Self Hosted Apps



a presentation about your data !

Serial: 2016 05 29 08

Disclaimer

- This presentation is trying to show you, how easy and simple is to keep your own data, yours.
- It's not 100% secure and may have errors.

Domain

- This is the first (and most important) step.
- Choose your own (personal) domain.
- Something easy to remember, something easy to spell, something easy that would remind people yourself.
- For this presentation we will use: librebit.net

DNS

librebit.net.	10800 IN SOA	a.dns.gandi.net. hostmaster.gandi.net. 1462877306 10800 3600 604800 10800
librebit.net.	10800 IN MX	10 librebit.net.
librebit.net. librebit.net.	10800 IN AA 10800 IN A	AA 2a03:b0c0:2:d0::4ce:8001 178.62.211.175

Notes based on CentOS

cat /etc/redhat-release CentOS Linux release 7.2.1511 (Core)

rpm -qa | grep -E 'postfix|dovecot|httpd|php'
dovecot-2.2.10-5.el7.x86_64
postfix-2.10.1-6.el7.x86_64
dovecot-pigeonhole-2.2.10-5.el7.x86_64
httpd-2.4.6-40.el7.centos.x86_64
php-5.4.16-36.el7_1.x86_64
php-xml-5.4.16-36.el7_1.x86_64
php-pdo-5.4.16-36.el7_1.x86_64
php-mbstring.x86 64

Postfix

smtpd_banner = "The sky above the port was the color of television, tuned to a dead channel"

inet_interfaces = all
inet_protocols = all

smtpd_sasl_type = dovecot

local_recipient_maps = static:/etc/dovecot/users
local_transport = lmtp:unix:private/dovecot-lmtp

Dovecot users

doveadm pw -s SHA512-CRYPT -u testuser Enter new password: testpassword Retype new password: testpassword

cat /etc/dovecot/users
testuser@librebit.net:{SHA512-CRYPT}
\$6\$1W2KyIXZnu.9Xu9z\$MmUKraP.lYu3rIgKHRWad7SAIeBYqvL.KtKic
f5H6DSxZ0tXS4AuA0cCWFchPyRHBln6BBgkMRn.RgJkSzQFj/:::

Mail Storage

Maildir

```
# mkdir -pv /storage/vmails/testuser/cur
# mkdir -pv /storage/vmails/testuser/new
# mkdir -pv /storage/vmails/testuser/tmp
```

HomeDir (for sieve)

mkdir -pv /storage/vhomes/testuser

chown -R dovecot:dovecot /storage

Protocols

```
# vim /etc/dovecot/dovecot.conf
protocols = imap sieve lmtp
```

```
Authentication Backend
# vim /etc/dovecot/conf.d/auth-system.conf.ext
passdb {
    driver = passwd-file
    args = /etc/dovecot/users
}
userdb {
    driver = passwd-file
    args = /etc/dovecot/users
}
```

Authentication & Lmtp service

```
# vim /etc/dovecot/conf.d/10-master.conf
service auth {
 unix listener /var/spool/postfix/private/auth {
    group = postfix
    mode = 0660
    user = postfix
service lmtp {
 unix listener /var/spool/postfix/private/dovecot-lmtp {
    group = postfix
    mode = 0600
    user = postfix
```

```
mail service
```

```
# vim /etc/dovecot/conf.d/10-mail.conf
```

```
mail_location = /storage/vmails/%n/
mail_home = /storage/vhomes/%n/
```

```
mail_uid = dovecot
mail_gid = dovecot
```

```
first_valid_uid = 97
first_valid_uid = 97
```

sieve

vim /etc/dovecot/conf.d/20-lmtp.conf

```
protocol lmtp {
   mail_plugins = sieve
}
```

Webmail

cd /var/www/html
wget -c http://repository.rainloop.net/v2/webmail/rainloopcommunity-latest.zip

unzip rainloop-community-latest.zip

find . -type d -exec chmod 755 {} \;
find . -type f -exec chmod 644 {} \;

chown -R apache:apache /var/www/html

RainLoop



default admin password: 12345

RainLoop admin - domains (i) librebit.net/?admin#/domains P ☆自 ← G RainLoop — Admin Panel Edit Domain "librebit.net" General × Login IMAP SMTP Branding Server Port Server Port Contacts 127.0.0.1 143 127.0.0.1 25 Domains Secure Secure Security • None None • Integrations Use short login (user@domain.com → user) Use short login (user@domain.com → user) Plugins Use authentication Packages ▼ Sieve configuration (beta) Use php mail() function (beta) About i Test White List X Close Update



cd /var/www/html

```
# wget -c
https://github.com/fruux/Baikal/releases/download/0.3.5
/baikal-0.3.5.zip
```

- # unzip baikal-0.3.5.zip
- # touch baikal/Specific/ENABLE_INSTALL
- # chown -R apache:apache /var/www/html/baikal

4							
Baï	<mark>kal</mark> Insta	ll Tool					
	(🗲) 🕕	librebit	.net/ba	ikal/htr	ml/adn	nin/install/	

The Baïkal initialization wizard

C

Configure your new Baïkal **0.3.5** installation.

Editing Standard 🏠 Baïkal Settings

Server Time zone	Europe/Athens
Enable CalDAV	\checkmark
Enable CardDAV	~
WebDAV authentication type	Digest
Admin password	•••••
Admin password, confirmation	•••••
Enable Web interface (recommended)	~
Web interface autolock	
	Save changes

☆ 🖨 🔄 🖉 🔅 | librebit.net/baikal/html/admin/install/?/databas∈ Baïkal Install Tool



Configure Baïkal Database.

