsync_url}/${file}
}

# rsync html file
function html {
        local file=$1
        rsync -az --delete $file /tmp/$file
}


$INOTIFYWAIT -mrq --event close_write --format '%w%f %e' $monitor_path | while read file event;
do
    if [ "$event" = "CLOSE_WRITE,CLOSE" ]; then
        ext=$(echo $file | awk -F'.' '{print $2}')
        if [ $ext = 'jpg' ]; then
                images $file
        fi
        if [ $ext = 'html' ]; then
                html $file
        fi
    fi
done &
```

4. pyinotify

```
[root@development ~]# easy_install pyinotify
[root@development ~]# yum install gcc
[root@development ctypes-1.0.2]# python setup.py install
```

第 58 章 Network Storage - Openfiler

目录

Openfiler is a powerful, intuitive browser-based network storage software distribution. Openfiler delivers file-based Network Attached Storage and block-based Storage Area Networking in a single framework.

openfiler 的官方网站

过程 58.1. Openfiler Storage Control Center

1. 登录管理界面

```
https://<ip address>:446/
```

初始帐号和密码是: openfiler/password

2. 首先要修改默认密码

Accounts->Admin Password

```
Current Password:  password
New Password:  新密码
Confirm New Password:  确认密码
```

Submit 提交

1. Accounts

- 用户认证

openfiler.ldif

```
dn: ou=people,dc=bg7nyt,dc=cn
ou: people
objectClass: organizationalUnit

dn: ou=Idmap,dc=bg7nyt,dc=cn
ou: Idmap
objectClass: organizationalUnit
```

添加people组织单元

```
[chenjingfeng@backup ldap]$ ldapadd -x -D "cn=root,dc=bg7nyt,dc=cn" -W -f openfiler.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=bg7nyt,dc=cn"

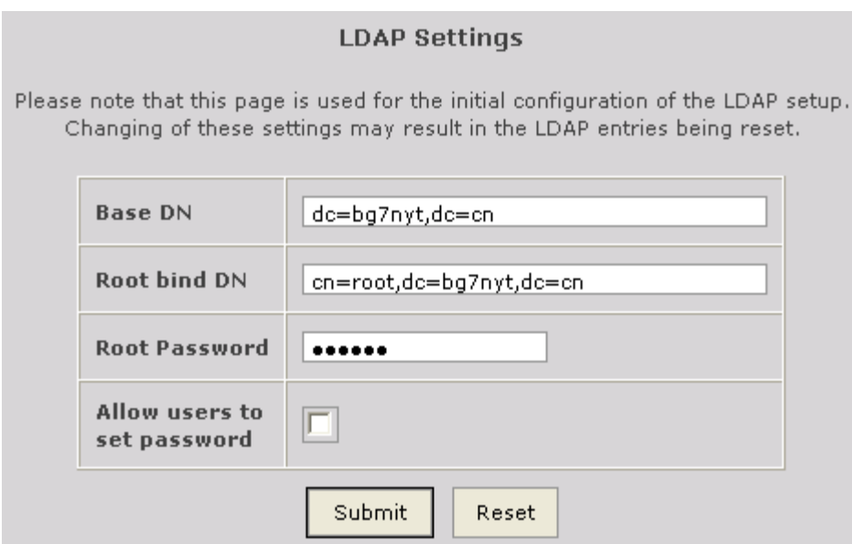
adding new entry "ou=Idmap,dc=bg7nyt,dc=cn"
```

a. Accounts->Authentication

Use LDAP: 打勾

```
Server:  ldap.bg7nyt.cn
Base DN:  dc=bg7nyt,dc=cn
Root bind DN:  cn=root,dc=bg7nyt,dc=cn
Root bind Password:  你的密码
```

b. Services->LDAP Settings




```
Base DN:  dc=bg7nyt,dc=cn
Root bind DN:  cn=root,dc=bg7nyt,dc=cn
Root Password:  你的密码
```

c. Services->Enable/Disable

Enable/Disable services		
Service Name	**Status**	**Modification**
SMB/CIFS	Enabled	Disable
NFSv3	Enabled	Disable
HTTP / WebDAV	Enabled	Disable
FTP	Enabled	Disable
iSCSI target	Enabled	Disable
Rsync	Disabled	Enable
UPS	Disabled	Enable
LDAP	Enabled	Disable

d. Accounts->Account Administration

i. Group Administration

```
Group Name: nfs
```

ii. User Administration

```
Username: 用户名
Password: 密码
Retype password: 确认密码
Primary Group: 用户组
```

查看组织单元：ou=people,dc=bg7nyt,dc=cn

```
[chenjingfeng@backup ldap]$ ldapsearch -x -b 'ou=people,dc=bg7nyt,dc=cn'
# extended LDIF
#
# LDAPv3
# base <ou=people,dc=bg7nyt,dc=cn> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# people, bg7nyt.cn
dn: ou=people,dc=bg7nyt,dc=cn
ou: people
objectClass: organizationalUnit

# neo, People, bg7nyt.cn
dn: uid=neo,ou=People,dc=bg7nyt,dc=cn
objectClass: inetOrgPerson
objectClass: posixAccount
homeDirectory: /dev/null
loginShell: /bin/false
cn: neo
givenName: neo
sn: neo
uid: neo
uidNumber: 500
gidNumber: 500

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

2. Volumes

- 卷管理 [Volumes]

  我这里是使用VMware做的试验,在VMware中增加一些硬盘即可.

  a. Volumes -> Physical Storage Mgmt.

Physical Storage Management

Edit Disk	Type	Description	Size	Label type	Partitions
/dev/sda	SCSI	VMware, VMware Virtual S	8.00 GB	msdos	3 (view)
/dev/sdb	SCSI	VMware, VMware Virtual S	8.00 GB	gpt	0 (view)
/dev/sdc	SCSI	VMware, VMware Virtual S	8.00 GB	gpt	0 (view)
/dev/sdd	SCSI	VMware, VMware Virtual S	8.00 GB	gpt	0 (view)

```
Edit Disk Type Description Size Label type Partitions
/dev/sda SCSI VMware, VMware Virtual S 8.00 GB msdos 3 (view)
/dev/sdb SCSI VMware, VMware Virtual S 8.00 GB gpt 0 (view)
/dev/sdc SCSI VMware, VMware Virtual S 8.00 GB gpt 0 (view)
/dev/sdd SCSI VMware, VMware Virtual S 8.00 GB gpt 0 (view)
...
```

openfiler安装在/dev/sda,/dev/sda硬盘空间不用太大,单独给openfiler使用.建议做RAID 1(硬件RAID卡或服务器主版提供的RAID)

其它硬盘是用于存储的硬盘,如果有条件这些硬盘组也最好做成硬RAID,没有条件我们可以在openfiler中做软件RAID.

点击"Edit Disk"列表内硬盘标签,之后可以看到"Create a partition in /dev/sdb"

Create a partition in /dev/sdb

You can use ranges within the following extents:

Mode	Starting cylinder	Ending cylinder	Space
Primary	1	1044	8.00 GB

Mode	Partition Type	Starting cylinder	Ending cylinder	Size	Create	Reset
Primary	Physical volume	1	1044	8 GB	Create	Reset

```
Mode: Primary
Partition Type: [Physical volume] / [RAID array member]
Starting cylinder: 1
Ending cylinder Size: 1044
Size: 自动产生
```

单击"Create"创建分区

Edit partitions in /dev/sdb (1044 cylinders with "gpt" label)

Device	Type	Number	Start cyl	End cyl	Blocks	Size	Type	Delete
/dev/sdb1	Linux Physical Volume (0x8e)	1	1	1044	8384495	8.00 GB	Primary	Delete

Back to the list of physical storage devices

Back to the list of physical storage devices

如果没有特别需求,不需要创建多个分区.

```
Edit partitions in /dev/sdb (1044 cylinders with "gpt" label)

Device Type Number Start cyl End cyl Blocks Size Type Delete
/dev/sdb1 Linux Physical Volume (0x8e) 1 1 10 78831 76.98 MB Primary Delete
/dev/sdb2 Linux Physical Volume (0x8e) 2 10 100 721920 705.00 MB Primary Delete
/dev/sdb3 Linux Physical Volume (0x8e) 3 100 200 801792 783.00 MB Primary Delete
/dev/sdb4 Linux Physical Volume (0x8e) 4 200 300 802816 784.00 MB Primary Delete
/dev/sdb5 Linux Physical Volume (0x8e) 5 300 400 801792 783.00 MB Primary Delete
```

b. Volumes->Volume Group Mgmt.

Volume Group 可以实现动态扩展空间,注意如果在使用中有一个成员盘损坏,你将无法恢复数据.

应急使用可以,不建议长期使用.

Create a new volume group

Volume group name		
vg0		
Select physical volumes to add		
☑	/dev/sdb1	8.00 GB
☑	/dev/sdc1	8.00 GB
☐	/dev/sdd1	8.00 GB

Add volume group

```
Volume group name: vg0
Select physical volumes to add: 在列表前面打勾
/dev/sdb1 8.00 GB
/dev/sdc1 8.00 GB
```

单击"Add volume group"创建vg0

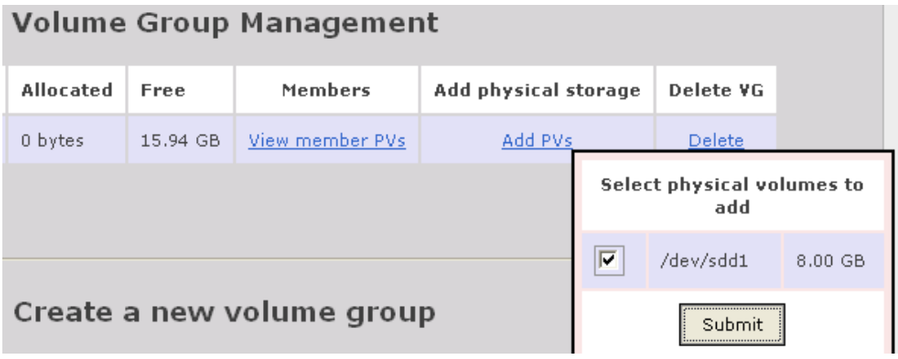
Volume Group Management

Volume Group Name	Size	Allocated	Free	Members	Add physical storage	Delete VG
vg0	15.94 GB	0 bytes	15.94 GB	View member PVs	Add PVs	Delete

表 58.1. Volume Group Management

Volume Group Name	Size	Allocated	Free	Members	Add physical storage	Delete VG
vg0	15.94 GB	0 bytes	15.94 GB	View member	PVs Add	PVs Delete

扩展Volume Group单击[PVs Add]按钮

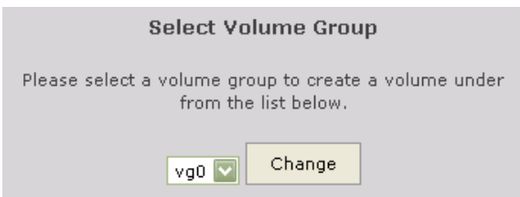


分区列表前面打勾

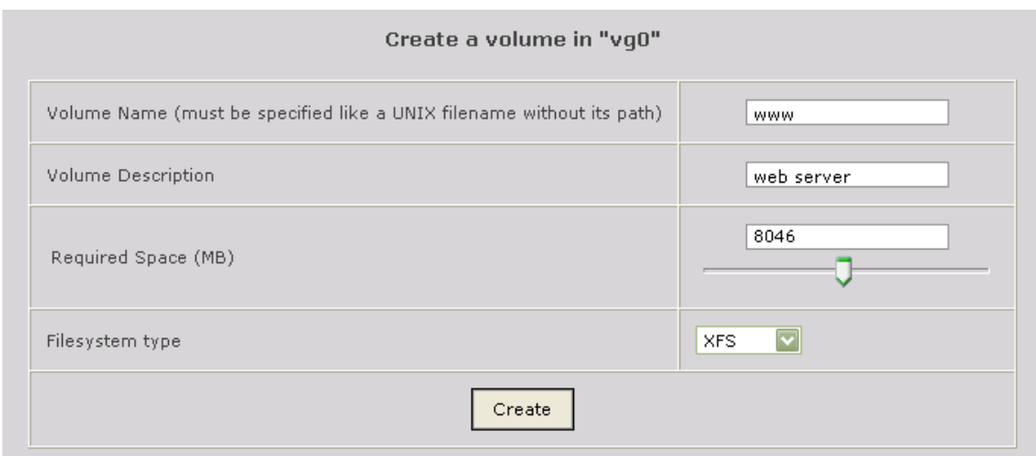
[Submit]提交

c. Volumes -> Create New Volume

选择VG



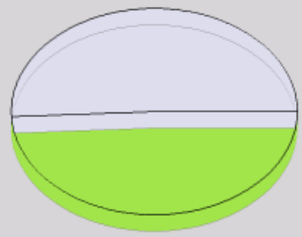
创建卷




```
Volume Name: 卷名
Volume Description: 描述
Required Space (MB): 配额
Filesystem type: 文件系统
```

单击[Create]按钮

Volumes in volume group "vg0" (16320 MB)



Legend	Volume name	Volume description	Volume size	File system type	File system size	FS used space	FS free space	Delete	Properties	Snapshots
	www	web server	8064 MB	XFS	7.9G	296K	7.9G	Delete	Edit	Create
	0 MB allocated to snapshots									
	8256 MB of free space left									

2.1. RAID

Openfiler提供软RAID.

