Installing a Mailserver with Postfix, Dovecot, SASL, LDAP & Roundcube

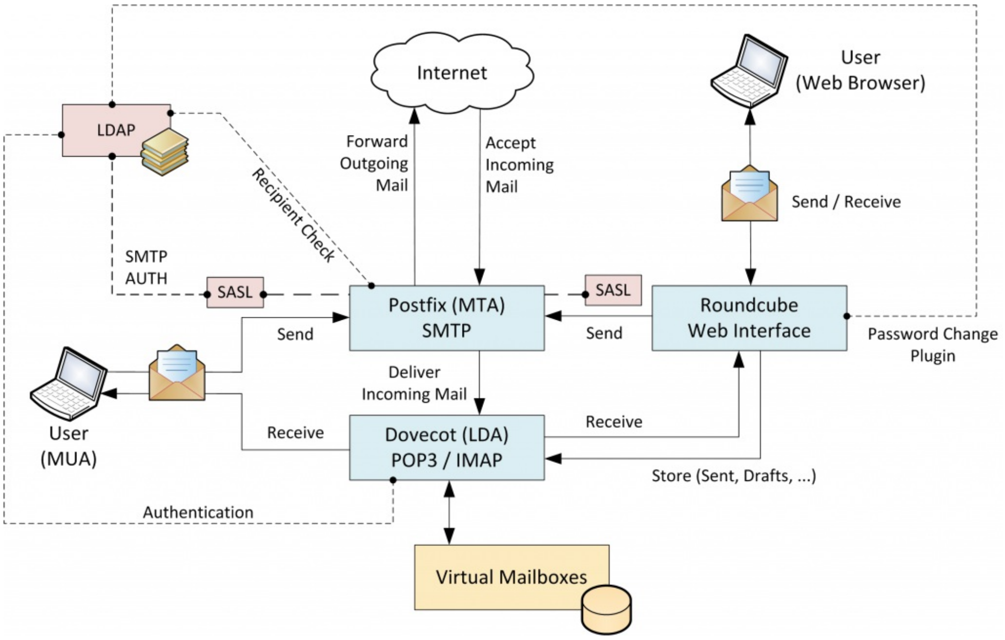
admin June 5, 2014 HowTo, Linux Leave a comment (17)

Installing a mailserver is a quite complex matter because several components are involved. Since there are many different operational scenarios, there are many different possible configurations, thus lots of different howtos around the internet. In this howto I'm going to describe the basic configuration of a mail server which has the following characteristics:

- Everything runs on Ubuntu 14.04 LTS x64
- All software packages are taken from the repository (no compiling necessary)
- The server is directly connected to the internet using a static IP address
- Users don't have system accounts on the Unix machine
- User accounts are virtual accounts stored in an LDAP
- Users with a valid LDAP account can …
  - Send and receive mail via POP3/IMAP
  - Send and receive mail via Web Interface

Spam and virus protection (amavis, clamav, spamassasin) is not covered by this howto.

Graphical overview of the set-up:



These are the necessary components:

- Postfix as MTA (Mail Transfer Agent) –> This is the SMTP server. It accepts incoming mail (after a successful LDAP lookup of the recipient address) and passes it to Dovecot. It forwards outgoing mail (after the user successfully authenticated) to the next responsible SMTP server.
- Dovecot as LDA (Local Delivery Agent) –> This is the POP3 and IMAP server. It accepts incoming mail from Postfix and stores it in virtual mailboxes. It is connected to the LDAP for user authentication and lookups.
- Cyrus SASL –> Provides authentication for the SMTP server (since users are only allowed to send mail after they authenticated). User and password verification is done via LDAP.
- LDAP –> This is the directory service that stores the (virtual) user accounts for the mail server. It uses the postfix-book scheme.
- Roundcube –> This is a web interface that lets users access their mail via web browser instead of a mail client (Mail User Agent). In addition to a webserver (i.e. Apache) Roundcube requires a database to store user settings (i.e. MySQL).

As for this howto, everything is running on a single machine. In real life (especially when you have to deal with a lot of users), it might be better to have dedicated machines for certain services. If you use dedicated machines, however, you have to make sure that the communication between these is secure!

