Gitea Jail

This will be our very own, lightweight personal Github/Gitlab. And we'll do something pretty cool with it later.

This should be easy by now, right? Now that it works, it sure looks short and easy...

Set up location of repos/db

```
zfs create -o compress=lz4 -o atime=off zroot/data/git
```

```
zfs create -o compress=lz4 -o atime=off zroot/data/dbs/gitea
```

Create the jail

```
bastille create git_jail 12.1-RELEASE 10.101.10.150
```

Setup - pre-login

Run `/usr/local/scripts/custom_cshrc git_jail` to copy the `.cshrc`.

```
bastille start git_jail
```

Setup - post-login

Log into console.

```
bastille console git_jail
```

Download packages possibly needed. (Possibly with `sqlite3` as well)

```
pkg install -y git gitea vim-console
```

Create the folder where the nullfs mount will occur (for one of the two; the other was created by installing gitea).

```
mkdir -p /usr/local/data/git
```

```
chown git:git /usr/local/data/git
```

The `chown` command is probably premature. After the jail is restarted with the updated `fstab`, you probably need to do it again (from within the jail), and it may need to be done for the other directory (nullfs-mounted) in the `fstab` as well.

`Exit` the console.

Finishing setup touches

Stop the jail.

```
bastille stop git_jail
```

Edit the `fstab` of this thin jail to mount the git dataset.

```
# Device                Mountpoint                                          FStype  Options Dump  Pass#
/usr/local/data/git     /usr/local/bastille/jails/git_jail/root/usr/local/data/git  nullfs  rw,late 0     0
/usr/local/data/dbs/gitea /usr/local/bastille/jails/git_jail/root/var/db/gitea      nullfs  rw,late 0     0
```

For the db, we'll need to allow raw sockets. (Actually, probably not needed if using `sqlite3`. Needed for `Mariadb` though.)

```
echo 'allow.raw_sockets = "1";' >> /usr/local/bastille/jails/git_jail/jail.conf
```

And we'll start up the jail again.

```
bastille start git_jail
```

May want to pop into the console now to change ownership (`chown`) of the "Device" entries from the `fstab`.

Jail is ready for package setup

Sqlite3

I tried to `pkg install` it, but it said it was already there. No further setup should be necessary. I was having issues at first, and I couldn't figure out the problem, so I ended up creating the db ahead of time in case that was it. I don't think it was, and so creating the db ahead of time should not be

needed.

Gitea

Enable it.

```
bastille sysrc git_jail gitea_enable=YES
```

Make a backup of the config file. First, log into the console.

```
bastille console git_jail
```

```
cp /usr/local/etc/gitea/conf/app.ini /usr/local/etc/gitea/conf/app.ini.bak
```

