lab10 - Support #74

Required infrastructure

07.03.2017 11:46 - didi

Status:	In Progress	**Start date:**	15.03.2017
Priority:	Normal	**Due date:**	
Assignee:	didi	**Estimated time:**	0.00 hour

Description

For an overview, see the Wiki: Infrastructure.

Subtasks:

Support # 25: Redmine Setup and workflows	**In Progress**
Support # 78: CRM tool	**New**

Related issues:

Related to lab10 - Feature #50: Get lab10 domain	**Closed**

History

#1 - 12.03.2017 18:14 - didi

- Status changed from New to In Progress

Domains:
lab10.is is being ordered. lab10.coop has been requested (not sure if we can get it before legally founding).
Using gandi.net, because it's seems the best of those offering coop domains and they have a nice slogan (*no bullshit*).
The website is a bit 90ish, but being revamped.
Anyway, who needs a frontend if there's a cli interface.

#2 - 15.03.2017 16:49 - didi

Setting up matrix on a Ubuntu 16.04 CT:

```
wget -q0 - https://matrix.org/packages/debian/repo-key.asc | apt-key add
apt update
apt install matrix-synapse
```

On the host:

```
# forward port
iptables -A PREROUTING -t nat -i eth0 -p tcp -m tcp --dport 8448 -j DNAT --to-destination 192.168.2.114:8448
```

matrix ct:

```
# get certificate
letsencrypt certonly --manual -d matrix.d10r.net --standalone-supported-challenges http-01
# (requires placing a specific file on a webserver this domain resolves to. Or a DNS entry)
# Update certificate path in `/etc/matrix-synapse/homeserver.yaml`.
# Start it
service matrix-synapse start
# takes a while the first time. Progress can be observed with
less +F /var/log/matrix-synapse/homeserver.log
```

Client - Server communication is encrypted.
There's also an option to use E2E encryption for channels, but that's in beta and probably has UX drawbacks.

Server config is currently the default one. Some of the settings:

```
media_store_path: "/var/lib/matrix-synapse/media"
database: "/var/lib/matrix-synapse/homeserver.db"
max_upload_size: "10M"
url_preview_enabled: False
enable_registration_captcha: False
# Enable registration for new users.
enable_registration: True
# If set, allows registration by anyone who also has the shared
# secret, even if registration is otherwise disabled.
registration_shared_secret: "lab10" # this one I set, but seems to have no effect with 'enable_registration' s
et
allow_guest_access: False

Next: [Slack bridge](https://github.com/matrix-org/matrix-appservice-slack)
```

#3 - 15.03.2017 17:59 - didi

- Description updated

#4 - 16.03.2017 00:15 - didi

got lab10.io domain.
Used new gandi web interface. Asked me to switch to "Live DNS".
Tried gandi.cli. Looks great, but seems to not yet work with this Live DNS (can't create record).

Redmine now lives at pm.lab10.io (redmine.d10r.net is redirected).
Updated theme.
Installed time logger plugin.

#5 - 16.03.2017 02:07 - didi

- Related to Feature #50: Get lab10 domain added

#6 - 17.03.2017 00:01 - didi

Installed Nextcloud in cloud.lab10.io (CT 115).
Instructions used:

- https://www.linuxbabe.com/cloud-storage/setup-nextcloud-server-ubuntu-16-04-apache-mariadb-php7 (without the final chmod everything)
- https://vroomtech.io/2016/09/15/installing-nextcloud-on-ubuntu-16-04-lts-with-apache2-lets-encrypt-redis-and-apcu/ (for redis. Except: using apcu for memcache.local as recommended by the docs).

Cronjob set up with crontab -u www-data -e.

Maintenance can be done on cmdline via occ. Example call:
sudo -u www-data php occ maintenance:update:htaccess (the permissions may however get in the way).

Mariadb as Database. Empty root password (bound to localhost only).

bin-log enabled as requested.

Proxied through h1.

TODO: switch to nginx reverse proxy for http/2 support (should considerably speed up Nextcloud).

#7 - 20.03.2017 17:18 - didi

Collabora Online for Nextcloud:
docs
Libreoffice based, allows live collaborative editing, just like GDocs.

```
docker pull collabora/code
docker run -t -d -p 127.0.0.1:9980:9980 -e 'domain=cloud\\.lab10\\.io' --restart always --cap-add MKNOD collab
ora/code
```

Changed the Nextcloud config to be served via https (self signed cert), even though it's reverse proxied. Required for Collabora to work (wants the same port).
First impression is good. Writing a bit laggy.