1. Volumes -> Physical Storage Mgmt.

Physical Storage Management

Edit Disk	Type	Description	Size	Label type	Partitions
/dev/sda	SCSI	VMware, VMware Virtual S	8.00 GB	msdos	3 (view)
/dev/sdb	SCSI	VMware, VMware Virtual S	8.00 GB	gpt	0 (view)
/dev/sdc	SCSI	VMware, VMware Virtual S	8.00 GB	gpt	0 (view)
/dev/sdd	SCSI	VMware, VMware Virtual S	8.00 GB	gpt	0 (view)

点击"Edit Disk"列表内硬盘标签,之后可以看到"Create a partition in /dev/sdb"

Create a partition in /dev/sdb

You can use ranges within the following extents:

Mode	Starting cylinder	Ending cylinder	Space
Primary	1	1044	8.00 GB

Mode	Partition Type	Starting cylinder	Ending cylinder	Size	Create	Reset
Primary	RAID array member	1	1044	8 GB	Create	Reset

单击[Create]按钮创建RAID组成员

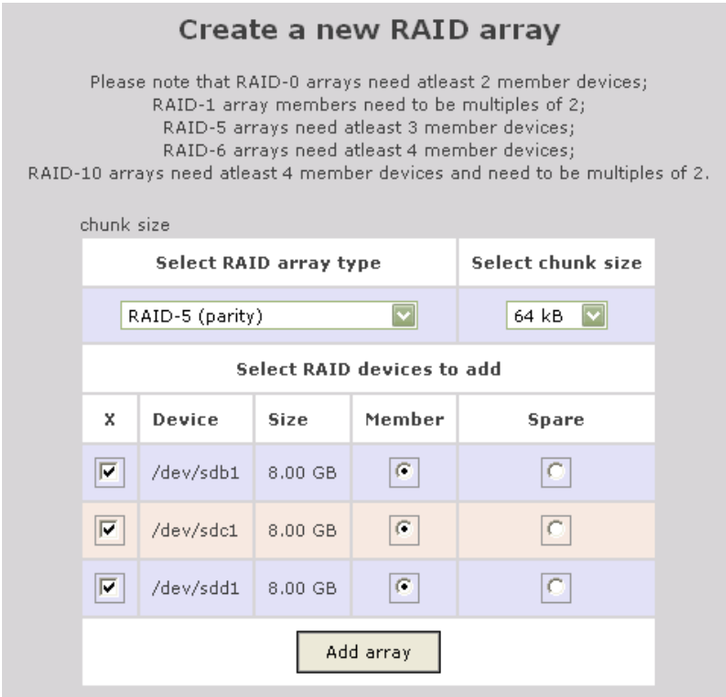
Edit partitions in /dev/sdb (1044 cylinders with "gpt" label)

Device	Type	Number	Start cyl	End cyl	Blocks	Size	Type	Delete
/dev/sdb1	Linux RAID Array Member (0xfd)	1	1	1044	8384495	8.00 GB	Primary	Delete

Back to the list of physical storage devices

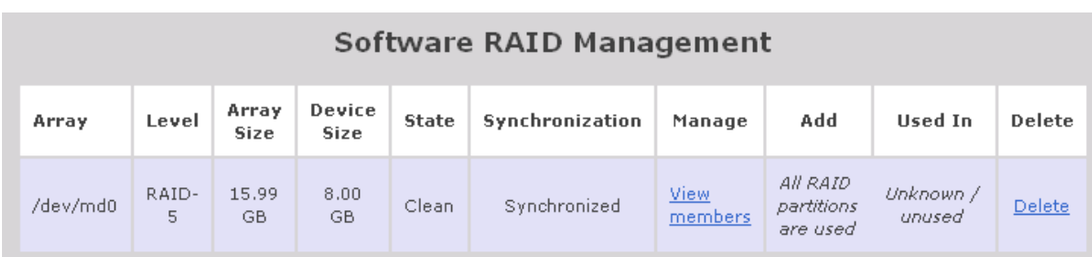
单击[Back to the list of physical storage devices]返回到 "Physical Storage Management"

2. Volumes -> Software RAID Mgmt.




```
Select RAID array type: RAID(0,1,5,6,10)
Select chunk size: 这可以针对你的需求做优化
Select RAID devices to add: 打勾选择
```

单击[Add array]创建RAID



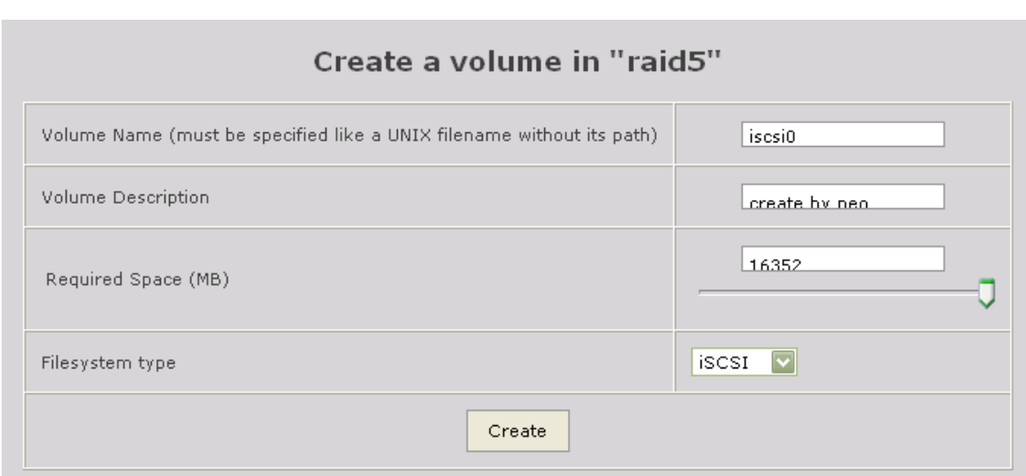
RAID创建完成后,就可以卷组和卷

Volumes -> Volume Group Mgmt. -> Create New Volume

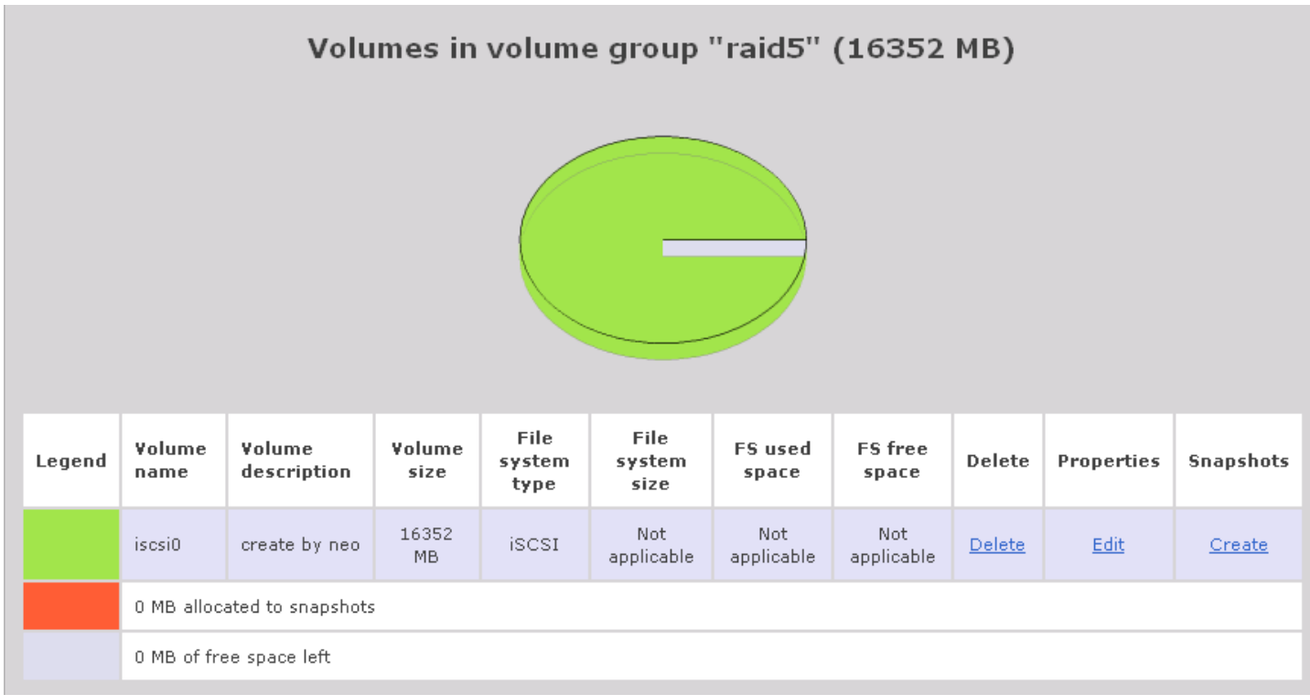
RAID 6 采用双校验盘最少4块硬盘

2.2. iSCSI

Volumes -> Create New Volume



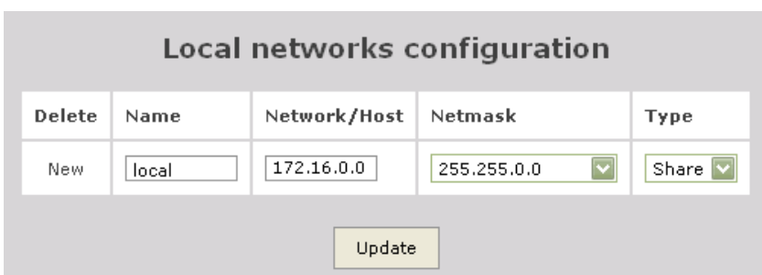
单击[Create]按钮



单击[Update]按钮

Services -> Enable/Disable -> iSCSI target 确认已经 Enable

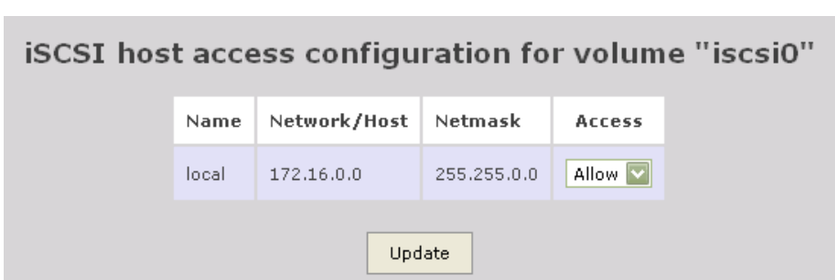
General -> Local Networks



单击[Update]按钮

Volumes -> List of Existing Volumes -> Select Volume Group

单击 iScsi 卷列表 Properties 下的 [Edit] 连接



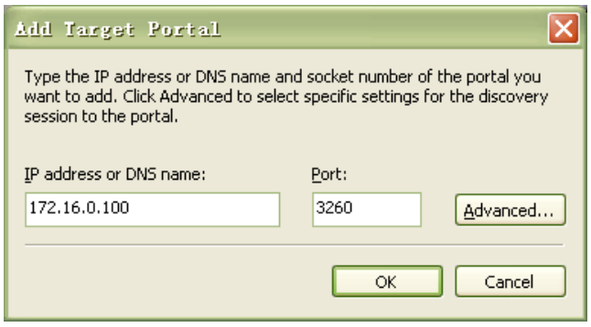
默认是:Deny, 修为Allow

2.2.1. Microsoft iSCSI Software Initiator

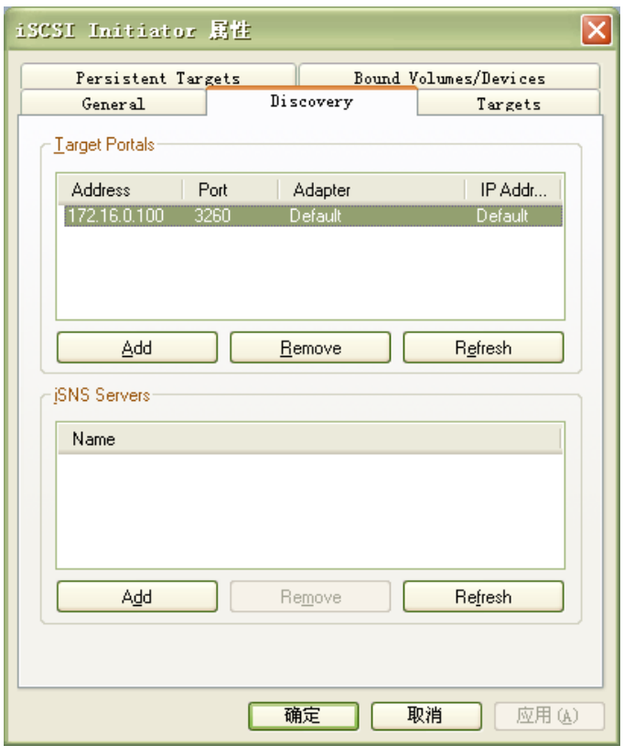
开始菜单 找到 Microsoft iSCSI Initiator 并运行

单击 Discovery 选项卡

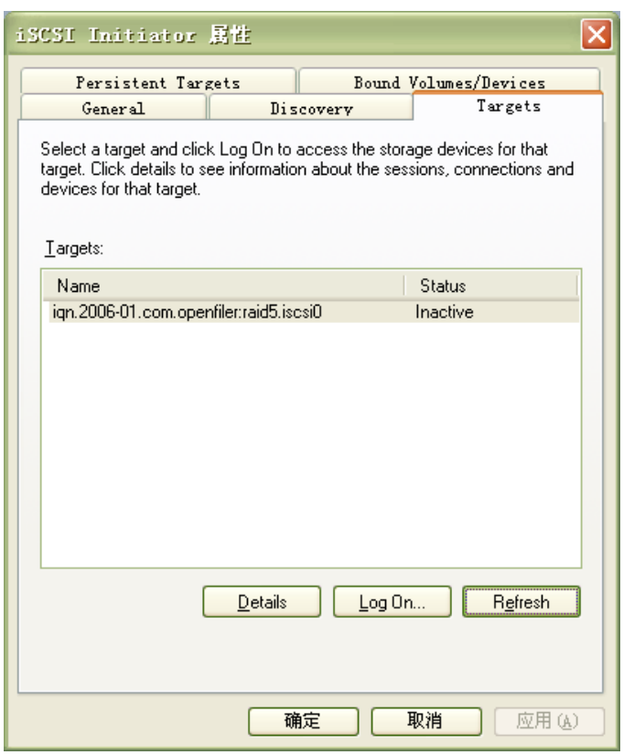
单击 [Add] 按钮



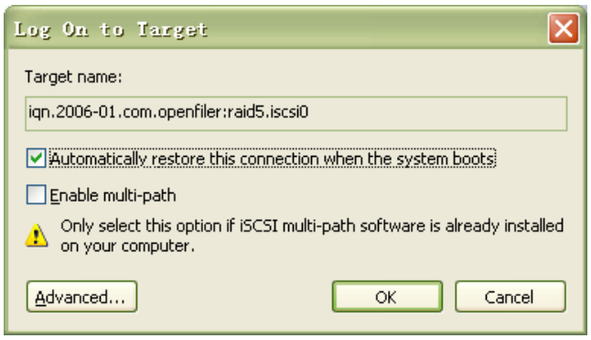
单击 [OK] 按钮



单击 Targets 选项卡



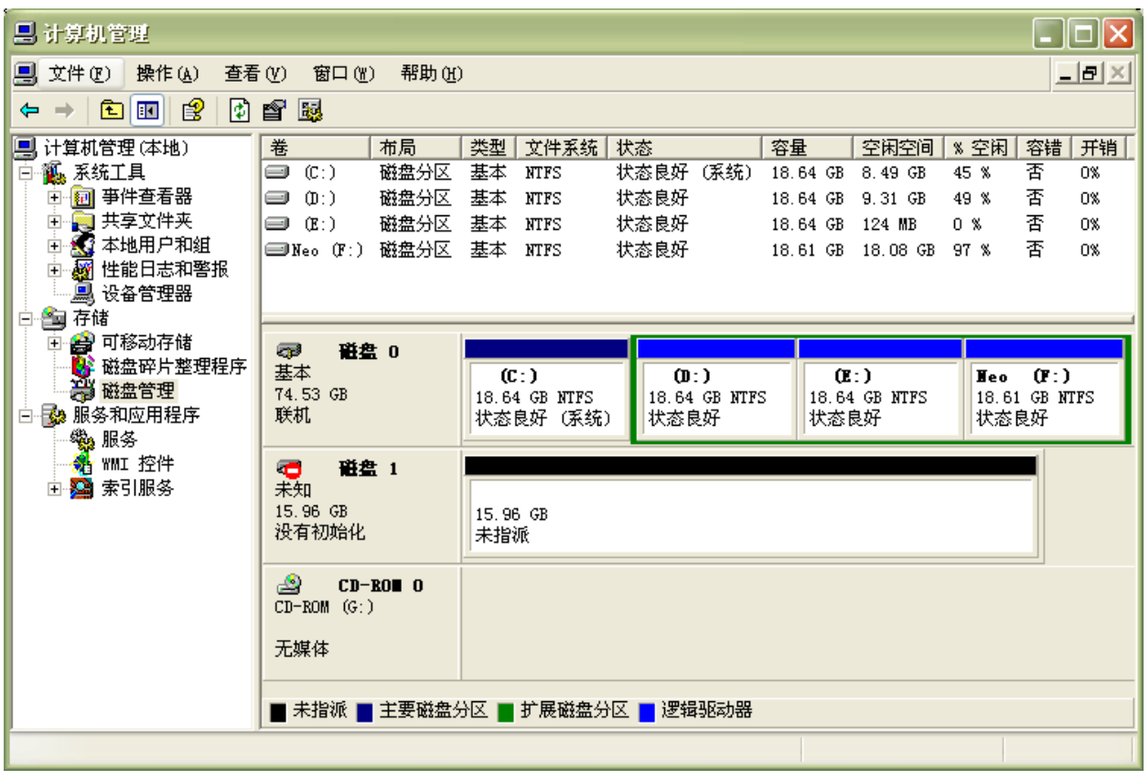
单击 [Refresh] 按钮 -> [Log On...]