Configure as necessary the `/usr/local/etc/gitea/app.ini`. (View the changes, but you can't make them all yet. See below.)

```
#APP_NAME can be fun to change

[database]
< USER = root
> USER = git

[oauth2]
< JWT_SECRET = D56bmu6xCtEKs9vKKgMKnsa4X9FDwo64HVyaS4fQ...
> JWT_SECRET = HO8YPNfNkhB_-ESE5e637TQcbja0WylppIsiFdgm...

[picture]
DISABLE_GRAVATAR = true

[repository]
# I copied (cp -a) the .gitconfig and .ssh file and dir from /usr/local/git (the default git home dir)
< ROOT = /var/db/gitea/gitea-repositories
> ROOT = /usr/local/data/git

# I have this for later.  I think I'll enable it, since I'm the only user.
> # Default is false. If true, user can create a repo by pushing local to remote (gitea)
> #ENABLE_PUSH_CREATE_USER = true

# See below for how to use gitea's built-in secret tool to replace the existing ones.
[security]
```

```
< INTERNAL_TOKEN = 1FFhAklka01JhgJTRUrFujWYiv4ijqcTlfXJ9o4n1fWxz+XVQdXhrqDTlsnD7fvz7g
< SECRET_KEY   = ChangeMeBeforeRunning
> INTERNAL_TOKEN = eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYmYiOjE1OTU2NDA4NjB9.oZEw2...
> SECRET_KEY = qVvCzqg4mqe2tQHmZfE99EvzADFvOMY9fO3BdTFw4vwcBVvfAdyxJyBL9Hg...

[server]
< DOMAIN       = localhost
< HTTP_ADDR    = 127.0.0.1
< ROOT_URL     = http://localhost:3000/
> DOMAIN       = gitea.mydomain.tld
> HTTP_ADDR    = 10.101.10.150
> ROOT_URL     = https://gitea.mydomain.tld:443/ # this is the "https clone address/port"
# Note that internally, it's still listening on port 3000.  ^^ that's for the clone button
< SSH_PORT     = 22
> SSH_PORT     = 40202 # this is the clone port for ssh

> START_SSH_SERVER = true # to make gitea manage ssh connections, instead of the host
> SSH_LISTEN_HOST = 10.101.10.150
> SSH_LISTEN_PORT = 22002 # non-root user can't listen on 22
> LANDING_PAGE = explore # this shows the repos, instead of a gitea advert

# to prevent web registrations
[service]
< DISABLE_REGISTRATION   = false
> DISABLE_REGISTRATION   = true
```

What is shown above is that the secrets have already been updated. Here's how to do it.

```
sed -i .tmp 's/^JWT_SECRET.*=.*$/JWT_SECRET = '`gitea generate secret JWT_SECRET`'/g' \
/usr/local/etc/gitea/conf/app.ini
```

```
sed -i .tmp 's/^INTERNAL_TOKEN.*=.*$/INTERNAL_TOKEN = '`gitea generate secret INTERNAL_TOKEN`'/g' \
/usr/local/etc/gitea/conf/app.ini
```

```
sed -i .tmp 's/^SECRET_KEY.*=.*$/SECRET_KEY = '`gitea generate secret SECRET_KEY`'/g' \
/usr/local/etc/gitea/conf/app.ini
```

Diff the new with the backup to make sure it looks right.

```
diff /usr/local/etc/gitea/conf/app.ini.bak /usr/local/etc/gitea/conf/app.ini
```

> Check file permissions for `/var/log/gitea` and `/var/db/gitea`. You may need to `chown -R git:git`. If it doesn't work, also check `/usr/local/data/git` and ...

And get it running.

```
service gitea start
```

And check the `status`, just to make sure.

Wrapping up

You're about to update the reverse proxy, so you better have the CNAME record by now.

Update Caddyfile. (v1)

```
gitea.mydomain.tld {
    proxy / 10.101.10.150:3000
}
```

DigitalOcean firewall

Since we're using a jail, we defined a different SSH port that PF will forward to the jail. We need to allow that port through the DigitalOcean firewall, in the Networking tab.

PF

```
git_ssh = "40202"

gitea_jail = "10.101.10.150"

rdr pass inet proto tcp from any to any port $git_ssh -> $gitea_jail port 22002
```

As usual, test with `pfctl -vnf /etc/pf.conf`, and then remove `vn` if it's all good.

Create gitea user

```
su git
```

```
gitea admin create-user --username c00ldude --password 1234superpass \
--email username@gmailorwhatever.com --admin -c /usr/local/etc/gitea/conf/app.ini
```

Repeat that command if you want to create additional users (because you turned off web registrations).

Log in to the web interface

You're ready to use the username and password to log in and start creating repos.

References

Used https://www.ccammack.com/posts/jail-gitea-in-freebsd/ for some help... but it was incomplete...

Helpful stuff here too: https://docs.gitea.io/en-us/config-cheat-sheet/

Revision #1
Created 5 August 2020 07:37:05 by scoob
Updated 31 July 2021 04:50:03 by scoob