CentOS 7. Установка пакета iRedMail (MySQL, OpenLDAP, Postfix, Dovecot, Amavisd, Roundcube Webmail, Fail2Ban) и интеграция с Windows 2008 R2 AD.

IredMail, пакет который содержит необходимый набор для создания почтовой системы. Для меня из него представляет интерес Postfix, Dovecot, Amavisd и интеграция этого безобразия с контроллером домена на базе Windows 2008 R2 AD (так уж было заведено и хотелось иметь единую авторизацию).
Подразумеваем, что система уже установлена, один сетевой интерфейс смотрит в мир, второй смотрит в локальную сеть. Для машины было установлено mail.mx.ob.ru имя домена. В зоне доменов прописаны записи типа A, CN, MX, для домена mail.mx.ob.ru, mx.ob.ru и ob.ru

Установим необходимые репозитарии и наборы пакетов для полноценного запуска и работы с системой в будущем.

Репозитарий RPMforge (в нем много готовых пакетов и утилит):

rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
rpm -i http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el7.rf.x86_64.rpm

Необходимые пакеты (содержат много библиотек и зависимостей для установки и компиляции других пакетов в будущем):

yum groupinstall "Development Tools"

Проверяем вывод (FQDN) для hostname:

hostname -f

Должно вывести:

mx.ob.ru

Если вывод отличается, необходимо файл /etc/sysconfig/network привести к виду:

mail.mx.ob.ru

Содержимое файла /etc/hosts привести к виду:

127.0.0.1   mail.mx.ob.ru mx.ob.ru mx mail localhost localhost.localdomain

Отключаем SELinux. Редактируем файл /etc/selinux/config и устанавливаем:

SELINUX=disabled

Перезагружаем сервер.

Процесс установки пакета iRedMail.

Выкачиваем последнюю версию пакета iRedMail с сайта:

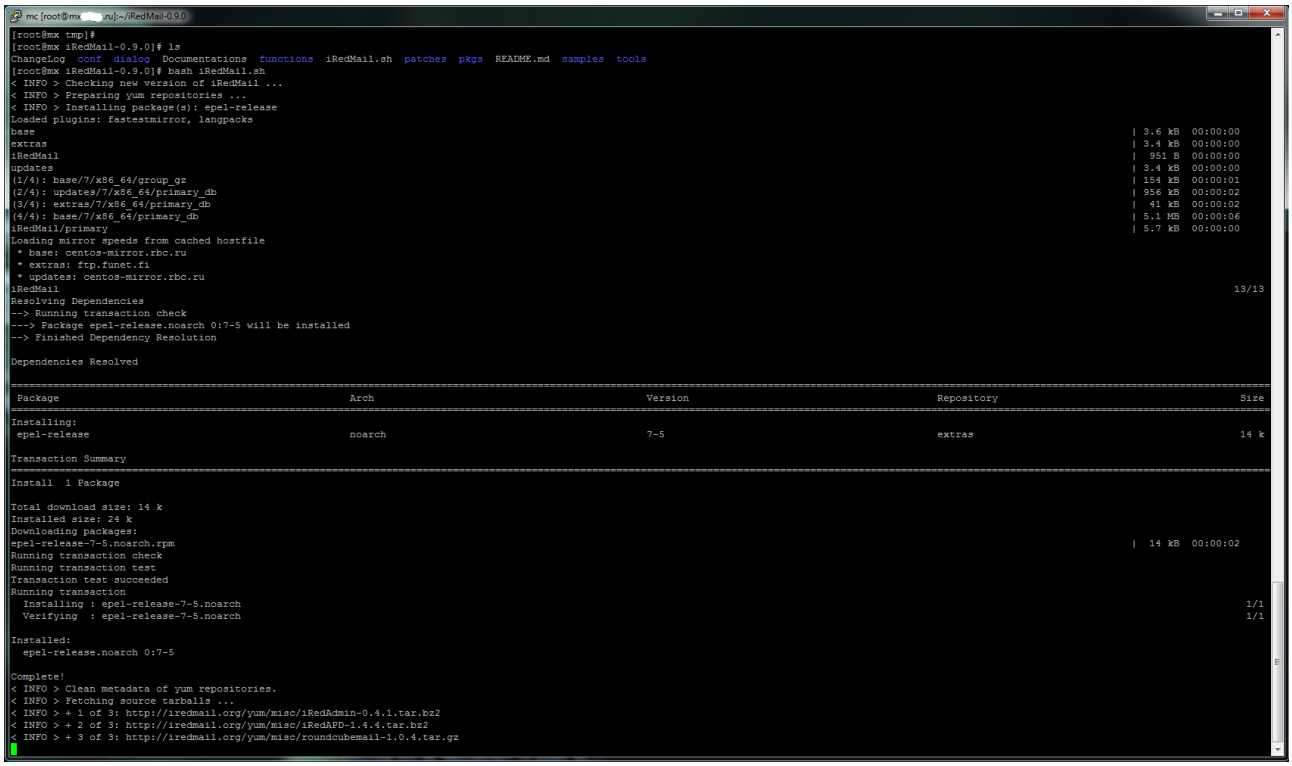
wget https://bitbucket.org/zhb/iredmail/downloads/iRedMail-0.9.0.tar.bz2

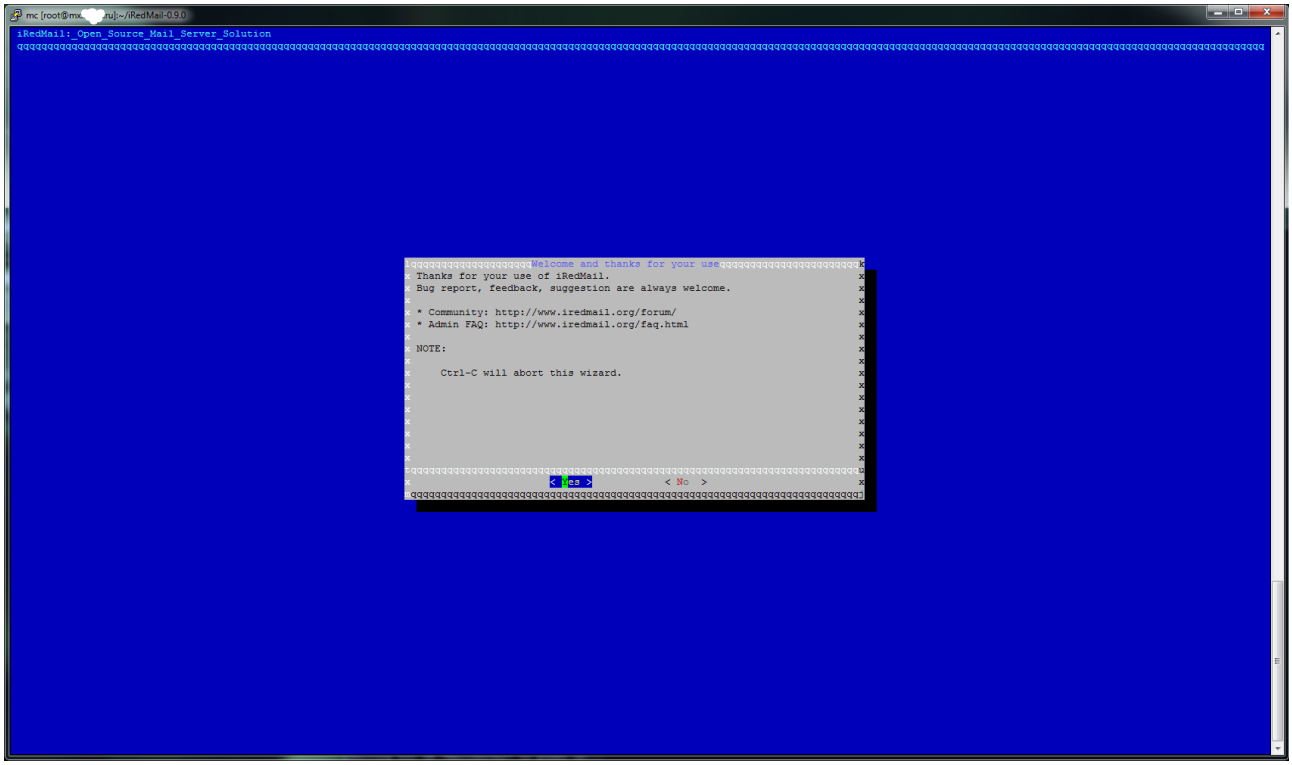
tar xjf iRedMail-0.9.0.tar.bz2

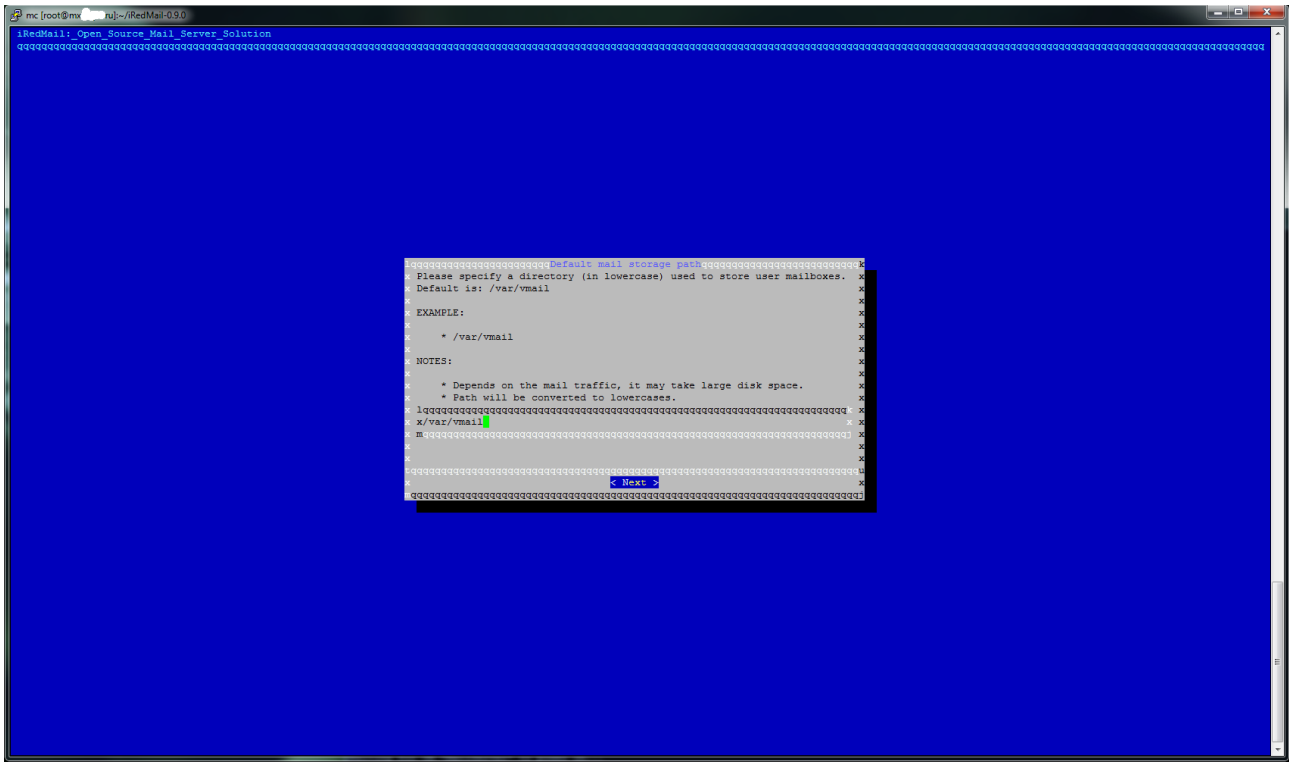
Запускаем установку:

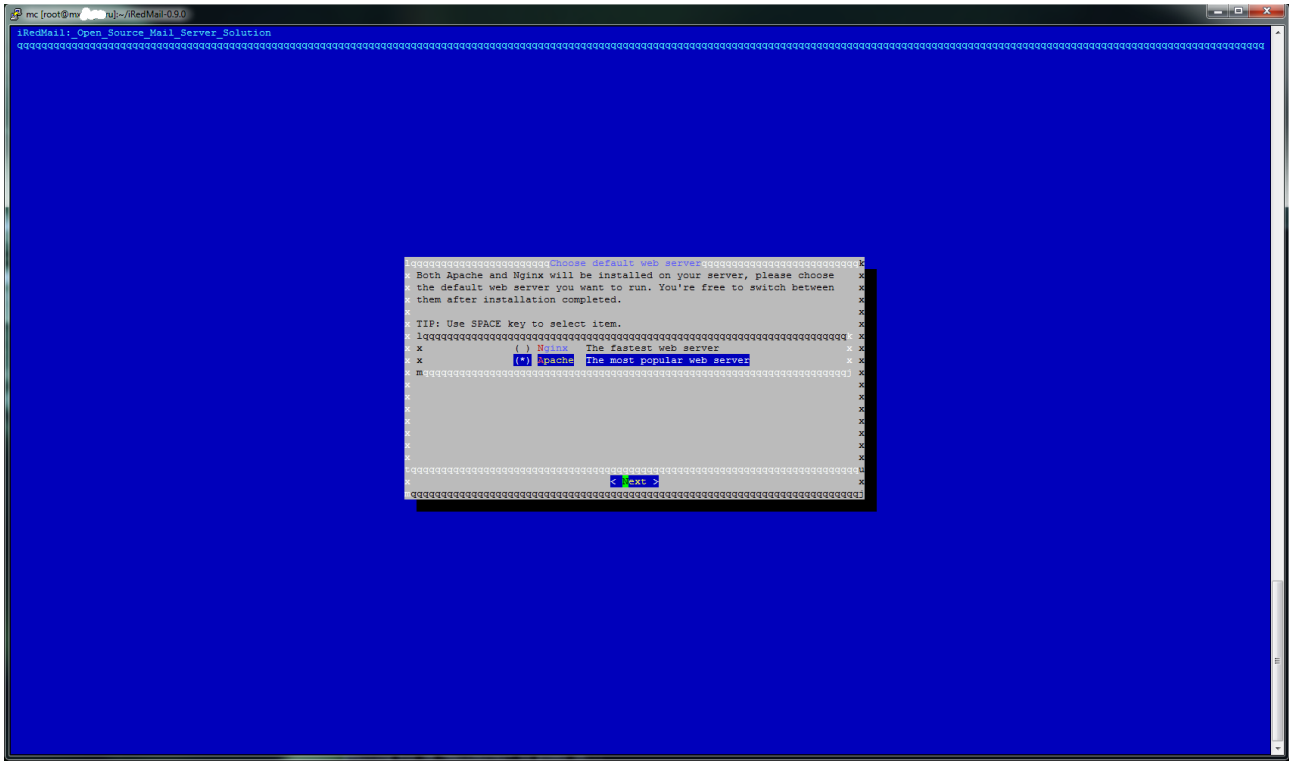
bash iRedMail.sh

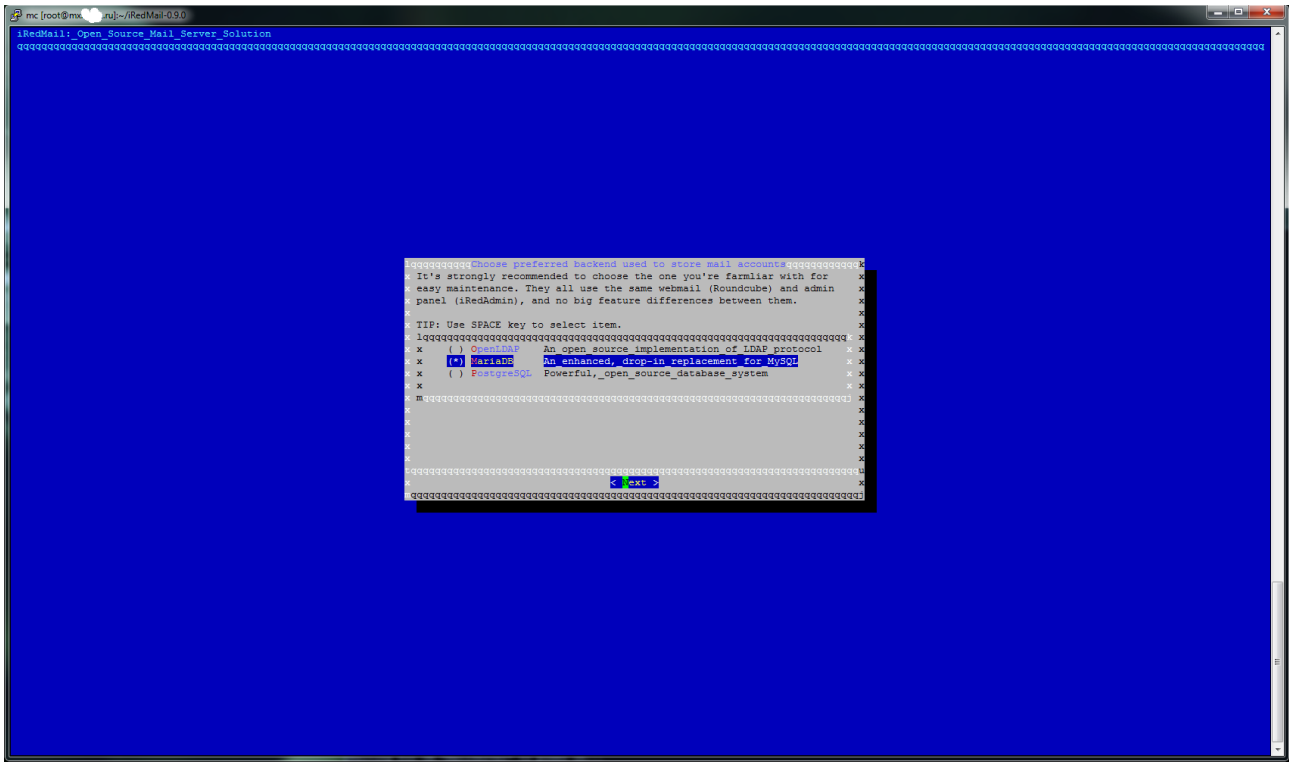
Вид процесса установки:

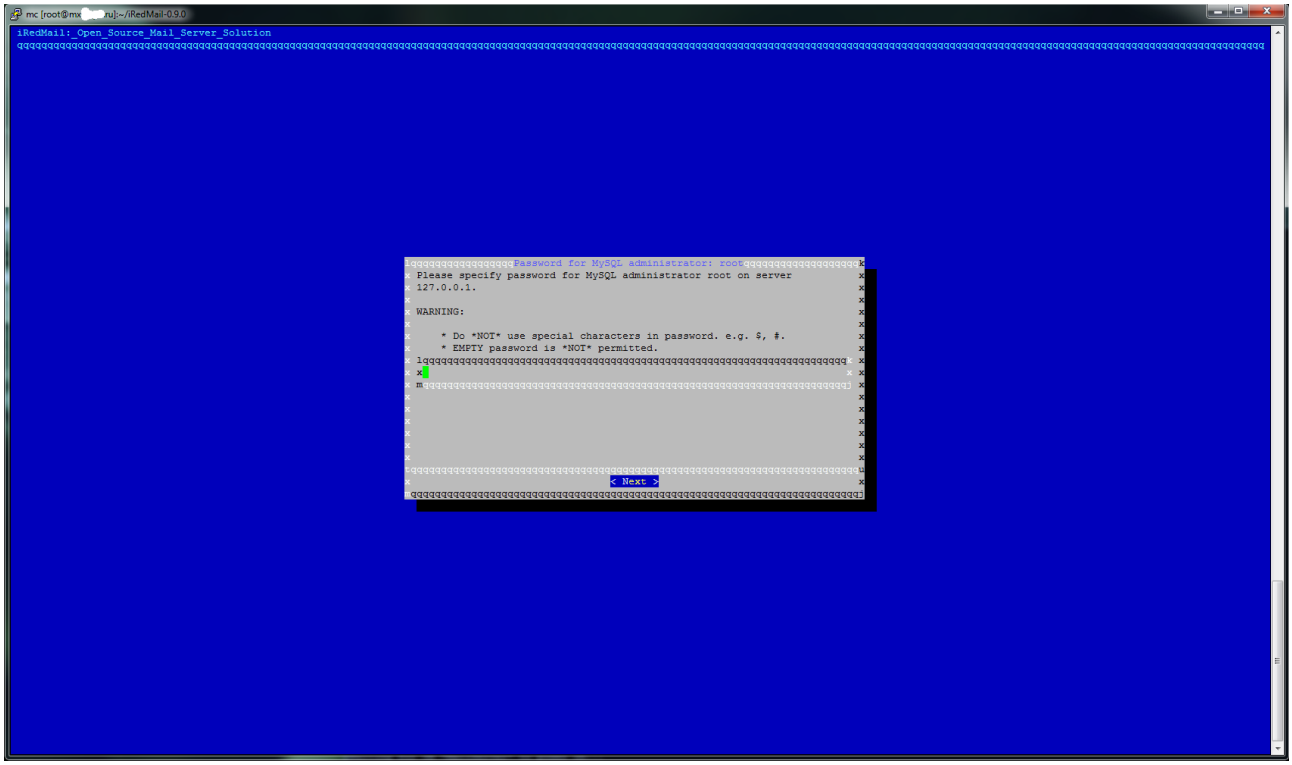


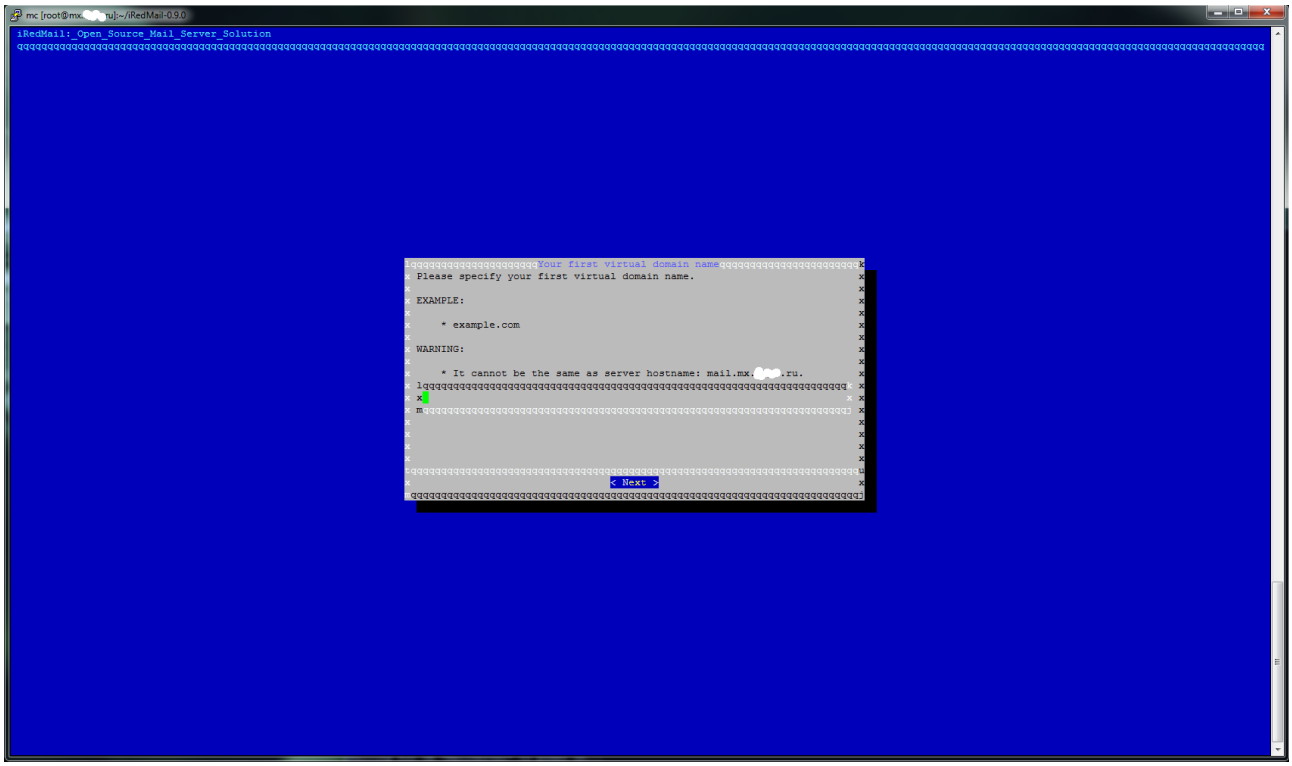


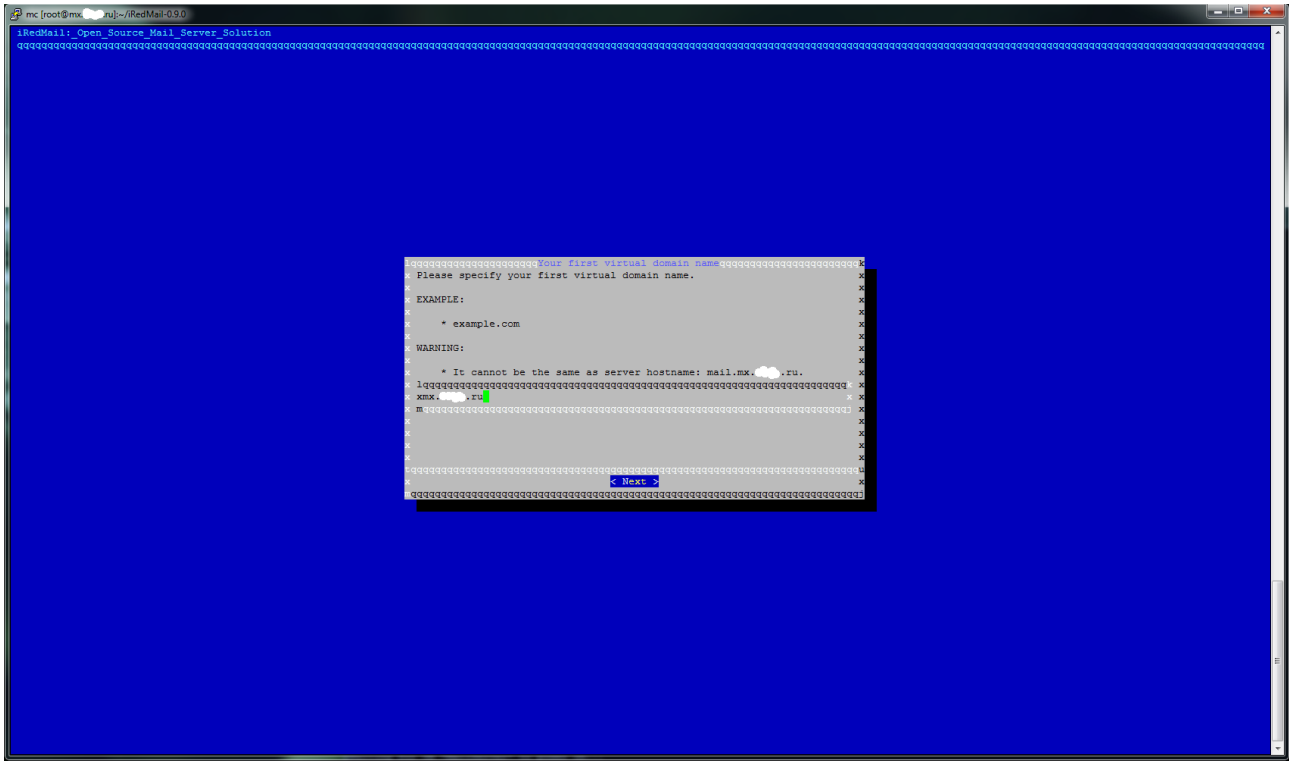

mc [root@mx ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Default mail storage path
Please specify a directory (in lowercase) used to store user mailboxes.
Default is: /var/vmail
EXAMPLE:
* /var/vmail
NOTES:
* Depends on the mail traffic, it may take large disk space.
* Path will be converted to lowercases.
/var/vmail
< Next >

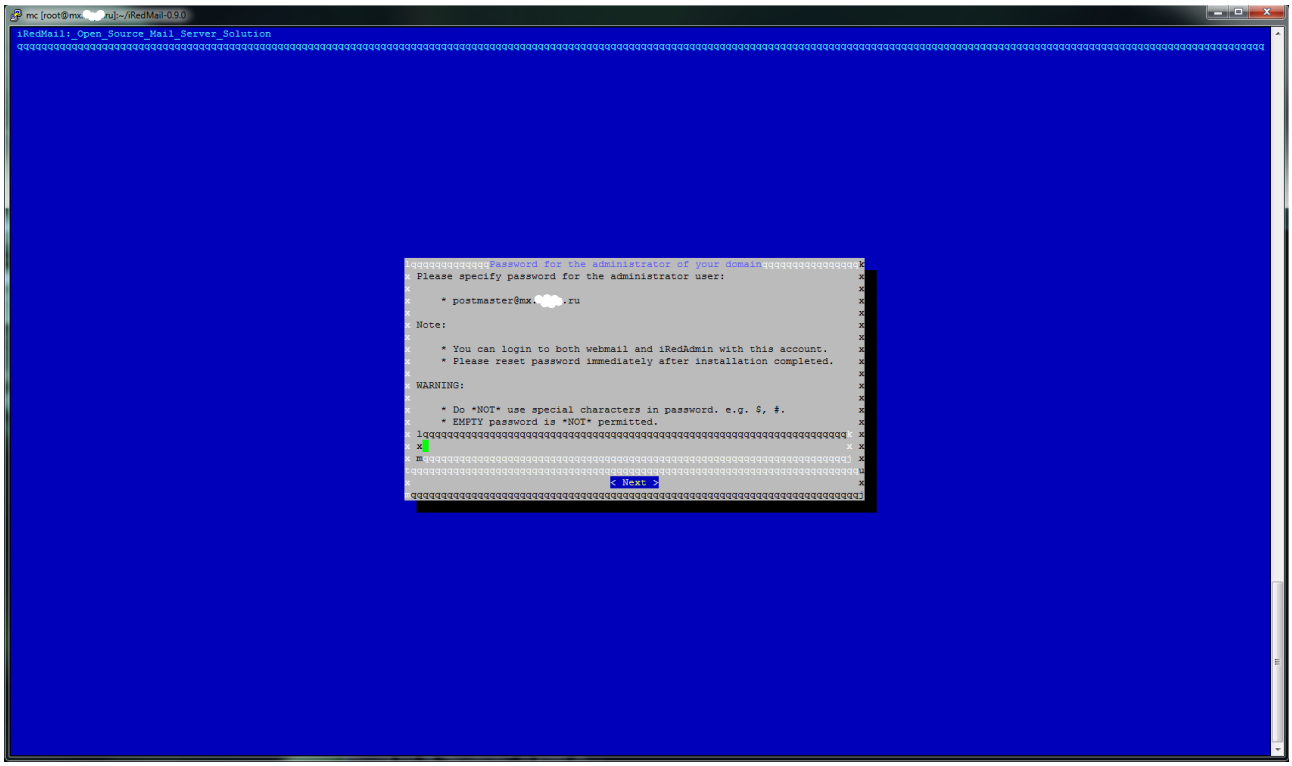

mc [root@mx ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Choose default web server
Both Apache and Nginx will be installed on your server, please choose
the default web server you want to run. You're free to switch between
them after installation completed.
TIP: Use SPACE key to select item.
( ) Nginx The fastest web server
(*) Apache The most popular web server
< Next >

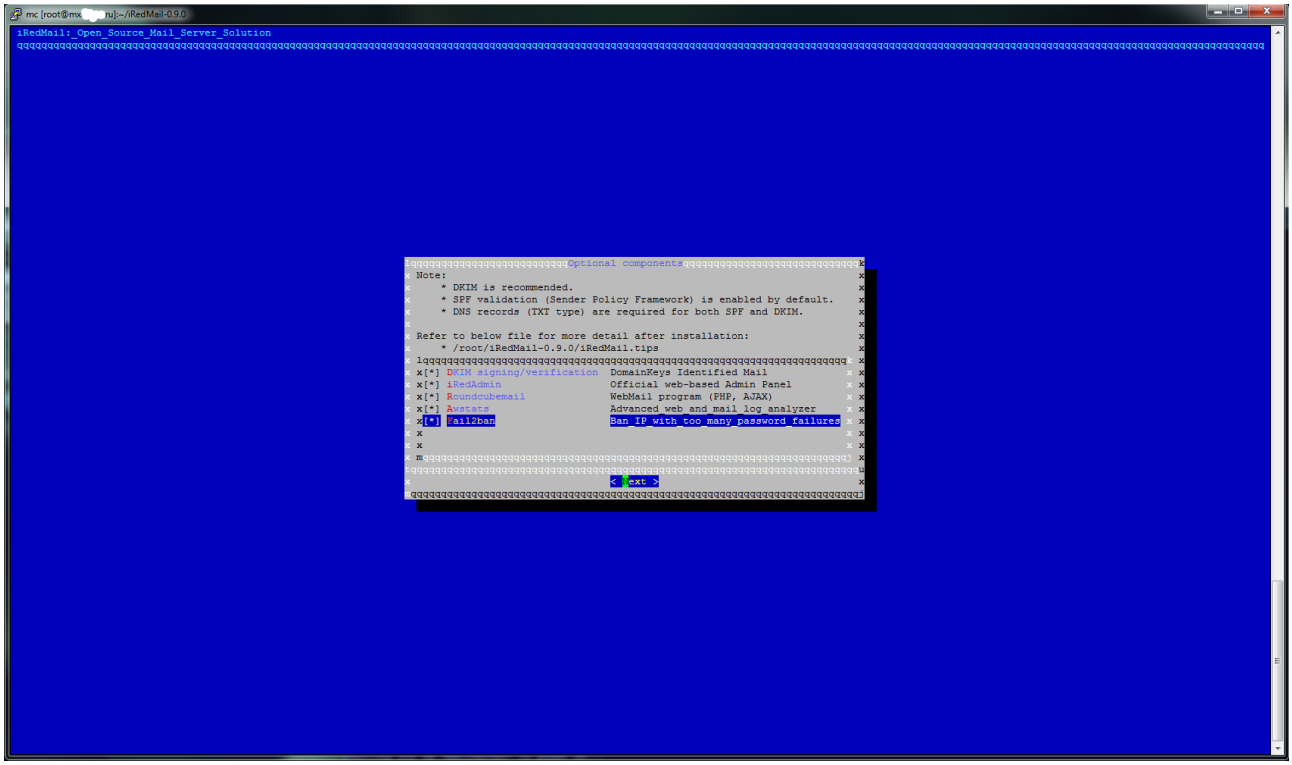

mc [root@mx ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Choose preferred backend used to store mail accounts
It's strongly recommended to choose the one you're farmliar with for easy maintenance. They all use the same webmail (Roundcube) and admin panel (iRedAdmin), and no big feature differences between them.
TIP: Use SPACE key to select item.
( ) OpenLDAP An open source implementation of LDAP protocol
(*) MariaDB An enhanced, drop-in replacement for MySQL
( ) PostgreSQL Powerful, open source database system
< Next >

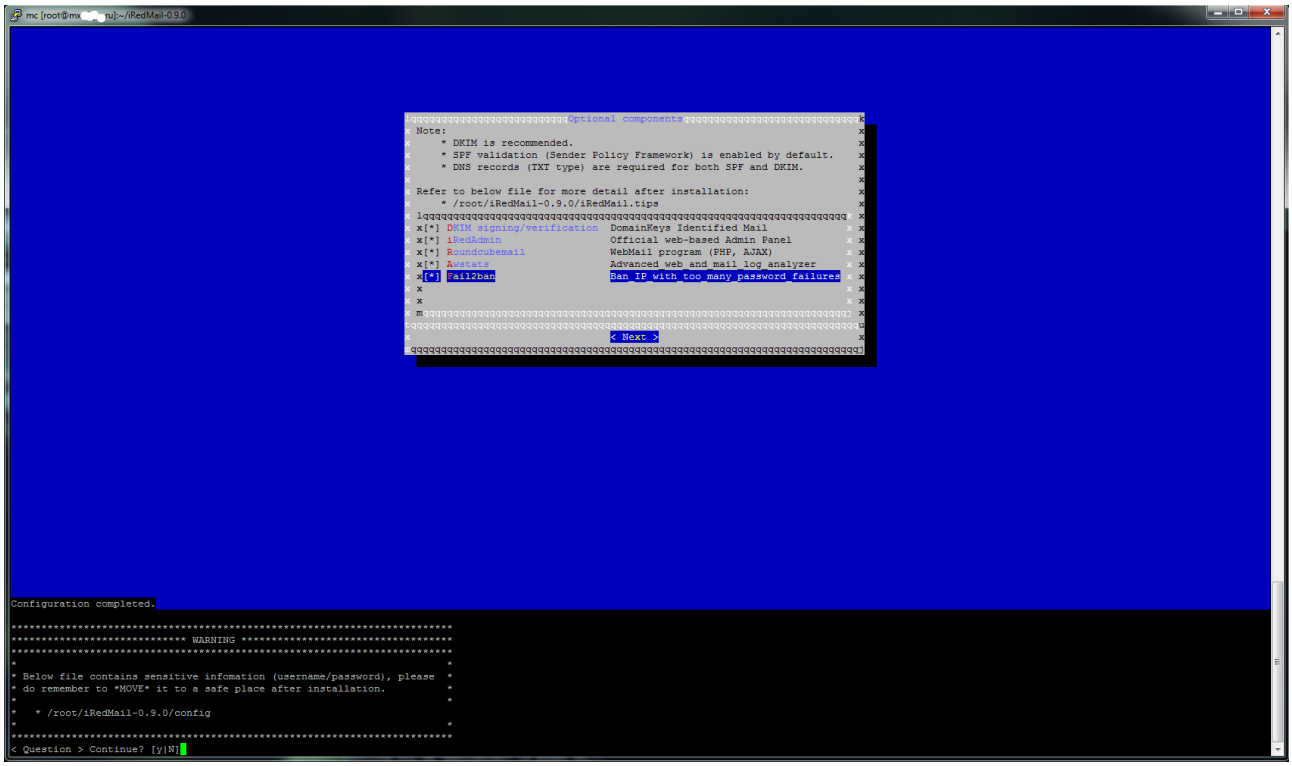

mc [root@mx ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Password for MySQL administrator: root
Please specify password for MySQL administrator root on server 127.0.0.1.
WARNING:
* Do *NOT* use special characters in password. e.g. $, #.
* EMPTY password is *NOT* permitted.
< Next >

