Настройки Linux-сервера

Debian, Ubuntu Server Edition

29.09.23
11:12:42

Оглавление

Используемые цветовые обозначения:

Текст, имя файла или папки, комментарии.
Материал, который нужно дописать.
Содержимое файлов конфигурации.
Команда с параметрами для запуска на сервере.
`Вывод системы на команду.`

Командная строка

^L – очистить экран
^S, ^Q – остановить, возобновить вывод на экран
^PgUp, ^PgDN – прокрутка экрана вверх, вниз
Shift-PgUp, Shift-PgDN – прокрутка постранично

Читать: **man bash** – управление процессами, редактирование в командной строке.
^C – прерывание выполнения команды
^D – завершение процесса
^Z – приостановить активный процесс немедленно
^Y – приостановить, когда процесс запросит ввод данных
jobs – список фоновых процессов
fg *id* – перевести процесс в активное состояние
bg *id* – перевести процесс в фоновый режим

Мышь в консоли

Если установить **gpm**, то в консоли можно использовать мышь:
- левая кнопка — выделяет текст и копирует выделенное в буфер
- средняя (или правая+левая одновременно) — вставляет текст из буфера

putty – левая кнопка — выделение, правая — вставка (средняя — выделение, какое?).

Для захвата и вставки текста в приложениях, которые сами используют мышь (например, **mc**), нужно удерживать нажатой клавишу Shift на клавиатуре.

Эти же кнопки можно использовать для копирования текста в среде X Window.

dpkg-reconfigure

Утилита для перенастройки пакетов в ubuntu/debian:

Выбор DM в ubuntu
 # dpkg-reconfigure gdm

Выбор локали
 # dpkg-reconfigure locales

Выбор часового пояса
 # dpkg-reconfigure tzdata

 # dpkg-reconfigure console-cyrillic

Установка системы

Инсталляция

При установке системы не на первый диск (/dev/sda) нужно отказаться от предложения «установить загрузчик в MBR», а установить его в MBR устройства /dev/sdb (или другого, где на самом деле находится /boot).
В случае ошибки выбора система не сможет загрузиться.
Восстановить загрузчик можно, загрузившись с Live-CD, как описано в главе «Устранение неисправностей — Восстановление загрузчика GRUB».

Конфигурация системы

SLES, OpenSuSe:
yast

ReadHat, CentOS:
system-config

SSH сервер

apt-get install ssh

Выбор ролей (задач) сервера

tasksel

Дополнительные программы

apt-get install mc zip unzip screen

Создание учётной записи нового пользователя

adduser *login*
adduser --force-badname *dotted.login*

Сменить пароль пользователя:
passwd *login*

usermod

usermod -s /bin/false ***login***
-L
-U

Приглашение системы

$ - пользователь
# - администратор (superuser)

Предоставление пользователю прав администратора

Debian: инсталлятор запрашивает пароль для пользователя root и данные для создания обычного пользователя (без права sudo).
Можно использовать su:
su [*login*]

Установка и настройка sudo:

apt-get install sudo
visudo
adduser *login* sudo

Ubuntu: вход пользователем root после установки системы заблокирован, обычный пользователь, созданный при установке, имеет право sudo.

adduser *login* sudo — 12.04 etc.
adduser *login* admin – до 12.xx версии

Up until Ubuntu 11.10, administrator access using the sudo tool was granted via the "admin" Unix group. In Ubuntu 12.04, administrator access will be granted via the "sudo" group. This makes Ubuntu more consistent with the upstream implementation and Debian. For compatibility purposes, the "admin" group will continue to provide sudo/administrator access in 12.04.

sudo -i
sudo *command*

RedHat, CentOS:
[/usr/sbin/]visudo

Добавить пользователя в группу wheel и добавить (раскомментировать) строку /etc/sudoers:
%wheel ALL=(ALL) ALL

Или добавить строку /etc/sudoers:
login ALL=(ALL) ALL

Процессы и пользователи

ps ax
top | htop
iostat
vmstat
cpustat
free
w

Run levels

0: System Halt
1: Single User (maintenance)
2 to 5: Multi-User Modes
6: System Reboot

init *runlevel*

Завершение работы

halt
shutdown [now]
reboot

Демоны

Дописать: initd, upstart, systemd

chkconfig *service* {on|off}
service *service* {start|stop}
/etc/init.d/*service* {start|stop|restart|reload}

selinux

Отключение selinux:
getenforce
setenforce 0

Системное время

/etc/default/rcS – аппаратное время локальное или UTC?
UTC=yes/no

Дописать: Начиная с версии 16.04. UTC-время в Windows.

Выбор часового пояса:
tzselect
dpkg-reconfigure tzdata

Синхронизация времени

apt-get install ntpdate
ntpdate pool.ntp.org

crontab -e — каждый час в hh:30 выполнять синхронизацию времени с сервером
30 * * * * /usr/sbin/ntpdate a.b.c.129

ntpdate -s ntp_src – adjust time
ntpdate -b ntp_src – step

Дописать:
apt-get install ntpdate-debian
/etc/default/ntpdate — серверы времени
hwclock --systohc

Планировщик заданий

crontab -{e|l|r} [user]
e – редактирование списка заданий
l – показать список заданий
r – удалить все задания

crontab

minute hour DoM month DoW command

minute – 0-59
hour – 0-23
DoM – 1-31
month – 1-12
DoW – 0-6 (0=Sunday)

A normal crontab entry looks like this:
* * * * * /usr/bin/command
That runs the command every minute.
The following is a crontab entry that runs a command every hour on the hour:
@hourly /usr/bin/command
And, there are many more: **@annually**, **@monthly**, **@daily**, **@midnight** and **@reboot**. If you have a crontab entry like this:
@reboot /usr/bin/command
it will execute when the system starts up with the ownership and permission of the person owning the crontab.

watch

watch [-n NNsec] *command*

screen | tmux

Запустить мультиплексор:
screen

Подключиться к запущенному сеансу:
screen [-D] -R

^A ? – помощь по сочетаниям клавиш

tmux

^B ? – помощь по сочетаниям клавиш

Установка оборудования

ethtool

Добавление интерфейса

RTL 8029AS:
modprobe ne2k-pci
ifup eth1

Модули ядра

/etc/modules:

```
# /etc/modules: kernel modules to load at boot time.
#
# This file contains the names of kernel modules that should be loaded
# at boot time, one per line. Lines beginning with "#" are ignored.
```

Дописать:
/etc/modules, blacklist

Управление устройствами UDEV

http://tux-the-penguin.blogspot.ru/2010/02/udev.html

Правила udev: /etc/udev/rules.d/*

Привязка имени сетевого интерфейса eth к MAC адаптера

/etc/udev/rules.d/70-persistent-net.rules:

```
# PCI device 0x8086:0x1229 (e100)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:d0:b7:51:c2:28",
ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"
```

Права доступа к устройствам

Права на устройства модемов:
 # chmod 0666 /dev/ttyUSB*

Чтобы при вынимании/включении устройства права не слетали:
cat 92-dongle.rules

```
KERNEL=="ttyUSB*", MODE="0666", OWNER="asterisk", GROUP="uucp"
```

adduser *login* dialup

Перезапуск демона udev

 # udevcontrol reload_rules
или
 # /etc/init.d/udev reload

Настройка производительности

Swappiness

(http://fastsql.ru/2009/02/10/linux-swappiness/)

free

```
total used free shared buffers cached
Mem: 2041888 1991096 50792 0 52 954592
-/+ buffers/cache: 1036452 1005436
Swap: 975200 1308 973892
```

cat /proc/sys/vm/swappiness

```
60
```

(При оставшихся 60% свободной памяти начинать использовать подкачку)

echo 0> /proc/sys/vm/swappiness
(Использовать подкачку только когда не останется свободной памяти)
/etc/sysctl.conf
vm.swappiness = 0

Десктоп
(http://habrahabr.ru/blogs/windows7/107637/
http://kerneltrap.org/node/3000)
«Swapout is good. It frees up unused memory. I run my desktop machines at swappiness=100»

COMPCACHE

Использовать сжатый раздел подкачки в оперативной памяти:

/etc/initramf/initramfs.conf:
COMPCACHE_SIZE="128 M"

update-initramfs -u

См. также ZRAM / ZSWAP.

Cache pressure

echo 50 > /proc/sys/vm/vfs_cache_pressure

vm.vfs_cache_pressure = 50

(100)

Управление сервером

Обновление пакетов и установка ПО

Использовать прокси-сервер при скачивании обновлений:
/etc/apt/apt.conf:
Acquire::http::proxy "http://192.168.43.4:3128/";

/etc/apt/sources.list – список источников ПО

apt-get update
apt-get dist-upgrade

apt-get update && apt-get dist-upgrade -y && apt-get autoremove

apt-cache search *package*
apt-cache showpkg *package*

apt-get install *package*

RedHat, CentOS:
yum update [-y]
yum upgrade [-y] [--skip-broken]
yum install *package*

Добавление источников ПО

http://help.ubuntu.ru/wiki/ppa?s=ppa

add-apt-repository ppa:*product-team*/ppa && apt-get update

/etc/apt/sources.list.d/*.list — списки источников ПО

Добавление ключей шифрования для проверки подписи пакетов

Скачать и добавить ключ:
wget -O - *http://download.site.org/repositories/Release.key* | apt-key add -

Импорт с сервера ключей:
gpg --keyserver keyserver.ubuntu.com --recv *key_ID*
gpg --export --armor *key_ID* | sudo apt-key add -

apt-key adv --recv-keys --keyserver keyserver.ubuntu.com *key_ID*

Уточнить опции.

RedHat:
rpm --import /path_to_keys/RPM-GPG-KEY-redhat-*

Обновление версии дистрибутива

Информация о текущей версии

root@mx2:/# lsb_release -a

No LSB modules are available.
Distributor ID: Ubuntu
Description:	Ubuntu 14.04.5 LTS
Release:	14.04
Codename:	trusty

Обновление сервера

sudo apt-get install update-manager-core
do-release-upgrade

Возможные ошибки обновления

ImportError: No module named GnuPGInterface

You can try this to solve the python interface error:
cp /usr/share/pyshared/ GnuPGInterface .py /usr/lib/python2.6/

reference: http://ulm.ccc.de/pipermail/ssls-dev/2009-February/000051.html

Error authenticating some packages

Some useful logs are located under /var/log/dist-upgrade/ and I bet you are going to find there something along these lines:

It was not possible to authenticate some packages. This may be a transient network problem. You may want to try again later. See below for a list of unauthenticated packages

Temporary workaround, create file

/etc/update-manager/release-upgrades.d/unauth.cfg

filled with the following

[Distro]
AllowUnauthenticated=yes

Now your sudo do-release-upgrade should run OK

Обновление системы с истёкшим сроком поддержки

Обновление списка источников установки

To begin the upgrade, make sure you have a sources.list like the following, with CODENAME being your release, e.g. quantal.

