

# 2025-03-15: git.lix.systems replication broke

On 2025-03-15, the git.lix.systems host (which runs gerrit.lix.systems and identity.lix.systems also) got migrated to the forkos infra repo.

Fixes: <https://git.lix.systems/the-distro/infra/pulls/193>

This broke Gerrit replication due to multiple reasons:

- Change in the user being used, causing loss of the weird home directory that was configured for ssh
  - Configuration drift: the ssh key for that user not being managed with agenix and thus not being known when reading the box's configuration
- Mistake in the NixOS configuration where the replication config wound up in `services.gerrit.settings` rather than `services.gerrit.replicationSettings`, and also lost its `remote.` prefix: was `services.gerrit.settings.replicationSettings.lix-forgejo` rather than `services.gerrit.replicationSettings.remote.lix-forgejo` during the migration.
- Terrible timing of someone force pushing a `sb/` ref to Gerrit, which exposed a broken branch protection rule in the `lix-project/lix` repo that prevented the force push being replicated. The branch protection rule had to be deleted since [Forgejo does not support force pushes to protected branches](#) at all.

This was merely terrible timing since it looked like it was related to the previous causes.

## Impact

Very little, it blocked some changes getting out to users for a few hours, but people being sleepy does that too.

## What could have gone better

- I wish the logging in either forgejo or gerrit replication actually output pre-receive hook failures to some visible log
- For some reason the box went offline when I deployed a nearly no-op NixOS config to it. Connectivity issues??
  - Do we have recovery root passwords for fixing our hosts from the console somewhere? Should we?
- Don't have monitoring for sync failures (though tbf it is kind of obvious if you hit the merge button on gerrit and the thing goes missing. it probably would never survive much more than a day).

# Notes on resolving it

## Misconfigurations

I queried the config remotely:

```
ssh -p 2022 jade@gerrit.lix.systems replication list
```

and there was nothing in there.

I looked in `journalctl -fu gerrit`, obtaining:

```
com.google.source.gerrit.plugins.replication.DestinationConfigParser : Replication config does not exist or it's empty; not replicating
```

This seemed suspicious. I opened a `colmena repl` on the old configuration and evaluated:

```
nix-repl> nodes.lix-systems.config.systemd.services.gerrit.preStart
"set -euo pipefail\n\n# bootstrap if nothing exists\nif [[ ! -d git ]]; then\n  gerrit init --batch -\n  -no-auto-start\nfi\n\n# install gerrit.war for the plugin manager\nrm -rf bin\nmkdir bin\nln -sfv /nix/store/r6sm94drx3mq16da3ycrz298f0sli0ir-gerrit-3.10.3/webapps/gerrit-3.10.3.war bin/gerrit.war\n\n# copy the config, keep it mutable because Gerrit\nln -sfv /nix/store/hbc7sdhzbpi3xy46hx1y5c4vix4zkk3l-gerrit.conf etc/gerrit.config\nln -sfv /nix/store/5szrq197711dxszk7f28mkjyq74gn3h8-replication.conf etc/replication.config\n\n# install the plugins\nrm -rf plugins\nln -sv /nix/store/9r8qq5hkkdhgjs2wsfjj5axlifqssqg-gerrit-plugins plugins\n"
```

Then to realise the old replication config I did:

```
nix-repl> builtins.getContext nodes.lix-systems.config.systemd.services.gerrit.preStart
{
  "/nix/store/7hsidqxc47vmwrgb5d6i8vmr9h80cirg-gerrit.conf.drv" = { ... };
  "/nix/store/8g04n8c32kd329b1wsfmm27c6s82i627-replication.conf.drv" = { ... };
  "/nix/store/lv9g1h4wyhc9fyxz22yf4q5raq1snhw0-gerrit-plugins.drv" = { ... };
  "/nix/store/qrh1zjf41m5dmcfjmy2aw6dh5gj0vgj-gerrit-3.10.3.drv" = { ... };
}
```

Copy pasted the string out of there (n.b. <https://git.lix.systems/lix-project/lix/issues/74> `nix-store -r` and looked at the config:

```
[remote "forgejo"]
  mirror = true
```

```
projects = "lix"
projects = "lix-installer"
push = "+refs/heads/*:refs/heads/*"
push = "+refs/tags/*:refs/tags/*"
remoteNameStyle = "dash"
replicatePermissions = false
threads = 3
timeout = 30
url = "git@git.lix.systems:lix-project/${name}.git"
```

```
[remote "github"]
  mirror = true
  projects = "lix"
  push = "+refs/heads/main:refs/heads/main"
  push = "+refs/heads/release-*:refs/heads/release-*"
  push = "+refs/tags/*:refs/tags/*"
  remoteNameStyle = "dash"
  replicatePermissions = false
  threads = 3
  timeout = 30
  url = "git@github.com:lix-project/${name}.git"
```

As intended!

