



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



Firecracker




# Astro microvm project

[astro / microvm.nix](#) Public

[Sponsor](#) [Notifications](#) [Fork 56](#) [Star 718](#)

[Code](#) [Issues 21](#) [Pull requests 1](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

[main](#) [7 branches](#) [11 tags](#) [Go to file](#) [Code](#)

 **astro** `nixos-modules/host: run ip tuntap del with $TAP_FLAGS` ✓ rb78ecd last week 🔄 631 commits

📁 .github	.github/workflows/flakehub-publish-rolling: remove what won't fly	last month
📁 checks	delint	2 months ago
📁 doc	simple-network.md: Fixed macvtap typo.	2 weeks ago
📁 examples	examples/microvms-host: don't noXlibs for stratovirt	2 months ago
📁 flake-template	flake-template/flake: simplify a little	last month
📁 lib	cloud-hypervisor: don't use mq with virtiofsd because it doesn't sup...	last week
📁 nixos-modules	nixos-modules/host: run <code>ip tuntap del</code> with \$TAP_FLAGS	last week
📁 pkgs	pkgs/spectrum-os/cloud-hypervisor: update from upstream	last month
📄 .gitignore	proof of concept: qemu	2 years ago
📄 LICENSE	LICENSE: add	2 years ago
📄 README.md	README: link the new Matrix chat room	3 weeks ago
📄 flake.lock	flake.lock: Update	2 months ago
📄 flake.nix	flake.nix: add waypipe with vsock support	last month

☰ README.md

## MicroVM.nix

## About

NixOS MicroVMs

[astro.github.io/microvm.nix/](#)


[nix](#) [nixos](#) [virtualization](#) [qemu](#) [flake](#) [flakes](#) [crosvm](#) [firecracker](#) [microvm](#) [microvms](#) [nix-flake](#) [cloud-hypervisor](#) [kvmtool](#)

📖 Readme  
📄 MIT license  
🔔 Activity  
⭐ 718 stars  
👁 15 watching  
🍴 56 forks  
Report repository

## Releases

🏷 11 tags

## Sponsor this project

 **astro** Astro [Sponsor](#)



# 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