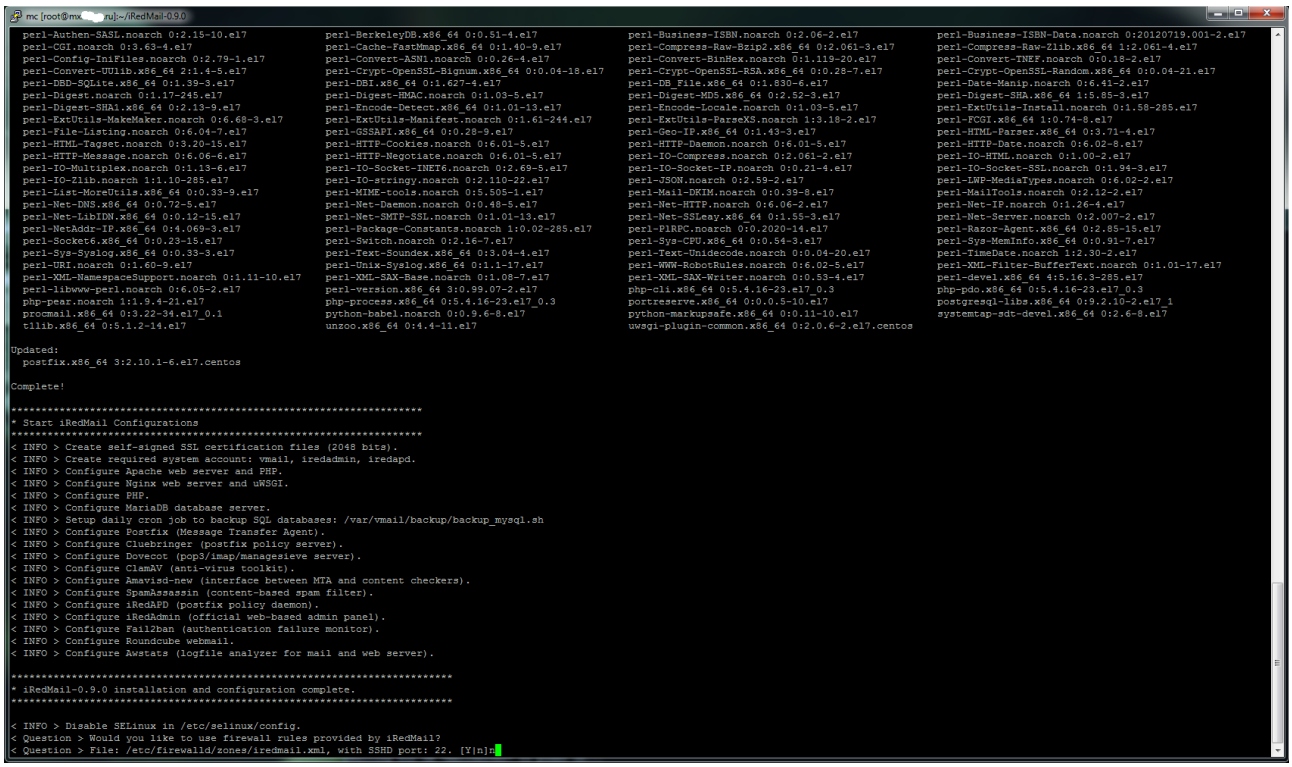

mc [root@mx[redacted]ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Your first virtual domain name
Please specify your first virtual domain name.
EXAMPLE:
* example.com
WARNING:
* It cannot be the same as server hostname: mail.mx.[redacted].ru.
< Next >

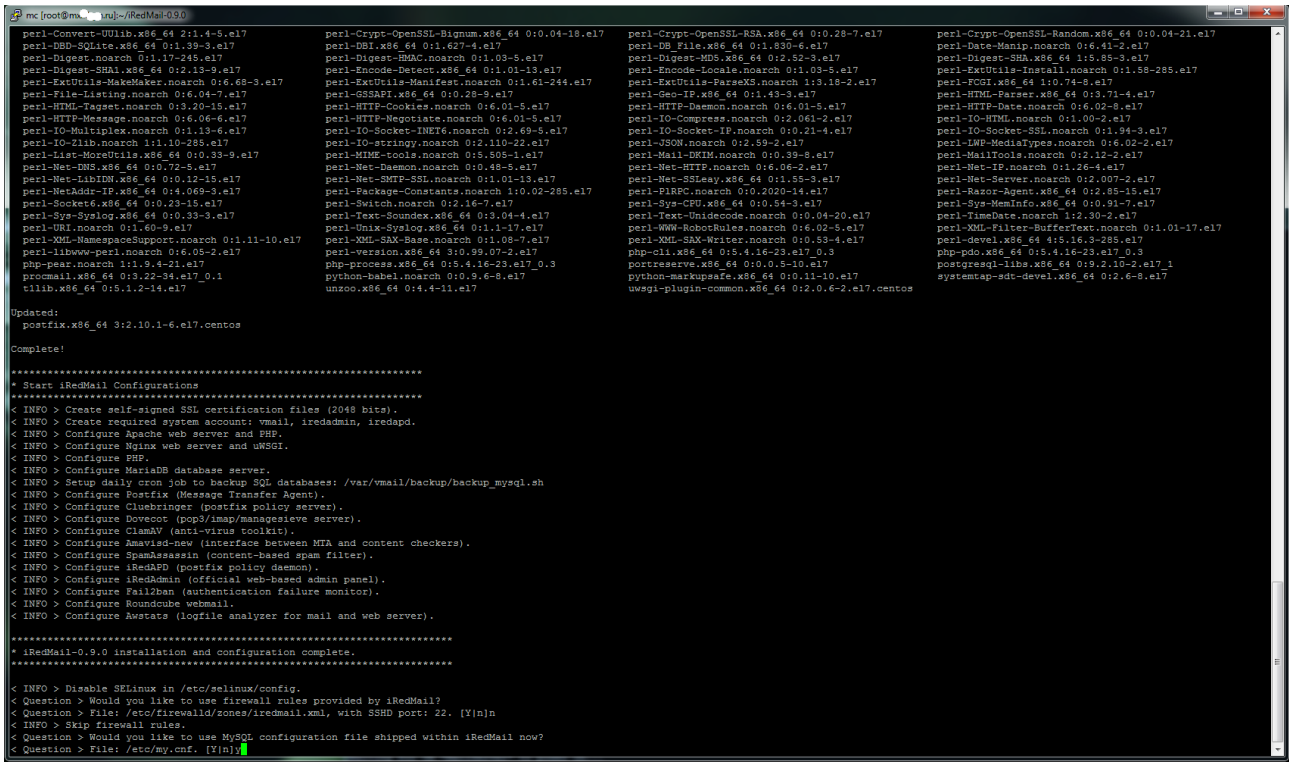

mc [root@mx[redacted]ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Your first virtual domain name
Please specify your first virtual domain name.
EXAMPLE:
* example.com
WARNING:
* It cannot be the same as server hostname: mail.mx.[redacted].ru.
xmx.[redacted].ru
< Next >

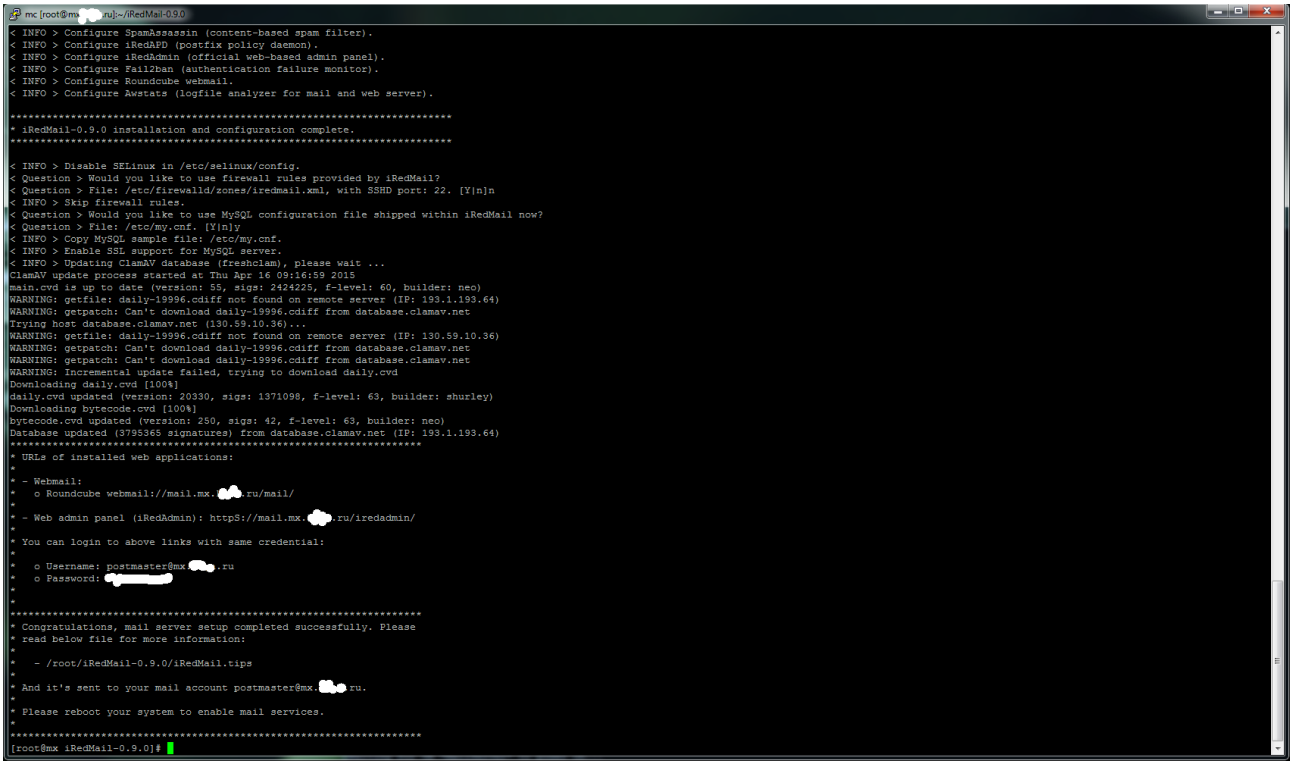

mc [root@mx[redacted]ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Password for the administrator of your domain
Please specify password for the administrator user:
* postmaster@mx[redacted].ru
Note:
* You can login to both webmail and iRedAdmin with this account.
* Please reset password immediately after installation completed.
WARNING:
* Do *NOT* use special characters in password. e.g. $, #.
* EMPTY password is *NOT* permitted.
< Next >


mc [root@mx[redacted]ru]:~/iRedMail-0.9.0
iRedMail: Open Source Mail Server Solution
Optional components
Note:
* DKIM is recommended.
* SPF validation (Sender Policy Framework) is enabled by default.
* DNS records (TXT type) are required for both SPF and DKIM.
Refer to below file for more detail after installation:
* /root/iRedMail-0.9.0/iRedMail.tips
x[*] DKIM signing/verification DomainKeys Identified Mail
x[*] iRedAdmin Official web-based Admin Panel
x[*] Roundcubemail WebMail program (PHP, AJAX)
x[*] Awstats Advanced web and mail log analyzer
x[*] Fail2ban Ban IP with too many password failures
< Next >


Optional components
Note:
* DKIM is recommended.
* SPF validation (Sender Policy Framework) is enabled by default.
* DNS records (TXT type) are required for both SPF and DKIM.
Refer to below file for more detail after installation:
* /root/iRedMail-0.9.0/iRedMail.tips
[*] DKIM signing/verification DomainKeys Identified Mail
[*] iRedAdmin Official web-based Admin Panel
[*] Roundcubemail WebMail program (PHP, AJAX)
[*] Awstats Advanced web and mail log analyzer
[*] Fail2ban Ban IP with too many password failures
< Next >
Configuration completed.
* Below file contains sensitive infomation (username/password), please
* do remember to *MOVE* it to a safe place after installation.
* /root/iRedMail-0.9.0/config
< Question > Continue? [y|N]