Recent Comments

- admin on Installing a Mailserver with Postfix, Dovecot, SASL, LDAP & Roundcube
- Andy on Installing a Mailserver with Postfix, Dovecot, SASL, LDAP & Roundcube
- admin on Installing a Mailserver with Postfix, Dovecot, SASL, LDAP & Roundcube
- Clément on Installing a Mailserver with Postfix, Dovecot, SASL, LDAP & Roundcube
- admin on Installing a Mailserver with Postfix, Dovecot, SASL, LDAP & Roundcube

Most Viewed Posts

- Retrieving System Information via Command Line on Windows
- Creating a Certification Authority and a Server Certificate on Ubuntu
- Data Recovery With Foremost & Scalpel
- How To Set Up a VPN on DD-WRT
- Fenix PD32 UE (Ultimate Edition) Review

Categories

- Flashlight
- Hardware
- HowTo
- Information
- Linux
- Mac
- Raspberry
- Review
- Windows

Meta

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

Web2PDF
converted by Web2PDFConvert.com

Basic Prerequisites

1. Connectivity

The server must be connected to the internet and should be accessible through the following ports:

- 25 (SMTP)
- 80 (HTTP)
- 110 (POP3)
- 143 (IMAP)
- 443 (HTTPS)

If you have any firewalls, don’t forget to open the necessary ports.

2. System Time

The server should have an accurate system time, i.e. by using NTP.

3. Hostname

The server needs a fully-qualified hostname (i.e. mail.example.com), because otherwise foreign mail servers might not accept mails from it. This can be checked with the following command: `hostname -f`

The hostname can be configured in the following config files:

- /etc/hostname
- /etc/hosts

4. DNS Resolution

The server must be configured to use a working DNS server. Traditionally, DNS servers have to be added to /etc/resolv.conf, but on Ubuntu these are configured via the Network Manager. Preferably by using the GUI, or by manually editing the config file in /etc/NetworkManager/system-connections.

5. DNS Records

The hostname needs to be resolvable in both directions (hostname –> ip & ip –> hostname), so your provider needs to set the following DNS Records for you:

- A Record (forward lookup, resolvs a hostname to an IPv4 address)
- AAAA Record (forward lookup, resolvs a hostname to an IPv6 address)
- PTR Record (reverse lookup, resolvs an IP address to a hostname)
- MX Record (provides the hostname of a domain’s mail server)

This can be checked with the following commands:

```
dig mail.example.com A +short # should return your server's IPv4 address
dig mail.example.com AAAA +short # should return your server's IPv6 address, if configured
dig -x <ip address> +short # should return your fully-qualified hostname
dig example.com MX +short # should return your mail server's fully-qualified hostname
```

6. Logging

For troubleshooting it is important that the logging service is working. This is rsyslogd by default, the configuration can be found in /etc/rsyslog.d. By default, mail-related log will go to /var/log/mail.log.

LDAP

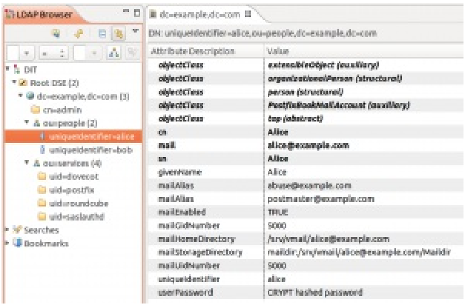
A basic LDAP guide can be found here: basic-openldap-installation-configuration

The BaseDN for this howto is “dc=example,dc=com” and it contains two organizationalUnits:

- “ou=people,dc=example,dc=com” for user accounts (RDN = uniqueIdentifier)
- “ou=services,dc=example,dc=com” for service accounts (RDN = uid)
  - You’ll need accounts for postfix, dovecot, saslauthd and roundcube

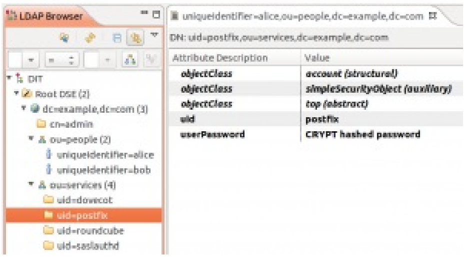
The following screenshots show the LDAP structure, the necessary objectClasses and attributes:

Web2PDF
converted by Web2PDFConvert.com



DN: uniqueIdentifier=alice,ou=people,dc=example,dc=com

Attribute Description	Value
objectClass	extensibleObject (auxiliary)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	PostfixBookMailAccount (auxiliary)
objectClass	top (abstract)
cn	Alice
mail	alice@example.com
sn	Alice
givenName	Alice
mailAlias	abuse@example.com
mailAlias	postmaster@example.com
mailEnabled	TRUE
mailGidNumber	5000
mailHomeDirectory	/srv/vmail/alice@example.com
mailStorageDirectory	maildir:/srv/vmail/alice@example.com/Maildir
mailUidNumber	5000
uniqueIdentifier	alice
userPassword	CRYPT hashed password



DN: uid=postfix,ou=services,dc=example,dc=com

Attribute Description	Value
objectClass	account (structural)
objectClass	simpleSecurityObject (auxiliary)
objectClass	top (abstract)
uid	postfix
userPassword	CRYPT hashed password

For testing purposes it might be a good idea to create an "allow everything" ACL (`{0}to * by * write`) — see the LDAP guide for that — but keep in mind that everyone who has access to the LDAP server will be able to read and edit the whole directory. So don't forget to create appropiate ACLs before you put the server into productive operation!

