

comin

GitOps For NixOS machines

github.com/nlewo/comin

What is GitOps

The core idea of GitOps is having

- ① a Git repository that contains declarative descriptions currently desired in the production environment
- ② and an automated process to make the production environment match the described state in the repository.

Source: <https://www.gitops.tech>

What is GitOps

The core idea of GitOps is having

- 1 a Git repository that contains declarative descriptions currently desired in the production environment
- 2 and an automated process to make the production environment match the described state in the repository.

Source: <https://www.gitops.tech>



How did I come to GitOps

In 2019, with a 10 lines shell script.

How did I come to GitOps

In 2019, with a 10 lines shell script.

Every 5 min, the shell script

- 1 checkouts new commits from the repository,
- 2 verifies Git commit signatures,
- 3 runs `nixos-rebuild --switch`

How did I come to GitOps

In 2019, with a 10 lines shell script.

Every 5 min, the shell script

- 1 checkouts new commits from the repository,
- 2 verifies Git commit signatures,
- 3 runs `nixos-rebuild --switch`

To deploy a change, a user

- 1 pushes the commit to the main branch

How did I come to GitOps

In 2019, with a 10 lines shell script.

Every 5 min, the shell script

- 1 checkouts new commits from the repository,
- 2 verifies Git commit signatures,
- 3 runs `nixos-rebuild --switch`

To deploy a change, a user

- 1 pushes the commit to the main branch

Advantages:

- Autonomy (no forge dependency)
- Simplicity (easy to setup, without any secrets)

Comin

`comin` is a NixOS deployment tool operating in pull mode.

Running on a machine, it periodically,

- polls Git repositories for new commits
- builds and deploys the NixOS configuration

- <https://github.com/nlewo/comin>
- Started in 2022
- Written in Go under MIT license
- v1 has not been released yet

Comin features

- On the main branch, only fast forward is allowed
- Support testing branches to try changes
 - Run `nixos-rebuild -test`
- Poll multiple Git remotes (to avoid SPOF)
- Fast iterations with local remotes
- Support machine migrations (optionally check the `machine-id`)
- Prometheus metrics
- Manage system profiles
- `comin status`

Comin planned features

- Git commit signature checks
- Non flake support
- Automatic reboots
- Deployment retries
- `comin pause` to stop deployments
- `comin fetch` to manually fetch a remote
- Webhooks to trigger remotes fetches

Conclusion

- + All my own machines are always on the main branch
- + Really easy to deploy a change on all my machines
- + Fun to write
- It is slower to try a change

Conclusion

- + All my own machines are always on the main branch
- + Really easy to deploy a change on all my machines
- + Fun to write
- It is slower to try a change

And I still need to replace the shell script by comin...

Thank you!

<https://github.com/nlewo/comin>