Then I just looked harder at how the nix code was generating the new one and why it didn't wind up there. Easy enough.

Set it up correctly, `systemctl restart gerrit` .

## Fixed config, still broken

However, it was still fucked. There was some stuff in the log about not having known hosts. Here I learned that Great Value brand java ssh ignores the global known hosts file in ssh, and that we had a `/var/lib/gerrit-home` which was set up manually (configuration drift) which was not `$HOME` for the Gerrit user but was the homedir in `/etc/passwd` for it, and this configuration got lost in the migration that changed gerrit to run as the `git` user.

```
/var/lib/gerrit/logs/replication_log :
```

```
[2025-03-16 05:23:57,706] Cannot replicate to git@git.lix.systems:lix-project/lix.git [CONTEXT
pushOnId="cd6a8964" ]
org.eclipse.jgit.errors.TransportException: git@git.lix.systems:lix-project/lix.git: Cannot log in at
```

```
git.lix.systems:22
publickey: no keys to try
```

So I migrated this directory to a `/run/gerrit-bogus-home-directory`, which is on tmpfs and cannot drift since it will vanish every boot. Then it is set up with systemd-tmpfiles with a pile of symlinks. Now I guess the `git` user has a bogus home directory for gerrit purposes.

## Replication still broken

And now we arrive at bad luck, finding out *today* that nobody has force pushed a `sb/` ref before it happening during an outage. Imao.

You can restart replication manually with:

```
ssh -p 2022 jade@gerrit.lix.systems replication start
```