Postfix

1. Installation

Install Postfix and the extensions for Pearl Compatible Regular Expressions and LDAP Connections. During installation select the "No Configuration" option:

```
apt-get install postfix postfix-pcre postfix-ldap
```

Optionally, you can install extra tools for managing mailboxes (mutt) and sending testmails (swaks):

```
apt-get install mutt swaks
```

2. Configuration

Before Postfix can be started, some configuration files need to be created in /etc/postfix:

- main.cf –> This is the main configuration file for Postfix (parameter documentation)

```
################################################################################
### Base Settings ###
#####################

# Listen on all interfaces
inet_interfaces = all

# Use TCP IPv4
inet_protocols = ipv4

# Greet connecting clients with this banner
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)

# Fully-qualified hostname
myhostname = mail.example.com

# Do not append domain part to incomplete addresses (this is the MUA's job)
```

- virtual_domains –> Contains the domains the server takes mails for

```
# Domain  Anything

example.com   OK
```

- ldap_virtual_recipients.cf –> LDAP query for recipient validation

```
bind = yes
bind_dn = uid=postfix,ou=services,dc=example,dc=com
bind_pw = secret
server_host = ldap://127.0.0.1:389
search_base = ou=people,dc=example,dc=com
domain = example.com
query_filter = (&(mail=%s)(mailEnabled=TRUE))
result_attribute = mail
```

- ldap_virtual_aliases.cf –> LDAP query to get aliases and forwarding addresses (forwarding can be achieved by putting the external address into the "email" field in the LDAP-Account and copying the main address from the "mail" field into an "aliasMail" field.)

Web2PDF
converted by Web2PDFConvert.com

```
bind = yes
bind_dn = uid=postfix,ou=services,dc=example,dc=com
bind_pw = secret
server_host = ldap://127.0.0.1:389
search_base = ou=people,dc=example,dc=com
domain = example.com
query_filter = (&(mailAlias=%s)(mailEnabled=TRUE))
result_attribute = mail, email
```

- identitycheck.pcre –> Regular expression to block clients that use your hostname

```
# Identity (RegEx)  Action

/^(mail\.example\.com)$/ REJECT Hostname Abuse: $1
/^(1\.2\.3\.4)$/  REJECT Hostname Abuse: $1
/^(\[1\.2\.3\.4\])$/  REJECT Hostname Abuse: $1
```

- drop.cidr –> Contains blacklisted IP addresses

```
# IP/CIDR   Action

1.2.3.0/24   REJECT Blacklisted
```

Since Dovecot and TLS are not configured yet, temporarily comment out the following lines in main.cf:

- dovecot_destination_recipient_limit = 1
- smtpd_tls_security_level = may
- smtpd_tls_auth_only = yes
- smtpd_tls_CAfile = /etc/postfix/certs/example-cacert.pem
- smtpd_tls_cert_file = /etc/postfix/certs/mail_public_cert.pem
- smtpd_tls_key_file = /etc/postfix/certs/mail_private_key.pem

3. Hashmap Creation

Certain maps (i.e. hashmaps) need to be converted to .db files before they can be used by Postfix. In main.cf the virtual_domains file is called as a hashmap, so it needs to be converted:

```
postmap hash:/etc/postfix/virtual_domains
```

4. Starting Postfix

Start Postfix with the following command: `service postfix start`

Check if it is running: `lsof -Pni :25`

Have a look at /var/log/mail.log to see if there are any errors.

5. SMTP Connection Test

Use Telnet to connect to the SMTP server: `telnet 127.0.0.1 25`. When you are connected, send an `EHLO client`. You should get the following response:

```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 mail.example.com ESMTP Postfix (Ubuntu)
EHLO client
250-mail.example.com
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH DIGEST-MD5 NTLM CRAM-MD5 LOGIN PLAIN
250-AUTH=DIGEST-MD5 NTLM CRAM-MD5 LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
QUIT
221 2.0.0 Bye
```

6. LDAP Lookup Test

With this test you can find out if Postfix is able to query the LDAP server:

```
postmap -q alice@example.com ldap:/etc/postfix/ldap_virtual_recipients.cf
postmap -q postmaster@example.com ldap:/etc/postfix/ldap_virtual_aliases.cf
```

Both of the above commands should return "alice@example.com", because …

1. there is an LDAP entry with "mail = alice@example.com", so it is a valid recipient and
2. there is an LDAP entry with "mailAlias = postmaster@example.com", which is an alias address for "alice@example.com".