#8 - 13.04.2017 03:31 - didi

Had first contact with mail spam problematic (see #37-45)
and installed gitlab (see #37-46).

#9 - 20.04.2017 00:07 - didi

We had a gitlab intro: #37-48

The gitlab server now has a dedicated IP: 5.9.14.94. (note that SSL certs were manually copied over from h1. Need to figure out a better config when expiring)
In progress: Trying the integrated Mattermost.
Mattermost has its own domain (chat.lab10.io), Gitlab provides SSO for it. (bad redirect_uri in proxy setup helped convince me to give it a dedicated IP).

Gitlab can act as OAuth provider. May be useful (instead of LDAP?)

Mattermost login with gitlab still not working. Error msg in /var/log/gitlab/mattermost/mattermost.log
[2017/04/20 00:39:43 UTC] [EROR] /signup/gitlab/complete:AuthorizeOAuthUser code=500 rid=kikk8cfnz3f6fdjrjkemmishxw uid= ip=80.109.207.136 Token request failed [details: Post https://code.lab10.io/oauth/token: x509: certificate signed by unknown authority]
as described here.

I already copied the chain and fullchain files to /etc/gitlab/trusted-certs and ran gitlab-ctl reconfigure, didn't help.
What finally solved it

The current Android App is shitty, but a new one (React Native based) in the making. Store link.

#10 - 26.04.2017 13:11 - didi

Android Beta of Mattermost doesn't yet support gitlab auth (ticket).

#11 - 04.05.2017 20:56 - didi

Check Linuxtage talk for optimal webserver config (security, performance).

#12 - 04.05.2017 23:08 - didi

A github organization was created: https://github.com/organizations/lab10-coop.
Owned by that org, an OAuth application was created: https://github.com/organizations/lab10-coop/settings/applications/524591
Which was added to the lab10 gitlab config as described here.

However it was not enabled for login (initial config missing) as I'm not sure what implications that has.
It's possible to enable it such that it's still necessary to create an account first. But what's the point then?
In case of enabling without account creation, are there disadvantages? E.g. does Mattermost login still work?

#13 - 04.05.2017 23:10 - didi

Slack -> Mattermost test migration done.
Export, doc.
The simple migration doesn't include files (retains links to Slack).

#14 - 20.05.2017 22:03 - didi

Removed most Nextcloud default files from /var/www/nextcloud/core/skeleton.

Pending: auto-assign new Nextcloud users to group *graz*.
Probably doable with cronjob using occ. Asked in Slack devops channel for help.

#15 - 02.06.2017 19:09 - didi

Added gitlab-mattermost command in /usr/local/bin as described here.

The upcoming Android App doesn't yet support gitlab login. But it's already implemented and should be available in the next update.
I decided to undo the Slack import. Since there will be a gradual switchover, it would mean that different channels have differently big holes in the history. Better start clean.

Backup script in /root/mattermost_backup.sh

#16 - 20.06.2017 19:54 - didi

SMTP Mail sending config for postfix:

Add to /etc/postfix/main.cf:

```
relayhost = mail.gandi.net
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_use_tls = yes
```

Then execute

```
echo "mail.gandi.net    <user>@lab10.io:<password>" > /etc/postfix/sasl_passwd
postmap hash:/etc/postfix/sasl_passwd
chmod 600 /etc/postfix/sasl_passwd
apt-get install libsasl2-modules
service postfix restart
```

Now applications can use localhost without auth for smtp config.
Make sure postfix is listening on the internal interface only: inet_interfaces = loopback-only.

#17 - 11.07.2017 12:56 - didi

Manual renewal of certs for code and chat:

On h1:
cd /etc/letsencrypt/live/ && cp -aL code.lab10.io/ chat.lab10.io/ /var/lib/lxc/116/rootfs/etc/gitlab/ssl.new/

In CT:
gitlab-ctl reconfigure

The Mattermost config is overwritten when upgrading gitlab or when running gitlab-ctl reconfigure.
Since that's very annoying, I looked for a solution.
The most confusing part is that the System Console of Mattermost is hereby basically rendered useless.
Others (e.g. Aral) seem to have the same issue, see https://gitlab.com/gitlab-org/gitlab-mattermost/issues/54.
Not all config options of the json seem to be present in /etc/gitlab/gitlab.rb, but it may cover all we need.