EOL upgrade sources.list
Required
deb http://old-releases.ubuntu.com/ubuntu/ CODENAME main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ CODENAME-updates main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ CODENAME-security main restricted universe multiverse

Optional
#deb http://old-releases.ubuntu.com/ubuntu/ CODENAME-backports main restricted universe multiverse

You can use -backports and or -proposed if you want. For more information about repositories see this page.

Dependencies

You should also make sure some meta-packages are installed so the upgrade can continue without problems.

From version 6.06 and up you will need to install the update-manager and update-manager-core packages. Note: You don't want to install the update-manager package on CLI-only servers.

sudo aptitude install update-manager-core update-manager

For upgrading from an LTS release to a non-LTS release, make sure that the update manager is correctly configured to upgrade any release. This is not needed when upgrading from one LTS release to the next LTS release:

sudo perl -pi -e 's/^Prompt=.*/Prompt=normal/' /etc/update-manager/release-upgrades

Run the upgrade

After you've done the above, run the updates and then the upgrade as usually:

sudo apt-get update
sudo apt-get dist-upgrade
sudo do-release-upgrade

Мониторинг сервера

collectd, graphite, grafana
icinga, zabbix

Контроль температуры

apt-get install lm-sensors

Поиск датчиков:
sensors-detect
Ответить YES на все вопросы.
Добавить предложенные модули в файл /etc/modules.

Для загрузки изменений запустить:
/etc/init.d/module-init-tools start

Проверка показаний датчиков:
sensors

SMART

apt-get install smartmontools
https://help.ubuntu.com/community/Smartmontools

smartctl -a /dev/sda
smartctl -t {short|long} /dev/sda
VALID ARGUMENTS ARE: offline, short, long, conveyance, vendor,N, select,M-N, pending,N, afterselect,[on|off], scttempint,N[,p]

smartd

/etc/default/smartmontools:
# uncomment to start smartd on system startup
start_smartd=yes

/etc/smartd.conf:

Syslog

apt-get install rsyslog

Разрешить регистрировать события, поступающие из сети.
/etc/default/rsyslog:
#8.04
#RSYSLOGD_OPTIONS="-m 0 **-r**"
#9.04
RSYSLOGD_OPTIONS="-c3"

Sysstat

apt-get install sysstat

iostat
vmstat
cpustat

SAR

/etc/default/sysstat:
ENABLED="true"

/etc/init.d/sysstat restart

sar

free
top

SNMPd

apt-get install snmpd

/etc/default/snmpd:
SNMPDRUN=yes
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid ~~127.0.0.1~~'

/etc/snmp/snmpd.conf:
com2sec readonly a.b.c.199 public
trapcommunuty public
trapsink a.b.c.199

Ubuntu 12.04 /etc/snmp/snmpd.conf:
rocommunity public a.b.c.199
rocommunity public 192.168.5.4
rocommunity public 127.0.0.1
trapcommunuty public
trapsink a.b.c.199

/etc/snmp/snmptrapd.conf:
authCommunity log public 192.168.5.1

/etc/init.d/snmpd restart

Также смотри: netstat, mrtg, rrdtool, tcpdump, wireshark, tshark, smokeping, rmon, netalyzr

MRTG

apt-get install mrtg apache2

cfgmaker --global "Options[_]: growright, bits" --show-op-down public@192.168.5.1 public@192.168.5.4 public@192.168.5.3 public@192.168.5.8 > /etc/scripts/router.cfg
indexmaker /etc/scripts/router.cfg > /var/www/mrtg/index.html

/etc/scripts/router.cfg
Options[_]: growright, bits

/etc/scripts/router.sh
#!/bin/bash
#run mrtg
LANG=C

```
export $LANG
/usr/bin/mrtg /etc/scripts/router.cfg --logging /var/log/mrtg.log
```

crontab -e

```
*/5 * * * * /etc/scripts/router.sh
```

На опрашиваемых устройствах должны быть разрешены SNMP-запросы с адреса сервера MRTG.

Webmin

Установка на сервер

/etc/apt/sources.list.d/webmin.list

```
deb http://download.webmin.com/download/repository sarge contrib
```

wget http://www.webmin.com/jcameron-key.asc
apt-key add jcameron-key.asc
apt-get update
apt-get install webmin

Подключение к Webmin

http://localhost:10000
Используется логин и пароль пользователя с правами root.

Nagios3

apt-get install nagios3
htpasswd -c /etc/nagios3/htpasswd.users nagiosadmin

/etc/nagios3/conf.d/my-hosts.cfg

```
define host {
        host_name       lexa
        alias     lexa comp
        address         192.168.140.4
        use       generic-host
}
define hostgroup {
        hostgroup_name  my-friends                      #имя группы
        alias           my-friends comps                # описание
        members         lexa, volodya, xz1,xz2, diman      #члены группы
}
define service {
        hostgroup_name      my-friends      #имя группы для проверки
        service_description     PING
        check_command       check_ping!100.0,20%!500.0,60%  #команда проверки
        use       generic-service
}
```

nagios3 -v /etc/nagios3/nagios.cfg
/etc/init.d/nagios3 restart
/etc/init.d/nagios3 reload

http://192.168.0.1/nagios3/

Безопасность системы

Добавление пользователей

Создать пользователя
adduser *login*
adduser --force-badname *login.name*

Дать пользователю право становиться администратором (sudo)
adduser *login* admin

Генерирование паролей

apt-get install pwgen

pwgen

Ограничение доступа к сетевым сервисам

/etc/hosts.allow
ALL: 94.19.75.49
ALL: a.b.c.221, a.b.c.199
ALL: 192.168.100.0/24

/etc/hosts.deny
ALL:ALL

Блокирование консоли

apt-get install vlock

vlock [-a|--all]
Будет заблокирован доступ к одной или всем виртуальным консолям.

Средства удалённого доступа

SSH

Читать M.W.Lucas “SSH Mastery”.

Файл конфигурации ssh-сервера

/etc/ssh/sshd_config – Debian, Ubuntu
/etc/openssh/sshd_config – AltLinux

Файл конфигурации ssh-клиента

~/.ssh/config:
Host ip.ad.dre.ss
 Port 22
 User *login*

Устаревшие методы шифрования и рукопожатия при подключении:

Q1:
Unable to negotiate with host: no matching key exchange method found.
Their offer: diffie-hellman-group1-sha1

A1:
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 user@host

~/.ssh/config:
Host ip.ad.dre.ss
 KexAlgorithms +diffie-hellman-group1-sha1

Q2:
Unable to negotiate with ip.ad.dre.ss port 22: no matching cipher found. Their offer: 3des-cbc,blowfish-cbc,aes128-cbc,aes192-cbc,aes256-cbc

A2:
ssh -c 3des-cbc @

~/.ssh/config:
Host ip.ad.dre.ss
 Ciphers 3des-cbc,blowfish-cbc,aes128-cbc,aes192-cbc,aes256-cbc

Ограничение доступа через SSH

Запретить входить root'ом. Разрешение на вход дано только указанным пользователям.
/etc/ssh/sshd_config:
PermitRootLogin ~~**yes**~~ **no**
AllowUsers al ministr

Использование пользовательских файлов ключей

Генерация пользовательского ключа на сервере:
ssh-keygen
cd ~/.ssh/
cp id_rsa.pub authorized_keys

Только владелец ключей должен иметь право записи в файлы, иначе доступ по ключу становится невозможен:
alice:~/.ssh$ **ls -la**

```
-rw-r--r--  1 al al  390 2011-03-28 02:20 authorized_keys
-rw-------  1 al al 1743 2011-03-28 02:16 id_rsa
-rw-r--r--  1 al al  390 2011-03-28 02:16 id_rsa.pub
-rw-r--r--  1 al al 4080 2011-03-10 18:21 known_hosts
```

Запретить на сервере вход по паролю, оставить возможность подключения только по ключу id_rsa.
/etc/ssh/sshd_config:
PubkeyAuthentication yes
PasswordAuthentication no

/etc/init.d/ssh restart

Подключение с Linux-машины

Генерация пользовательского ключа на клиенте:
ssh-keygen

Скопировать ключ на сервер:
ssh-copy-id d.e.f.98

Подключение к удалённому хосту (логин из файла конфигурации, используется ключевой файл):
ssh d.e.f.98

Подключение с Windows-машины

Преобразование файла личного ключа в формат, поддерживаемый putty –
puttygen.exe:
Conversions – Import key = id_rsa
Save private key = private.ppk

Настройка подключения —
putty, winscp:
Connection – SSH – Auth – Private key file = private.ppk

При подключении потребуются: логин пользователя, файл с личным ключом и пароль от него.

Защита от попыток подбора пароля

Модуль iptables hashlimit умеет подсчитывать количество пакетов за определенный промежуток времени и через некоторое время сбрасывать счетчик:
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m hashlimit --hashlimit 1/hour --hashlimit-burst 2 --hashlimit-mode srcip --hashlimit-name SSH --hashlimit-htable-expire 60000 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 22 --tcp-flags SYN,RST,ACK SYN -j DROP
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

Можно использовать recent:
iptables -A INPUT -p tcp -m state --state NEW --dport 22 -m recent --update --seconds 20 -j DROP
iptables -A INPUT -p tcp -m state --state NEW --dport 22 -m recent --set -j ACCEPT

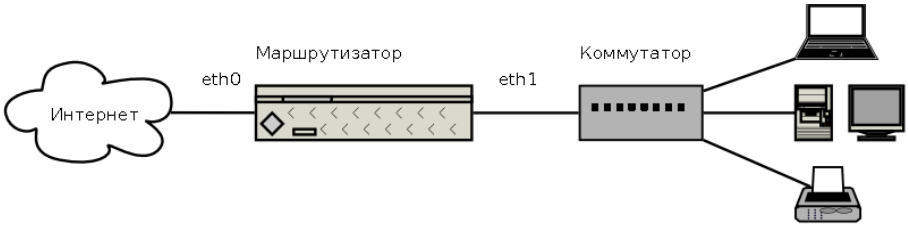
SSH-туннели

См. назначение ключей: -D, -L

ssh d.e.f.98 -24CX -L 3128:127.0.0.1:3128 – пробросить локальный порт 3128 на удалённый хост, порт 3128 (например, прокси-сервер squid).

Подключение к сети

Схема сети



Разные версии Debian и Ubuntu имеют различные способы настройки подключения к сети:

Версия	interfaces	resolv.conf	netplan	NetworkManager
Файлы:	/etc/networking/*	/etc/resolv.conf	/etc/netplan/*	/etc/NetworkManager/*
classic	Статические настройки сети	Настройки серверов имён		Управляются интерфейсы не из interfaces
16.04 или ранее	dns-*	Создаётся resolvconf на основе interfaces		
18.04 или ранее	Не используется		YAML-описание интерфейсов	Управляет Managed interfaces

Настройка разрешения имён

Имя компьютера

/etc/hostname – имя хоста

```
userver
```

Hosts

/etc/hosts

```
127.0.0.1       localhost
127.0.1.1       userver.home.local userver
```

Серверы имен

Если установлен пакет resolvconf, то настройки DNS производятся через опции dns-* в файле конфигурации /etc/network/interfaces.

