

Building and testing untrusted Code with NixOS

Why?

- Want to automatically run tests and build code
- Untrusted input

Traditional VMs

- Hardware emulation
- Full UEFI firmware
- Slow Boot
- VMM is large and complex

Strong isolation possible (VM guest cannot easily escape into host)

Containers

- Flexible
- Fast
- Many deployment options (docker, kubernetes, podman)

- No strong isolation between container and host

Let's meet in the middle

We want the flexibility of containers and the isolation of VMs

What is a microvm

- Remove all of the bloat
- Minimize overhead
- Almost no device support
 - Filesystem
 - Networking
 - vsock
- Fast boot (few milliseconds to boot into linux)

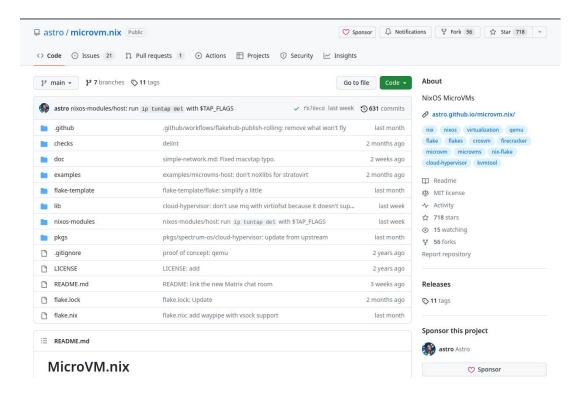
What is a microvm







Astro microvm project



Astro microvm project

Tool to run microvms on top of NixOS

Input:

nixosConfiguration

Output:

- Bootable microvm image

TODO

- Create base images for CI pipelines
 - GitHub Actions
 - GitLab
- Tools for automatic scheduling and registration