Web2PDF
converted by Web2PDFConvert.com

7. Useful Commands

Config-related:

```
# Show all Postfix parameters and their effective values
postconf

# Show value for the given parameter
postconf smtpd_tls_security_level

# Show all parameters that have been explicitly set in main.cf
postconf -n

# Show all default values
postconf -d

# Show default value of the given parameter
postconf -d alias_maps
```

Queue-related:

```
# Show mails that are currently queued
postqueue -p

# Flush the queue (try to send)
postqueue -f

# Delete a mail from the queue (ids can be found in mail.log)
postsuper -d <id>

# Delete all mails from the queue
postsuper -d ALL
```

Dovecot

1. Installation

Install Dovecot and the necessary extensions. During installation, you will be asked if a certificate should be created. If you skip this, you can add your own certificate later.

```
apt-get install dovecot-core dovecot-imapd dovecot-pop3d dovecot-lmtpd dovecot-ldap
```

2. Configuration

Disable unwanted protocols (IMAPS and POP3S) by setting the ports to 0 in /etc/dovecot/conf.d/10-master.conf. Also, set the permissions, user and group for the authentication-userdb:

```
inet_listener imaps {
    port = 0
    #port = 993
    #ssl = yes
}
```

```
inet_listener pop3s {
    port = 0
    #port = 995
    #ssl = yes
}
```

```
unix_listener auth-userdb {
    mode = 0600
    user = vmail
    group = vmail
}
```

Define the desired authentication mechanisms in /etc/dovecot/conf.d/10-auth.conf, disable system-based authentication and enable LDAP-based authentication instead:

```
auth_mechanisms = plain login
#!include auth-system.conf.ext
!include auth-ldap.conf.ext
```

Set the LDAP-related parameters in /etc/dovecot/dovecot-ldap.conf.ext:

Web2PDF
converted by Web2PDFConvert.com

```
hosts = 127.0.0.1
dn = uid=dovecot,ou=services,dc=example,dc=com
dnpass = secret
ldap_version = 3
base = ou=people,dc=example,dc=com
user_attrs = mailHomeDirectory=home,mailUidNumber=uid,mailGidNumber=gid,mailStorageDirect
user_filter = (&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=%n))
pass_attrs = uniqueIdentifier=user,userPassword=password
pass_filter = (&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=%n))
default_pass_scheme = CRYPT
```

Activate logging in /etc/dovecot/conf.d/10-logging.conf:

```
log_path = syslog
syslog_facility = mail
auth_debug = yes
```

Set the path to your certificates in /etc/dovecot/conf.d/10-ssl.conf:

```
ssl_cert = </etc/dovecot/mail_public_cert.pem
ssl_key = </etc/dovecot/private/mail_private_key.pem
```

Add a system user and group named vmail with uid and gid 5000:

```
addgroup --system --gid 5000 vmail
adduser --system --home /srv/vmail --uid 5000 --gid 5000 --disabled-password --disabled-lo
```

Make sure that /srv/vmail has been created.

4. Starting Dovecot

Start Dovecot with `service dovecot start` and check if it is running with `lsof -Pni` — port 110 and 143 should be open. If it isn't running, check the logfiles (mail.log and syslog). If there are no errors in the log, start Dovecot in foreground mode to have the errors printed to the console: `dovecot -F`.

5. IMAP Connection & Authentication Test

Use Telnet to connect to Dovecot's IMAP Server: `telnet 127.0.0.1 143`. Then send a login request (`1 login alice@example.com secret`) to see if authentication (plain) is working:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=P
1 login alice@example.com secret
1 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPL
2 logout
* BYE Logging out
```

6. Postfix Integration

Activate Dovecot Deliver in Postfix by adding these lines to /etc/postfix/master.cf:

```
dovecot   unix  -       n       n       -       -       pipe
        flags=ODRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -e -f ${sender} -d ${re
```

Set the postmaster address in /etc/dovecot/conf.d/15-lda.conf:

```
postmaster_address = postmaster@example.com
```

Restart Dovecot and Postfix:

```
service dovecot restart
service postfix restart
```

7. Dovecot Deliver Test

Send a testmail to alice@example.com using one of the following methods:

```
echo Testmail | sendmail -f bob@example.com alice@example.com
```

```
swaks --from bob@example.com --to alice@example.com --server 127.0.0.1:25
```

Web2PDF
converted by Web2PDFConvert.com