单击 [OK] 按钮

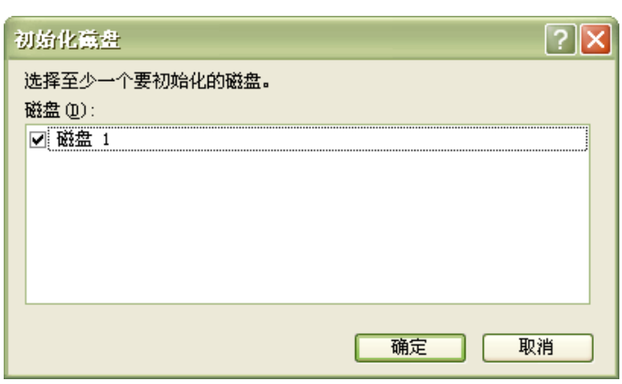
完成Initiator设置

我的电脑 -> 单击鼠标右键 -> 管理



初始化硬盘

选择硬盘



初始化完成，红色图标消失后你就可以对磁盘分区，挂载卷，格式化。

使用 iSCSI 与使用本地磁盘完全一样。

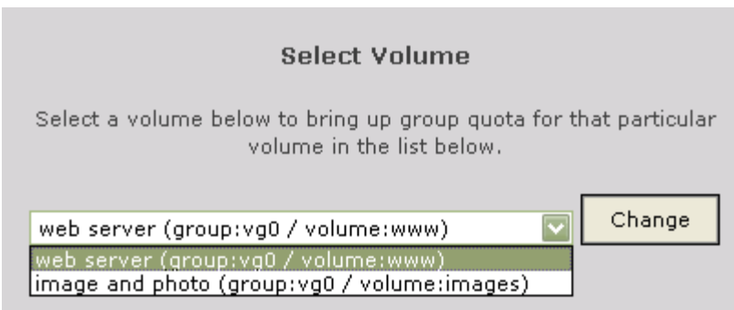
Status -> iSCSI

3. Quota

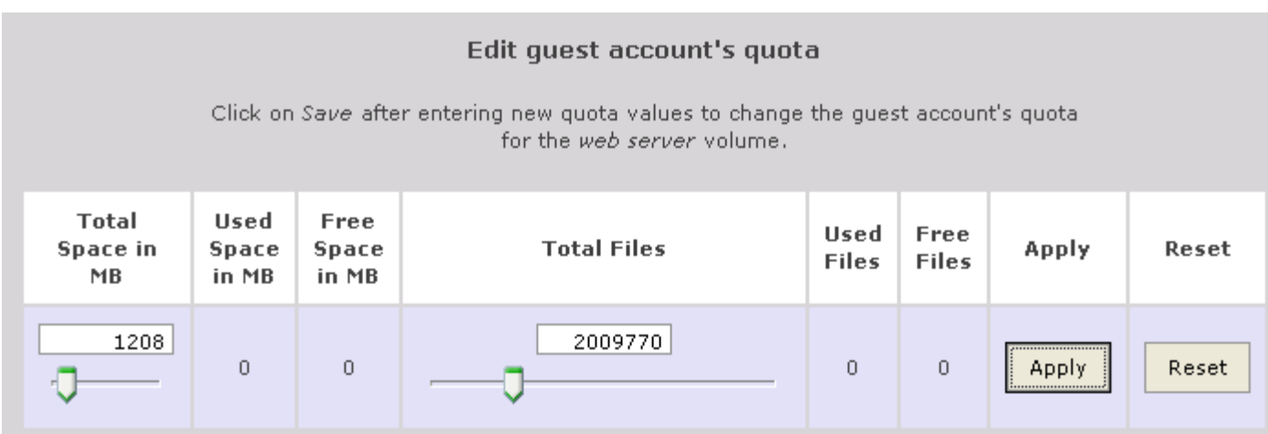
- 注意

有些文件系统不支持Quota

a. Quota -> Guest Quota



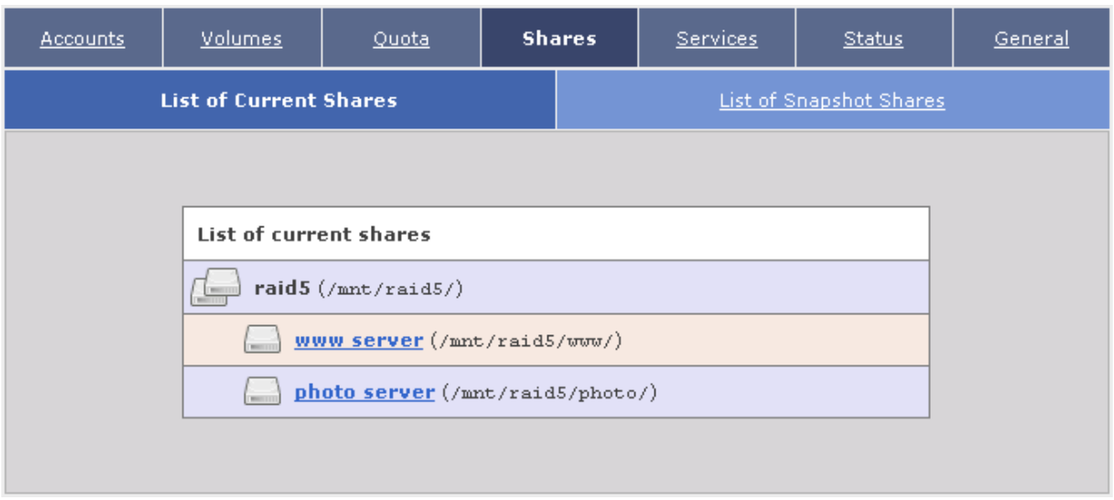
单击[Change]按钮



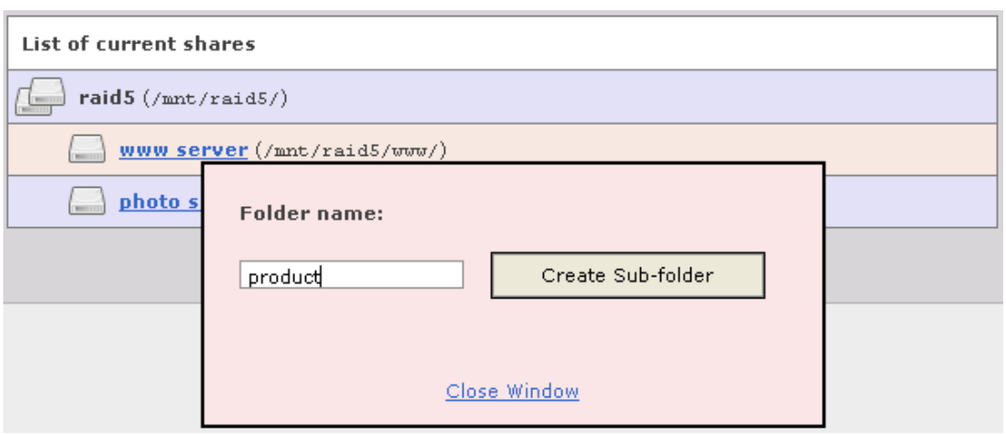
单击[Apply]按钮

4. Shares

- Shares

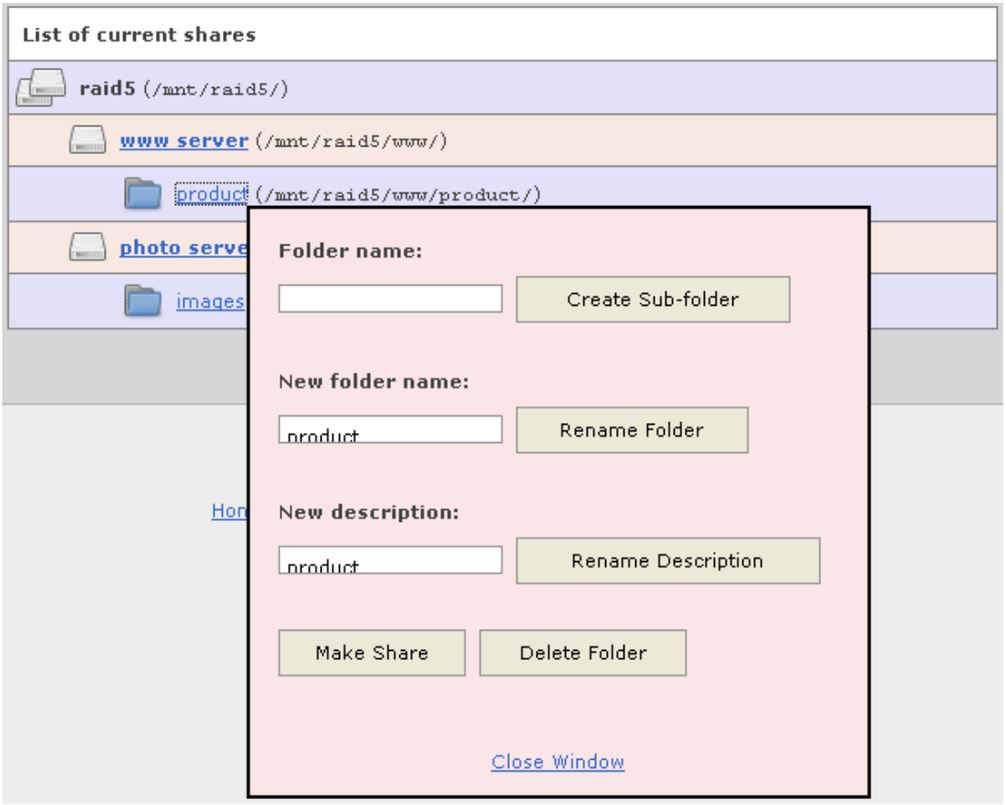


单击列表内的连接.

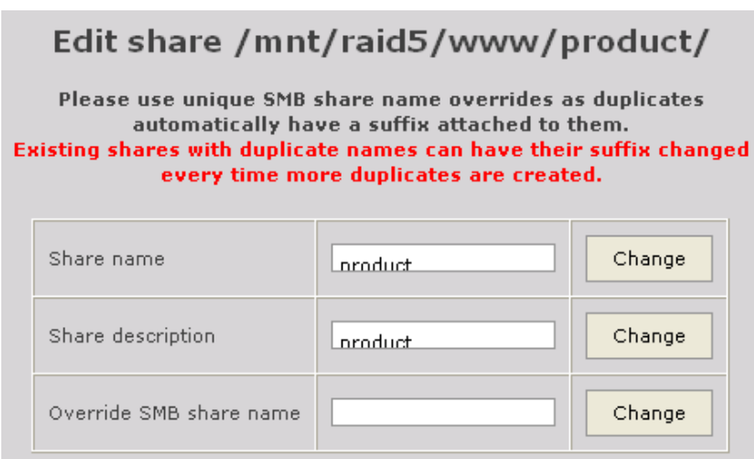



```
Folder name: 输入文件夹名
```

单击 [Create Sub-folder] 按钮 创建文件夹

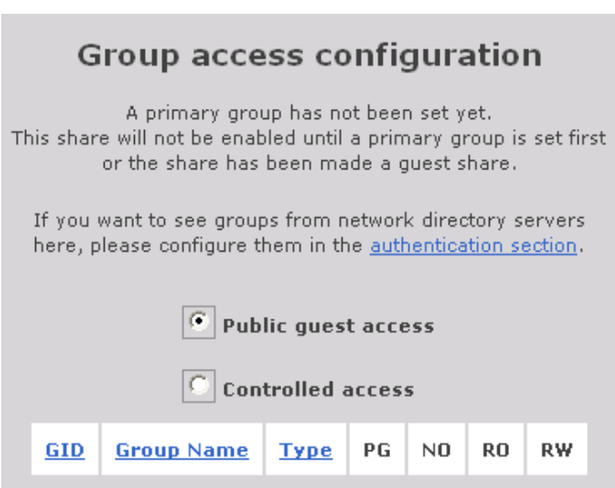



```
Share name: 输入共享名
Share description: 描述
Override SMB share name:
```



