GoToSocial and SELinux

Making SELinux Happy

If you try to run the service right now:

```
sudo systemctl enable --now gotosocial.service
```

you'll notice it fails right away with an odd error.

```
Sep 26 05:22:34 vultr.guest systemd[1]: Starting GoToSocial Server...
Sep 26 05:22:34 vultr.guest systemd[4941]: gotosocial.service: Failed to locate executable
/gotosocial/gotosocial: Permission denied
Sep 26 05:22:34 vultr.guest systemd[4941]: gotosocial.service: Failed at step EXEC spawning
/gotosocial/gotosocial: Permission denied
Sep 26 05:22:34 vultr.guest systemd[1]: gotosocial.service: Main process exited, code=exited,
status=203/EXEC
Sep 26 05:22:34 vultr.guest systemd[1]: gotosocial.service: Failed with result 'exit-code'.
Sep 26 05:22:34 vultr.guest systemd[1]: Failed to start GoToSocial Server.
```

This is because the permissions don't quite fit with SELinux, and so SELinux has decided to deny GoToSocial from starting.

SELinux is something that runs in Rocky Linux and other Linux distros like it. Its purpose is to put limits on things like what resources applications are allowed to access. If its permissions aren’t properly set, it can cause issues like the ones we’re seeing here.

We can solve this in one of two ways: the easy way, or the secure way. (You're probably perfectly fine just doing it the easy way, but I prepared the secure way in case you want it!) Follow the instructions according to which path you're comfortable taking:

The Easy Way

We set SELinux into permissive mode - effectively, make it not really matter what SELinux thinks.

```
sudo setenforce 0
```

This sets it temporarily into permissive mode, so it takes effect right away. We then edit a line in /etc/selinux/config to make this permanent so it continues to persist after restarts:

```
# change
SELINUX=enforcing
# to
SELINUX=permissive
```

You can also set it to "disabled" in this file if you want to completely disable SELinux. Either way, it should not hinder starting GoToSocial anymore. Skip "The Secure Way" and continue onwards to "Creating a User".

The Secure Way

This might be a bit of a headache, but it'll be more secure - we basically import an SELinux policy for GoToSocial, and patch it over time if GoToSocial ever needs new permissions. Doing this has the benefit of not having to disable SELinux.

Use git to clone a fork of this selinux policy modified to work with our setup:

```
git clone https://git.tenna.zip/tenna/gotosocial-selinux
```

Compile it and run the included script to re-label some files:

```
cd gotosocial-selinux
sudo make -f /usr/share/selinux/devel/Makefile load
sudo ./gotosocial-selinux-relabel
```

Run gotosocial again, and see what happens!

```
sudo systemctl start gotosocial
```

If it works, great! If SELinux doesn't allow it to do something for some reason, get SELinux to give you a config that would fix that problem:

```
sudo sepolgen-ifgen
sudo audit2allow -larR
```

It'll spit out some code - add this to the selinux files where relevant. Re-compile it and restart GoToSocial.

> If you're having trouble with this, feel free to ask about it in Zulip. There is, also, of course, the option of just disabling SELinux if worst comes to worst, but it's good to keep it enabled if at all possible!

Revision #1
Created 2025-10-14 07:55:27 UTC by alloyed
Updated 2025-10-14 07:56:47 UTC by alloyed