/etc/resolv.conf - серверы имен Google DNS:

```
nameserver 8.8.8.8
nameserver 8.8.4.4
domain home.local
search home.local
```

Настройка сетевых интерфейсов

Используется DHCP-сервер:
/etc/network/interfaces:

```
# The primary network interface
auto eth0
iface eth0 inet dhcp
```

/etc/network/interfaces – настройки интерфейсов

```
auto eth0
iface eth0 inet static
        address 192.168.0.200
        netmask 255.255.255.0
        network 192.168.0.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
        dns-nameservers 93.100.1.3 94.19.255.2
        dns-search home.local
        # dns-* options are implemented by the resolvconf package, if installed

auto eth1
iface eth1 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        pre-up iptables-restore < /etc/iptables.up.rules
```

RedHat, CentOS:
/etc/sysconfig/network-scripts/*
system-config-network

Действия при изменении состояния сетевых интерфейсов

/etc/network/interfaces:

```
        up …
        down …
        pre-up …
```

и т.д.

/proc/sys/net/ipv4/*
/etc/sysctl.conf
ifconfig
ifup, ifdown

Подмена MAC-адреса

/etc/network/interfaces:

```
iface eth0 inet static
hwaddress ether 00:00:00:00:00:00
```

Применение настроек

Обновить сетевые настройки без перезагрузки сервера
/etc/init.d/networking restart **или** **/etc/init.d/network-manager restart**
service networking restart **или** **service network-manager restart**

Проверка

hostname
```
userver
```
hostname -f
```
userver.home.local
```
ping, traceroute etc.

Сетевые функции

Включение маршрутизатора

Включение функции маршрутизации:
echo 1 > /proc/sys/net/ipv4/ip_forward

Чтобы маршрутизатор автоматически включался при запуске системы
/etc/sysctl.conf:
net.ipv4.ip_forward = 1

NAT, masquerade

Включение трансляции адресов NAT:
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
где eth0 — название интерфейса, через который осуществляется выход в интернет.

Сохраняем настройки iptables в файл:
iptables-save > /etc/iptables.up.rules

Чтобы NAT заработал после перезагрузки, добавляем строку в файл
/etc/networks/interfaces:
pre-up iptables-restore < /etc/iptables.up.rules

Чтобы через NAT работали некоторые сложные протоколы, нужно загрузить модули:
modprobe ip_conntrack_ftp
modprobe ip_conntrack_irc
modprobe ip_conntrack_tftp
modprobe ip_conntrack_amanda
ip_nat_ftp, ip_nat_irc и т.д.

/etc/modules

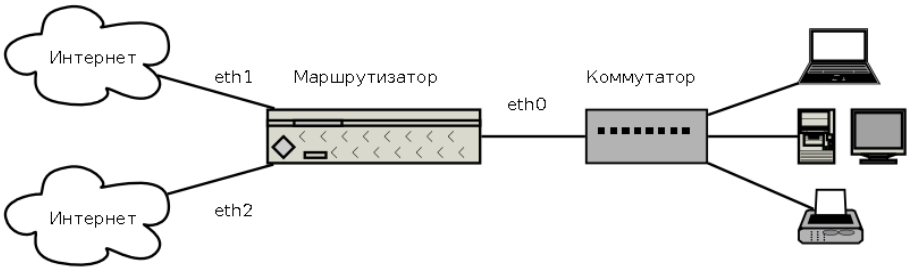
Запрет IPv6

/etc/sysctl.conf
```
# IPv6
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

sysctl -p

Маршрутизатор IPROUTE2

Схема сети при подключении к двум провайдерам



Интерфейсы

/etc/network/interfaces:

```
auto eth0
iface eth0 inet static
   address 192.168.43.201
   netmask 255.255.255.0

auto eth1
iface eth1 inet static
   address a.b.c.201
   netmask 255.255.255.128

auto eth2
iface eth2 inet static
   address 192.168.3.1
   netmask 255.255.255.0
```

 # /etc/init.d/networking restart

 # route

```
Destination Gateway Genmask Flags Metric Ref Use Iface
a.b.c.128   *               255.255.255.128 U     0      0        0 eth1
192.168.3.0     *               255.255.255.0   U     0      0        0 eth2
192.168.43.0    *               255.255.255.0   U     0      0        0 eth0
link-local      *               255.255.0.0     U     1000   0        0 eth0
```

С этого места *route* больше не используется.

Маршрутизация

/etc/iproute2/rt_tables:

```
#
43 private
195 public
```

 # ip rule add from 192.168.43.201 table private
 # ip rule add from a.b.c.201 table public

 # ip rule list

```
0:      from all lookup local
32764:  from a.b.c.201 lookup public
32765:  from 192.168.43.201 lookup private
32766:  from all lookup main
32767:  from all lookup default
```

 # ip route add default via a.b.c.129 dev eth1 table public
 # ip route add default via 192.168.43.254 dev eth1 table private
 # ip route flush cache

 # ip route add default via a.b.c.129
 # ip route add 192.168.81.0/24 nexthop via a.b.c.129 dev eth1 nexthop via 192.168.43.254 dev eth0

 # ip route

```
a.b.c.128/25 dev eth1  proto kernel  scope link  src a.b.c.201
192.168.81.0/24
        nexthop via a.b.c.129  dev eth1 weight 1
        nexthop via 192.168.43.254  dev eth0 weight 1
192.168.3.0/24 dev eth2  proto kernel  scope link  src 192.168.3.1
192.168.43.0/24 dev eth0  proto kernel  scope link  src 192.168.43.201
169.254.0.0/16 dev eth0  scope link  metric 1000
default via a.b.c.129 dev eth1
```

 # tracert 192.168.81.59

```
traceroute to 192.168.81.59 (192.168.81.59), 30 hops max, 60 byte packets
 1  a.b.c.129 (a.b.c.129)  0.478 ms  0.542 ms *
 2  * * *
```

 # tracert 192.168.81.2

```
traceroute to 192.168.81.2 (192.168.81.2), 30 hops max, 60 byte packets
 1  192.168.43.254 (192.168.43.254)  0.833 ms  2.004 ms *
 2  * * *
```

Автоматизация загрузки правил маршрутизации

Подключение к локальной сети через три интерфейса.

/etc/iproute2/rt_tables:

```
10 pcompany
11 metrocom
12 peterstar
```

/etc/network/interfaces:

```
# The loopback network interface
auto lo
iface lo inet loopback
    post-up ip route add default scope global nexthop via d.e.f.97 dev eth2
##    post-up ip route add default scope global nexthop via a.b.c.129 dev eth1
    post-up ip route add 10.0.0.0/8 scope global nexthop via a.b.c.129 dev eth1 nexthop via 192.168.43.254
dev eth0
    post-up ip route add 172.16.0.0/12 scope global nexthop via a.b.c.129 dev eth1 nexthop via
192.168.43.254 dev eth0
    post-up ip route add a.b.c.0/25 scope global nexthop via a.b.c.129 dev eth1 nexthop via 192.168.43.254
dev eth0
    post-up ip route add 192.168.0.0/16 scope global nexthop via 192.168.43.254 dev eth0

# pcompany LAN
auto eth0
iface eth0 inet static
    address 192.168.43.201
    netmask 255.255.255.0
    post-up ip rule add from 192.168.43.201 table pcompany
    post-up ip route add default via 192.168.43.254 dev eth1 table pcompany
    post-down ip rule del from 192.168.43.201 table pcompany

# Metrocom internet
auto eth1
iface eth1 inet static
    address a.b.c.201
    netmask 255.255.255.128
    post-up ip rule add from a.b.c.201 table metrocom
    post-up ip route add default via a.b.c.129 dev eth1 table metrocom
    post-down ip rule del from a.b.c.201 table metrocom

# Peterstar internet
auto eth2
iface eth2 inet static
    address d.e.f.98
    netmask 255.255.255.224
    post-up ip rule add from d.e.f.98 table peterstar
    post-up ip route add default via d.e.f.97 dev eth2 table peterstar
    post-down ip rule del from d.e.f.98 table peterstar
```

Транковое подключение к сети

Подключение к локальной сети через транковый порт коммутатора.

Читать: https://wiki.ubuntu.com/vlan

Cisco switch:

```
interface GigabitEthernet8/23
 description LynxTrunk
 switchport
 switchport trunk allowed vlan 10,102,105
 switchport mode trunk
 no ip address
!
```

Устанавливаем поддержку vlan:

```
sudo apt-get install vlan
modprobe 8021q
update-initramfs -u
echo "8021q" >> /etc/modules
```

Маршрутизация через транковое подключение

/etc/iproute2/rt_tables:

```
10 pcompany
11 metrocom
12 peterstar
```

/etc/network/interfaces

```
# The loopback network interface
auto lo
iface lo inet loopback
    pre-up iptables-restore < /etc/iptables.up.rules

# pcompany LAN
auto vlan10
iface vlan10 inet static
    address 192.168.43.202
    netmask 255.255.255.0
    vlan_raw_device eth0
    post-up ip rule add from 192.168.43.202 table pcompany
    post-up ip route add default via 192.168.43.254 dev vlan10 table pcompany
    post-down ip rule del from 192.168.43.202 table pcompany

# Metrocom internet
auto vlan102
iface vlan102 inet static
    address a.b.c.200
    netmask 255.255.255.128
    vlan_raw_device eth0
    post-up ip rule add from a.b.c.200 table metrocom
    post-up ip route add default via a.b.c.129 dev vlan102 table metrocom
    post-down ip rule del from a.b.c.200 table metrocom

# Peterstar internet
auto vlan105
iface vlan105 inet static
    address d.e.f.98
    netmask 255.255.255.224
```

```
    vlan_raw_device eth0
    post-up ip rule add from d.e.f.98 table peterstar
    post-up ip route add default via d.e.f.97 dev vlan105 table peterstar
    post-down ip rule del from d.e.f.98 table peterstar
```

/etc/network/if-up.d/iproute

```
#!/bin/sh
ip route add default scope global nexthop via d.e.f.97 dev vlan105
ip route add 10.0.0.0/8 scope global nexthop via a.b.c.129 dev vlan102 nexthop via 192.168.43.254 dev
vlan10
ip route add 172.16.0.0/12 scope global nexthop via a.b.c.129 dev vlan102 nexthop via 192.168.43.254 dev
vlan10
ip route add a.b.c.0/25 scope global nexthop via a.b.c.129 dev vlan102 nexthop via 192.168.43.254 dev
vlan10
ip route add 192.168.0.0/16 scope global nexthop via 192.168.43.254 dev vlan10
exit 0
```

/etc/network/if-up.d/iproute /etc/iptables.up.rules