```
telnet 127.0.0.1 25

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.example.com ESMTP Postfix (Ubuntu)
EHLO test.local
250-mail.example.com
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH DIGEST-MD5 NTLM CRAM-MD5 LOGIN PLAIN
250-AUTH=DIGEST-MD5 NTLM CRAM-MD5 LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<bob@example.com>
250 2.1.0 Ok
RCPT TO:<alice@example.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Testmail
.
250 2.0.0 Ok: queued as 51586A1146
QUIT
221 2.0.0 Bye
```

Check the log (/var/log/mail.log) and Alice's mailbox: `mutt -f /srv/vmail/alice@example.com/Maildir/`

SASL (Cyrus)

1. Installation

```
apt-get install libsasl2-2 sasl2-bin
```

2. Configuration

Create an "smtpd.conf" in /etc/postfix/sasl/ with the following content:

```
log_level: 3
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN
```

Enable autostart, set the mechanism to LDAP and set the options for a chrooted Postfix in /etc/default/saslauthd:

```
START=yes
MECHANISMS="ldap"
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

Create the LDAP configuration for SASL in /etc/saslauthd.conf:

```
ldap_servers: ldap://127.0.0.1/
ldap_bind_dn: uid=saslauthd,ou=services,dc=example,dc=com
ldap_bind_pw: secret
ldap_timeout: 10
ldap_time_limit: 10
ldap_scope: sub
ldap_search_base: ou=people,dc=example,dc=com
ldap_auth_method: bind
ldap_filter: (&(uniqueIdentifier=%u)(mailEnabled=TRUE))
ldap_debug: 0
ldap_verbose: off
ldap_ssl: no
ldap_starttls: no
ldap_referrals: yes
```

Set permissions for the config file:

```
chown root:sasl /etc/saslauthd.conf
chmod 640 /etc/saslauthd.conf
```

Add the postfix user to the sasl group: `adduser postfix sasl`

And start the daemon: `service saslauthd start`

3. SASL Authentication Test

Use the following command to test if SASL is working:

Web2PDF
converted by Web2PDFConvert.com

```
testsaslauthd -u alice -p secret -f /var/spool/postfix/var/run/saslauthd/mux
```

It should return 0: OK "Success."

4. SMTP Authentication Test

To test if SASL works with SMTP, we first need the username and password in Base64 format. Use this command to convert it (@ needs to be escaped with a backslash):

```
perl -MMIME::Base64 -e 'print encode_base64("alice\@example.com");'
perl -MMIME::Base64 -e 'print encode_base64("secret");'
```

Open up a Telnet session, send an `EHLO test.local`, followed by an `AUTH LOGIN`. The server will ask for the username by sending "334 VXNlcm5hbWU6". Just paste your encoded username now. Then the server will ask for the password ("334 UGFzc3dvcmQ6"):

```
telnet localhost 25

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.example.com ESMTP Postfix (Ubuntu)
EHLO test.local
250-mail.example.com
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH LOGIN
334 VXNlcm5hbWU6
YWxpY2VAZXhhbXBsZS5jb20=
334 UGFzc3dvcmQ6
c2VjcmV0
235 2.7.0 Authentication successful
QUIT
221 2.0.0 Bye
```

If everything went well, the server should return 235 2.7.0 Authentication successful. If it did not work, check /var/log/auth.log for any errors. If that file doesn't help, activate extended logging in the SMTP server by adding a "-v" to the smtpd command in master.cf:

```
smtp      inet  n       -       -       -       -       smtpd -v
```

TLS (Postfix)

With the current configuration, the mail server only offers plaintext (and login) authentication. This is good, because all clients support this and the passwords can be stored encrypted in the LDAP. Other authentication methods would require storing the passwords in plaintext. To make the authentication process secure (and not have the passwords trasferred in plaintext) the session needs to be encrypted — this is done with TLS.

1. Certificate Files & Permissions

Save your certificate and key files in /etc/postfix/certs (see main.cf for filenames). Also save the Diffie-Hellman files (for perfect forward secrecy) in this folder. These can be created as follows:

```
openssl dhparam -2 -out dh_512.pem 512
openssl dhparam -2 -out dh_1024.pem 1024
```

Set the permissions to:

```
chown -R root:root /etc/postfix/certs/
chmod -R 600 /etc/postfix/certs/
```

2. Activate TLS

In main.cf uncomment the six parameters that have been commented out in step 2 of the Postfix chapter, restart Postfix and check the log for any errors. If everything went well, the server should no longer offer AUTH PLAIN LOGIN, but STARTTLS instead. You can check this by looking at the EHLO response (see step 5 of the Postfix chapter).