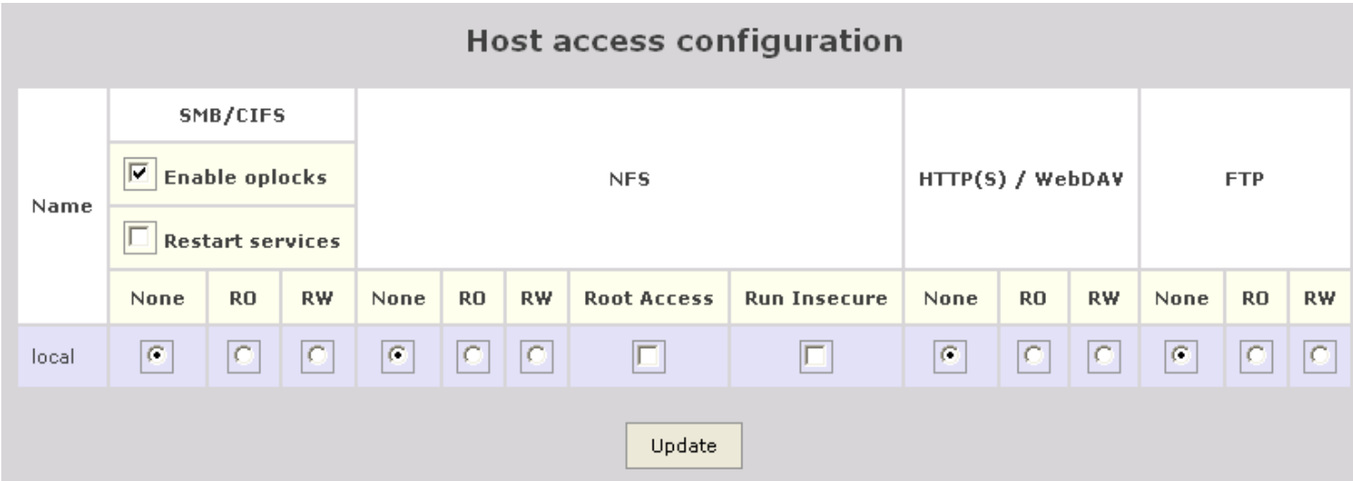
单击[Change]按钮 修改

组的权限制



单击[Update]按钮

主机访问权限配置


Host access configuration
Name
SMB/CIFS
Enable oplocks
Restart services
NFS
HTTP(S) / WebDAV
FTP
None
RO
RW
None
RO
RW
Root Access
Run Insecure
None
RO
RW
None
RO
RW
local
Update

单击[Update]按钮

第 59 章 Backup / Restore

目录

1. 备份策略

1.1. Incremental backup

1.2. Differential backup

2. Bacula, the Open Source, Enterprise ready, Network Backup Tool for Linux, Unix, Mac and Windows.

http://www.bacula.org/

ubuntu 10.10

```
neo@backup:~$ apt-cache search bacula
bacula - network backup, recovery and verification - meta-package
bacula-client - network backup, recovery and verification - client meta-package
bacula-common - network backup, recovery and verification - common support files
bacula-common-mysql - network backup, recovery and verification - MySQL common files
bacula-common-pgsql - network backup, recovery and verification - PostgreSQL common files
bacula-common-sqlite3 - network backup, recovery and verification - SQLite v3 common files
bacula-console - network backup, recovery and verification - text console
bacula-director-common - network backup, recovery and verification - Director common files
bacula-director-mysql - network backup, recovery and verification - MySQL storage for Director
bacula-director-pgsql - network backup, recovery and verification - PostgreSQL storage for
Director
bacula-director-sqlite3 - network backup, recovery and verification - SQLite 3 storage for
Director
bacula-fd - network backup, recovery and verification - file daemon
bacula-sd - network backup, recovery and verification - storage daemon
bacula-sd-mysql - network backup, recovery and verification - MySQL SD tools
bacula-sd-pgsql - network backup, recovery and verification - PostgreSQL SD tools
bacula-sd-sqlite3 - network backup, recovery and verification - SQLite 3 SD tools
bacula-server - network backup, recovery and verification - server meta-package
bacula-console-qt - Bacula Administration Tool Console
bacula-director-sqlite - network backup, recovery and verification - SQLite 2 director
transition
bacula-doc - Documentation for Bacula
bacula-sd-sqlite - network backup, recovery and verification - SQLite SD tools
bacula-traymonitor - network backup, recovery and verification - tray monitor
```

2.1. Install Backup Server

过程 59.1.

1. 安装bacula服务器

```
$ sudo apt-get install bacula
```

启动脚本.

```
neo@backup:/etc/bacula$ ls -1 /etc/init.d/bacula-*
/etc/init.d/bacula-director
/etc/init.d/bacula-fd
/etc/init.d/bacula-sd
```

Bacula Config files

```
neo@backup:~$ ls -1 /etc/bacula/
bacula-dir.conf
bacula-fd.conf
bacula-sd.conf
bconsole.conf
common_default_passwords
```

```
scripts
```

Checking Bacula Daemons Status

```
neo@backup:~$ ps auwx | grep bacula
bacula   25044  0.0  0.1  72624  2092 ?        Ssl  14:55   0:00 /usr/sbin/bacula-sd -c
/etc/bacula/bacula-sd.conf -u bacula -g tape
root     25659  0.0  0.0  60068  1376 ?        Ssl  14:56   0:00 /usr/sbin/bacula-fd -c
/etc/bacula/bacula-fd.conf
bacula   29551  0.0  0.1  87672  3096 ?        Ssl  15:48   0:00 /usr/sbin/bacula-dir -c
/etc/bacula/bacula-dir.conf -u bacula -g bacula
neo      30344  0.0  0.0   7748   876 pts/0    S+   15:57   0:00 grep --color=auto bacula
```

2. bconsole

```
neo@backup:/etc/bacula$ sudo bconsole
Connecting to Director localhost:9101
1000 OK: backup.xiu.com-dir Version: 5.0.2 (28 April 2010)
Enter a period to cancel a command.
*help
  Command       Description
  =======       ===========
  add           Add media to a pool
  autodisplay   Autodisplay console messages
  automount     Automount after label
  cancel        Cancel a job
  create        Create DB Pool from resource
  delete        Delete volume, pool or job
  disable       Disable a job
  enable        Enable a job
  estimate      Performs FileSet estimate, listing gives full listing
  exit          Terminate Bconsole session
  gui           Non-interactive gui mode
  help          Print help on specific command
  label         Label a tape
  list          List objects from catalog
  llist         Full or long list like list command
  messages      Display pending messages
  memory        Print current memory usage
  mount         Mount storage
  prune         Prune expired records from catalog
  purge         Purge records from catalog
  python        Python control commands
  quit          Terminate Bconsole session
  query         Query catalog
  restore       Restore files
  relabel       Relabel a tape
  release       Release storage
  reload        Reload conf file
  run           Run a job
  status        Report status
  setdebug      Sets debug level
  setip         Sets new client address -- if authorized
  show          Show resource records
  sqlquery      Use SQL to query catalog
  time          Print current time
  trace         Turn on/off trace to file
  unmount       Unmount storage
  umount        Umount - for old-time Unix guys, see unmount
  update        Update volume, pool or stats
  use           Use catalog xxx
  var           Does variable expansion
  version       Print Director version
  wait          Wait until no jobs are running

When at a prompt, entering a period cancels the command.

*
```

3. 修改配置文件，增加备份策略.

备份配置文件，以免把文件改坏。

```
root@backup:~# cd /etc/bacula/
root@backup:/etc/bacula# mkdir original
root@backup:/etc/bacula# cp *.conf original/
root@backup:/etc/bacula#
```

bacula-dir.conf

```
root@backup:/etc/bacula# vim bacula-dir.conf
Job {
  Name = "BackupClient2"
  Client = web-fd
```

```
  JobDefs = "DefaultJob"
}
```

2.2. Install Backup Client

- ```
  neo@web:~$ sudo apt-get install bacula-client
  ```
  ```

3. Amanda: Open Source Backup

http://www.amanda.org/

Amanda is the most popular open source backup and recovery software in the world. Amanda protects more than half a million of servers and desktops running various versions of Linux, UNIX, BSD, Mac OS-X and Microsoft Windows operating systems worldwide.

4. Opendedup

http://www.opendedup.org/

部分 V. Monitoring

目录

第 60 章 System Infomation

目录

1. Cpu Bit

```
neo@netkiller:~$ uname -a
Linux netkiller 2.6.28-15-server #52-Ubuntu SMP Wed Sep 9 11:34:09 UTC 2009 x86_64 GNU/Linux

neo@netkiller:~$ getconf LONG_BIT
64
```

第 61 章 shutdown

```
shutdown -h now
shutdown -h 10:00        10点关机
shutdown -h +10          10mins后关机
shutdown -r now          reboot at once
shutdown -r +30          'System will reboot in 30mins'
shutdown -k              'System will reboot'
```

第 62 章 Profile

目录

1. shell

```
$ chsh /bin/bash
```

第 63 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. 案例

2.6.1. 监控80端口与icmp,arp

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

2.6.2. 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.=" $_";
  }
}'
```

2.6.3. HTTP 包

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

2.6.4. 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

4. Unicornscan，Zenmap，nast

上一页 上一级 下一页

3. nc - TCP/IP swiss army knife

起始页

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

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 64 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 65 章 Network Management Software & Network Monitoring

目录

1. Webmin

网站

http://www.webmin.com/

过程 65.1. 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
```

上一页 上一级 下一页

2. OpenVAS 起始页 2. Mrtg

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 65.1. 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 65.2. 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
```

上一页 上一级 下一页

2. Mrtg 起始页 4. Nagios

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

  ┌──────────────────────────────────────────┤ BandwidthD
├─────────────────────────────────────────┐
  │ Bandwidthd needs to know which interface it should listen for traffic on. Only a single
  │ interface can be specified. If you want to listen on all interfaces you should specify the
  │ metainterface "any". Running "bandwidthd -l" will list available interfaces.
  │
  │ Interface to listen on:
  │
  │                                                any
  │                                                lo
  │                                                eth0
  │                                                eth1
  │                                                tun0
  │
  │
  │                                               <Ok>
  │
└──────────────────────────────────────────────────────────────────────────────────────────────┘

 ┌──────────────────────────────────────────┤ BandwidthD
├─────────────────────────────────────────┐
 │ Bandwidthd can create graphs for one or several ip-subnets. Subnets are specified either in
 │ dotted-quad format (192.168.0.0 255.255.0.0) or in CIDR format (192.168.0.0/16) and
 │ separated by a comma. Example: 192.168.0.0/16, 10.0.0.0 255.0.0.0, 172.16.1.0/24. If you
 │ don't know what to specify then you can use 0.0.0.0/0 but it is strongly discouraged.
 │
 │ Subnets to log details about:
 │
 │ 10.8.0.2/32, 172.16.2.0/24, 10.8.0.0/24, 172.16.1.0/24_____________________________________
 │
 │                                               <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 ]
```

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 66 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 67 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 68 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  ]
```

上一页 上一级 下一页

2. AT Commands 起始页 2. freeipmi

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 69 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 69.1. 安装步骤

1. netams netams-web

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

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

2. NeTAMS administrator password

```
┌──────────────────────┤ Configuring netams ├──────────────────────┐
│ Please enter password for "admin" user in NeTAMS database.        │
│                                                                   │
│ NeTAMS administrator password:                                    │
│                                                                   │
│ *******_____________________________________________________      │
│                                                                   │
│                            <Ok>                                   │
└───────────────────────────────────────────────────────────────────┘

┌────────────┤ Configuring netams ├────────────┐
│                                               │
│ Repeat password for NeTAMS user "admin":      │
│                                               │
│ *******_____________________________________  │
│                                               │
│                   <Ok>                        │
└───────────────────────────────────────────────┘
```

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 70 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
```

部分 VI. Cluster

Load Balancing / HA

目录

第 71 章 Linux Virtual Server

目录

Session

当选用持久服务（-p选项）支持HTTP session时，来自同一IP地址的请求将被送到同一台服务器。所以在这种状况下，一个ab生成的请求都会被调度到一台服务器，达不到性能测试的目的。在真实系统使用中，持久服务时间一般设置好几个小时。 当ldirectord监测到并且在列表中删除一台应用服务器时，之前有建立连接的,继续转发到这台机上，确实是这样。因为IPVS并不立即淘汰刚删除的服务器，考虑到服务器太忙被删除，可能很快会被加回来。如果你需要马上淘汰已删除服务器的连接，可以用 echo 1 > /proc/sys/net/ipv4/vs/expire_nodest_conn 不用担心记录连接所消耗的内存，因为一个连接只占用128个字节，所以512M可用内存可以支持四百万条连接数。 可以考虑用分布式的测试工具，或者多台机器一起跑ab。

1. 环境配置

ssh

```
neo@ubuntu:~$ sudo apt-get install ssh
```

network

```
neo@ubuntu:~$ sudo ifconfig eth0 172.16.0.250
neo@ubuntu:~$ sudo route add default gw 172.16.0.254
```

install ipvsadm

```
neo@ubuntu:~$ apt-cache search ipvsadm
ipvsadm - Linux Virtual Server support programs
neo@ubuntu:~$ sudo apt-get install ipvsadm
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  heartbeat keepalived ldirectord
The following NEW packages will be installed:
  ipvsadm
0 upgraded, 1 newly installed, 0 to remove and 30 not upgraded.
Need to get 0B/43.9kB of archives.
After unpacking 238kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously deselected package ipvsadm.
(Reading database ... 16572 files and directories currently installed.)
Unpacking ipvsadm (from .../ipvsadm_1.24+1.21-1.1ubuntu3_i386.deb) ...
Setting up ipvsadm (1.24+1.21-1.1ubuntu3) ...