perl-Authen-SASL.noarch 0:2.15-10.el7
perl-BerkeleyDB.x86_64 0:0.51-4.el7
perl-Business-ISBN.noarch 0:2.06-2.el7
perl-Business-ISBN-Data.noarch 0:20120719.001-2.el7
perl-CGI.noarch 0:3.63-4.el7
perl-Cache-FastMmap.x86_64 0:1.40-9.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-Config-IniFiles.noarch 0:2.79-1.el7
perl-Convert-ASN1.noarch 0:0.26-4.el7
perl-Convert-BinHex.noarch 0:1.119-20.el7
perl-Convert-TNEF.noarch 0:0.18-2.el7
perl-Convert-UUlib.x86_64 2:1.4-5.el7
perl-Crypt-OpenSSL-Bignum.x86_64 0:0.04-18.el7
perl-Crypt-OpenSSL-RSA.x86_64 0:0.28-7.el7
perl-Crypt-OpenSSL-Random.x86_64 0:0.04-21.el7
perl-DBD-SQLite.x86_64 0:1.39-3.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-DB_File.x86_64 0:1.830-6.el7
perl-Date-Manip.noarch 0:6.41-2.el7
perl-Digest.noarch 0:1.17-245.el7
perl-Digest-HMAC.noarch 0:1.03-5.el7
perl-Digest-MD5.x86_64 0:2.52-3.el7
perl-Digest-SHA.x86_64 1:5.85-3.el7
perl-Digest-SHA1.x86_64 0:2.13-9.el7
perl-Encode-Detect.x86_64 0:1.01-13.el7
perl-Encode-Locale.noarch 0:1.03-5.el7
perl-ExtUtils-Install.noarch 0:1.58-285.el7
perl-ExtUtils-MakeMaker.noarch 0:6.68-3.el7
perl-ExtUtils-Manifest.noarch 0:1.61-244.el7
perl-ExtUtils-ParseXS.noarch 1:3.18-2.el7
perl-FCGI.x86_64 1:0.74-8.el7
perl-File-Listing.noarch 0:6.04-7.el7
perl-GSSAPI.x86_64 0:0.28-9.el7
perl-Geo-IP.x86_64 0:1.43-3.el7
perl-HTML-Parser.x86_64 0:3.71-4.el7
perl-HTML-Tagset.noarch 0:3.20-15.el7
perl-HTTP-Cookies.noarch 0:6.01-5.el7
perl-HTTP-Daemon.noarch 0:6.01-5.el7
perl-HTTP-Date.noarch 0:6.02-8.el7
perl-HTTP-Message.noarch 0:6.06-6.el7
perl-HTTP-Negotiate.noarch 0:6.01-5.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-IO-HTML.noarch 0:1.00-2.el7
perl-IO-Multiplex.noarch 0:1.13-6.el7
perl-IO-Socket-INET6.noarch 0:2.69-5.el7
perl-IO-Socket-IP.noarch 0:0.21-4.el7
perl-IO-Socket-SSL.noarch 0:1.94-3.el7
perl-IO-Zlib.noarch 1:1.10-285.el7
perl-IO-stringy.noarch 0:2.110-22.el7
perl-JSON.noarch 0:2.59-2.el7
perl-LWP-MediaTypes.noarch 0:6.02-2.el7
perl-List-MoreUtils.x86_64 0:0.33-9.el7
perl-MIME-tools.noarch 0:5.505-1.el7
perl-Mail-DKIM.noarch 0:0.39-8.el7
perl-MailTools.noarch 0:2.12-2.el7
perl-Net-DNS.x86_64 0:0.72-5.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-Net-HTTP.noarch 0:6.06-2.el7
perl-Net-IP.noarch 0:1.26-4.el7
perl-Net-LibIDN.x86_64 0:0.12-15.el7
perl-Net-SMTP-SSL.noarch 0:1.01-13.el7
perl-Net-SSLeay.x86_64 0:1.55-3.el7
perl-Net-Server.noarch 0:2.007-2.el7
perl-NetAddr-IP.x86_64 0:4.069-3.el7
perl-Package-Constants.noarch 1:0.02-285.el7
perl-PlRPC.noarch 0:0.2020-14.el7
perl-Razor-Agent.x86_64 0:2.85-15.el7
perl-Socket6.x86_64 0:0.23-15.el7
perl-Switch.noarch 0:2.16-7.el7
perl-Sys-CPU.x86_64 0:0.54-3.el7
perl-Sys-MemInfo.x86_64 0:0.91-7.el7
perl-Sys-Syslog.x86_64 0:0.33-3.el7
perl-Text-Soundex.x86_64 0:3.04-4.el7
perl-Text-Unidecode.noarch 0:0.04-20.el7
perl-TimeDate.noarch 1:2.30-2.el7
perl-URI.noarch 0:1.60-9.el7
perl-Unix-Syslog.x86_64 0:1.1-17.el7
perl-WWW-RobotRules.noarch 0:6.02-5.el7
perl-XML-Filter-BufferText.noarch 0:1.01-17.el7
perl-XML-NamespaceSupport.noarch 0:1.11-10.el7
perl-XML-SAX-Base.noarch 0:1.08-7.el7
perl-XML-SAX-Writer.noarch 0:0.53-4.el7
perl-devel.x86_64 4:5.16.3-285.el7
perl-libwww-perl.noarch 0:6.05-2.el7
perl-version.x86_64 3:0.99.07-2.el7
php-cli.x86_64 0:5.4.16-23.el7_0.3
php-pdo.x86_64 0:5.4.16-23.el7_0.3
php-pear.noarch 1:1.9.4-21.el7
php-process.x86_64 0:5.4.16-23.el7_0.3
portreserve.x86_64 0:0.0.5-10.el7
postgresql-libs.x86_64 0:9.2.10-2.el7_1
procmail.x86_64 0:3.22-34.el7_0.1
python-babel.noarch 0:0.9.6-8.el7
python-markupsafe.x86_64 0:0.11-10.el7
systemtap-sdt-devel.x86_64 0:2.6-8.el7
t1lib.x86_64 0:5.1.2-14.el7
unzoo.x86_64 0:4.4-11.el7
uwsgi-plugin-common.x86_64 0:2.0.6-2.el7.centos
Updated:
postfix.x86_64 3:2.10.1-6.el7.centos
Complete!
* Start iRedMail Configurations
< INFO > Create self-signed SSL certification files (2048 bits).
< INFO > Create required system account: vmail, iredadmin, iredapd.
< INFO > Configure Apache web server and PHP.
< INFO > Configure Nginx web server and uWSGI.
< INFO > Configure PHP.
< INFO > Configure MariaDB database server.
< INFO > Setup daily cron job to backup SQL databases: /var/vmail/backup/backup_mysql.sh
< INFO > Configure Postfix (Message Transfer Agent).
< INFO > Configure Cluebringer (postfix policy server).
< INFO > Configure Dovecot (pop3/imap/managesieve server).
< INFO > Configure ClamAV (anti-virus toolkit).
< INFO > Configure Amavisd-new (interface between MTA and content checkers).
< INFO > Configure SpamAssassin (content-based spam filter).
< INFO > Configure iRedAPD (postfix policy daemon).
< INFO > Configure iRedAdmin (official web-based admin panel).
< INFO > Configure Fail2ban (authentication failure monitor).
< INFO > Configure Roundcube webmail.
< INFO > Configure Awstats (logfile analyzer for mail and web server).
* iRedMail-0.9.0 installation and configuration complete.
< INFO > Disable SELinux in /etc/selinux/config.
< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/firewalld/zones/iredmail.xml, with SSHD port: 22. [Y|n]n


mc [root@mx.[redacted].ru]:~/iRedMail-0.9.0
perl-Convert-UUlib.x86_64 2:1.4-5.el7
perl-Crypt-OpenSSL-Bignum.x86_64 0:0.04-18.el7
perl-Crypt-OpenSSL-RSA.x86_64 0:0.28-7.el7
perl-Crypt-OpenSSL-Random.x86_64 0:0.04-21.el7
perl-DBD-SQLite.x86_64 0:1.39-3.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-DB_File.x86_64 0:1.830-6.el7
perl-Date-Manip.noarch 0:6.41-2.el7
perl-Digest.noarch 0:1.17-245.el7
perl-Digest-HMAC.noarch 0:1.03-5.el7
perl-Digest-MD5.x86_64 0:2.52-3.el7
perl-Digest-SHA.x86_64 1:5.85-3.el7
perl-Digest-SHA1.x86_64 0:2.13-9.el7
perl-Encode-Detect.x86_64 0:1.01-13.el7
perl-Encode-Locale.noarch 0:1.03-5.el7
perl-ExtUtils-Install.noarch 0:1.58-285.el7
perl-ExtUtils-MakeMaker.noarch 0:6.68-3.el7
perl-ExtUtils-Manifest.noarch 0:1.61-244.el7
perl-ExtUtils-ParseXS.noarch 1:3.18-2.el7
perl-FCGI.x86_64 1:0.74-8.el7
perl-File-Listing.noarch 0:6.04-7.el7
perl-GSSAPI.x86_64 0:0.28-9.el7
perl-Geo-IP.x86_64 0:1.43-3.el7
perl-HTML-Parser.x86_64 0:3.71-4.el7
perl-HTML-Tagset.noarch 0:3.20-15.el7
perl-HTTP-Cookies.noarch 0:6.01-5.el7
perl-HTTP-Daemon.noarch 0:6.01-5.el7
perl-HTTP-Date.noarch 0:6.02-8.el7
perl-HTTP-Message.noarch 0:6.06-6.el7
perl-HTTP-Negotiate.noarch 0:6.01-5.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-IO-HTML.noarch 0:1.00-2.el7
perl-IO-Multiplex.noarch 0:1.13-6.el7
perl-IO-Socket-INET6.noarch 0:2.69-5.el7
perl-IO-Socket-IP.noarch 0:0.21-4.el7
perl-IO-Socket-SSL.noarch 0:1.94-3.el7
perl-IO-Zlib.noarch 1:1.10-285.el7
perl-IO-stringy.noarch 0:2.110-22.el7
perl-JSON.noarch 0:2.59-2.el7
perl-LWP-MediaTypes.noarch 0:6.02-2.el7
perl-List-MoreUtils.x86_64 0:0.33-9.el7
perl-MIME-tools.noarch 0:5.505-1.el7
perl-Mail-DKIM.noarch 0:0.39-8.el7
perl-MailTools.noarch 0:2.12-2.el7
perl-Net-DNS.x86_64 0:0.72-5.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-Net-HTTP.noarch 0:6.06-2.el7
perl-Net-IP.noarch 0:1.26-4.el7
perl-Net-LibIDN.x86_64 0:0.12-15.el7
perl-Net-SMTP-SSL.noarch 0:1.01-13.el7
perl-Net-SSLeay.x86_64 0:1.55-3.el7
perl-Net-Server.noarch 0:2.007-2.el7
perl-NetAddr-IP.x86_64 0:4.069-3.el7
perl-Package-Constants.noarch 1:0.02-285.el7
perl-PlRPC.noarch 0:0.2020-14.el7
perl-Razor-Agent.x86_64 0:2.85-15.el7
perl-Socket6.x86_64 0:0.23-15.el7
perl-Switch.noarch 0:2.16-7.el7
perl-Sys-CPU.x86_64 0:0.54-3.el7
perl-Sys-MemInfo.x86_64 0:0.91-7.el7
perl-Sys-Syslog.x86_64 0:0.33-3.el7
perl-Text-Soundex.x86_64 0:3.04-4.el7
perl-Text-Unidecode.noarch 0:0.04-20.el7
perl-TimeDate.noarch 1:2.30-2.el7
perl-URI.noarch 0:1.60-9.el7
perl-Unix-Syslog.x86_64 0:1.1-17.el7
perl-WWW-RobotRules.noarch 0:6.02-5.el7
perl-XML-Filter-BufferText.noarch 0:1.01-17.el7
perl-XML-NamespaceSupport.noarch 0:1.11-10.el7
perl-XML-SAX-Base.noarch 0:1.08-7.el7
perl-XML-SAX-Writer.noarch 0:0.53-4.el7
perl-devel.x86_64 4:5.16.3-285.el7
perl-libwww-perl.noarch 0:6.05-2.el7
perl-version.x86_64 3:0.99.07-2.el7
php-cli.x86_64 0:5.4.16-23.el7_0.3
php-pdo.x86_64 0:5.4.16-23.el7_0.3
php-pear.noarch 1:1.9.4-21.el7
php-process.x86_64 0:5.4.16-23.el7_0.3
portreserve.x86_64 0:0.0.5-10.el7
postgresql-libs.x86_64 0:9.2.10-2.el7_1
procmail.x86_64 0:3.22-34.el7_0.1
python-babel.noarch 0:0.9.6-8.el7
python-markupsafe.x86_64 0:0.11-10.el7
systemtap-sdt-devel.x86_64 0:2.6-8.el7
t1lib.x86_64 0:5.1.2-14.el7
unzoo.x86_64 0:4.4-11.el7
uwsgi-plugin-common.x86_64 0:2.0.6-2.el7.centos
Updated:
postfix.x86_64 3:2.10.1-6.el7.centos
Complete!
* Start iRedMail Configurations
< INFO > Create self-signed SSL certification files (2048 bits).
< INFO > Create required system account: vmail, iredadmin, iredapd.
< INFO > Configure Apache web server and PHP.
< INFO > Configure Nginx web server and uWSGI.
< INFO > Configure PHP.
< INFO > Configure MariaDB database server.
< INFO > Setup daily cron job to backup SQL databases: /var/vmail/backup/backup_mysql.sh
< INFO > Configure Postfix (Message Transfer Agent).
< INFO > Configure Cluebringer (postfix policy server).
< INFO > Configure Dovecot (pop3/imap/managesieve server).
< INFO > Configure ClamAV (anti-virus toolkit).
< INFO > Configure Amavisd-new (interface between MTA and content checkers).
< INFO > Configure SpamAssassin (content-based spam filter).
< INFO > Configure iRedAPD (postfix policy daemon).
< INFO > Configure iRedAdmin (official web-based admin panel).
< INFO > Configure Fail2ban (authentication failure monitor).
< INFO > Configure Roundcube webmail.
< INFO > Configure Awstats (logfile analyzer for mail and web server).
* iRedMail-0.9.0 installation and configuration complete.
< INFO > Disable SELinux in /etc/selinux/config.
< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/firewalld/zones/iredmail.xml, with SSHD port: 22. [Y|n]n
< INFO > Skip firewall rules.
< Question > Would you like to use MySQL configuration file shipped within iRedMail now?
< Question > File: /etc/my.cnf. [Y|n]y