3. TLS Test

With the following command you can connect to the server using STARTTLS:

Web2PDF
converted by Web2PDFConvert.com

```
openssl s_client -CAfile certs/example-cacert.pem -starttls smtp -connect localhost:25
```

Then you can talk to the server like in a Telnet session, but do not type a capital "R" since this will trigger a Renegotiation. If you want to send a mail, use "rcpt to:" instead of "RCPT TO:".

This also works from external hosts (just change the -connect value to your mail server name). The -CAfile parameter is optional and can be omitted for a quick test.

Roundcube

1. Installation

Download the Roundcube archive (v1.0.1 at this time) from http://roundcube.net/download/ and extract it to your webroot (/var/www/html on Ubuntu 14.04, /var/www on previous versions). See the INSTALL file for installation instructions. These are the essential steps:

Install the necessary software:

```
apt-get install apache2 php5 mysql-server php5-mysql php5-mcrypt php5-intl php-pear php5-l
```

Set permissions of the webdir:

```
cd /var/www/html
chown -R root:www-data roundcube
chmod -R 750 roundcube
chmod -R 720 roundcube/temp roundcube/logs
```

Configure your timezone in /etc/php5/apache2/php.ini:

```
date.timezone = Europe/Berlin
```

Activate mcrypt:

```
php5enmod mcrypt
service apache2 restart
```

2. Database Setup

Connect to the database:

```
mysql -u root -p
```

Create a database for Roundcube:

```
CREATE DATABASE roundcubemail CHARACTER SET utf8 COLLATE utf8_general_ci;
GRANT ALL PRIVILEGES ON roundcubemail.* TO roundcube@localhost IDENTIFIED BY 'password';
QUIT;
```

3. Config File Creation

Open Firefox and go to http://127.0.0.1/roundcube/installer to start the Roundcube installer, which will perform some system checks, initialize the database and create a config file for you. Two notes:

- Set tls://localhost as smtp_server
- Check "Use the current IMAP username and password for SMTP authentication"

Save the generated config file to /var/www/html/roundcube/config/config.inc.php and set the permissions like above. You might have to call the installer again to get the "Initialize Database" option.

Delete (or chmod -R 000) the installer directory.

Add the Override option for the Roundcube directory in /etc/apache2/sites-enabled/000-default.conf so that its .htaccess file will be loaded (this will also deactivate Indexes):

```
<Directory /var/www/html/roundcube>
        AllowOverride All
</Directory>
```

4. Roundcube Test

Go to http://127.0.0.1/roundcube and try to log in as "alice@example.com" with password "secret".

Before any real users log in, HTTPS should be enabled on the webserver!

5. Enable The Password Change Plugin

Web2PDF
converted by Web2PDFConvert.com

Add it to the plugin array in /var/www/html/roundcube/config/config.inc.php:

```
$config['plugins'] = array('password');
```

Copy the necessary options from /var/www/html/roundcube/plugins/password/config.inc.php.dist to /var/www/html/roundcube/config/config.inc.php:

```
// Password Plugin options
// -----------------------
$config['password_driver'] = 'ldap_simple';
$config['password_confirm_current'] = true;
$config['password_minimum_length'] = 6;
$config['password_require_nonalpha'] = false;
$config['password_log'] = false;
$config['password_login_exceptions'] = null;
$config['password_hosts'] = null;
$config['password_force_save'] = false;


// LDAP and LDAP_SIMPLE Driver options
// -----------------------------------
$config['password_ldap_host'] = '127.0.0.1';
$config['password_ldap_port'] = '389';
$config['password_ldap_starttls'] = false;
$config['password_ldap_version'] = '3';
$config['password_ldap_basedn'] = 'dc=example,dc=com';
$config['password_ldap_method'] = 'user';
$config['password_ldap_searchDN'] = 'uid=roundcube,ou=services,dc=example,dc=com';
$config['password_ldap_searchPW'] = 'secret';
$config['password_ldap_search_base'] = 'ou=people,dc=example,dc=com';
$config['password_ldap_search_filter'] = '(uniqueIdentifier=%name)';
$config['password_ldap_encodage'] = 'crypt';
$config['password_ldap_pwattr'] = 'userPassword';
$config['password_ldap_force_replace'] = true;
```

Users should now be able to change their LDAP password in the Roundcube Settings.

Closing Words

This was an attempt to create an as short as possible mailserver howto. It only addresses the most essential parts. Depending on your environment things might have to be different, though.

Please consider: in this howto LDAP and Apache communication is completely unencrypted. On a real server you should do something about that! Also, don't forget to keep your private keys and password files safe by chown- and chmod-ing them properly!