`/var/lib/gerrit/logs/replication_log`:

```
[2025-03-16 05:36:36,655] Replication to git@git.lix.systems:lix-project/lix.git started... [CONTEXT
pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:36,660] Replication to git@git.lix.systems:lix-project/lix-installer.git started... [CONTEXT
pushOnId="62ca8c96" request="SSH" ]
[2025-03-16 05:36:36,659] Replication to git@github.com:lix-project/lix.git started... [CONTEXT
pushOnId="2261f48a" request="SSH" ]
[2025-03-16 05:36:36,911] Push to git@git.lix.systems:lix-project/lix.git references:
RemoteRefUpdate{refSpec=refs/heads/sb/rbt/justfile:refs/heads/sb/rbt/justfile, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[12499a6b0586fe8481bf71767908f775c6f84224], force=yes, delete=no, fwd=no},
RemoteRefUpdate{refSpec=refs/heads/sb/pennae/ci-config:refs/heads/sb/pennae/ci-config, statu
s=NOT_ATTEMPTED, id=(null)..AnyObjectId[5e95db3e1ce1dc57439dfc487f40b34237426840], force=yes,
delete=no, fwd=no}, RemoteRefUpdate{refSpec=refs/heads/sb/pennae/io-rewrite:refs/heads/sb/pennae/io-
rewrite, status=NOT_ATTEMPTED, id=(null)..AnyObjectId[e0beb9b1185ca484ea31248e651ef036f94bea6c],
force=yes, delete=no, fwd=no}, RemoteRefUpdate{refSpec=refs/heads/main:refs/heads/ma
in, status=NOT_ATTEMPTED, id=(null)..AnyObjectId[29732f19a2a9e0d9e7a5bad953c4fad6f719c50e],
force=yes, delete=no, fwd=no}, RemoteRefUpdate{refSpec=refs/heads/sb/tom-hubrecht/primops.cc-
v2:refs/heads/sb/tom-hubrecht/primops.cc-v2, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[78c286a97d2da59783fedbba9cd57360207a9e74], force=yes, delete=no, fwd=no},
RemoteRefUpdate{refSpec=re
fs/heads/sb/raito/phantom-referrers-gc:refs/heads/sb/raito/phantom-referrers-gc, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[64a2f038b19d2b6d3f66df29da80c965496afb6d], force=yes, delete=no, fwd=no},
RemoteRefUpdate{refSpec=null:refs/heads/rbt/pre-commit-update, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, ff
wd=no}, RemoteRefUpdate{refSpec=null:refs/heads/sb/arcuru/commit-msg, status=NOT_ATTEMPTED,
```

```
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no},
RemoteRefUpdate{refSpec=null:refs/heads/sb/fuck/what, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no},
RemoteRefUp
date{refSpec=null:refs/heads/sb/lunaphied/meow, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no},
RemoteRefUpdate{refSpec=null:refs/heads/sb/pamplemousse/diff-closures-json, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no},
RemoteRefUp
date{refSpec=null:refs/heads/sb/pennae/parser-rewrite, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no},
RemoteRefUpdate{refSpec=null:refs/heads/sb/rbt/makeflags, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no},
RemoteRefUpdate{refSpe
c=null:refs/heads/sb/rbt/pre-commit, status=NOT_ATTEMPTED,
id=(null)..AnyObjectId[0000000000000000000000000000000000000000], force=yes, delete=yes, fwd=no}
[CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:36,922] Replication to git@git.lix.systems:lix-project/lix-installer.git completed in 262ms,
15000ms delay, 0 retries [CONTEXT pushOnId="62ca8c96" request="SSH" ]
[2025-03-16 05:36:37,500] Failed replicate of refs/heads/sb/rbt/justfile to git@git.lix.systems:lix-project/lix.git,
reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,501] Failed replicate of refs/heads/sb/pennae/ci-config to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,501] Failed replicate of refs/heads/sb/pennae/io-rewrite to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,502] Failed replicate of refs/heads/main to git@git.lix.systems:lix-project/lix.git, reason:
pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,502] Failed replicate of refs/heads/sb/tom-hubrecht/primops.cc-v2 to
git@git.lix.systems:lix-project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63"
request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/railto/phantom-referrers-gc to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/rbt/pre-commit-update to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/arcuru/commit-msg to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/fuck/what to git@git.lix.systems:lix-project/lix.git,
reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/lunaphied/meow to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
```

```
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/pamplermousse/diff-closures-json to
git@git.lix.systems:lix-project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63"
request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/pennae/parser-rewrite to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/rbt/makeflags to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,503] Failed replicate of refs/heads/sb/rbt/pre-commit to git@git.lix.systems:lix-
project/lix.git, reason: pre-receive hook declined [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,504] Replication to git@git.lix.systems:lix-project/lix.git completed in 847ms, 15001ms
delay, 0 retries [CONTEXT pushOnId="e26afc63" request="SSH" ]
[2025-03-16 05:36:37,538] Replication to git@github.com:lix-project/lix.git completed in 877ms, 15002ms delay,
0 retries [CONTEXT pushOnId="2261f48a" request="SSH" ]
```

So. What's this? What is this purported pre-receive hook? Where are the error logs? Well, you see, gerrit replication plugin was really hungry and ate them for lunch. Oops. Sorry.

I had enough of bad logging at this point and applied some force: I changed the pre-receive hook of the Lix repo to use funnily named tools to dump the output from the hook into syslog so I could actually debug it:

```
#!/usr/bin/env bash
# AUTO GENERATED BY GITEA, DO NOT MODIFY
/nix/store/19c03xa1hmv10pgqhs73y7ahhs7c253c-forgejo-10.0.1/bin/forgejo hook --
config=/var/lib/forgejo/custom/conf/app.ini pre-receive 2>&1 | /nix/store/l2hq7lzyw3s93ca0hlg61dn68rz8fazv-
moreutils-0.70/bin/pee /run/current-system/sw/bin/logger /run/current-system/sw/bin/cat
```

Auto generated, whatever. And then:

```
Forbidden: Branch: sb/rbt/justfile in <Repository 2:lix-project/lix> is protected from force push
```

Well there's your problem. I deleted the branch protection rule and filed a bug in Forgejo about supporting our use case.

---

Revision #1

Created 16 March 2025 06:17:00 by jade

Updated 16 March 2025 06:48:56 by jade