```
# Generated by iptables-save v1.4.4 on Tue Mar  1 19:55:24 2011
*filter
:INPUT DROP [953:145880]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2782:995353]
-A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m hashlimit --hashlimit-upto 1/hour --hashlimit-burst
2 --hashlimit-mode srcip --hashlimit-name SSH --hashlimit-htable-expire 60000 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 --tcp-flags SYN,RST,ACK SYN -j DROP
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i vlan10 -j ACCEPT
-A INPUT -i vlan102 -j ACCEPT
-A INPUT -i lo -j ACCEPT
COMMIT
# Completed on Tue Mar  1 19:55:24 2011
```

Фильтр IPTABLES

Фильтрация подключений

Запретить все входящие подключения:
iptables -P INPUT DROP

Принимать только данные, пришедшие в ответ на наши запросы:
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Разрешить входящие подключения SSH:
iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

Из «своих» сетей разрешить все подключения:
iptables -A INPUT -i eth1 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT

Запрет доступа к портам

HTTP:
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 80 -j DROP

Squid:
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 3128 -j DROP

Webmin:
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 10000 -j DROP

Регистрировать попытки неудавшихся подключений:
iptables -A INPUT -i eth0 -j LOG

Некоторые номера портов, используемые сервисами, перечислены в Приложении 1.

Сервис iptables

Отключить файрвол:
chkconfig iptables off
service iptables stop

Автоматизация загрузки правил фильтрации

/etc/network/interfaces:

```
# The loopback network interface
auto lo
iface lo inet loopback
    pre-up iptables-restore < /etc/iptables.up.rules
```

/etc/iptables.up.rules:

```
# Generated by iptables-save v1.4.4 on Wed Dec 22 19:31:23 2010
*filter
:INPUT DROP [3013:198673]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [151022:34811595]
-A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m hashlimit --hashlimit-upto 1/hour --hashlimit-burst
2 --hashlimit-mode srcip --hashlimit-name SSH --hashlimit-htable-expire 60000 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 --tcp-flags SYN,RST,ACK SYN -j DROP
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i eth0 -j ACCEPT
-A INPUT -i eth1 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth2 -j LOG
COMMIT
# Completed on Wed Dec 22 19:31:23 2010
```

RedHat:
system-config-firewall-tui
/etc/sysconfig/iptables

Сетевые сервисы

Сервер имен DNS, BIND

apt-get install bind9

/etc/bind/named.conf.options:

```
acl "trusted" {
   172.16.0/12; 192.168.0/16; 127.0.0.1;
};

options {
        directory "/var/cache/bind";

   allow-query { any; };
   allow-transfer { trusted; };
   allow-recursion { trusted; };

//   forwarders { 8.8.8.8; 8.8.4.4; };

…

};
```

/etc/default/bind9:

```
# startup options for the server
OPTIONS="-4 -u bind"
```

/etc/bind/named.conf – файл конфигурации BIND:

```
include "/etc/bind/named.conf.local";
```

/etc/bind/named.conf.local:

```
zone "wcompany.spb.ru" {
   type master;
   file "/etc/bind/db.wcompany.spb.ru";
};
```

/etc/bind/db.wcompany.spb.ru:

```
$TTL    86400
@       IN      SOA     ns.wcompany.spb.ru. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      ns.wcompany.spb.ru.
@       IN      NS      ns1.wcompany.spb.ru.
ns      IN      A       127.0.0.1
ns1     IN      A       127.0.0.2
@       IN      A       127.0.0.1
www     IN      A       127.0.0.1
```

Чистка кеша, перезапуск сервиса:

rndc flush
rndc reload

iptables -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -j ACCEPT

Конфигурация вторичного DNS-сервера

/etc/bind/named.conf.local:

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "domain.ru" {
        type slave;
        masters {
                a.b.c.195;
                };
        file "/var/lib/bind/domain.ru.hosts";
        };
```

DHCP-сервер

apt-get install dhcp3-server

/etc/dhcp3/dhcpd.conf

```
# pcompany local net 43
subnet 192.168.43.0 netmask 255.255.255.0 {
        option netbios-node-type 8;
        option netbios-name-servers a.b.c.195;
        max-lease-time 864000;
        default-lease-time 86400;
        range 192.168.43.101 192.168.43.199;
        option domain-name-servers a.b.c.195 , a.b.c.194;
        option domain-name "ccompany.ru";
        option routers 192.168.43.254;
        option broadcast-address 192.168.43.255;
        }
```

Резервация адреса:

```
host kubandroid {
        hardware ethernet f8:db:7f:81:33:b6;
        fixed-address 192.168.43.103;
}
```

/etc/default/dhcp3-server

```
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="vlan10"
```

Прокси-сервер, SQUID

apt-get install squid

/etc/squid/squid.conf – конфигурация прокси-сервера

```
###cache_peer 192.168.3.4 parent 8000 0 no-query

# maximum_object_size 4096 KB
maximum_object_size 32768 KB

acl Network10 src 10.10.10.0/24
acl Network43 src 192.168.43.0/24
acl Network3 src 192.168.3.4

http_access allow Network10
http_access allow Network43
http_access allow Network3
http_access deny

forwarded_for off

http_port 192.168.43.4:3128
```

Пуск, останов, обновление конфигурации прокси-сервера:

/etc/init.d/squid start
squid -k reconfigure
/etc/init.d/squid stop

Прозрачное кеширование

/etc/squid/squid.conf:

```
http_port 3128 transparent
```

Перехват HTTP-соединения и направление его на Squid:

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128

Статистика SQUID

apt-get install squid-cgi calamaris sarg
См. webmin.

Lightsquid

```
http://lightsquid.sourceforge.net/
# cat /var/www/lightsquid/doc/install.txt
```

cd /var/www/htdocs/
mkdir lightsquid
cd lightsquid
tar -xzf lightsquid.tgz

chmod +x *.cgi
chmod +x *.pl

chown -R apache:apache *

httpd.conf:

```
<Directory "/var/www/html/lightsquid">
   AddHandler cgi-script .cgi
   AllowOverride All
</Directory>
```

/etc/init.d/apache2 restart

lightsquid.cfg

check-setup.pl

lightparser.pl
./lightparser.pl access.log.1.{gz|bz2}
./lightparser.pl access.log.2.{gz|bz2}
./lightparser.pl access.log.3.{gz|bz2}

http://192.168.0.1/lightsquid/

crontab -e — каждые 20 минут запускать обновление статистики

```
*/20 * * * * /var/www/htdocs/lightsquid/lightparser.pl today
```

! Установить патчи на ошибку 2020 года **!**

Web-сервер Apache2

apt-get install apache2 apache2-utils apache2-doc

AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message

Userdir

https://httpd.apache.org/docs/2.2/mod/mod_userdir.html

/etc/apache2/mods-enabled#
ln -s ../mods-available/userdir.load
ln -s ../mods-available/userdir.conf

/etc/apache2/mods-enabled/userdir.conf:

```
<IfModule mod_userdir.c>
        UserDir public_html
#         UserDir disabled root
        UserDir disabled
        UserDir enabled al

        <Directory /home/*/public_html>
                AllowOverride FileInfo AuthConfig Limit Indexes
                Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
                <Limit GET POST OPTIONS>
                        Order allow,deny
                        Allow from all
                </Limit>
                <LimitExcept GET POST OPTIONS>
                        Order deny,allow
                        Deny from all
                </LimitExcept>
        </Directory>
</IfModule>
```

/etc/init.d/apache2 restart

~/public_html/index.html

```
It works!
```

FTP-сервер, vsftpd

apt-get install vsftpd

/etc/vsftpd.conf
```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
#anonymous_enable=YES
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
...
#
use_localtime=YES
```

TFTPd: tftpd-hpa

apt-get tftpd-hpa

По умолчанию TFTPd стартует с помощью inetd.

/etc/inetd.conf
```
tftp        dgram   udp     wait    root  /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot -c -v -u root
```

Параметр “-c” — возможность записи файлов на сервер.

invoke-rc.d openbsd-inetd restart

Для запуска демона TFTPd самостоятельным процессом:

Закомментировать /etc/inetd.conf
```
# tftp        dgram   udp     wait    root  /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

invoke-rc.d openbsd-inetd restart

Исправить /etc/default/tftpd-hpa
```
#Defaults for tftpd-hpa
RUN_DAEMON="yes"
OPTIONS="-c -l -s /var/lib/tftpboot"
```

invoke-rc.d tftpd-hpa start

NTP – сервер времени

apt-get install ntp

Серверы времени в сети Интернет:
/etc/ntp.conf
```
server ntp.ubuntu.com
server pool.ntp.org
server ntp.vlady.ru
```

Удалённый доступ

Dial-in: доступ через модем

apt-get install mgetty

/etc/mgetty/mgetty.config
```
port ttyS0
 speed 115200
 data-only y
```

mgetty ttyS0

Модем должен ответить на входящий звонок.

Автоматизация запуска и перезапуска демона mgetty

Если система поддерживает инициализацию через inittab:

/etc/inittab:
```
S0:2345:respawn:/sbin/mgetty ttyS0
```

sudo init q

Начиная с версии Ubuntu 6.10 inittab не поддерживается:

/etc/event.d/ttyS0:
```
start on runlevel 2
start on runlevel 3
start on runlevel 4
start on runlevel 5

stop on shutdown

respawn
exec /sbin/mgetty ttyS0
```

initctl list
initctl start ttyS0

PPP

? Дописать !

Доступ к серверу через COM-порт

/etc/mgetty/mgetty.config
```
port ttyS1
 speed 115200
 data-only y
 direct y
```

/etc/event.d/ttyS1:
```
start on runlevel 2
start on runlevel 3
start on runlevel 4
start on runlevel 5