Files and folders containing passwords:

- /etc/postfix/ldap_virtual_aliases.cf
- /etc/postfix/ldap_virtual_recipients.cf
- /etc/dovecot/dovecot-ldap.conf.ext
- /etc/saslauthd.conf
- /var/www/html/roundcube/config/config.inc.php

Folders containing private keys:

- /etc/postfix/certs
- /etc/dovecot/private
- /etc/ssl/private (possibly for your Apache key)

« Previous | Next »

17 Comments. **[Leave a comment]**

Clément October 27, 2014 at 5:25 pm

Hello,

Thanks for this very detailed tutorial. I was looking for one up to date for Ubuntu for a while.
However, I'm stuck at the IMAP log in step. I followed every step carefully, I think.
Here the logs:

In ldap

```
Oct 27 17:17:50 ldap slapd[4656]: conn=1011 op=1 SRCH base=”ou=people,dc=,dc=fr” scope=2 deref=0 filter=”(&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=clement))”
Oct 27 17:17:50 ldap slapd[4656]: conn=1011 op=1 SRCH attr=uniqueIdentifier userPassword
Oct 27 17:17:50 ldap slapd[4656]: <= bdb_equality_candidates: (uniqueIdentifier) not indexed
Oct 27 17:17:50 ldap slapd[4656]: conn=1011 op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=
```

In dovecot

```
Oct 27 17:16:15 mail dovecot: auth: Debug: client in:
AUTH#0111#011PLAIN#011service=imap#011secured#011session=ZTaZ2WkGKQB/AAAB#011lip=127.0.0.1#011rip=
Oct 27 17:16:15 mail dovecot: auth: Debug: ldap(clement@.fr,127.0.0.1,): pass search:
```

Web2PDF
converted by Web2PDFConvert.com

```
base=ou=people,dc=,dc=fr scope=subtree filter=(&(objectClass=PostfixBookMailAccount)
(uniqueIdentifier=clement)) fields=uniqueIdentifier,userPassword
Oct 27 17:16:15 mail dovecot: auth: Debug: ldap(clement@.fr,127.0.0.1,): result:
uniqueIdentifier=clement; uniqueIdentifier unused
Oct 27 17:16:15 mail dovecot: auth: Debug: auth(clement@.fr,127.0.0.1,): username changed
clement@.fr -> clement
Oct 27 17:16:15 mail dovecot: auth: Debug: ldap(clement,127.0.0.1,): result: uniqueIdentifier=clement;
userPassword missing
Oct 27 17:16:15 mail dovecot: auth: ldap(clement,127.0.0.1,): No password returned (and no
nopassword)
Oct 27 17:16:17 mail dovecot: auth: Debug: client passdb out: FAIL#0111#011user=clement
```

Is someone has a clue about what's wrong?
Thank you 😃

admin October 27, 2014 at 7:59 pm

Hi, in your log it says "ou=people,dc=,dc=fr". Did you remove the domain name on purpose or does it really look like that in the log?

Clément October 27, 2014 at 9:34 pm

I removed the domain on purpose.

admin October 27, 2014 at 9:53 pm

Ok 😉 Can you post the content of your /etc/dovecot/dovecot-ldap.conf.ext file?

Clément October 27, 2014 at 10:09 pm

Sure. I removed all commented lines and change the domain and dnspass variable :

```
hosts = 192.168.1.12
dn = uid=dovecot,ou=services,dc=mydomain,dc=fr
dnpass = mypassword
ldap_version = 3
base = ou=people,dc=mydomain,dc=fr
user_attrs = mailHomeDirectory=home,mailUidNumber=uid,mailGidNumber=gid,mailStorageDirectory=mail
user_filter = (&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=%n))
pass_attrs = uniqueIdentifier=user,userPassword=password
pass_filter = (&(objectClass=PostfixBookMailAccount)(uniqueIdentifier=%n))
default_pass_scheme = CRYPT
```

admin October 27, 2014 at 11:01 pm

Well, that config file looks fine, but for some reason the query doesn't return the password. I checked my logs and it also says "uniqueIdentifier unused" so that doesn't seem to be a problem.

In your LDAP, the "userPassword"-attribute for the account "uniqueIdentifier=clement,ou=people,dc=yourdomain,dc=fr" is existent and set?