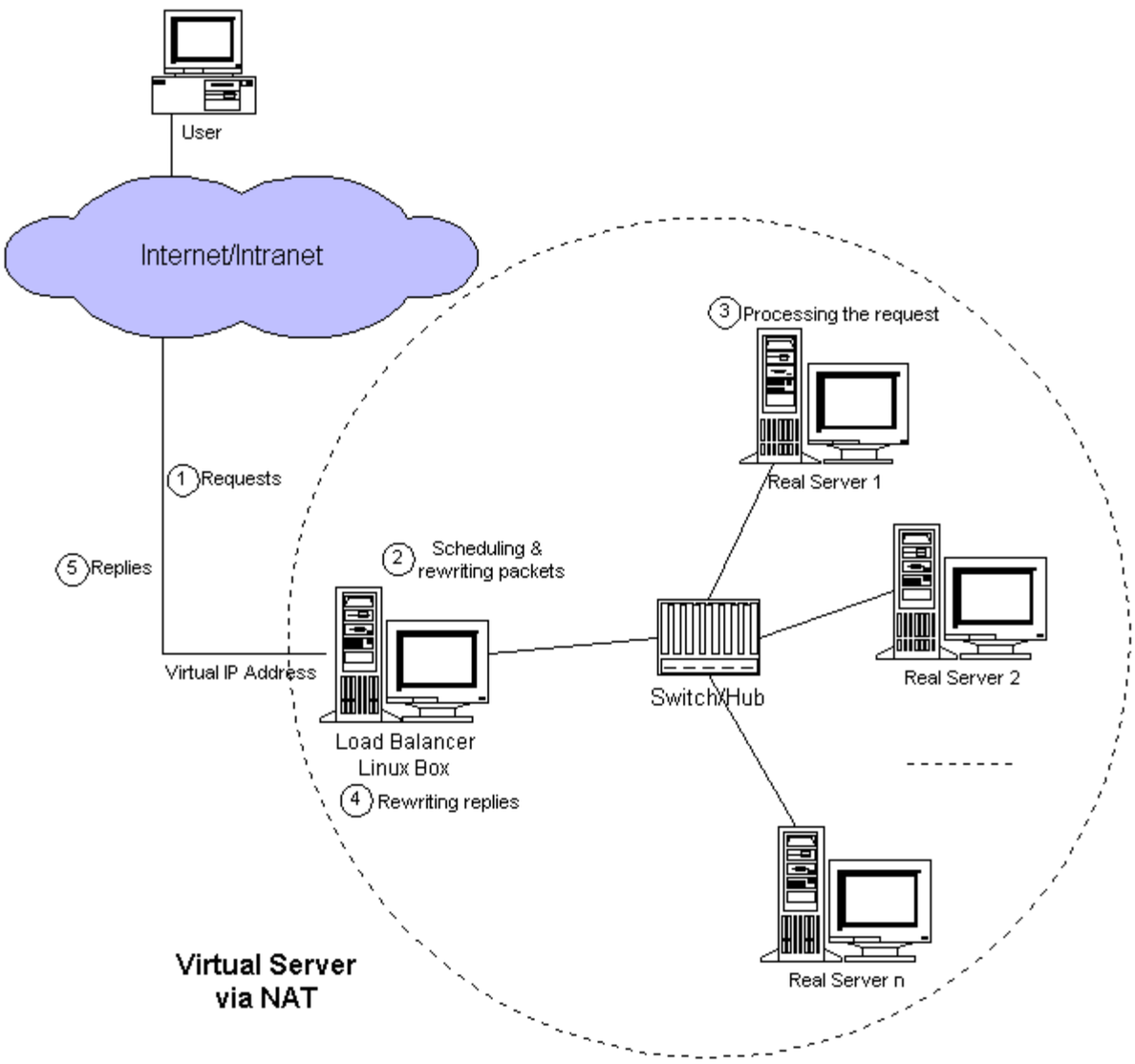
neo@ubuntu:~$
```

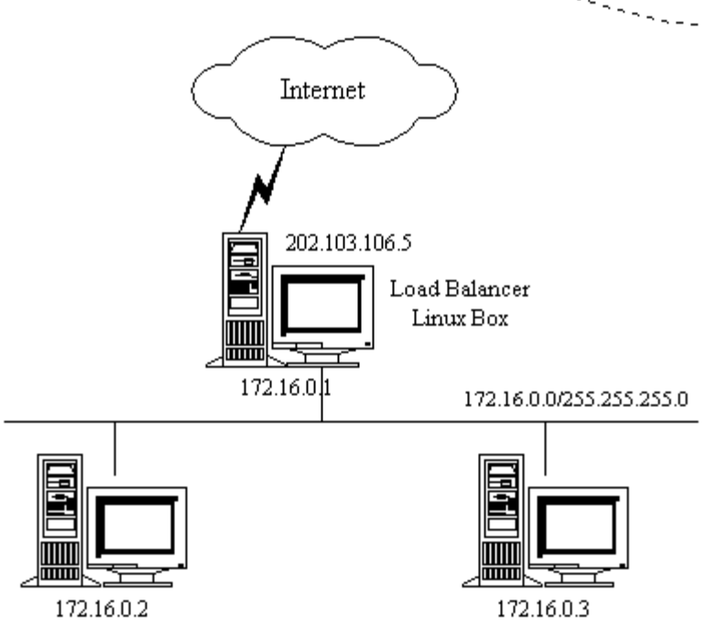
test

```
neo@ubuntu:~$ sudo ipvsadm
IP Virtual Server version 1.2.1 (size=4096)
Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
neo@ubuntu:~$
```

---

2. VS/NAT





ip_forward

```
sysctl -w net.ipv4.ip_forward=1
or
echo 1 > /proc/sys/net/ipv4/ip_forward
or
/etc/sysctl.conf 文件，保证其中有如下一行:
net.ipv4.ip_forward = 1

执行:
sysctl -p
```

iptables

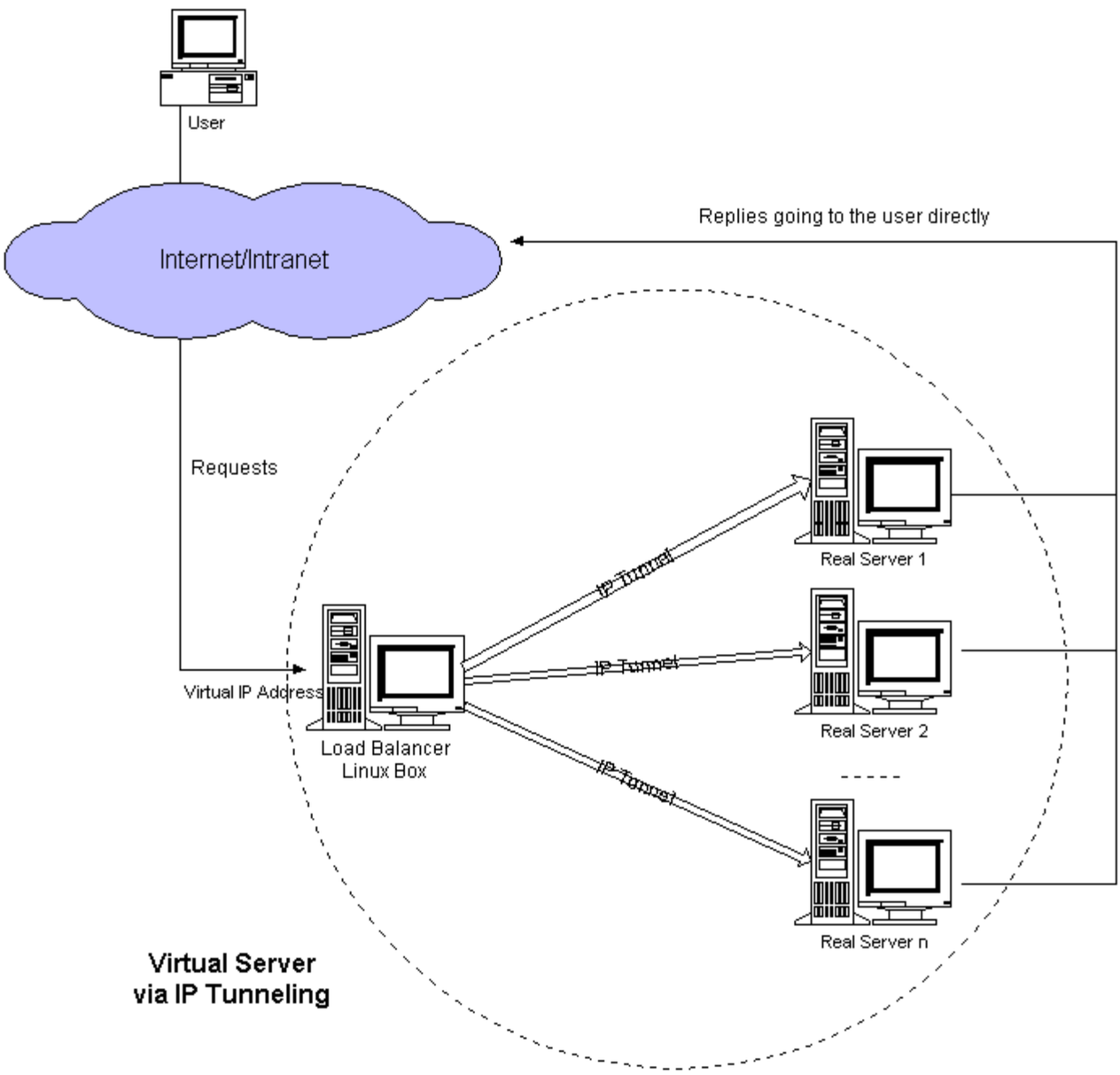
```
sudo iptables -t nat -A POSTROUTING -j MASQUERADE -p tcp -o eth0 -s 172.16.0.0/16 -d 0.0.0.0/0
sudo iptables -t nat -A POSTROUTING -j MASQUERADE -p tcp -o eth1 -s 192.168.1.0/24 -d 0.0.0.0/0
```

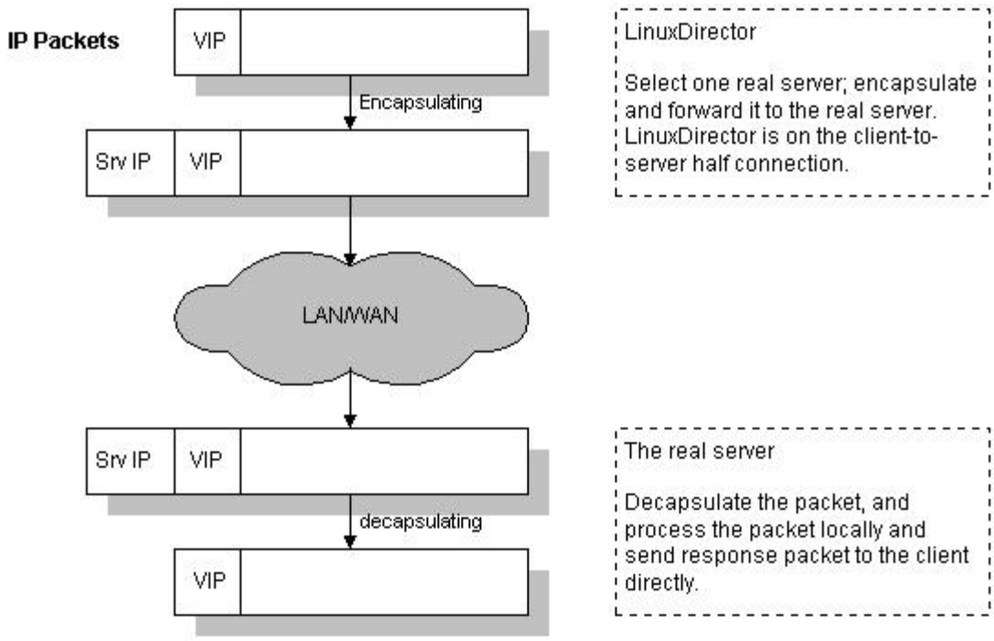
ipvsadm

```
sudo ipvsadm -A -t 172.16.0.1:80 -s wlc
sudo ipvsadm -a -t 172.16.0.1:80 -r 192.168.0.4:80 -m
sudo ipvsadm -a -t 172.16.0.1:80 -r 192.168.0.5:80 -m -w 2
```

---

3. VS/TUN


User
Internet/Intranet
Replies going to the user directly
Requests
Virtual IP Address
Load Balancer
Linux Box
IP Tunnel
IP Tunnel
IP Tunnel
Real Server 1
Real Server 2
Real Server n
Virtual Server
via IP Tunneling



Director

```
ifconfig eth0:0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
```

ifconfig eth0:0 <VIP> netmask 255.255.255.255 broadcast <VIP> up

```
ipvsadm -A -t 172.16.0.1:80 -s wlc
ipvsadm -a -t 172.16.0.1:80 -r 172.16.0.10 -i
ipvsadm -a -t 172.16.0.1:80 -r 172.16.0.20 -i
ipvsadm -a -t 172.16.0.1:80 -r 172.16.0.30 -i
```

ifconfig

```
[root@centos etc]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:15:2B:CF
          inet addr:172.16.0.40  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fe15:2bcf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2340 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2524 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:995068 (971.7 KiB)  TX bytes:327201 (319.5 KiB)
          Interrupt:177 Base address:0x1400

eth0:0    Link encap:Ethernet  HWaddr 00:0C:29:15:2B:CF
          inet addr:172.16.0.1  Bcast:172.16.0.1  Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:177 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2460 (2.4 KiB)  TX bytes:2460 (2.4 KiB)

[root@centos etc]#
```

route

```
[root@centos etc]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
169.254.0.0     *               255.255.0.0     U     0      0        0 eth0
172.16.0.0      *               255.255.0.0     U     0      0        0 eth0
default         172.16.0.254    0.0.0.0         UG    0      0        0 eth0
[root@centos etc]#
```

ipvsadm

```
[root@centos etc]# ipvsadm
IP Virtual Server version 1.2.1 (size=4096)
Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
TCP  172.16.0.1:http wlc
  -> 172.16.0.30:http             Tunnel  1      0          0
  -> 172.16.0.20:http             Tunnel  1      0          0
  -> 172.16.0.10:http             Tunnel  1      0          0
[root@centos etc]#
```

realserver

```
echo 1 > /proc/sys/net/ipv4/ip_forward
modprobe ipip
ifconfig tunl0 0.0.0.0 up
echo 1 > /proc/sys/net/ipv4/conf/all/hidden
echo 1 > /proc/sys/net/ipv4/conf/tunl0/hidden
ifconfig tunl0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
route add -host 172.16.0.1 dev tunl0
```

ubuntu real server