stop on shutdown

respawn
exec /sbin/mgetty 115200 ttyS1
```

Начиная с Ubuntu 9.10:
/etc/init/ttyS1.conf:
```
# ttyS1 - mgetty
start on runlevel [2345]
stop on runlevel [!2345]
respawn
exec /sbin/mgetty ttyS1
```

initctl list
initctl start ttyS1

Подключение через COM-порт

Linux:
apt-get install minicom

adduser login dialout
minicom -s
minicom
minicom -b 9600 -D /dev/ttyS0

Windows:
Hyper-terminal
Если на сервере используется язык, отличный от английского, и на экране отображаются «крокозябры», то после начала сеанса ввести:
LANG=en_US

putty
В свойствах подключения задать кодировку UTF-8, Linux-клавиатура.

VPN-сервер PPTPd

(http://blog.rootshell.be/2008/11/07/iphone-linux-vpn/)

apt-get install pptpd bcrelay

/etc/pptpd.conf – какие адреса выдавать удалённому клиенту
localip 192.168.0.1
remoteip 192.168.0.234-238,192.168.0.245

/etc/ppp/pptpd-options — клиент будет использовать этот сервер DNS
ms-dns 192.168.0.1

/etc/ppp/chap-secrets – имена и пароли клиентов, фиксированный адрес клиента
user_login pptpd user_password *
user1 pptpd passwd1 192.168.0.200

Разрешить доступ извне к VPN-серверу — порт TCP:1723 и протокол GRE(47):
iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
iptables -A INPUT -i eth0 -p 47 -j ACCEPT

На маршрутизаторе должен быть прописан маршрут в сеть 192.168.0.0/24, иначе – NAT клиентам:
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j SNAT --to d.e.f.99
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -j SNAT --to 192.168.43.4
Или так:
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE

Разрешить доступ клиенту с фиксированным адресом только к определенному сервису в сети:
iptables -A FORWARD -s 192.168.0.200 -p tcp -m tcp -d 192.168.81.91 --dport 3389 -j ACCEPT
iptables -A FORWARD -s 192.168.0.200 -j DROP

Перезапуск демона:
/etc/init.d/pptpd restart
service pptpd restart

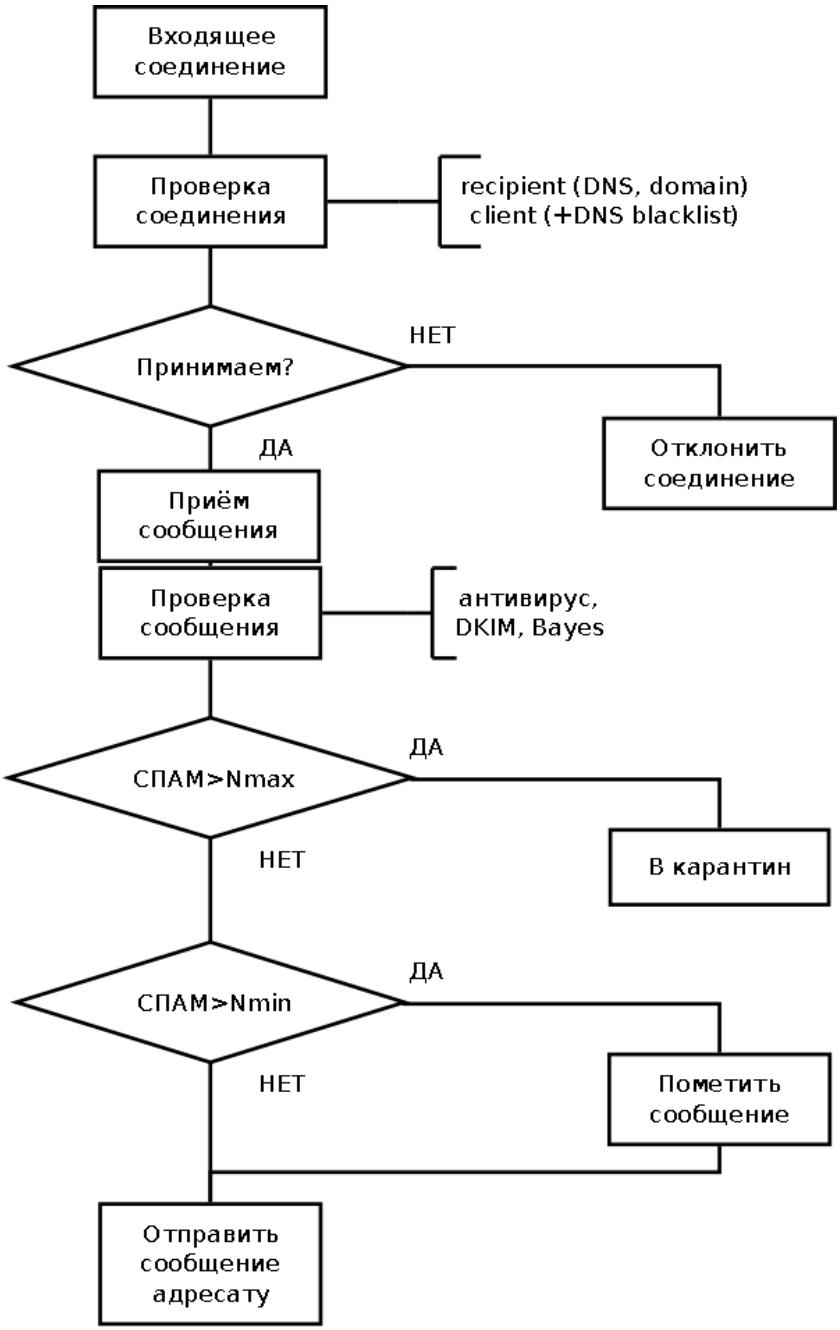
Диагностика:
ps ax | grep pptpd
tail -f /var/log/daemon.log
netstat -anp | grep pptpd
lsmod | grep ^ppp

Почтовый сервер

Разрешение имён

Настроить DNS, получить результат:
hostname -f
`alice.ccompany.ru`

Схема прохождения входящих писем



Postfix — почтовый шлюз

Установка

tasksel
Выбрать роль ”почтовый сервер”
или
apt-get install postfix
dpkg-reconfigure postfix
Выбрать конфигурацию сервера ”internet-site”, полное имя сервера, получатель сообщений для root и postmaster, свои домены, сетевые адреса, с которых разрешено принимать почту.

Ключи postconf

-e 'key=value' – изменить значение параметра в файле конфигурации main.cf
-n – показать значения конфигурации, отличающиеся от значений по умолчанию

Файлы конфигурации Postfix

Дописать:
/etc/postfix/*
main.cf
master.cf

main.cf

```
# SOFT BOUNCE
soft_bounce = no

# INTERNET HOST AND DOMAIN NAMES
myhostname = mx.domain.tld
mydomain = domain.tld

# SENDING MAIL
myorigin = $myhostname

# RECEIVING MAIL
inet_interfaces = all

mydestination = $myhostname, localhost.$mydomain,
localhost

# CONTENT FILTERING
# CLIENT RESTRICTIONS

#HELO
smtpd_helo_required = yes
```

DNS-имя почтового шлюза
DNS-имя почтового домена

Каким именем представляться другим серверам при отправке

С каких интерфейсов принимать почту[1]
Для кого принимать почту

1 *inet_interfaces* defines which IPs (and ergo interfaces) postfix RECEIVES mail on.
This can be overridden per-service by providing the desired IP in the master.cf service definition.
smtp_bind_address defines which IP postfix uses to SEND mail.
This can be overridden for any outgoing smtp(8) transport.

```
smtpd_helo_restrictions =
```

Проверка HELO. От каких хостов можно принимать почту

```
    reject_invalid_hostname,
    permit_mynetworks,
    check_helo_access
hash:/etc/postfix/helo_access,
```

Список имён и адресов хостов, с которых можно или нельзя принимать почту

```
    reject_non_fqdn_hostname,
    permit

#MAIL FROM
smtpd_sender_restrictions =
```

Проверка MAIL FROM. От каких отправителей можно пересылать почту

```
    regexp:/etc/postfix/sender_deny,
```

Разрешение или запрет на отправку

```
    permit_sasl_authenticated,
    permit_mynetworks,
    regexp:/etc/postfix/sender_access,
```

Разрешение или запрет на отправку

```
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    permit

#RCPT TO
smtpd_recipient_restrictions =
```

Проверка RCPT TO. Для каких получателей можно принимать почту

```
    permit_mynetworks,
    reject_unauth_destination,
    reject_non_fqdn_recipient,
    check_policy_service inet:127.0.0.1:10023,
    permit

smtpd_client_restrictions =
```

От каких отправителей можно пересылать почту

```
    permit_mynetworks,
    regexp:/etc/postfix/client_access,
```

Разрешение или запрет на отправку

```
    regexp:/etc/postfix/dul_checks,
    reject_rbl_client bl.spamcop.net,
    reject_rbl_client cbl.abuseat.org,
#   reject_rbl_client spamsources.fabel.dk,
    reject_rbl_client dul.ru,
    reject_rbl_client dialup.blacklist.jippg.org,
#    reject_rbl_client relays.mail-abuse.org,

# TRUST AND RELAY CONTROL
mynetworks = 172.16.250.23/32, 85.172.9.83/32,
127.0.0.0/8, 192.168.201.195/32
relay_domains = hash:/etc/postfix/relay_domains
```

Список разрешённых хостов-отправителей
Для каких почтовых доменов принимать почту

```
# INTERNET OR INTRANET
transport_maps = hash:/etc/postfix/transport
```

На какие серверы внутри

сети пересылать входящие сообщения

```
# REJECTING UNKNOWN RELAY USERS
relay_recipient_maps =
hash:/etc/postfix/relay_recipients
```

Список почтовых адресов, для которых принимать почту

```
# ALIAS DATABASE
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

Правила подмены адресов

```
# JUNK MAIL CONTROLS
#header_checks = regexp:/etc/postfix/header_checks

# SHOW SOFTWARE VERSION OR NOT
smtpd_banner = $myhostname ESMTP

sender_bcc_maps=hash:/etc/postfix/sender_bcc
```

Дублирование исходящих писем

```
recipient_bcc_maps=hash:/etc/postfix/recipient_bcc
```

Дублирование входящих писем

```
softwaremessage_size_limit = 20480000
```

Ограничение на размер пересылаемых писем

```
message_size_limit = 20480000
```

Приём почты

/etc/postfix/main.cf:
(имя хоста, для каких доменов принимать почту, с каких адресов сообщения принимать)
myhostname = alice.ccompany.ru
mydestination = alice.ccompany.ru, localhost.ccompany.ru, localhost, wcompany.spb.ru
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

/etc/init.d/postfix reload
postconf

Postfix SMTP relay and access control

http://www.postfix.org/SMTPD_ACCESS_README.html

The table below summarizes the purpose of each SMTP access restriction list. All lists use the exact same syntax; they differ only in the time of evaluation and in the effect of a REJECT or DEFER result.