mc [root@mx.[redacted].ru]:~/iRedMail-0.9.0
< INFO > Configure SpamAssassin (content-based spam filter).
< INFO > Configure iRedAPD (postfix policy daemon).
< INFO > Configure iRedAdmin (official web-based admin panel).
< INFO > Configure Fail2ban (authentication failure monitor).
< INFO > Configure Roundcube webmail.
< INFO > Configure Awstats (logfile analyzer for mail and web server).
* iRedMail-0.9.0 installation and configuration complete.
< INFO > Disable SELinux in /etc/selinux/config.
< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/firewalld/zones/iredmail.xml, with SSHD port: 22. [Y|n]n
< INFO > Skip firewall rules.
< Question > Would you like to use MySQL configuration file shipped within iRedMail now?
< Question > File: /etc/my.cnf. [Y|n]y
< INFO > Copy MySQL sample file: /etc/my.cnf.
< INFO > Enable SSL support for MySQL server.
< INFO > Updating ClamAV database (freshclam), please wait ...
ClamAV update process started at Thu Apr 16 09:16:59 2015
main.cvd is up to date (version: 55, sigs: 2424225, f-level: 60, builder: neo)
WARNING: getfile: daily-19996.cdiff not found on remote server (IP: 193.1.193.64)
WARNING: getpatch: Can't download daily-19996.cdiff from database.clamav.net
Trying host database.clamav.net (130.59.10.36)...
WARNING: getfile: daily-19996.cdiff not found on remote server (IP: 130.59.10.36)
WARNING: getpatch: Can't download daily-19996.cdiff from database.clamav.net
WARNING: getpatch: Can't download daily-19996.cdiff from database.clamav.net
WARNING: Incremental update failed, trying to download daily.cvd
Downloading daily.cvd [100%]
daily.cvd updated (version: 20330, sigs: 1371098, f-level: 63, builder: shurley)
Downloading bytecode.cvd [100%]
bytecode.cvd updated (version: 250, sigs: 42, f-level: 63, builder: neo)
Database updated (3795365 signatures) from database.clamav.net (IP: 193.1.193.64)
* URLs of installed web applications:
* - Webmail:
* o Roundcube webmail://mail.mx.[redacted].ru/mail/
* - Web admin panel (iRedAdmin): https://mail.mx.[redacted].ru/iredadmin/
* You can login to above links with same credential:
* o Username: postmaster@mx.[redacted].ru
* o Password: [redacted]
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
* - /root/iRedMail-0.9.0/iRedMail.tips
* And it's sent to your mail account postmaster@mx.[redacted].ru.
* Please reboot your system to enable mail services.
[root@mx iRedMail-0.9.0]#

Iptables или Firewalld.

Обнаружил, что в CentOS 7ке, вместо привычного для меня iptables работает firewalld. Поэтому я отключаю его и возвращаюсь к iptables.

Останавливаем и убираем из автозапуска firewalld:

systemctl stop firewalld.service
systemctl disable firewalld.service

Устанавливаем сервис для Iptables:

yum install iptables-services

Добавляем в автозапуск и стартуем iptables:

systemctl enable iptables.service
systemctl start iptables.service

Добавляем в файл /etc/sysconfig/iptables необходимые правила разрешения:

-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 25 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 587 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 110 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 995 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 143 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 993 -j ACCEPT

Перезапускаем сервис:

systemctl restart iptables.service

Postfix.

Настройка Postfix для работы с учетными записями из Win2008R2 AD.

В локальной сети есть контроллер домен его IP 192.168.111.2, домен имеет имя developer.com, в дереве от корня домена есть оргюнит Структура, в этом оргюнити живут все пользователи.

Установим пакет openldap-clients, если его еще нет в системе, он нужен для тестирования соединения с контроллером домена:

yum install openldap-clients

Пробуем теперь подключиться к контроллеру домена developer.com и прочитать данные от имени пользователя user:

ldapsearch -x -h 192.168.111.2 -D 'user@developer.com' -W -b 'dc=developer,dc=com'

Далее вводим пароль и если есть связь с контроллером и пользователь опознан, вернуться данные об этом пользователе.

Т.к. мы будем использовать интеграцию с AD, необходимо отключить параметры в конфиге postfix, которые используются для работы с MySQL.

Выполняем:

postconf -e virtual_alias_maps=''
postconf -e sender_bcc_maps=''
postconf -e recipient_bcc_maps=''
postconf -e relay_domains=''
postconf -e relay_recipient_maps=''

Добавляем почтовый домен:

postconf -e smtpd_sasl_local_domain='mx.ob.ru'
postconf -e virtual_mailbox_domains='mx.ob.ru'

Меняем транспорт:

postconf -e transport_maps='hash:/etc/postfix/transport'

Добавляем запросы для подключения к AD:

postconf -e smtpd_sender_login_maps='proxy:ldap:/etc/postfix/ad_sender_login_maps.cf'
postconf -e virtual_mailbox_maps='proxy:ldap:/etc/postfix/ad_virtual_mailbox_maps.cf'
postconf -e virtual_alias_maps='proxy:ldap:/etc/postfix/ad_virtual_group_maps.cf'

Создаем или добавляем в файл /etc/postfix/transport строку для транспорта:

mx.ob.ru dovecot

Выполняем:

postmap hash:/etc/postfix/transport

Создаем файл /etc/postfix/ad_sender_login_maps.cf для подключения к AD:

###
server_host = 192.168.111.2
server_port = 389
version = 3
bind = yes
start_tls = no
bind_dn = user@developer.com

```
bind_pw = 123qwe
search_base = ou=Структура,dc=developer,dc=com
scope = sub
query_filter = (&(mail=%s)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
result_attribute = mail
debuglevel = 0
###
```

Создаем файл /etc/postfix/ad_virtual_mailbox_maps.cf для подключения к AD:

```
###
server_host = 192.168.111.2
server_port = 389
version = 3
bind = yes
start_tls = no
bind_dn = user@developer.com
bind_pw = 123qwe
search_base = ou=Структура,dc=developer,dc=com
scope = sub
query_filter = (&(objectclass=person)(mail=%s))
result_attribute = mail
result_format  = %d/%u/Maildir/
debuglevel  = 0
###
```

Создаем файл /etc/postfix/ad_virtual_group_maps.cf для подключения к AD:

```
###
server_host = 192.168.111.2
server_port  = 389
version = 3
bind  = yes
start_tls = no
bind_dn = user@developer.com
bind_pw = 123qwe
search_base = ou=Структура,dc=developer,dc=com
scope = sub
query_filter = (&(objectClass=group)(mail=%s))
special_result_attribute = member
leaf_result_attribute = mail
result_attribute = mail
debuglevel      = 0
###
```

Открываем конфиг /etc/postfix/main.cf и удалем:

check_policy_service inet:127.0.0.1:7777

Теперь будем проверять подключение и выборку данных из AD. Пусть у нас уже создан пользователь buh в нашем домене developer.com и у него в закладке “Общие” в поле “Эл.почта”, в AD внутреннее название его mail, мы прописали buh@mx.ob.ru его ящик.

Выполняем для проверки и смотрим как будет формироваться виртуальный ящик на диске сервера:

postmap -q buh@mx.ob.ru ldap:/etc/postfix/ad_virtual_mailbox_maps.cf

Если все правильно выполняется, то получим ответ:

mx.ob.ru/buh/Maildir/

Такая структура будет создана автоматически тут /var/vmail/vmail1 для этого пользователя при первом входе в свой ящик и будет иметь такой вид /var/vmail/vmail1/mx.ob.ru/buh/Maildir/.

Выполняем для проверки формирования логина отправителя:

postmap -q buh@mx.ob.ru ldap:/etc/postfix/ad_sender_login_maps.cf

Если все правильно выполняется, то получим ответ:

buh@mx.ob.ru

Выполняем для проверки формирования группы рассылки. Предварительно создаем группу в домене контроллера, пусть её название будет backup. В свойствах этой группы в поле “Эл.почта” прописываем псевдоним ящика для этой группы backup@mx.ob.ru, а в “Члены группы” добавляем пользователей. Пусть это будет buh, ssh и postmaster, они уже созданы в контроллере.

postmap -q buh@mx.ob.ru ldap:/etc/postfix/ad_virtual_group_maps.cf

Если все правильно выполняется, то получим ответ со списком пользователей:

postmaster@mx.ob.ru,buh@mx.ob.ru,ssh@mx.ob.ru

Свои дополнительные нюансы.

Необходимо разрешить отправку во внешний мир нескольким пользователям, оставшимся пользователям только локальная переписка.

Создаем файл /etc/postfix/local_domains и добавляем в него:

mx.ob.ru OK

Создаем файл /etc/postfix/restricted_senders и добавляем в него:

mx.ob.ru local_only

Правим файл /etc/postfix/main.cf:

```
smtpd_recipient_restrictions = check_sender_access ldap:/etc/postfix/restricted_senders.cf,
                               check_sender_access texthash:/etc/postfix/restricted_senders,
                               ...,
                               ...
smtpd_restriction_classes = local_only
local_only = check_recipient_access texthash:/etc/postfix/local_domains, reject
```

Создаем файл /etc/postfix/restricted_senders.cf для выборки из Win AD:

```
###
server_host = 192.168.111.2
server_port = 389
version = 3
bind = yes
start_tls = no
bind_dn = user@developer.com
bind_pw = 123qwe
search_base = ou=Структура,dc=developer,dc=com
scope = sub
query_filter = (&(mail=%s)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
result_attribute = postalCode
debuglevel = 0
###
```

В AD у юзера которому необходимо будет разрешить отправку почты наружу в закладке свойств “Адрес” в поле "Почтовый индекс" прописываем параметр permit.

У остальных пользователей у кого это поле будет пустым переписка только локальная разрешена. При попытке отправки будет появляться подобное сообщение:

SMTP ошибка (554): Невозможно добавить получателя "ivanov@gmail.com" (5.7.1 <buh@mx.ob.ru>: Sender address rejected: Access denied)

Проверить возврат параметров из учетной записи юзера в AD можно выполнив:
postmap -q buh@mx.ob.ru ldap:/etc/postfix/restricted_senders.cf

Перезапускаем сервис:

systemctl restart postfix.service

Dovecot.

Настройка Dovecot для работы с учетными записями из Win2008R2 AD. POP3 и IMAP сервер установленный из iRedMail.

В локальной сети есть контроллер домена его IP 192.168.111.2, домен имеет имя developer.com, в дереве от корня домена есть оргюнит Структура, в этом оргюнити живут все пользователи.

Настройка Dovecot для работы с учетными записями из Win2008R2 AD, с установкой квот на ящиках пользователей.

Редактируем файл конфига /etc/dovecot/dovecot.conf и приводим секцию Virtual mail accounts к виду:

```
# Virtual mail accounts.
userdb {
   args = /etc/dovecot/dovecot-ldap.conf
   driver = ldap
}
passdb {
   args = /etc/dovecot/dovecot-ldap.conf
   driver = ldap
}
```

Создаем файл подключения к AD /etc/dovecot/dovecot-ldap.conf:

```
###
hosts = 192.168.111.2:389
ldap_version = 3
auth_bind = yes
dn = user@developer.com
dnpass = 123qwe
base = ou=Структура,dc=developer,dc=com
scope = subtree
deref = searching
user_filter = (&(mail=%u)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
pass_filter = (&(mail=%u)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
pass_attrs = userPassword=password
default_pass_scheme = CRYPT
user_attrs = =home=/var/vmail/vmail1/%Ld/%Ln/Maildir/,=mail=maildir:/var/vmail/vmail1/%Ld/
%Ln/Maildir/,=quota_rule=*:bytes=%{ldap:st}
debug_level = 0
##
```

Важное для нас это строка с параметрами user_attrs, она модернизирована в отличии от стандартной, чтобы можно было использовать квоты для ящиков юзеров используя настройки из AD.

В ней это =quota_rule=*:bytes=%{ldap:st}, в этой строке самый важный параметр это st. Так вот, st, это есть, не что иное, как поле в свойствах юзера находящегося в AD.

Почему именно поле st? Да просто мне так удобно, я выбрал это поле. Вы можете себе назначит любое пустое, т.е. не занятое значением.

И так, поле st принадлежит свойствам юзера живущего в AD, это поле "Область, край" в закладке "Адрес". Так вот, сюда в это поле забиваем нужный размер ящика в числовом виде, размерность байты. Т.е. если необходимо пользователю сделать объем ящика 10мб, то вбиваем 10000000 или можно вписать 10MB.

Теперь в конфиге /etc/dovecot/dovecot.conf

В секции plugin, приводим параметр quota к виду:

```
plugin {
      quota = maildir:User quota
}
```

И не забываем, что пользователь для почтового ящика берется из свойств юзера, закладка “Общие” в поле “Эл.почта”, и в AD внутреннее название его mail, это было мною так же расписано в Postix.

Перезапускаем сервис:

systemctl restart dovecot.service

Общие папки (Public) в действии (не забываем, при создании структуры папок и файлов, владелец и группа должны быть той, от которой работает dovecot, это может быть vmail).