```
neo@backup:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
neo@backup:~$ sudo modprobe ipip
neo@backup:~$ sudo ifconfig tunl0 0.0.0.0 up

neo@backup:~$ sudo ifconfig tunl0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
neo@backup:~$ sudo route add -host 172.16.0.1 dev tunl0
neo@backup:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.16.0.1      *               255.255.255.255 UH    0      0        0 tunl0
localnet        *               255.255.0.0     U     0      0        0 eth0
default         172.16.0.254    0.0.0.0         UG    0      0        0 eth0
neo@backup:~$
```

script

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo modprobe ipip
sudo ifconfig tunl0 0.0.0.0 up
sudo ifconfig tunl0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
```

ifconfig

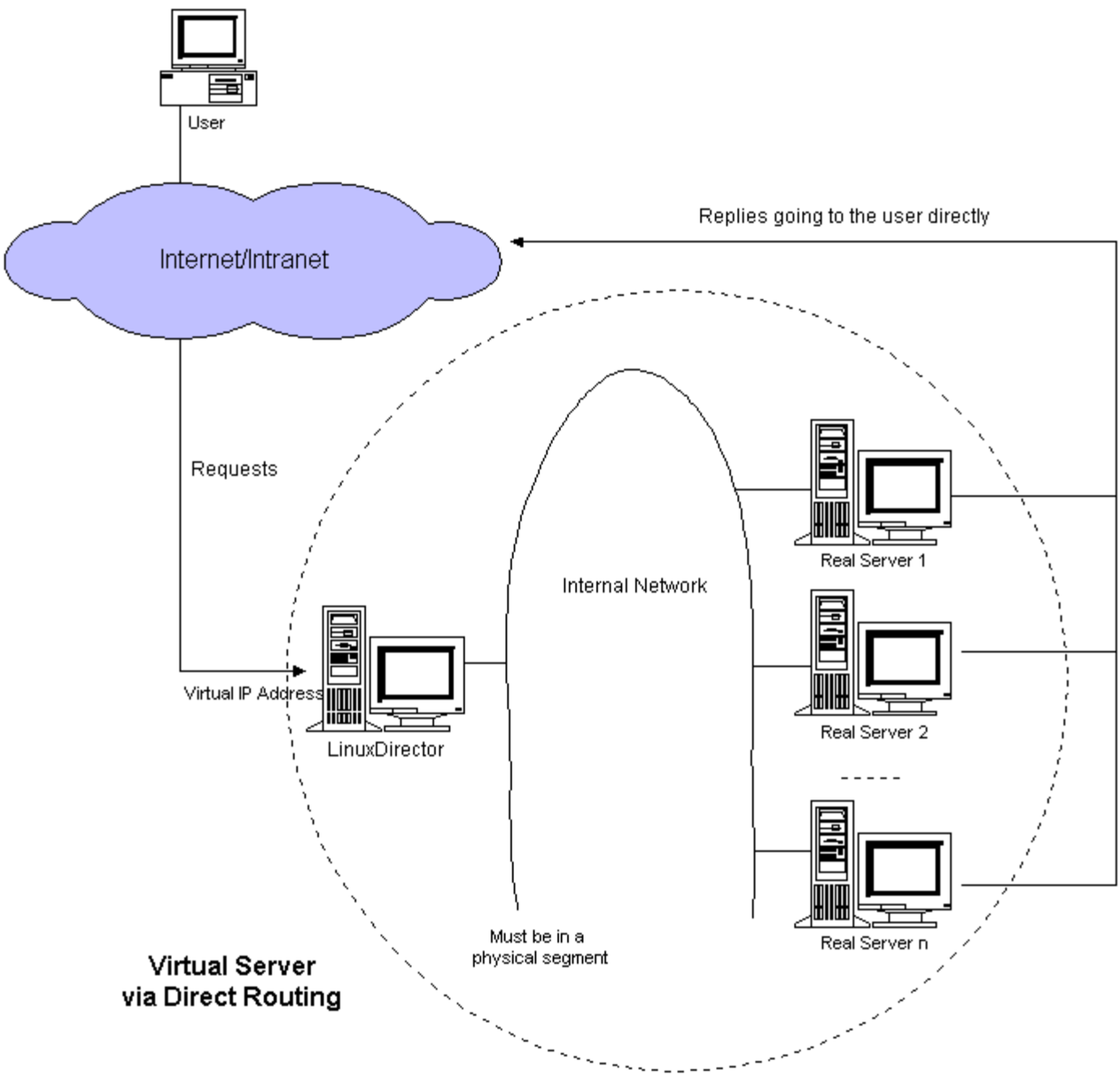
```
neo@master:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:CC:CF:A2
          inet addr:172.16.0.10  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fecc:cfa2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5006 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4692 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2866792 (2.7 MiB)  TX bytes:639042 (624.0 KiB)
          Interrupt:177 Base address:0x1400

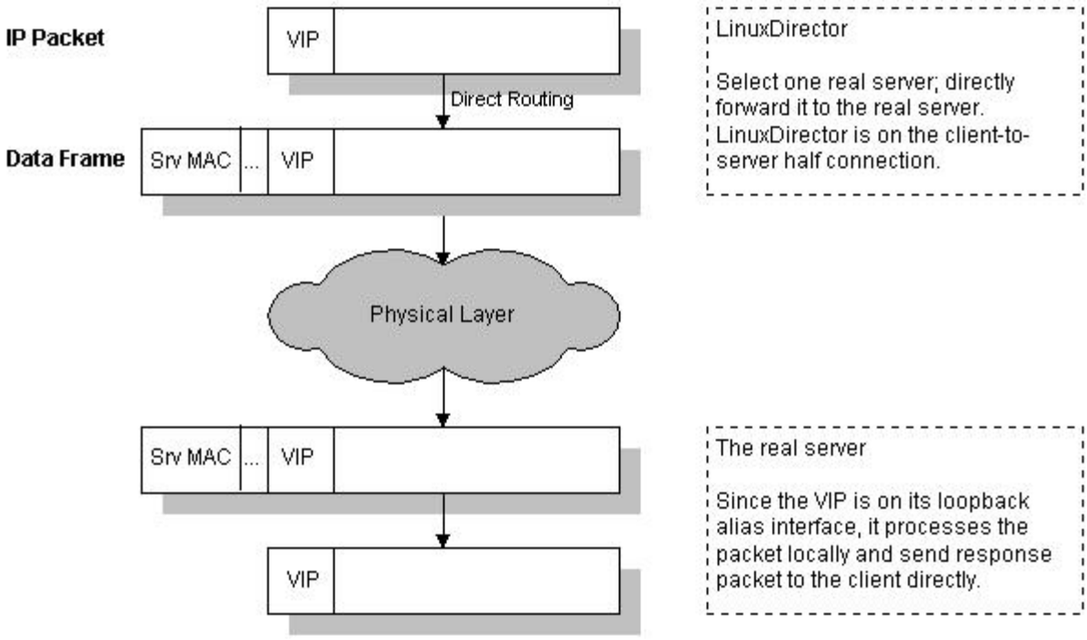
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

tunl0     Link encap:IPIP Tunnel  HWaddr
          inet addr:172.16.0.1  Mask:255.255.255.255
          UP RUNNING NOARP  MTU:1480  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19511 (19.0 KiB)  TX bytes:0 (0.0 b)

neo@master:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
172.16.0.0      *               255.255.0.0     U     0      0        0 eth0
default         172.16.0.254    0.0.0.0         UG    0      0        0 eth0
neo@master:~$
```

4. VS/DR


User
Internet/Intranet
Replies going to the user directly
Requests
Virtual IP Address
LinuxDirector
Internal Network
Real Server 1
Real Server 2
Real Server n
Must be in a
physical segment
Virtual Server
via Direct Routing



VS/DR方式是通过改写请求报文中的MAC地址部分来实现的。

Director和RealServer必需在物理上有一个网卡通过不间断的局域网相连。

Director

VIP:172.16.0.1

```
neo@ubuntu:~$ sudo ifconfig eth0 172.16.0.1/16
or
ifconfig eth0 172.16.0.x netmask 255.255.0.0 broadcast 172.16.0.255 up
ifconfig eth0:0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up

sudo sysctl -w net.ipv4.ip_forward=1
```

ipvsadm

```
#!/bin/bash
ipvsadm -C
ipvsadm -A -t 172.16.0.1:80 -s wlc
ipvsadm -a -t 172.16.0.1:80 -r 172.16.0.10 -g
ipvsadm -a -t 172.16.0.1:80 -r 172.16.0.20 -g
ipvsadm -a -t 172.16.0.1:80 -r 172.16.0.30 -g
```

script

```
ifconfig eth0 172.16.0.x netmask 255.255.0.0 broadcast 172.16.0.255 up
ifconfig eth0:0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
echo 1 > /proc/sys/net/ipv4/ip_forward
```

RealServer

Ubuntn

```
neo@master:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
neo@master:~$ sudo sysctl -w net.ipv4.conf.lo.arp_ignore=1
net.ipv4.conf.lo.arp_ignore = 1
neo@master:~$ sudo sysctl -w net.ipv4.conf.lo.arp_announce=2
net.ipv4.conf.lo.arp_announce = 2
neo@master:~$ sudo sysctl -w net.ipv4.conf.all.arp_ignore=1
net.ipv4.conf.all.arp_ignore = 1
neo@master:~$ sudo sysctl -w net.ipv4.conf.all.arp_announce=2
net.ipv4.conf.all.arp_announce = 2
neo@master:~$
neo@master:~$ sudo ifconfig lo:0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
neo@master:~$ sudo route add -host 172.16.0.1 dev lo:0
```

script

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo sysctl -w net.ipv4.conf.lo.arp_ignore=1
sudo sysctl -w net.ipv4.conf.lo.arp_announce=2
sudo sysctl -w net.ipv4.conf.all.arp_ignore=1
sudo sysctl -w net.ipv4.conf.all.arp_announce=2
sudo ifconfig lo:0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
sudo route add -host 172.16.0.1 dev lo:0
```

redhat

```
echo 1 > /proc/sys/net/ipv4/ip_forward
echo 1 > /proc/sys/net/ipv4/conf/all/hidden
echo 1 > /proc/sys/net/ipv4/conf/lo/hidden
ifconfig lo:0 172.16.0.1 netmask 255.255.255.255 broadcast 172.16.0.1 up
```

test

```
neo@ubuntu:~$ sudo tcpdump -i eth0|grep "172.16.0.1"
```

4.1. 配置文件

4.1.1. Director

ifconfig

```
neo@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:C2:FC:D7
          inet addr:172.16.0.250  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fec2:fcd7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8566 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11544 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:726365 (709.3 KiB)  TX bytes:2638735 (2.5 MiB)
          Interrupt:177 Base address:0x1400

eth0:0    Link encap:Ethernet  HWaddr 00:0C:29:C2:FC:D7
          inet addr:172.16.0.1  Bcast:255.255.255.255  Mask:0.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:177 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

neo@ubuntu:~$
```

ipvsadm

```
neo@ubuntu:~$ sudo ipvsadm
IP Virtual Server version 1.2.1 (size=4096)
Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
TCP  172.16.0.1:www wlc
  -> 172.16.0.20:www              Route   1      0          0
  -> 172.16.0.10:www              Route   1      0          0
neo@ubuntu:~$
```

4.1.2. RealServer

ifconfig

```
neo@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:CC:CF:A2
          inet addr:172.16.0.20  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fecc:cfa2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1897 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1511 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:229334 (223.9 KiB)  TX bytes:205973 (201.1 KiB)
          Interrupt:177 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

lo:0      Link encap:Local Loopback
          inet addr:172.16.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1

neo@ubuntu:~$
```

5. ipvsadm script

save/restore

```
$ ipvsadm-sav > ipvsadm.sav
$ ipvsadm-restore < ipvsadm.sav
```

同步

```
#sync daemon.
ipvsadm --start-daemon=master --mcast-interface=eth1
ipvsadm --start-daemon=backup --mcast-interface=eth1
```

cancel

```
[root@centos etc]# ipvsadm -C
[root@centos etc]# ifconfig eth0:0 down
and
[root@centos etc]# ifconfig lo:0 down
```

6. Timeout

```
# ipvsadm -L --timeout
Timeout (tcp tcpfin udp): 900 120 300
```

7. debug

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

正确的IP包

```
20:39:01.222810 IP 172.16.0.253.4086 > 172.16.0.1.www: S 4092656017:4092656017(0) win 65535 <mss
1460,nop,wscale 2,nop,nop,sackOK>
20:39:01.225684 IP 172.16.0.253.4086 > 172.16.0.1.www: . ack 3272377939 win 64240
20:39:01.225697 IP 172.16.0.1.www > 172.16.0.253.4086: S 3272377938:3272377938(0) ack 4092656018
win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 1>
20:39:01.225726 IP 172.16.0.253.4086 > 172.16.0.1.www: P 1:186(185) ack 1 win 64240
20:39:01.246167 IP 172.16.0.1.www > 172.16.0.253.4086: . ack 186 win 3456
20:39:01.284672 IP 172.16.0.1.www > 172.16.0.253.4086: P 1:524(523) ack 186 win 3456
20:39:01.386049 IP 172.16.0.253.4086 > 172.16.0.1.www: . ack 524 win 64109
```

8. ipvsadm monitor

monitor.py

```
#!/usr/bin/env python

class Ipvs:
    types = ''
    vip = '0.0.0.0'
    vport = '0'
    scheduler = ''
    nodes = []
    """
    def __init__(self, vs):
        self.types = vs[0]
        self.vip = vs[1]
        self.vport = vs[2]
        self.scheduler = vs[3]
        self.nodes = vs[4]
    """
class Node:
    nip     = '0.0.0.0'
    nport   = ''
    forward = ''
    weight = 0
    active = 0
    inact  = 0
    def __init__(self, node):
        nip = node[0]
        nport = node[1]
        forward = node[2]
        weight = node[3]
        active = node[4]
        incat = node[5]
        self.nip     = nip
        self.nport   = nport
        self.forward = forward
        self.weight = weight
        self.active = active
        self.inact  = incat

class Monitor:
    buffer = []
    ipvsdict = {}
    def __init__(self):
        self.buffer.append('<?xml version="1.0"?>')
        self.buffer.append('<?xml-stylesheet type="text/xsl" href="vs.xsl"?>')
        #self.make()
        pass
    def clear(self):
        self.buffer = []
        self.ipvss = []
    def make(self):
        self.buffer.append('<ipvs>')
        for key in self.ipvsdict:
            ipvs = self.ipvsdict[key]
            self.node(ipvs.nodes,ipvs.vip+':'+ipvs.vport+' '+ipvs.scheduler)
        self.buffer.append('</ipvs>')
    def header(self,vs):
        self.buffer.append('<!-- ---------------------------------------- -->')
    def node(self, nodes, caption):
        self.buffer.append('<table>')
        self.buffer.append('<caption>'+caption+'</caption>')
        for node in nodes:
            self.buffer.append('<node>')
            self.buffer.append('<nip>'+node.nip+'</nip>')
            self.buffer.append('<nport>'+node.nport+'</nport>')
            self.buffer.append('<forward>'+node.forward+'</forward>')
            self.buffer.append('<weight>'+node.weight+'</weight>')
            self.buffer.append('<active>'+node.active+'</active>')
            self.buffer.append('<inact>'+node.inact+'</inact>')
            self.buffer.append('</node>')
        self.buffer.append('</table>')
    def display(self):
        for buf in self.buffer:
            print buf
    def saveAs(self,filename):
#       if filename:
        f = open(filename,'w')
        for buf in self.buffer:
            f.write(buf)
        f.close()
```