Restriction list name	Version	Status	Effect of REJECT or DEFER result
smtpd_client_restrictions	All	Optional	Reject all client commands
smtpd_helo_restrictions	All	Optional	Reject HELO/EHLO information
smtpd_sender_restrictions	All	Optional	Reject MAIL FROM information
smtpd_relay_restrictions	≥ 2.10	Required if smtpd_recipient_restrictions	Reject RCPT TO information

		does not enforce relay policy	
	< 2.10	Not available	
smtpd_recipient_restrictions	≥ 2.10	Required if smtpd_relay_restrictions does not enforce relay policy	Reject RCPT TO information
	< 2.10	Required	
smtpd_data_restrictions	≥ 2.0	Optional	Reject DATA command
smtpd_end_of_data_restrictions	≥ 2.2	Optional	Reject END-OF-DATA command
smtpd_etrn_restrictions	All	Optional	Reject ETRN command

The order of evaluation is:

smtpd_client_restrictions
smtpd_helo_restrictions
smtpd_sender restrictions
smtpd_recipient_restrictions
smtpd_data_restrictions

DNS Blacklist

/etc/postfix/main.cf:

```
smtpd_client_restrictions =
 permit_mynetworks
 permit_sasl_authenticated
 check_client_access hash:/etc/postfix/access.cf
 reject_rbl_client cbl.abuseat.org
 reject_rbl_client bl.spamcop.net
 reject_rbl_client zen.spamhaus.org
 permit
```

/etc/postfix/access.cf:

```
127.0.0.1 OK
1.2.3.4 REJECT
```

postmap /etc/postfix/access.cf
/etc/init.d/postfix {restart | reload}

Пересылка почты с MX на основной сервер

/etc/postfix/main.cf:

```
relay_domains = hash:/etc/postfix/relay_domains.cf
transport_maps = hash:/etc/postfix/transport.cf
smtpd_recipient_restrictions = reject_unknown_sender_domain, reject_unknown_recipient_domain,
reject_unauth_pipelining, permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination,
permit_mx_backup
```

/etc/postfix/relay_domains.cf – для каких доменов пересылать почту

```
gcompany.ru OK
net.gcompany.ru OK
ccompany.ru OK
c-company.ru OK
ocompany.ru OK
ncompany.ru OK
ghcompany.ru OK
```

postmap relay_domains.cf

/etc/postfix/transport.cf – куда пересылать почту для доменов

```
gcompany.ru     smtp:[a.b.c.4]
ccompany.ru     smtp:[a.b.c.194]
c-company.ru    smtp:[a.b.c.194]
net.gcompany.ru         smtp:[a.b.c.194]
ocompany.ru     smtp:[a.b.c.194]
ncompany.ru     smtp:[a.b.c.194]
ghcompany.ru    smtp:[a.b.c.194]
```

postmap transport.cf

Ограничить количество одновременных исходящих подключений на один адрес.
/etc/postfix/main.cf:

```
default_destination_concurrency_limit = 10
```

/etc/init.d/postfix reload

Очередь сообщений SMTP

mailq

```
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
00FD7B299      2358 Wed Dec  1 17:09:26  fuser@yandex.ru
              (connect to a.b.c.194[a.b.c.194]:25: Connection refused)
                                         al@ccompany.ru

-- 2 Kbytes in 1 Request.
```

postqueue -f
postsuper -d -

Почтовые рассылки

/etc/aliases:

```
postmaster: root
clamav: root
root: al
```

newaliases

Фильтрация почты

Установка пакетов

apt-get install amavisd-new spamassassin clamav-daemon
apt-get install dkim-filter python-policyd-spf
apt-get install pyzor razor
apt-get install arj cabextract cpio lha nomarch pax rar unrar unzip zip

ClamAV

Антивирус должен иметь права доступа к файлам, создаваемым, amavis.
adduser clamav amavis

Обновление базы антивируса:
/etc/clamav/freshclam.conf:
HTTPProxyServer serveraddress
HTTPProxyPort portnumber

freshclam

/etc/init.d/clamav-daemon start
/etc/init.d/clamav-daemon restart

Spamassassin

Spamassassin сам обнаружит модули razor и pyzor.

Разрешить работу spamassassin:
/etc/default/spamassassin
ENABLED=1

/etc/init.d/spamassassin start

Обучение Spamassassin для начала работы Bayes-фильтра:
sa-learn --spam ~path/spams
sa-learn --ham ~path/hams

База spamassassin: /var/lib/amavis/.spamassassin/*

Amavisd-new

/etc/amavis/conf.d/15-content_filter_mode:

```
# Default antivirus checking mode
# Uncomment the two lines below to enable it
@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);

# Default SPAM checking mode
# Uncomment the two lines below to enable it
@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);
```

Удалять полученный спам.
/etc/amavis/conf.d/20-debian_defaults:
$final_virus_destiny   = D_DISCARD; # (data not lost, see virus quarantine)

$final_banned_destiny = ~~D_BOUNCE~~ **D_REJECT**; # D_REJECT when front-end MTA
$final_spam_destiny = ~~D_BOUNCE~~ **D_DISCARD**;
$final_bad_header_destiny = D_PASS; # False-positive prone (for spam)

Что считать спамом:
/etc/amavis/conf.d/20-debian_defaults:

$sa_spam_subject_tag = '***SPAM*** ';
$sa_tag_level_deflt = 2.0; # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.31; # add 'spam detected' headers at that level
$sa_kill_level_deflt = ~~6.31~~ **9.31**; # triggers spam evasive actions
$sa_dsn_cutoff_level = 10; # spam level beyond which a DSN is not sent

Уведомление администратора:
/etc/amavis/conf.d/21-ubuntu_defaults:

$virus_admin = "postmaster\@$mydomain";
$spam_admin = "postmaster\@$mydomain";

/etc/amavis/conf.d/50-user:

$myhostname = 'alice.ccompany.ru';
@local_domains_acl = ("alice.ccompany.ru", "wcompany.spb.ru", "gcompany.ru", "net.gcompany.ru", "ccompany.ru", "c-company.ru", "ocompany.ru", "ncompany.ru", "ghcompany.ru");

/etc/init.d/amavis restart

?Что хранится в базе?
Dec 28 18:21:08 lynx amavis[25401]: Creating db in /var/lib/amavis/db/; BerkeleyDB 0.39, libdb 4.8

DKIM Whitelist

/etc/amavis/conf.d/40-policy_banks

There are multiple ways to configure the Whitelist for a domain:
'example.com' => 'WHITELIST',: will whitelist any address from the "example.com" domain.
'.example.com' => 'WHITELIST',: will whitelist any address from any subdomains of "example.com" that have a valid signature.
'.example.com/@example.com' => 'WHITELIST',: will whitelist subdomains of "example.com" that use the signature of example.com the parent domain.
'./@example.com' => 'WHITELIST',: adds addresses that have a valid signature from "example.com". This is usually used for discussion groups that sign thier messages.

/etc/amavis/conf.d/40-policy_banks:

'nic.ru' => 'WHITELIST',

##/etc/amavis/conf.d/20-debian_defaults:
/etc/amavis/conf.d/21-ubuntu_defaults:

$enable_dkim_verification = 1;

/etc/init.d/amavis restart

Если нужен просто белый список, то надо раскомментировать
#read_hash(\%whitelist_sender, '/etc/amavis/conf.d/whitelist');
и заполнить файл whitelist
Белый список надо заполнять доменами без @
mail.ru;
yandex.ru

Подключение фильтра к Postfix

postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'

/etc/postfix/master.cf
Добавить:

```
smtp-amavis     unix    -       -       -       -       2       smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20
127.0.0.1:10025 inet    n       -       -       -       -       smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Добавить:

```
pickup    fifo  n       -       -       60      1       pickup
    -o content_filter=
    -o receive_override_options=no_header_body_checks
```

/etc/init.d/postfix reload
/etc/init.d/postfix restart

Карантин

Amavis помещает отфильтрованные сообщения в /var/lib/amavis/virusmails/
Разблокировка письма, попавшего в карантин, и доставка его адресату:
amavisd-release *message-id*

Удаление из карантина сообщений старше 30 дней:
find /var/lib/amavis/virusmails/ -type f -mtime +30 -delete

Отладка

Amavisd-new: /var/log/mail.log
/etc/amavis/conf.d/50-user (1..5)

```
$log_level = 2;
```

/etc/init.d/amavis restart

ClamAV: /var/log/clamav/clamav.log
/etc/clamav/clamd.conf

LogVerbose true

/etc/init.d/clamav-daemon restart

amavisd-nanny – мониторинг загрузки процессов amavisd
Количество исполняемых копий amavisd — руководство по настройке:
zcat /usr/share/doc/amavisd-new/README.performance.gz | less

/etc/postfix/master.cf
smtp-amavis unix - - - - **N** smtp
...
/etc/amavis/conf.d/50-user
$max_servers = **N**;

/etc/init.d/amavis restart
/etc/init.d/postfix reload

Тестирование подключения

Открыть необходимые порты на файрволе.

telnet 192.168.43.4 25

```
Trying 192.168.43.4...
Connected to 192.168.43.4.
Escape character is '^]'.
220 zorba.ccompany.ru ESMTP Postfix (Ubuntu)
helo alex
250 zorba.ccompany.ru
mail from:<fuser@yandex.ru>
250 2.1.0 Ok
rcpt to:<al@ccompany.ru>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: hello
test
.
250 2.0.0 Ok: queued as 4910112E6E8
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Импорт списка почтовых адресов из Active Directory

Получение из AD списка почтовых адресов пользователей на примере ccompany.ru.

Каждый час в hh:30 запускать скрипт
crontab:

```
30 *  * * * /etc/scripts/adusers.sh
```

aduser.sh:

```
#!/bin/sh
cd /etc/scripts
cp -f recipients.list recipients.old
rm recipients.list

/etc/scripts/adusers.pl

LINES=`wc -l recipients.list | awk '{print $1}'`
if test "$LINES" = "0" ; then
cp recipients.old recipients.list
echo "DCs are not accessible. Recipients list was not updated." | mail -s "DC access error"
postmaster@ccompany.ru
fi

/usr/bin/tr "[:lower:]" "[:upper:]" < recipients.list|uniq|sort >recipients.cf

cat << EOF >> recipients.cf
@gcompany.ru OK

EOF

cp -f recipients.cf /etc/postfix/recipients.cf
/usr/sbin/postmap /etc/postfix/recipients.cf
```

Также будет приняты сообщения для любых адресов в почтовом домене gcompany.ru.