Общие папки отображаются сразу у всех пользователей и могут иметь свои настройки для доступа в них. Задача, сделать общую папку Public, в которой будут доступны папки DOCs и Warning. Причем, DOCs будет доступен только для листинга и чтения всем, а Warning будет доступен полностью для одного юзера.

Создаем папку, пусть /home/vmail/public. Назначаем на ней владельца и группу, ту от которой работает dovecot, это может быть vmail.

Создаем папки, /home/vmail/public/.DOCs и /home/vmail/public/.Warning. Назначаем на них владельца и группу, ту от которой работает dovecot, это может быть vmail.

В папках /home/vmail/public, /home/vmail/public/.DOCs и /home/vmail/public/.Warning, создаем пустой файл dovecot-shared.

В папке /home/vmail/public создаем файл dovecot-acl. В него пишем права доступа, листинг для всех, т.е. чтобы папки DOCs и Warning были видны всем, т.е. структура в папке /home/vmail/public:

anyone l

В папке /home/vmail/public/.DOCs создаем файл dovecot-acl. В него пишем права доступа, листинг и чтение для всех:

anyone lr

В папке /home/vmail/public/. Warning создаем файл dovecot-acl. В него пишем права для полного доступа пользователю ivanov@mx.ob.ru:

user=ivanov@mx.ob.ru lrwstipekxa

Теперь открываем конфиг /etc/dovecot/dovecot.conf и правим нем секцию:

```
namespace  Public {
   type = public
   separator = /
   prefix = Public/
   location = maildir:/home/vmail/public/:INDEX=/home/vmail/vmail1/%d/%n/public
   subscriptions = no
}
```

Перезапускаем dovecot:

systemctl restart dovecot.service

В итоге получим следующее, если у пользователя подписать эти папки, то они будут отображаться в почтовом дереве и исходя из того, какой пользователь сейчас видит эти папки, те права на них он и имеет.

Идентификаторы которые можно применять для доступа к папкам в файле dovecot-acl:

group-override=group name
user=user name
owner
group=group name
authenticated
anyone

Параметры для управления идентификаторами:

l - /lookup, ящик виден в списке/
r - /read, ящик может быть открыт на чтение/
w - /write, флаги и ключевые слова сообщения могут быть изменены, за исключением “Просмотрено” и “Удалено”
s - /write-seen, флаг сообщения ”Просмотрено” (\Seen) может быть изменён
t - /write-deleted, флаг сообщения “Удалён” (\Deleted) может быть изменён
i - /insert, сообщения могут быть записаны или скопированы в ящик
p - /post, сообщения могут быть размещены через LDA, например через Sieve
e - /expunge, сообщения могут быть исключены
k - /create, ящики могут быть созданы или переименованы под управлением этого ящика (переименование требует прав на удаление)
x - /delete, ящик может быть удалён
a - /admin, административные права на ящик (изменение списков ACL)

Если необходимо создать кириллические папки, то необходимо их названия конвертировать перед созданием. Выполняем:

```
echo -n ".Документы" | iconv -f utf-8 -t utf-7 | tr "+" "&"
```

Результатом будет .&BBQEPgQ6BEMEPAQ1BD0EQgRL- название для этой папки.

Если нам необходимо автоподписание (автоподключение папок), т.е. чтобы пользователь не задумывался как это делать в клиенте необходимо дописать в конфиг dovecot необходимое в секцию namespace Public и привести её к виду:

```
###
namespace Public {
   type = public
   separator = /
   prefix = "ОАО КБПА/"
   location = maildir:/home/vmail/public/:INDEX=/home/vmail/vmail1/%d/%n/public
   subscriptions = no

   mailbox DOCs {
      auto = subscribe
   }

   mailbox Warning {
      auto = subscribe
   }
}
###
```

Amavis.

Проверка антивируса и спам фильтра из пакета Amavis, который работает у нас в связке с Postfix, установленный из iRedMail.

Для проверки антивируса создадим файл /home/monstr/Mail_Server/eicar.txt и вставим в него содержимое этой строки:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Теперь отправим его с сервера:

mailx -a /home/monstr/Mail_Server/eicar.txt buh@mx.od.ru

Смотрим результат из лога /var/log/maillog:

Apr 9 08:12:35 mail amavis[9839]: (09839-07) Blocked INFECTED () {DiscardedInternal,Quarantined}, MYUSERS <root@mail.mx.ob.ru> -> <buh@mx.ob.ru>, quarantine: tsTUf7-kAoaf, Message-ID: <20150409051235.591B8414B43A@mail.mx.ob.ru>, mail_id: tsTUf7-kAoaf, Hits: -, size: 1024, 196 ms
Apr 9 08:12:35 mail postfix/smtp[10481]: 591B8414B43A: to=<buh@mx.ob.ru>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.33, delays=0.09/0.01/0/0.23, dsn=2.7.0, status=sent (250 2.7.0 Ok, discarded, id=09839-07 - INFECTED:)

Так же при срабатывании антивируса на ящик postmaster приходит об этом уведомление.

Для проверки антиспама создадим файл /home/monstr/Mail_Server/spam.txt и вставим в него содержимое этой строки:

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

Теперь отправим его с сервера:

mailx -a /home/monstr/Mail_Server/spam.txt buh@mx.ob.ru

Смотрим результат из лога /var/log/maillog:

Apr 9 08:14:13 mail amavis[9839]: (09839-08) Passed SPAM {RelayedTaggedInternal}, MYUSERS <root@mail.mx.ob.ru> -> <buh@mx.ob.ru>, Message-ID: <20150409051412.93110414B43A@mail.mx.ob.ru>, mail_id: CxIMsRkQB4Pz, Hits: 1000, size: 1023, queued_as: 3B9AD41733A9, 663 ms
Apr 9 08:14:13 mail postfix/smtp[10481]: 93110414B43A: to=<buh@mx.ob.ru>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.82, delays=0.05/0/0/0.76, dsn=2.0.0, status=sent (250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 3B9AD41733A9)

При обнаружении спама и большого числа очков присвоенных этому сообщению, оно помечается как спам, и далее пользователь будет знать, что с ним делать.

Roundcube.

Настройка Roundcube для работы с учетными записями из Win2008R2 AD, установленный из iRedMail. Это позволит получить адресную книгу на основе прописанных ящиков юзеров из AD.

Открываем файл /var/www/roundcubemail/config/config.inc.php и добавляем в него:

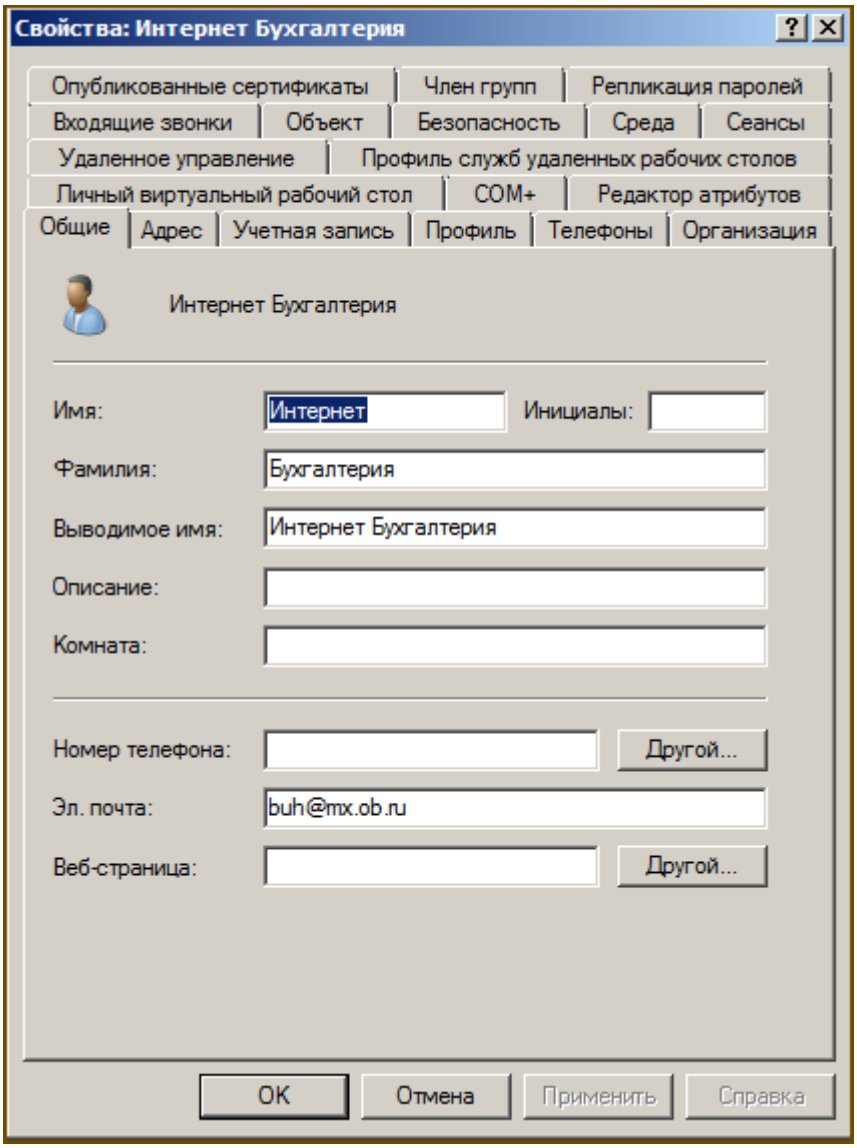
```
#
# Global LDAP Address Book with AD.
#

$config['autocomplete_addressbooks'] = array("sql", "global_ldap_abook");

$config['ldap_public']["global_ldap_abook"] = array(
   'name'          => 'Адресная книга ОАО Рога',
   'hosts'         => array("192.168.111.2"),      // <- Set AD hostname or IP address here.
   'port'          => 389,
   'use_tls'       => false,   // <- Set to true if you want to use LDAP over TLS.
   'ldap_version'  => '3',
   'network_timeout' => 10,
   'user_specific' => false,

   'base_dn'       => "dc=developer,dc=com", // <- Set base dn in AD
   'bind_dn'       => "user@developer.com",                    // <- bind dn
   'bind_pass'     => "123qwe",          // <- bind password
   'writable'      => false,                     // <- Do not allow mail user write data back to AD.

   'search_fields' => array('mail'),

   // mapping of contact fields to directory attributes
   'fieldmap' => array(
      'name'        => 'cn',
      'surname'     => 'sn',
      'firstname'   => 'givenName',
      'title'       => 'title',
      'email'       => 'mail:*',
      'department'  => 'departmentNumber',
      'photo' => 'thumbnailPhoto'
   ),
   'sort'          => 'cn',
   'scope'         => 'sub',
   //'filter'       => "(&(objectclass=person)(mail=*@mx.ob.ru)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))",
   'filter'        => "(mail=*@*)",
   'fuzzy_search'  => true,
   'vlv'           => false,   // Enable Virtual List View to more efficiently fetch paginated data (if server supports it)
   'sizelimit'     => '0',     // Enables you to limit the count of entries fetched. Setting this to 0 means no limit.
   'timelimit'     => '0',     // Sets the number of seconds how long is spend on the search. Setting this to 0 means no
limit.
   'referrals'     => false,  // Sets the LDAP_OPT_REFERRALS option. Mostly used in multi-domain Active Directory
setups
);
```

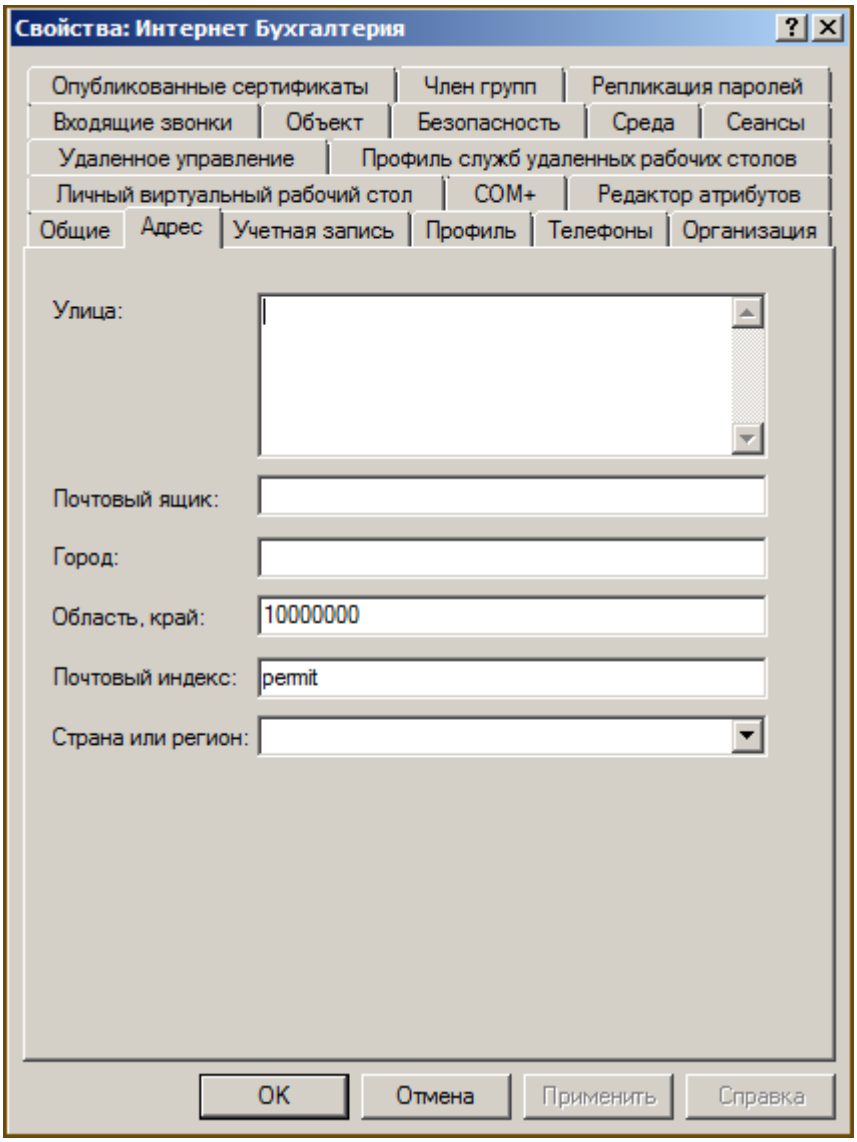
Fail2Ban.