```
    def save(self):
        self.saveAs('vs.xml')

    def ipvslist(self):
        w,r = os.popen2(IPVSADM)
        w.close()
        version = r.readline()
        vsfield = r.readline()
        nodefield = r.readline()

        pattern_vs = r'(\w+)\s+([0-9.]+):(\w+)\s+(\w+)'
        pattern_node = r'\s->\s([0-9.]+):(\w+)\s+(\w+)\s+(\d+)\s+(\d+)\s+(\d+)'
        cp_vs = re.compile(pattern_vs)
        cp_node = re.compile(pattern_node)

        current_vs = ''
        for line in r.readlines():
            if line[:3] == 'TCP' or line[:3] == 'UDP':
                current_vs = line

                result = cp_vs.search(line).groups()
                ipvs = Ipvs()
                ipvs.types = result[0]
                ipvs.vip = result[1]
                ipvs.vport = result[2]
                ipvs.scheduler = result[3]
                ipvs.nodes = []
                self.ipvsdict[current_vs] = ipvs
            elif line[2:4]== '->':
                result = cp_node.search(line).groups()
                oneNode = Node(result)
                #nodes.append(oneNode)
                self.ipvsdict[current_vs].nodes.append(oneNode)

class Network:
    interface = []
    def __init__(self):
        pass
    def hostname:
        pass

class Ipvsadmin:
    cmdline = ''
    vscache = []
    forward = {'nat':'','route':'','tunel':''}

    def load(self, config):
        pass
    def vip(self, vip, vport, scheduler):
        pass
    def rip(self, vip,rip,rport,forward,weight):
        pass
    def list(self):
        pass
    def saveAs(self):
        pass
    def restore(self):
        pass

class Deploy:
    src = ['vs.xml','vs.xsl']
    dst = ''
    def __init__(self):
        pass
    def target(self, dst):
        self.dst = dst
    def start(self):
        try:
            for srcfile in self.src:
                shutil.copy(srcfile,self.dst)
        except (IOError, os.error), why:
            print "Can't copy %s to %s: %s" % (`self.src`, `self.dst`, str(why))



import os,re
import shutil
IPVSADM='/sbin/ipvsadm'

def main():
    xml = Monitor()
    xml.ipvslist()
    xml.make()
    #xml.display()
    xml.save()
    #xml.saveAs('/var/www/vs.xml')
    deploy = Deploy()
    deploy.target('/var/www')
    deploy.start()

if __name__ == "__main__":
    main()
```

ipvs.xsl

```
<?xml version="1.0" encoding="utf-8"?>
<!-- stylesheet by netkiller -->
```

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">

<xsl:output method="html"/>

<xsl:template match="/">
<html>
<head>
<title><xsl:value-of select="table/caption"/></title>
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<meta content="陈景峰,网路杀手,网络杀手,bg7nyt,ham,火腿" name="keywords" />
<meta content="陈景峰" name="description" />
<!--
<link rel="shortcut icon" href="favicon.ico" />
<link rel="Bookmark" href="favicon.ico" />
-->
<link rel="stylesheet" type="text/css" href="style.css" />

</head>

<body bgcolor="DFEFFF" text="#000000">
<a name="top" />



<xsl:apply-templates/>

</body>
</html>
</xsl:template>

<xsl:template match="/ipvs">
<xsl:for-each select="table">
<table width="90%" border="1" cellspacing="0" cellpadding="5" bgcolor="E0F0FF" align="center"
bordercolor="4FA7FF">
<caption><xsl:value-of select="caption"/></caption>
<xsl:for-each select="node">
<tr>
<td><xsl:value-of select="nip"/></td>
<td><xsl:value-of select="nport"/></td>
<td><xsl:value-of select="forward"/></td>
<td><xsl:value-of select="weight"/></td>
<td><xsl:value-of select="active"/></td>
<td><xsl:value-of select="inact"/></td>
</tr>
</xsl:for-each>
</table>
<br />
</xsl:for-each>
</xsl:template>

<xsl:template match="chapter/title">
<center><h1>
<xsl:apply-templates/>
</h1>
</center>
<hr />

</xsl:template>

<xsl:template match="ulink">
<a href="{@url}" border="0" >
<xsl:apply-templates/> </a> <br />
</xsl:template>


<!--
<xsl:apply-templates select="title"/><br />
<xsl:for-each select="setp">
</xsl:for-each>
-->
</xsl:stylesheet>
```

第 72 章 keepalived

目录

VRRP（Virtual Router Redundancy Protocol）协议

网站: http://www.keepalived.org/

http://www.lvwnet.com/vince/linux/Keepalived-LVS-NAT-Director-ProxyArp-Firewall-HOWTO.html

http://www.keepalived.org/LVS-NAT-Keepalived-HOWTO.html

http://archive.linuxvirtualserver.org/html/lvs-users/2002-12/msg00189.html

http://www.linuxvirtualserver.org/docs/ha/keepalived.html

1. 安装

两台已经安装好Ubuntu的服务器

分别安装ssh以方便putty登录

```
neo@master:~$ sudo apt-get install ssh
neo@slave:~$ sudo apt-get install ssh
```

install keepalived

```
neo@master:~$ apt-cache search lvs
keepalived - Failover and monitoring daemon for LVS clusters
neo@master:~$ sudo apt-get install keepalived
```

配置 keepalived.conf

```
neo@master:/etc/keepalived$ sudo touch keepalived.conf
neo@master:/etc/keepalived$ sudo vi keepalived.conf
```

例 72.1. keepalived.conf

```
vrrp_sync_group VG1 {
```

```
    group {
        VI_1
        VI_2
    }
}

vrrp_instance VI_1 {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        172.16.0.1
    }
}

vrrp_instance VI_2 {
    state MASTER
    interface eth1
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        172.18.1.254
    }
}

virtual_server 172.16.0.1 80 {
    delay_loop 6
    lb_algo wlc
    lb_kind NAT
    persistence_timeout 600
    protocol TCP

    real_server 172.16.0.2 80 {
        weight 100
        TCP_CHECK {
            connect_timeout 3
        }
    }
    real_server 172.16.0.3 80 {
        weight 100
        TCP_CHECK {
            connect_timeout 3
        }
    }
    real_server 172.16.0.4 80 {
        weight 100
        TCP_CHECK {
            connect_timeout 3
        }
    }
}
```

enable ip_forward

$ sudo sysctl -w net.ipv4.ip_forward=1

```
neo@master:~$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

Starting keepalived

```
neo@master:/etc/keepalived$ sudo /etc/init.d/keepalived start
Starting keepalived: keepalived.
```

virtual_ipaddress

virtual_ipaddress { 172.16.0.1/16 } 正常直接写IP即可.但在ubuntu中如果不写子网掩码,它会默认为172.16.0.1/32.

2. test

Log

Keepalived 日志输出位置

Debian/Ubutun: /var/log/daemon.log

Other: /var/log/messages

```
tail -f  /var/log/daemon.log |grep Keepalived
```

$ sudo ipvsadm

链接测试

```
$ w3m -no-cookie -dump 'http://172.16.0.1'
```

查看vip

```
neo@master:/etc/keepalived$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:07:40:14 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.2/16 brd 172.16.255.255 scope global eth0
    inet6 fe80::20c:29ff:fe07:4014/64 scope link
       valid_lft forever preferred_lft forever
neo@master:/etc/keepalived$

neo@master:/etc/keepalived$ sudo /etc/init.d/keepalived start
Starting keepalived: keepalived.

neo@master:/etc/keepalived$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:07:40:14 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.2/16 brd 172.16.255.255 scope global eth0
    inet 172.16.0.1/16 scope global secondary eth0
    inet6 fe80::20c:29ff:fe07:4014/64 scope link
       valid_lft forever preferred_lft forever
neo@master:/etc/keepalived$
```

正确应该显示： inet 172.16.0.1/16 scope global secondary eth0

genhash 生成web hash类似md5sum，对比每次输出是否一样

```
genhash -s 172.16.0.1 -p 80 -u /
genhash -s 172.16.0.1 -p 80 -u /
genhash -s 172.16.0.1 -p 80 -u /
...
genhash -s 172.16.0.1 -p 80 -u /
```

第 73 章 heartbeat+ldirectord

目录

1. heartbeat

```
neo@ubuntu:~$ apt-cache search  heartbeat
heartbeat - Subsystem for High-Availability Linux
heartbeat-dev - Subsystem for High-Availability Linux - development files
ipvsadm - Linux Virtual Server support programs

neo@ubuntu:~$ sudo apt-get install heartbeat
```

2. ldirectord

当前环境

```
[root@backup ~]# cd /etc/ha.d/
[root@backup ha.d]# ls
authkeys       harc           ldirectord.cf  README.config  shellfuncs
ha.cf          haresources    rc.d/          resource.d/
```

heartbeat主要有三个配置文件:

1. /etc/ha.d/authkeys
2. /etc/ha.d/ha.cf
3. /etc/ha.d/haresources

过程 73.1. 配置步骤:

1. /etc/ha.d/authkeys

   auth 3

   3 md5 hello

```
[root@backup ha.d]# vi authkeys
auth 3
#1 crc
#2 sha1 HI!
3 md5 hello
```

2. /etc/ha.d/ha.cf

   master

   logfile /var/log/ha-log

   logfacility local0

keepalive 2

deadtime 30

warntime 10

initdead 120

udpport 694

ucast eth1 10.10.10.161

ucast eth1 <backup node ip>

auto_failback on

node master.example.org

node backup.example.org

ping_group group1 10.10.10.160 10.10.10.161

respawn hacluster /usr/lib/heartbeat/ipfail

apiauth ipfail gid=haclient uid=hacluster

```
[root@backup ha.d]# vi ha.cf
logfile /var/log/ha-log
```

backup

ucast eth1 master node ip

3. /etc/ha.d/haresources

<node> <vip>/<netmask>/<interface>/<vip> ldirectord

master.example.org 211.100.37.164/32/eth0:0/211.100.37.164 ldirectord

```
[root@master ha.d]# cat haresources
master.example.org 211.100.37.164/32/eth0:0/211.100.37.164 ldirectord
```

backup.example.org 211.100.37.164/32/eth0:0/211.100.37.164 ldirectord

```
[root@backup ha.d]# cat haresources
backup.example.org 211.100.37.164/32/eth0:0/211.100.37.164 ldirectord
```

4. /etc/ha.d/ldirectord.cf

```
checktimeout=3
checkinterval=1
autoreload=yes
logfile="/var/log/ldirectord.log"
quiescent=yes
virtual=211.100.37.164:80
        real=10.10.0.7:80 gate
        real=10.10.0.8:80 gate
        real=10.10.0.9:80 gate
        service=http
        virtualhost=netkiller.8800.org
        scheduler=wrr
        protocol=tcp
        checkport=80
...
```

3. test

debug

```
tail -f /var/log/ha-log
```

察看心跳监听是否工作:

```
[root@master ha.d]# tcpdump -i eth1 icmp
[root@backup ha.d]# tcpdump -i eth1 icmp
```

IPaddr2 Script

IPAddr2::10.10.0.1/32/0:0/10.10.0.1

```
resource.d/IPaddr2 10.10.0.1/32/0:0/10.10.0.1 start
```

第 74 章 Piranha

CentOS Piranha

第 75 章 HAProxy - fast and reliable load balancing reverse proxy

```
$ apt-cache search haproxy
haproxy - fast and reliable load balancing reverse proxy
```

```
yum install haproxy
```

```
 cd /etc/haproxy/
 cp haproxy.cfg haproxy.cfg.old


# cat /etc/haproxy/haproxy.cfg
#---------------------------------------------------------------------
# Example configuration for a possible web application.  See the
# full configuration options online.
#
#   http://haproxy.1wt.eu/download/1.4/doc/configuration.txt
#
#---------------------------------------------------------------------

#---------------------------------------------------------------------
# Global settings
#---------------------------------------------------------------------
global
    # to have these messages end up in /var/log/haproxy.log you will
    # need to:
    #
    # 1) configure syslog to accept network log events.  This is done
    #    by adding the '-r' option to the SYSLOGD_OPTIONS in
    #    /etc/sysconfig/syslog
    #
    # 2) configure local2 events to go to the /var/log/haproxy.log
    #   file. A line like the following can be added to
    #   /etc/sysconfig/syslog
    #
    #    local2.*                       /var/log/haproxy.log
    #
    log         127.0.0.1 local2

    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     40000
    user        haproxy
    group       haproxy
    daemon

    # turn on stats unix socket
    stats socket /var/lib/haproxy/stats

#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 40000

#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
frontend  main *:80
#    acl url_static       path_beg       -i /static /images /javascript /stylesheets
#    acl url_static       path_end       -i .jpg .gif .png .css .js
```

```
#    use_backend static          if url_static
    default_backend             app

#---------------------------------------------------------------------
# static backend for serving up images, stylesheets and such
#---------------------------------------------------------------------
#backend static
#    balance     roundrobin
#    server      static 172.16.0.6:80 check

#---------------------------------------------------------------------
# round robin balancing between the various backends
#---------------------------------------------------------------------
backend app
    balance     roundrobin
    server  app1 10.0.0.68:80 check
    server  app2 10.0.0.69:80 check
#    server  app3 127.0.0.1:5003 check
#    server  app4 127.0.0.1:5004 check


[root@r610 haproxy]# /etc/init.d/haproxy start
Starting haproxy:                                          [  OK  ]
```

第 76 章 Voice over IP

目录

安装环境 ubuntu 7.10

1. Gnu Gatekeeper

http://www.gnugk.org/

1.1. Gnu Gatekeeper Install

```
sudo apt-get install gnugk
sudo apt-get install ohphone
```

start|stop|restart|force-reload

```
netkiller@shenzhen:~$ sudo /etc/init.d/gnugk
Usage: /etc/init.d/gnugk {start|stop|restart|force-reload}
```

Start

```
netkiller@shenzhen:~$ sudo /etc/init.d/gnugk start
Starting H.323 gatekeeper: gnugk.
netkiller@shenzhen:~$

netkiller@shenzhen:~$ sudo /etc/init.d/gnugk stop
Stopping H.323 gatekeeper: gnugk.
netkiller@shenzhen:~$
```

1.2. Gnu Gatekeeper Configure

gatekeeper.ini

```
[Gatekeeper::Main]
Fourtytwo=42
[GkStatus::Auth]
rule=allow
```

1.3. Gnu Gatekeeper Test

How do I test Gatekeeper

first, telnet tools