Формируется список /etc/postfix/recipients.cf следующего вида:

```
ABUSE@ccompany.RU OK
...
@gcompany.ru OK
```

К контроллерам домена обращается скрипт adusers.pl:

```
#!/usr/bin/perl -T -w

# This script will pull all users' SMTP addresses from your Active Directory
# (including primary and secondary email addresses) and list them in the
# format "user@example.com OK" which Postfix uses with relay_recipient_maps.
# Be sure to double-check the path to perl above.

# This requires Net::LDAP to be installed.  To install Net::LDAP, at a shell
# type "perl -MCPAN -e shell" and then "install Net::LDAP"

use Net::LDAP;
use Net::LDAP::Control::Paged;
use Net::LDAP::Constant ( "LDAP_CONTROL_PAGED" );

# Enter the path/file for the output
$VALID = "/etc/scripts/recipients.list";
open VALID, ">$VALID" or die "CANNOT OPEN $VALID $!";

# Enter the FQDN of your Active Directory domain controllers below
```

```
$dc1="altair.ccompany.ru";
$dc2="exsrv.ccompany.ru";

# Enter the LDAP container for your userbase.
# The syntax is CN=Users,dc=example,dc=com
# This can be found by installing the Windows 2000 Support Tools
# then running ADSI Edit.
# In ADSI Edit, expand the "Domain NC [domaincontroller1.example.com]" &
# you will see, for example, DC=example,DC=com (this is your base).
# The Users Container will be specified in the right pane as
# CN=Users depending on your schema (this is your container).
# You can double-check this by clicking "Properties" of your user
# folder in ADSI Edit and examining the "Path" value, such as:
# LDAP://domaincontroller1.example.com/CN=Users,DC=example,DC=com
# which would be $hqbase="cn=Users,dc=example,dc=com"
# Note:  You can also use just $hqbase="dc=example,dc=com"
$hqbase="dc=ccompany,dc=ru";

# Enter the username & password for a valid user in your Active Directory
# with username in the form cn=username,cn=Users,dc=example,dc=com
# Make sure the user's password does not expire.  Note that this user
# does not require any special privileges.
# You can double-check this by clicking "Properties" of your user in
# ADSI Edit and examining the "Path" value, such as:
# LDAP://domaincontroller1.example.com/CN=user,CN=Users,DC=example,DC=com
# which would be $user="cn=user,cn=Users,dc=example,dc=com"
# Note: You can also use the UPN login: "user\@example.com"
$user="test\@ccompany.ru";
$passwd="testpasswordhere";

# Connecting to Active Directory domain controllers
$noldapserver=0;
$ldap = Net::LDAP->new($dc1) or
  $noldapserver=1;
if ($noldapserver == 1)  {
  $ldap = Net::LDAP->new($dc2) or
    die "Error connecting to specified domain controllers $@ \n";
}

$mesg = $ldap->bind ( dn => $user,
                password =>$passwd);
if ( $mesg->code()) {
   die ("error:", $mesg->error_text((),"\n"));
}

# How many LDAP query results to grab for each paged round
# Set to under 1000 for Active Directory
$page = Net::LDAP::Control::Paged->new( size => 990 );

@args = ( base     => $hqbase,
# Play around with this to grab objects such as Contacts, Public Folders, etc.
# A minimal filter for just users with email would be:
filter => "(&(sAMAccountName=*)(mail=*))",
#         filter => "(& (mailnickname=*) (| (&(objectCategory=person)
#                   (objectClass=user)(!(homeMDB=*))(!(msExchHomeServerName=*)))
#                   (&(objectCategory=person)(objectClass=user)(|(homeMDB=*)
#                   (msExchHomeServerName=*))) ))",
         control  => [ $page ],
         attrs  => "proxyAddresses",
);
```

```
my $cookie;
while(1) {
  # Perform search
  my $mesg = $ldap->search( @args );

# Filtering results for proxyAddresses attributes
  foreach my $entry ( $mesg->entries ) {
    my $name = $entry->get_value( "cn" );
    # LDAP Attributes are multi-valued, so we have to print each one.
    foreach my $mail ( $entry->get_value( "proxyAddresses" ) ) {
     # Test if the Line starts with one of the following lines:
     # proxyAddresses: [smtp|SMTP]:
     # and also discard this starting string, so that $mail is only the
     # address without any other characters...
     if ( $mail =~ s/^(smtp|SMTP)://gs ) {
       print VALID $mail." OK\n";
     }
    }
  }

  # Only continue on LDAP_SUCCESS
  $mesg->code and last;

  # Get cookie from paged control
  my($resp)  = $mesg->control( LDAP_CONTROL_PAGED ) or last;
  $cookie    = $resp->cookie or last;

  # Set cookie in paged control
  $page->cookie($cookie);
}

if ($cookie) {
  # We had an abnormal exit, so let the server know we do not want any more
  $page->cookie($cookie);
  $page->size(0);
  $ldap->search( @args );
  # Also would be a good idea to die unhappily and inform OP at this point
     die("LDAP query unsuccessful");
}
# Add additional restrictions, users, etc. to the output file below.
#print VALID "user\@domain1.com OK\n";
#print VALID "user\@domain2.com 550 User unknown.\n";
#print VALID "domain3.com 550 User does not exist.\n";

close VALID;
```

Postfix принимает и пересылает почту только для известных получателей:

main.cf:

```
relay_domains = hash:/etc/postfix/relay_domains.cf
relay_recipient_maps = hash:/etc/postfix/recipients.cf
transport_maps = hash:/etc/postfix/transport.cf
```

SMTP-аутентификация пользователей

1. Configure Postfix for SMTP-AUTH using SASL (Dovecot SASL):

postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth-client'
postconf -e 'smtpd_sasl_local_domain ='
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
postconf -e 'inet_interfaces = all'

2. Сгенерировать ключ и сертификат для почтового сервера

3. Configure Postfix to provide TLS encryption for both incoming and outgoing mail:

postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/mailserver.key'
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/mailserver.crt'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'myhostname = alice.ccompany.ru'

4. If you are using your own Certificate Authority to sign the certificate enter:
sudo postconf -e 'smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem'

/etc/postfix/main.cf:

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete
# version

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

myhostname = server1.example.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = server1.example.com, localhost.example.com, localhost
relayhost =
mynetworks = 127.0.0.0/8
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
smtpd_sasl_local_domain =
```

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject _unauth_destination
smtpd_tls_auth_only = no
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/ssl/private/smtpd.key
smtpd_tls_cert_file = /etc/ssl/certs/smtpd.crt
smtpd_tls_CAfile = /etc/ssl/certs/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

/etc/init.d/postfix restart

Конфигурация SASL

Postfix supports two SASL implementations Cyrus SASL and Dovecot SASL. To enable Dovecot SASL the dovecot-common package will need to be installed. From a terminal prompt enter the following:

sudo apt-get install dovecot-common

Next you will need to edit /etc/dovecot/dovecot.conf. In the auth default section uncomment the socket listen option and change the following:

```
 socket listen {
   #master {
     # Master socket provides access to userdb information. It's typically
     # used to give Dovecot's local delivery agent access to userdb so it
     # can find mailbox locations.
     #path = /var/run/dovecot/auth-master
     #mode = 0600
     # Default user/group is the one who started dovecot-auth (root)
     #user =
     #group =
   #}
   client {
     # The client socket is generally safe to export to everyone. Typical use
     # is to export it to your SMTP server so it can do SMTP AUTH lookups
     # using it.
     path = /var/spool/postfix/private/auth-client
     mode = 0660
     user = postfix
     group = postfix
   }
 }
```

In order to let Outlook clients use SMTPAUTH, in the auth default section of /etc/dovecot/dovecot.conf add "login":

```
 mechanisms = plain login
```

Once you have Dovecot configured restart it with:
sudo /etc/init.d/dovecot restart

Postfix-Dovecot

Another option for configuring Postfix for SMTP-AUTH is using the dovecot-postfix package. This package will install Dovecot and configure Postfix to use it for both SASL authentication and as a Mail Delivery Agent

(MDA). The package also configures Dovecot for IMAP, IMAPS, POP3, and POP3S.

You may or may not want to run IMAP, IMAPS, POP3, or POP3S on your mail server. For example, if you are configuring your server to be a mail gateway, spam/virus filter, etc. If this is the case it may be easier to use the above commands to configure Postfix for SMTPAUTH.

To install the package, from a terminal prompt enter:
apt-get install dovecot-postfix

You should now have a working mail server, but there are a few options that you may wish to further customize. For example, the package uses the certificate and key from the ssl-cert package, and in a production environment you should use a certificate and key generated for the host. See the section called “Certificates” for more details.

Once you have a customized certificate and key for the host, change the following options in /etc/postfix/main.cf:
smtpd_tls_cert_file = /etc/ssl/certs/ssl-mail.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-mail.key

Then restart Postfix:
sudo /etc/init.d/postfix restart

Dovecot – доставка почты пользователям

Установка Dovecot

apt-get install dovecot-imapd dovecot-pop3d

Конфигурация Dovecot

/etc/dovecot/dovecot.conf

```
# Протоколы
protocols = pop3 pop3s imap imaps
```

/etc/init.d/dovecot restart

Конфигурация SSL-подключений

/etc/dovecot/dovecot.conf

```
# Файлы сертификата и ключа
ssl_cert_file = /etc/ssl/certs/mailserver.crt
ssl_key_file = /etc/ssl/private/mailserver.key
# Пароль к файлу с ключем сертификата
ssl_key_password = key_password
#ssl_disable = no
#disable_plaintext_auth = no
```

Ошибки dovecot

http://wiki.dovecot.org/TimeMovedBackwards

syslog:

```
Apr 15 17:37:48 mail dovecot: dovecot: Fatal: Time just moved backwards by 6
seconds. This might cause a lot of problems, so I'll just kill myself now.
http://wiki.dovecot.org/TimeMovedBackwards
```

После чего dovecot падает.

Чтобы не происходило скачков времени, нужно на почтовом сервере с установленным dovecot настроить ntp и не использовать ntpdate.

Самоподписанные сертификаты

openssl genrsa -des3 -out mailserver.key 1024
openssl req -new -key mailserver.key -out mailserver.csr
openssl x509 -req -days 365 -in mailserver.csr -signkey mailserver.key -out mailserver.crt
cp mailserver.crt /etc/ssl/certs
cp mailserver.key /etc/ssl/private

Запомнить key_password — он нужен для работы.

Ubuntu 10.04

PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
dropping root privileges, so keep the key file unreadable by anyone but
root.
#ssl_cert_file = /etc/ssl/certs/dovecot.pem
#ssl_key_file = /etc/ssl/private/dovecot.pem

Ubuntu 16.04

/etc/dovecot/conf.d/10-ssl.conf

PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
dropping root privileges, so keep the key file unreadable by anyone but
root. Included doc/mkcert.sh can be used to easily generate self-signed
certificate, just make sure to update the domains in dovecot-openssl.cnf
#ssl_cert = </etc/dovecot/dovecot.pem
#ssl_key = </etc/dovecot/private/dovecot.pem
ssl_cert = </etc/dovecot/dovecot.pem
ssl_key = </etc/dovecot/private/dovecot.pem

/usr/lib/dovecot/ doc/mkcert.sh

Доступ к серверу

Открыть необходимые порты на файрволе.
Разрешить доступ к портам:
25 (SMTP)
110, 995 (POP3, POP3S)
143, 993 (IMAP, IMAPS)

iptables -A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 110 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 995 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 143 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 993 -j ACCEPT

Проверка сервера

https://mxtoolbox.com/diagnostic.aspx – Online SMTP diagnostics tool

Пересылка входящих писем

~/.forward:
\localmbox
mbox@remote.domain

См. формат файла .forward

aliases

Вид почтового ящика MBOX/Maildir

По умолчанию postfix и dovecot используют тип ящиков mbox.

Изменить вид ящика на Maildir:
postconf -e 'home_mailbox = Maildir/'

/etc/dovecot/dovecot.conf
mail_location = maildir:~/Maildir # (for maildir)
#mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u # (for mbox)

Вид почтового ящика Dovecot должен совпадать с настройкой Postfix.

Перезапустить сервисы postfix и dovecot.

Настройки консольного почтового клиента mutt – см. в документе «Настройки рабочего стола Linux».

Web-интерфейс к почтовому серверу (Squirrelmail)

Установка

apt-get install squirrelmail
squirrelmail-configure

Конфигурация Apache

cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available/squirrelmail
ln -s /etc/apache2/sites-available/squirrelmail /etc/apache2/sites-enabled/squirrelmail
/etc/init.d/apache2 force-reload

http://localhost/squirrelmail

Устранение неисправностей

Восстановление загрузчика GRUB

GRUB (первая версия)

sudo grub
find /boot/grub/stage1
root (hd0,6)
setup (hd0)
quit

GRUB 2

mount /dev/sdb1 /mnt/boot
grub-install --root-directory=/mnt /dev/sdb

nomodeset

/etc/default/grub:

GRUB_CMDLINE_LINUX_DEFAULT="nomodeset"
GRUB_TERMINAL=console

update-grub

Свободное место на диске

http://eduard.kozachek.net/blog/it/shamanism/no-space-left-on-device-%D0%BD%D0%B0-%D0%BF%D0%BE%D0%BB%D1%83%D0%BF%D1%83%D1%81%D1%82%D0%BE%D0%BC-%D0%B4%D0%B8%D1%81%D0%BA%D0%B5/