What's the result for this manual query?

```
ldapsearch -x -W -D uid=dovecot,ou=services,dc=yourdomain,dc=fr -b ou=people,dc=yourdomain,dc=fr -
LLL 'uniqueIdentifier=clement'
```

Clément October 27, 2014 at 11:10 pm

Yes, it's set with a value {ssha}n…..

```
# ldapsearch -x -W -D uid=dovecot,ou=services,dc=mydomain,dc=fr -b ou=people,dc=mydomain,dc=fr -
LLL 'uniqueIdentifier=clement'
Enter LDAP Password:
dn: uniqueIdentifier=clement,ou=people,dc=mydomain,dc=fr
objectClass: organizationalPerson
objectClass: person
objectClass: top
objectClass: PostfixBookMailAccount
objectClass: extensibleObject
cn: Clement
givenName: Clement
mail: clement@…
mailEnabled: TRUE
mailGidNumber: 5000
mailHomeDirectory: /home/clement
mailQuota: 0
mailStorageDirectory: maildir:/home/clement/Maildir
mailUidNumber: 5000
uniqueIdentifier: clement
sn: Clement
mailAlias: postmaster@…
```

//edited by admin: real domain name changed to 'mydomain'

admin October 27, 2014 at 11:20 pm

The userPassword is missing in that result, which means that the problem is within your LDAP configuration / ACL (olcAccess)

Clément November 1, 2014 at 6:44 pm

converted by Web2PDFConvert.com

Thank you! Actually, I had two problems. First I configured the ACL, then, I tried to use a remote disk connected with sshfs (not a good idea ^^).

So I followed the rest of the tutorial until the TLS part (included). But I can't send emails although it works if I send an email to the same domain. I configured thunderbird with starttls on port 25.

```
Nov 1 18:33:55 mail postfix/smtpd[811]: connect from myclient.tld[192.168.1.1]
Nov 1 18:33:55 mail postfix/smtpd[811]: NOQUEUE: reject: RCPT from myclient.tld[192.168.1.1]: 554
5.7.1 : Relay access denied; from= to= proto=ESMTP helo=
Nov 1 18:34:00 mail postfix/smtpd[811]: disconnect from myclient.tld[192.168.1.1]
```

Do I need to enable something in postfix?

admin November 1, 2014 at 7:33 pm

Relay access denied means that you're not allowed to send mail. Maybe SMTP authentication didn't work? Are the two tests in the SASL chapter successful?

Clément November 1, 2014 at 7:49 pm

Yes, it was. But now, I can't connect with telnet (but I think it's the normal behavior):

```
# telnet localhost 25
Trying 127.0.0.1…
Connected to localhost.
Escape character is '^]'.
220 mail.forumanalogue.fr ESMTP Postfix (Ubuntu)
ehlo client
250-mail.mydomain.fr
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

Now with tls:

```
% openssl s_client -starttls smtp -connect mail.mydomain.fr:25
[…]
—
250 DSN
ehlo client
250-mail.mydomain.fr
250-PIPELINING
250-SIZE 10240000
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
auth login
334 VXNlcm5hbWU6
Y2xlbWVudEBmb3J1bWFuYWxvZ3VlLmZy
334 UGFzc3dvcmQ6
Q2xlbWVudDAx
DONE
%
```

Clément November 1, 2014 at 8:11 pm

I think I found what's wrong in my configuration. It's the parameter reject_unauth_destination in smtpd_recipient_restrictions. If I understood, it forbids to send email to another domain.

admin November 1, 2014 at 9:19 pm

'reject_unauth_destination' prevents the mailserver from being an open relay, so I think it is better to keep that parameter. Clients that do not authenticate will only be able to send mail to your domain. 'permit_sasl_authenticated' ensures that authenticated clients will be able to send mail to any domain.

Clément November 1, 2014 at 9:25 pm

I probably miss something because since there is 'reject_unauth_destination', I can't send email to other domains.

admin November 2, 2014 at 12:29 am

As for the last log you posted: It is correct, that the server doesn't offer authentication when you connect with Telnet. Authentication is only offered when the connection is established using TLS, so that part seems to be fine.

It still looks like a SASL problem to me. If you do an "AUTH LOGIN" and enter your base64 encoded credentials, does the server repsond with "DONE"? I think it should respond with "Authentication successful" – unless it has been changed in newer versions..

Andy November 13, 2014 at 6:03 pm

Thanks for a great tutorial.

Could you tell me what modifications I would need to make to this setup if I wanted to connect from say a Thunderbird (Windows) or K9 (Android) client?

Web2PDF
converted by Web2PDFConvert.com

admin November 13, 2014 at 7:45 pm

There are no modifications necessary. It should be possible to connect with any email client. SMTP port is 25, IMAP port is 143 and POP3 port is 110. Authentication method is PLAIN and TLS needs to be checked.

Leave a Comment

NAME

EMAIL

Website URL

CAPTCHA Code

SUBMIT

© Copyright 2014 Acidx's Blog ☐ Theme by zwwooooo & schiy ☐ Powered by WordPress

converted by Web2PDFConvert.com