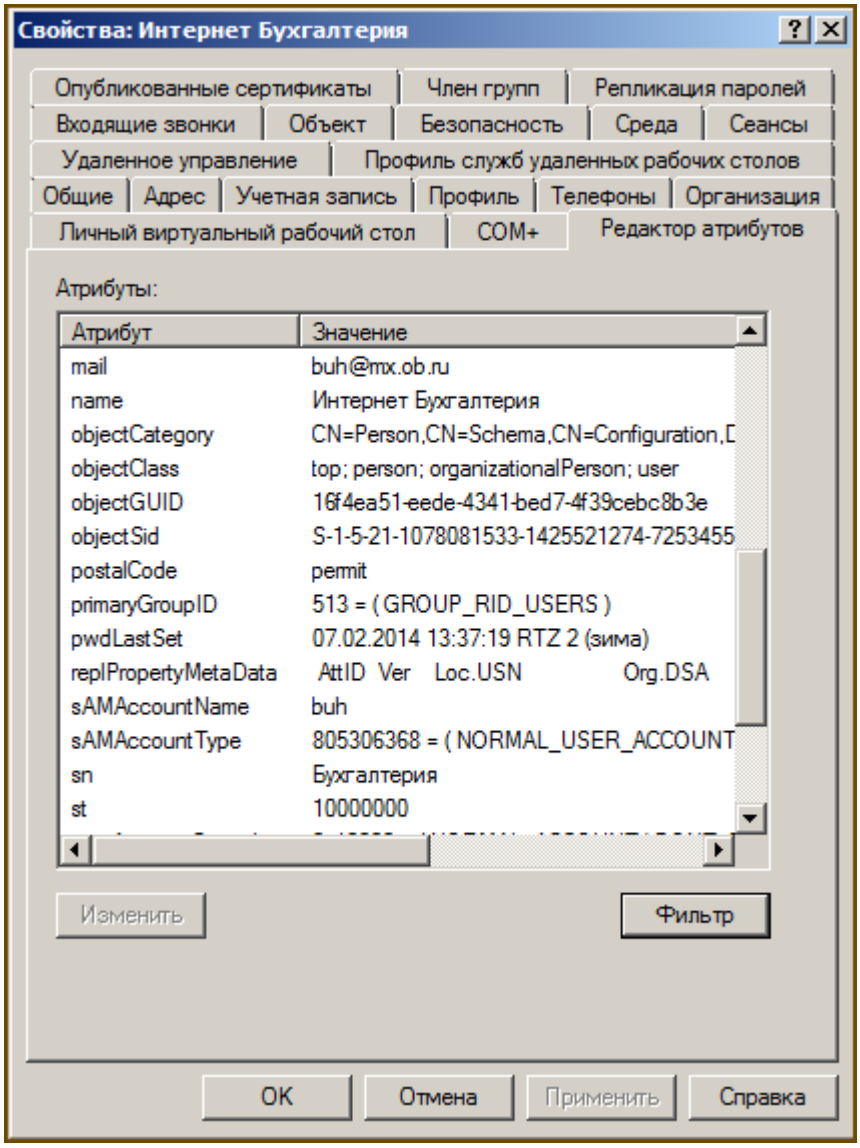
Замечательный пакет, о нем я уже писал. Здесь он устанавливается вместе с почтовиком. И играет важную роль в отсечении «переборщиков» паролей. Но не забываем, что Fail2Ban это инструмент управления фаерволом, т.е. Fail2Ban анализирует нужные логи и создает правила блокировки для фаервола, например IPTables.

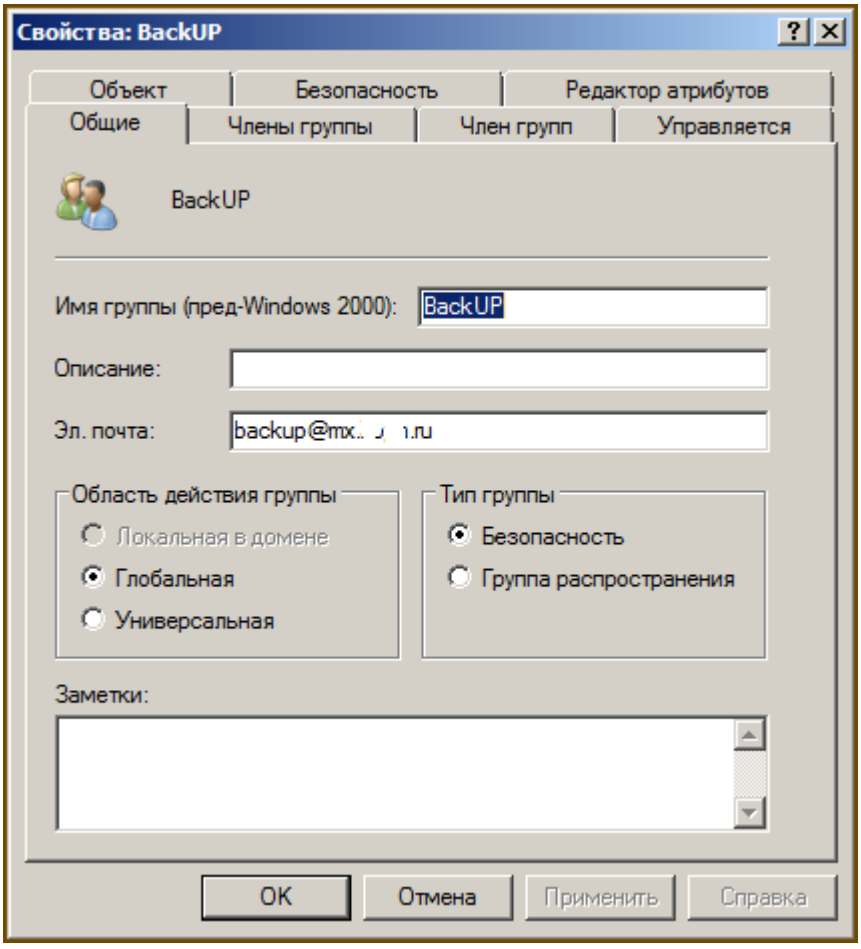
По дефолту в конфиге /etc/fail2ban/jail.local уже все необходимые проверки для почтовика настроены. Единственное, что можно подкрутить, это параметр maxretry - количество неправильных попыток авторизации, причем эти попытки складываются. Т.е., если перебирать пароль в промежутке заданным параметром findtime, и будет три неправильных попытки, которые заданы параметром maxretry, то сработает правило для фаервола. Параметр bantime задает время блокировки.

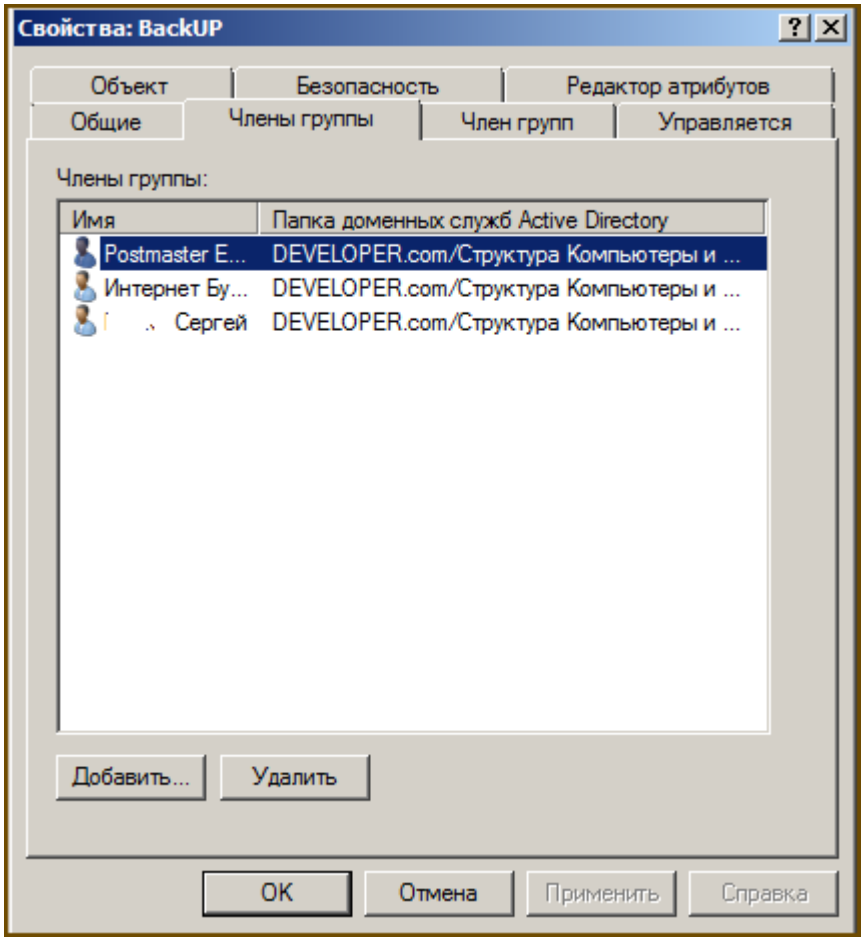
Пример настройки пользователей и групп.




Свойства: Интернет Бухгалтерия
Опубликованные сертификаты
Член групп
Репликация паролей
Входящие звонки
Объект
Безопасность
Среда
Сеансы
Удаленное управление
Профиль служб удаленных рабочих столов
Личный виртуальный рабочий стол
COM+
Редактор атрибутов
Общие
Адрес
Учетная запись
Профиль
Телефоны
Организация
Улица:
Почтовый ящик:
Город:
Область, край:
10000000
Почтовый индекс:
permit
Страна или регион:
OK
Отмена
Применить
Справка


Свойства: Интернет Бухгалтерия
Опубликованные сертификаты
Член групп
Репликация паролей
Входящие звонки
Объект
Безопасность
Среда
Сеансы
Удаленное управление
Профиль служб удаленных рабочих столов
Общие
Адрес
Учетная запись
Профиль
Телефоны
Организация
Личный виртуальный рабочий стол
COM+
Редактор атрибутов
Атрибуты:
Атрибут
Значение
mail
buh@mx.ob.ru
name
Интернет Бухгалтерия
objectCategory
CN=Person,CN=Schema,CN=Configuration,D
objectClass
top; person; organizationalPerson; user
objectGUID
16f4ea51-eede-4341-bed7-4f39cebc8b3e
objectSid
S-1-5-21-1078081533-1425521274-7253455
postalCode
permit
primaryGroupID
513 = (GROUP_RID_USERS)
pwdLastSet
07.02.2014 13:37:19 RTZ 2 (зима)
replPropertyMetaData
AttID Ver Loc.USN Org.DSA
sAMAccountName
buh
sAMAccountType
805306368 = (NORMAL_USER_ACCOUNT
sn
Бухгалтерия
st
10000000
Изменить
Фильтр
OK
Отмена
Применить
Справка


Свойства: BackUP
Объект
Безопасность
Редактор атрибутов
Общие
Члены группы
Член групп
Управляется
BackUP
Имя группы (пред-Windows 2000):
BackUP
Описание:
Эл. почта:
backup@mx
.ru
Область действия группы
Локальная в домене
Глобальная
Универсальная
Тип группы
Безопасность
Группа распространения
Заметки:
OK
Отмена
Применить
Справка


Свойства: BackUP
Объект
Безопасность
Редактор атрибутов
Общие
Члены группы
Член групп
Управляется
Члены группы:
Имя
Папка доменных служб Active Directory
Postmaster E...
DEVELOPER.com/Структура Компьютеры и ...
Интернет Бу...
DEVELOPER.com/Структура Компьютеры и ...
Сергей
DEVELOPER.com/Структура Компьютеры и ...
Добавить...
Удалить
OK
Отмена
Применить
Справка