```
netkiller@shenzhen:~$ telnet 127.0.0.1 7000
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Version:
Gatekeeper(GNU) Version(2.2.5)
Ext(pthreads=1,radius=1,mysql=1,pgsql=1,firebird=1,large_fdset=0,crypto/ssl=1) Build(Feb  2
2007, 21:39:07) Sys(Linux i686 2.6.20-15-server)
GkStatus: Version(2.0) Ext()
Toolkit: Version(1.0) Ext(basic)
Startup: Fri, 09 Nov 2007 17:26:23 -0500   Running: 0 days 00:08:34
;
```

1.3.1. Part I - Microsoft Windows NetMeeting

Windows XP

Start NetMeeting

Start->Run->conf

NetMeeting

一个目录服务器列出了您可以使用 NetMeeting 呼叫的人。如果您登录到一个目录服务器，别人就可以看得到您并且可以呼叫您。

☐ 当 NetMeeting 启动时登录到目录服务器(L)

服务器名 osoft Internet Directory

☐ 不要在目录中列出我的名字(I)。

< 上一步(B) 下一步(N) > 取消

NetMeeting

您将用网络打 NetMeeting 电话，请指定连接到该网络的速度。

○ 14400 bps 的调制解调器(1)

○ 28800 bps 或更快的调制解调器(2)

◉ 电缆、 xDSL 或 ISDN(C)

○ 局域网(L)

< 上一步(B) 下一步(N) > 取消

NetMeeting

NetMeeting 将使用下列视频捕获设备。

主要视频捕获设备(P):

VivaPix WebCam

< 上一步(B) 下一步(N) > 取消

NetMeeting

要想更容易找到 NetMeeting，您可以在您的桌面上并且/或您的栏上快速启动部分放一个快捷键。

☑ 请在桌面上创建 NetMeeting 的快捷键(P)。

☑ 请在快速启动栏上创建 NetMeeting 的快捷键(Q)。

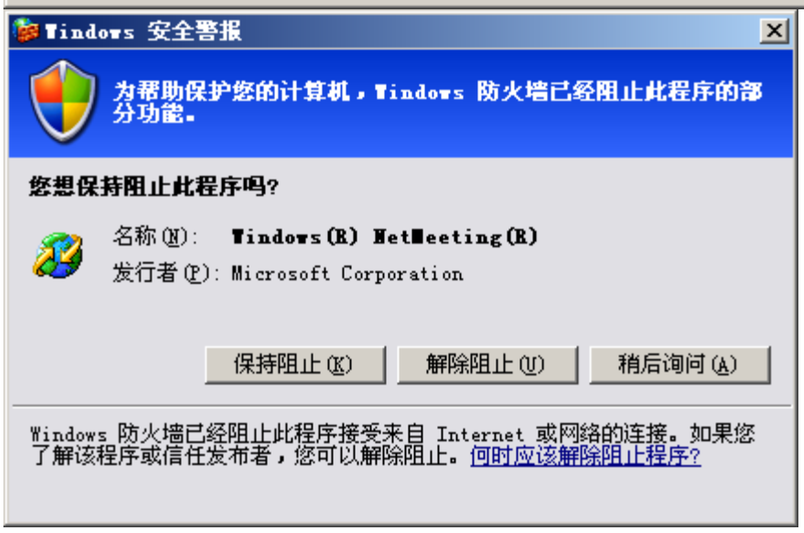
< 上一步(B) 下一步(N) > 取消


音频调节向导
本向导将帮助您调节音频设置。
关闭其它所有放音或录音程序，然后单击“下一步”继续。
< 上一步(B)
下一步(N) >
取消

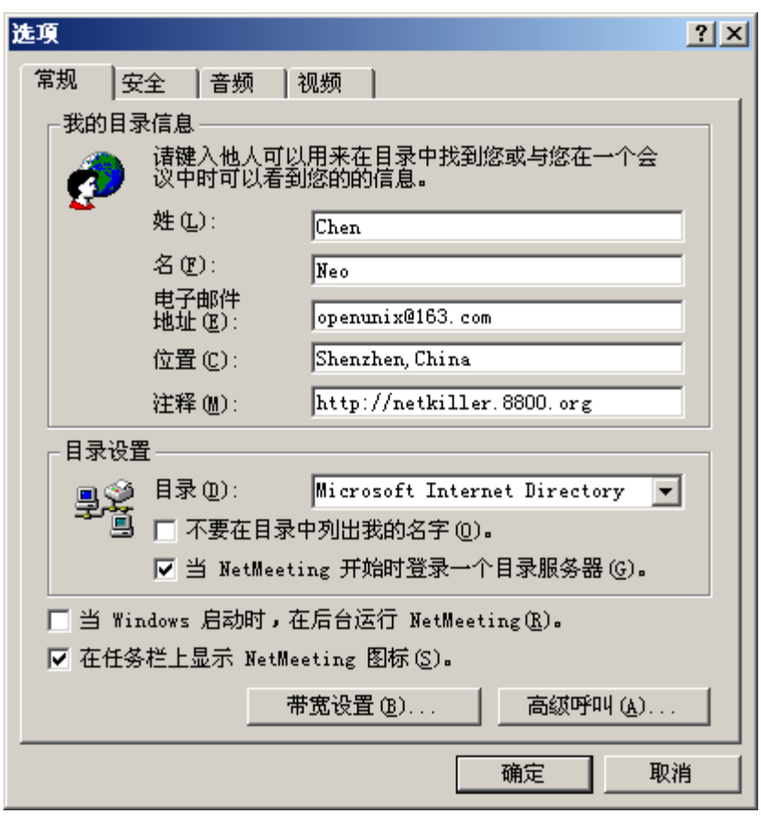

音频调节向导
NetMeeting 将使用下列音频波形设备。
录音(R)
Intel(r) Integrated Audio
回放(P)
Intel(r) Integrated Audio
< 上一步(B)
下一步(N) >
取消


音频调节向导
您应该检查扬声器或耳机是否已连接，重放音量是否合适。
要调节回放音量，请使用下面的滑块。单击“测试”按钮收听采样声音。
音量(V)
停止(S)
< 上一步(B)
下一步(N) >
取消

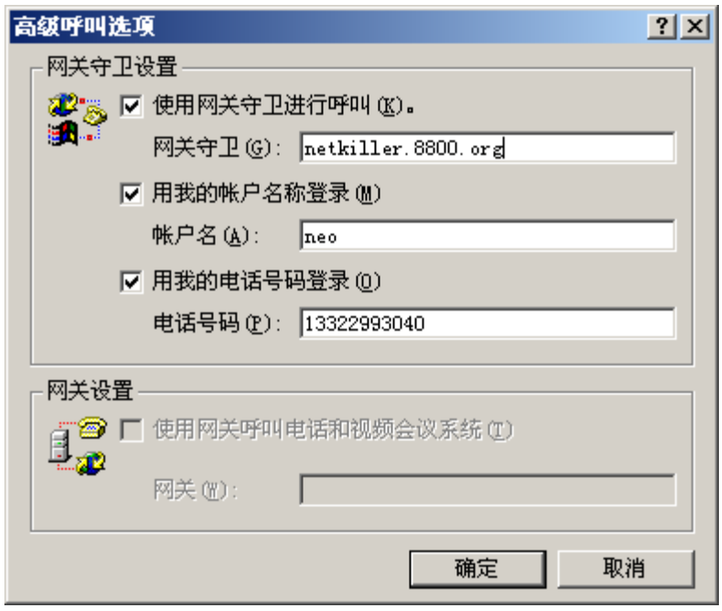

音频调节向导
向导将确保麦克风处于工作状态，并且录音音量合适。
对着麦克风读出下列文字:
“正在使用安装程序向导。它正在检查我的麦克风是否已插好、工作是否正常。”
录音音量(R)
< 上一步(B)
下一步(N) >
取消



Tools -> Option -> Advence



网关守卫设置



1.3.2. Part II - ohphone

For example:

netkiller

```
neo@machine1:~$ ohphone -l -a -u neo
```

neo

```
netkiller@machine2:~$ ohphone -u netkiller neo
```

上一页 下一页

第 75 章 HAProxy - fast and reliable load balancing reverse proxy

起始页

2. Asterisk (OpenSource Linux PBX that supports both SIP and H.323)

2. Asterisk (OpenSource Linux PBX that supports both SIP and H.323)

http://www.asteriskpbx.com/

```
netkiller@shenzhen:~$ apt-cache search Asterisk
asterisk-app-dtmftotext - Text entry application for Asterisk
asterisk-app-fax - Softfax application for Asterisk
asterisk-app-misdn-v110 - V.110 protocol handler for Asterisk
asterisk-chan-capi - Common ISDN API 2.0 implementation for Asterisk
asterisk-chan-misdn - mISDN support for Asterisk
asterisk-oh323 - oh323 channel driver for Asterisk
asterisk-prompt-de - German voice prompts for the Asterisk PBX
asterisk-prompt-es-co - Colombian Spanish voice prompts for Asterisk
asterisk-prompt-fr - French voice prompts for Asterisk
asterisk-prompt-it - Italian voice prompts for the Asterisk PBX
asterisk-prompt-se - Swedish voice prompts for Asterisk
asterisk-rate-engine - Asterisk least cost routing module
asterisk-sounds-extra - Additional sound files for the Asterisk PBX
destar - management interface for the Asterisk PBX
gastman - GUI tool for Asterisk administration and monitoring
iaxmodem - software modem with IAX2 connectivity
kiax - IAX VoIP softphone
libiax-dev - implementation of the Inter-Asterisk eXchange protocol (devel)
libiax0 - implementation of the Inter-Asterisk eXchange protocol
op-panel - switchboard type application for the Asterisk PBX
asterisk-prompt-es - Spanish prompts for the Asterisk PBX
asterisk - Open Source Private Branch Exchange (PBX)
asterisk-bristuff - Open Source Private Branch Exchange (PBX) - BRIstuff-enabled version
asterisk-classic - Open Source Private Branch Exchange (PBX) - original Digium version
asterisk-config - config files for asterisk
asterisk-dev - development files for asterisk
asterisk-doc - documentation for asterisk
asterisk-h323 - asterisk H.323 VoIP channel
asterisk-sounds-main - sound files for asterisk
asterisk-web-vmail - Web-based (CGI) voice mail interface for Asterisk
netkiller@shenzhen:~$
```

3. OpenSER SIP Server

http://www.openser.org/

```
netkiller@shenzhen:~$ apt-cache search openser
openser - very fast and configurable SIP proxy
openser-cpl-module - CPL module (CPL interpreter engine) for OpenSER
openser-dbg - very fast and configurable SIP proxy [debug symbols]
openser-jabber-module - Jabber module (SIP-Jabber message translation) for OpenSER
openser-mysql-module - MySQL database connectivity module for OpenSER
openser-postgres-module - PostgreSQL database connectivity module for OpenSER
openser-radius-modules - radius modules for OpenSER
openser-unixodbc-module - unixODBC database connectivity module for OpenSER
```

第 77 章 FAQ

目录

1. 通过SSH与控制台不能登录

通过SSH与控制台不能登录，登录后立即退出。

我在做压力测试的时候将所有用户的 nofile 设置为 1050000 导致 SSH 与控制台均不能登录Linux 系统。

```
# cat /etc/security/limits.conf |tail
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#@student        -       maxlogins       4

# End of file
* soft nofile 1050000
* hard nofile 1050000
```

后来发现/var/log/secure 日志，提示Could not set limit for 'nofile': Operation not permitted

```
# tail -f /var/log/secure

Aug  6 04:07:56 r510 sshd[20858]: Accepted password for root from 192.168.80.129 port 51798
ssh2
Aug  6 04:07:56 r510 sshd[20858]: pam_limits(sshd:session): Could not set limit for 'nofile':
Operation not permitted
Aug  6 04:07:56 r510 sshd[20858]: pam_unix(sshd:session): session opened for user root by
(uid=0)
Aug  6 04:07:56 r510 sshd[20858]: error: PAM: pam_open_session(): Permission denied
```

附录 A. 附录

目录

1. 参考文档

http://www.faqs.org/docs/Linux-HOWTO/Bash-Prog-Intro-HOWTO.html

http://xiaowang.net/bgb-cn/index.html

2. Linux 下载排名

http://distrowatch.com/

3. Ubuntu Server Edition

http://www.ubuntu.com/

Netkiller Ubuntu Linux 手札

4. CentOS - The Community ENTerprise Operating System

http://www.centos.org/

Netkiller CentOS Linux 手札

上一页

附录 B. 历史记录

修订历史

修订 1.0 2007-1-12

- 开始
- ubuntu linux

修订 1.1 2007-5-10

Application (Zope)

修订 1.2 2007-5-15

Memcached

修订 1.3 2007-5-18

Jboss

修订 1.4 2007-5-21

php memcache,lighttpd script

修订 1.5 2007-5-22

rsync

修订 1.6 2007-5-24

openfiler

修订 1.7 2007-5-25

openfiler, php sql server

修订 1.8 2007-5-28

openfiler, zend optimizer

修订 1.9 2007-6-9

ip tunnel, memcached script, lighttpd script

修订 1.10 2007-11-13

栏目重新排版，增加很多新内容

修订 1.11 2008-1-17

awstats, webalizer

修订 1.12 2008-1-22

TUTOS, TRAC

修订 1.2 2008-3-21

栏目重新排版，增加很多新内容

修订 1.2.1 2008-3-21

Shorewall

修订 1.2.2 2008-6-20

FreeRADIUS

修订 1.2.3 2008-10-7

MySQL Replication

修订 1.2.4 2008-10-8

MySQL Cluster

修订 1.2.5 2008-10-9

modi: Openldap

修订 1.2.6 2008-10-21

ufw - program for managing a netfilter firewall

inotify-tools

DRBD (Distributed Replicated Block Device)

修订 1.2.7 2008-10-31

modify rsync chapter

add csync2

修订 1.2.8 2008-12-3

modified system chapter

add nagios, and remove developer chapter

修订 1.2.9 2008-12-16

the system chapter was modified

修订 1.2.10 2008-12-22

added loop devices

added ACL - Access Control List under chapter security.

added ncftp, ncftpget, ncftpput

修订 1.3.0 2009-3-10

bash

added if, for, while, until

and function

修订 1.3.1 2009-3-22

vsftpd

修订 1.3.2 2009-4-5

to move chapter database to new docbook.

修订 1.3.2 2009-4-15

Stunnel.

修订 1.3.3 2009-5-7

增加很多新内容,章节重新排版。

修订 1.3.4 2009-10-27

PPTPD

上一页

4. CentOS - The Community ENTerprise Operating System

起始页

Netkiller Linux 手札

Netkiller Linux Cookbook

Mr. Neo Chan, 陈景峰 (BG7NYT)

中国广东省深圳市宝安区龙华镇

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 Tue Dec 6 12:12:43 UTC 2011

内容摘要

本文档讲述Linux系统涵盖了系统管理与配置包括:

对初学Linux的爱好者忠告

玩Linux最忌reboot（重新启动）这是windows玩家坏习惯

Linux只要接上电源你就不要再想用reboot,shutdown,halt,poweroff命令,Linux系统和应用软件一般备有reload,reconfigure,restart/start/stop...不需要安装软件或配置服务器后使用reboot重新引导计算机

在Linux系统里SIGHUP信号被定义为刷新配置文件,有些程序没有提供reload参数,你可以给进程发送HUP信号,让它刷新配置文件,而不用restart.通过pkill,killall,kill 都可以发送HUP信号例如: pkill -HUP httpd

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 MySQL 手札	Netkiller LDAP 手札	Netkiller Security 手札	Netkiller Version 手札
Netkiller Intranet 手札	Netkiller Cisco IOS 手札	Netkiller Writer 手札	Netkiller Studio Linux 手札

鸣谢

目录

表格清单

范例清单

下一页

自述