Editing Database 🏟 Baïkal Database Settings

SQLite file path	PROJECT_PATH_SPECIFIC . "db/db.sqlite"
	The absolute server path to the SQLite file
Use MySQL	
	lf checked, Baïkal will use MySQL instead of SQLite.
	Save changes

Version

server.com

This systems runs Baïkal 0.3.5 http://baikal-

Statistics

' 🗈 < 🖉 🔅 librebit	.net/baikal	/html/admin/		C	<u>e</u> o	d	
Baï <mark>kal</mark> Web Admin	Dashboard	Users and resources ഫ്ര	Settings	System settings	≜ Lo	gout	
Dashb	oard	I					
About this sys	stem						

License and credits

Baïkal is open source software licensed under the terms of the GNU GPL v3.

Baïkal is based upon other open source projects. Read the README.md file to learn about that.

Baïkal is developed by Jérôme Schneider.

Users		CalDAV		CardDAV	
Registered users	0	Number of calendars	0	Number of address books	0
		Number of events	0	Number of contacts	0

On

On

On

Services

Web admin

CalDAV

CardDAV

● 合 ☆ 自	(ilbrebit.net/baikal/html/admin/?/users/
Baï <mark>kal</mark> Web Adı	min Dashboard Users and resources Settings System
Use	ers
Manage Baïkal u	ser accounts, and associated resources.
Creating new 上	User
Username	testuser
	May be an email, but not forcibly.
Display name	Test User
Email	testuser@librebit.net
Password	••••••
Confirm password	••••••
	Save changes Close

Webmail & DAV

Username: testuser Password: testpassword

http://librebit.net/baikal/html/dav.php/
addressbooks/testuser/default/

Now with SSL !



Let's Encrypt

- # yum -y install letsencrypt
- # letsencrypt certonly \
 -t --agree-tos \
 -d librebit.net \
 --email testuser@librebit.net \
 --webroot -w /var/www/html /
 --dry-run

remove "--dry-run" to activate your Certs

Web Server with SSL !

yum -y install mod_ssl.x86_64

vim /etc/httpd/conf.d/ssl.conf

SSLCertificateFile/etc/letsencrypt/live/librebit.net/cert.pemSSLCertificateKeyFile/etc/letsencrypt/live/librebit.net/privkey.pemSSLCertificateChainFile/etc/letsencrypt/live/librebit.net/chain.pem

systemctl restart httpd.service

https://librebit.net/

Postfix with TLS !

```
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtpd_tls_ask_ccert = yes
smtpd_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt
smtpd_tls_CApath = /etc/pki/tls/certs
smtpd_tls_cert_file= /etc/letsencrypt/live/librebit.net/fullchain.pem
smtpd_tls_key_file = /etc/letsencrypt/live/librebit.net/privkey.pem
smtpd_tls_ciphers = high
smtpd_tls_exclude_ciphers = aNULL, MD5, EXPORT
```

```
smtpd_tls_loglevel = 1
smtpd tls protocols = !SSLv2, !SSLv3
```

Postfix submission TLS

vim /etc/postfix/master.cf

submission inet n - n - - smtpd

vim /etc/postfix/main.cf

smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes

CheckTLS



TestReceiver

CheckTLS Confidence Factor for "info@librebit.net": 100

MX Server	Pref	Con- nect	All- owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
librebit.net [178.62.211.175]	10	OK (117ns)	OK (588ns)	OK (108ns)	OK (108ns)	OK (431ns)	OK (109ns)	OK (130ns)	OK (157ns)
Average		100%	100%	100%	100%	100%	100%	100%	100%
(double click mat	rix to	select	all for	conv	and na	(ate)			

Check OpenRelay

自俞	🗲 i 🎽 www.mailra	dar.com/openrelay/		C.	- 9
YOUR FAVOU					Feedback Be
Home	Mail Servers Statistics	Articles & Tutorials	SysAdmin Tools	Link to us	Free re

rticles & tutorials	🔊 🛛 Open Relay Test
ackup & Archiving	What is an open relay?
Email Clients	An open relay is a smtp server configured in such a way that is allows a third party t
Mobility	Therefore, such servers are usually targets for spam senders.
Operating Systems	How to test if your mail server is open relay
Reporting Tools	Enter the IP address of your mail server and click the "Test" button below to see if it is an open relay.
Security	
Antispam Antivirus Reports	Please enter IP number of the target host: 178.62.211.175 Test Port 25 is Open at 178.62.211.175
Server Administration	[Method 19 @ 1464514970]
Smart Setups Clustering Virtualization	<<< 220 librebit.net ESMTP Postfix >>> HELO mailradar.com <<< 250 librebit.net >>> MAIL FROM: <postmaster@mailradar.com></postmaster@mailradar.com>
Studies & Benchmarks	<pre><<< 250 2.1.0 Ok >>> RCPT TO: <relaytest@mailradar.com></relaytest@mailradar.com></pre>
Support Services	<< 454 4.7.1 <relaytest@mailradar.com>: Relay access denied</relaytest@mailradar.com>
Neh Integration	>>> QUII <<< 221.2.0.0 Byp

Dovecot with SSL !

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

ssl_cert = </etc/letsencrypt/live/librebit.net/fullchain.pem
ssl_key = </etc/letsencrypt/live/librebit.net/privkey.pem
ssl_ca = </etc/pki/tls/certs/ca-bundle.crt</pre>

ssl_protocols = !SSLv2 !SSLv3



Webmail with SSL !

https://librebit.net

Dav with SSL !

https://librebit.net/baikal/html/dav.php/addressbooks
/testuser/default/

Firewall

Yes, **iptables**! Something like this:

*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT -A INPUT -i lo -j ACCEPT

services
-A INPUT -p tcp --match multiport
 --dports 80,443,25,587,143,993 -j ACCEPT

COMMIT

Questions?