```
dpkg: error processing /var/cache/apt/archives/linux-image-2.6.32-70-generic-
pae_2.6.32-70.137_i386.deb (--unpack):
 unable to create `/lib/modules/2.6.32-70-generic-
pae/kernel/drivers/power/bq27x00_battery.ko.dpkg-new' (while processing
`./lib/modules/2.6.32-70-generic-pae/kernel/drivers/power/bq27x00_battery.ko'):
No space left on device
No apport report written because the error message indicates a disk full error
dpkg-deb: subprocess paste killed by signal (Broken pipe)
```

df [-h]

```
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1              7688360   5600348   1697460  77% /
none                    508780       168    508612   1% /dev
none                    513008         0    513008   0% /dev/shm
none                    513008        56    512952   1% /var/run
none                    513008         0    513008   0% /var/lock
none                    513008         0    513008   0% /lib/init/rw
```

df -i

```
Filesystem            Inodes   IUsed   IFree IUse% Mounted on
/dev/sda1             488640  487177    1463  100% /
none                  127195     590  126605    1% /dev
none                  128252       1  128251    1% /dev/shm
none                  128252      33  128219    1% /var/run
none                  128252       1  128251    1% /var/lock
none                  128252       1  128251    1% /lib/init/rw
```

Решение проблемы некорректного GPG-ключа в Ubuntu

http://www.propheta.ru/2009/02/w-gpg-error-httpaudi.html

При обновлении списка доступных пакетов может случиться такая ошибка:

```
W: GPG error: http://mirror.ubuntu.com hardy-updates Release: The following
signatures were invalid: BADSIG 40976EAF437D05B5 Ubuntu Archive Automatic
Signing Key <ftpmaster@ubuntu.com>
W: You may want to run apt-get update to correct these problems
```

Решение:
apt-get update -o Acquire::http::No-Cache=True

Кеш пакетов

sudo mkdir -p /var/cache/apt/archives/partial
sudo touch /var/cache/apt/archives/lock
sudo chmod 640 /var/cache/apt/archives/lock

Removing this directory manually is a bad idea generally. To clean archives cleanly, use:
sudo apt-get clean

apt-get -f install

Обслуживание сервера

Резервное копирование файлов

Локальный архив

tar -cvzf /tmp/`hostname`-`date +%y%m%d`.tgz /etc/. /var/lib/bind/. /var/lib/dhcp3/. /var/spool/cron/.

/* - все файлы в каталоге, кроме скрытых
/. - все файлы, включая скрытые (содержат «.» в начале имени)

Передача файлов через SSH

Архивирование запускается на удалённом хосте, архив сохраняется в локальный файл:
ssh -24C -i/root/.ssh/id_dsa remote_user@remote_ip "tar -cvz /etc/. /var/spool/cron/. /root/. /home/." | dd of=/tmp/*servername*-`date +%y%m%d`.tgz

Архивирование локальных файлов с записью на удалённый хост:
tar -cvz /etc/. /var/spool/cron/. /root/. /home/. | ssh -24C -i/root/.ssh/id_dsa remote_user@remote_ip "dd of=/tmp/*servername*-`date +%y%m%d`.tgz"

(Пайпы — это просто :-)

SCP

scp -24 -i/root/.ssh/id_dsa /local/file remote_ip:/remote/folder/

Файл копируется на удалённый хост.

Rsync синхронизация с сервером

Синхронизация по протоколу ssh:
rsync -av --delete --force /local/folder/ remote_user@remote_ip:/remote/folder

Дописать:
Синхронизация по протоколу rsync

```
Access via remote shell:
  Pull: rsync [OPTION...] [USER@]HOST:SRC... [DEST]
  Push: rsync [OPTION...] SRC... [USER@]HOST:DEST

Access via rsync daemon:
  Pull: rsync [OPTION...] [USER@]HOST::SRC... [DEST]
        rsync [OPTION...] rsync://[USER@]HOST[:PORT]/SRC... [DEST]
  Push: rsync [OPTION...] SRC... [USER@]HOST::DEST
        rsync [OPTION...] SRC... rsync://[USER@]HOST[:PORT]/DEST
```

Netcat

Дописать:

```
nc [-46CDdhklnrStUuvz] [-I length] [-i interval] [-O length]
   [-P proxy_username] [-p source_port] [-s source] [-T toskeyword]
   [-V rtable] [-w timeout] [-X proxy_protocol] [-x proxy_address[:port]]
   [destination] [port]
```

Приложение 1. Номера портов для доступа к сервисам

Без защиты данных		Данные защищены шифрованием			
		SSL/TLS		Другое	
udp/69	TFTP				
udp/161,162	SNMP v1, 2 agent / server				
tcp/udp 514	Syslog	6514	Syslog-TLS		
udp/68	DHCP/BOOTP				
tcp/43	whois				
tcp/udp 53	DNS				
udp/123	NTP				
tcp/23	Telnet	992/tcp 992/udp	telnets	tcp/22	SSH/SCP/SFTP
tcp/513	Rlogin				
tcp/21,20	FTP control/data	990, 991	FTPS		
tcp/80	HTTP	443	HTTPS		
tcp/25	SMTP	465	SSMTP, SMTPS, SMTP-TLS/SSL	587	SMTP submission STARTTLS
tcp/110	POP3	995	POP3S		
tcp/143	IMAP	585	IMAP4-SSL		
		993	IMAPS		
tcp/119	NNTP	563	NNTPS		
tcp/5222	XMPP	5223	XMPP-SSL		
				tcp/udp 5190	ICQ
p7 icmp	ICMP				
p47 gre	GRE				
tcp/1723	pptp				
p50 esp, p51 ah	ESP/AH IPSec				
udp/500,4500 tcp/10000	IKE IPSec Cisco VPN				
tcp/389	LDAP	636 tcp	LDAPS		
tcp/1719,1720	H.323 RAS/Trunk				
tcp/udp 5060	SIP	5061 t/u	SIPS		
				5900 tcp	VNC
				4899 tcp	Remote Administrator
				3389 tcp	MS RDP
tcp/873	rsync				

Приложение 2. Литература

1. SSH Mastery. OpenSSH, PuTTY, Tunnels and Keys by Michael W Lucas.
2. UNIX and Linux System Administration Handbook by Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley. (Есть перевод на русский язык)
3. The Debian Administrator's Handbook. Debian Squeeze from Discovery to Mastery by Raphaël Hertzog and Roland Mas.
4. Official Ubuntu Documentation, https://help.ubuntu.com
5. Unix Toolbox, http://cb.vu/unixtoolbox.xhtml
6. Time Management for System Administrators by Thomas A. Limoncelli. (Есть перевод на русский язык)
7. The Practice of System and Network Administration by Thomas A. Limoncelli, Christina J. Hogan, Strata R. Chalup. (Есть перевод на русский язык)
8. The UNIX Programming Environment by Brian W. Kernighan, Rob Pike (Есть перевод на русский язык)
9. Debian 7: System Administration Best Practices by Rich Pinkall Pollei
10. Ubuntu Linux TOOLBOX. 1000+ Commands for Ubuntu and Deblan Power Users by Christopher Negus & Francois Caen. (Есть перевод на русский язык)
11.

Приложение 3. Файловые системы

ext3

inodes

https://en.wikipedia.org/wiki/Ext3

The maximum number of inodes (and hence the maximum number of files and directories) is set when the file system is created. If V is the volume size in bytes, then the default number of inodes is given by V/2^13 (or the number of blocks, whichever is less), and the minimum by V/2^23. The default was deemed sufficient for most applications. The max number of subdirectories in one directory is fixed to 32000.

Реальный сервер:

```
# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1              7688360   2934824   4362984  41% /
none                    508780       168    508612   1% /dev
none                    513008         0    513008   0% /dev/shm
none                    513008        60    512948   1% /var/run
none                    513008         0    513008   0% /var/lock
none                    513008         0    513008   0% /lib/init/rw
none                   7688360   2934824   4362984  41%
/var/lib/ureadahead/debugfs

# df -i
Filesystem            Inodes   IUsed   IFree IUse% Mounted on
/dev/sda1             488640  152566  336074   32% /
none                  127195     587  126608    1% /dev
none                  128252       1  128251    1% /dev/shm
none                  128252      34  128218    1% /var/run
none                  128252       1  128251    1% /var/lock
none                  128252       1  128251    1% /lib/init/rw
none                  488640  152566  336074   32% /var/lib/ureadahead/debugfs
```

8 GB размер диска
2^13 = 8192
1 block = 1K = 2 x 512-byte sectors

8G / 8192 / 2 = 524288 inodes

После записи на диск большого количества «мелких» файлов inodes закончились раньше, чем свободное место на диске.

Приложение 4. Новое оглавление

I. НАЧАЛО
Установка системы
Выбор приложений
После первой загрузки

II. ОКРУЖЕНИЕ
shell
горячие клавиши
мышь
консольные мультиплексоры
man
vi

III. БЕЗОПАСНОСТЬ
Пользователи
su, sudo, visudo
ssh

IV. СЕТЬ
Подключение к сети
Маршрутизация

V. УСТАНОВКА ПРОГРАММ
Источники приложений
Обновление системы
Установка приложений

VI. ЕЩЁ БОЛЬШЕ СЕТЕВЫХ НАСТРОЕК
Файрвол
VLAN, Trunking
Расширенная маршрутизация
Удалённый доступ VPN

VII. МОНИТОРИНГ
Производительность сервера
Оборудование
Nagios

ОБСЛУЖИВАНИЕ СЕРВЕРА
Резервное копирование

VIII. СЕРВЕРНЫЕ ПРИЛОЖЕНИЯ
Сервисы DNS, DHCP, NTP etc.
Прокси-сервер
Почтовый сервер
Файловый сервер
Web-сервер
FTP-сервер