sysdig

Nix your Python mess

Fede Barcelona

Technical Enablement Engineer

Agenda

1 **The mess**

2 **Introducing Nix**

3 **Nixify your workflow**

4 **Nix Everything Everywhere All at Once**

The mess

The mess: Developer workflow

It works on my machine™...

	Developer Setup	CI/CD Setup	Production/Cloud Setup
OS Setup	GNU-Linux / MacOS		
Package manager (OS)	homebrew / apt / rpm / pacman		
Python version	Which one you need? OS-provided python version?		
Python project manager	pip, poetry, uv, pyenv, pipenv, pip-tools, ...		
Assist software	ruff, black, isort, flake8, mypy, pytest, hypthesis, tox, bandit, vulture, pyright, pre-commit, python-lsp-server		
Install the dependencies for this project	requests, sqlalchemy, pydantic, fastapi, python-jose, redis, emails, reportlab, celery, pendulum		

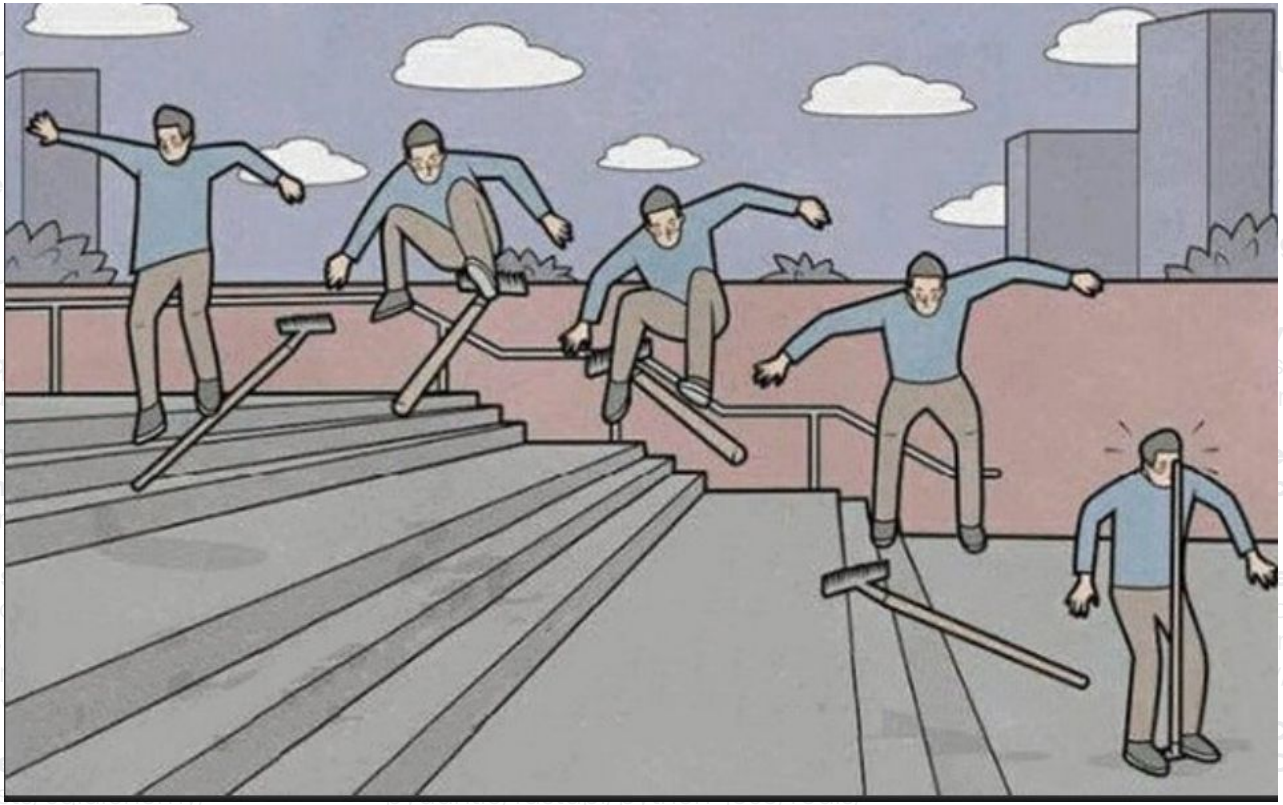
It works on my machine™...

	Developer Setup	CI/CD Setup	Production/Cloud Setup
OS Setup	GNU-Linux / MacOS	GNU-Linux	
Package manager (OS)	homebrew / apt / rpm / pacman	apt / rpm	
Python version	Which one you need? OS-provided python version?	Team decides	
Python project manager	pip, poetry, uv, pyenv, pipenv, pip-tools, ...	pip, poetry, uv, pyenv, pipenv, pip-tools, ...	
Assist software	ruff, black, isort, flake8, mypy, pytest, hypthesis, tox, bandit, vulture, pyright, pre-commit, python-lsp-server	ruff, black, isort, flake8, mypy, pytest, hypthesis, tox, bandit, vulture, pyright, pre-commit	
Install the dependencies for this project	requests, sqlalchemy, pydantic, fastapi, python-jose, redis, emails, reportlab, celery, pendulum	requests, sqlalchemy, pydantic, fastapi, python-jose, redis, emails, reportlab, celery, pendulum	

It works on my machine™...

	Developer Setup	CI/CD Setup	Production/Cloud Setup
OS Setup	GNU-Linux / MacOS	GNU-Linux	GNU-Linux
Package manager (OS)	homebrew / apt / rpm / pacman	apt / rpm	apt / rpm
Python version	Which one you need? OS-provided python version?	Team decides	Platform team decides, multiple projects may depend on the same
Python project manager	pip, poetry, uv, pyenv, pipenv, pip-tools, ...	pip, poetry, uv, pyenv, pipenv, pip-tools, ...	pip
Assist software	ruff, black, isort, flake8, mypy, pytest, hypthesis, tox, bandit, vulture, pyright, pre-commit, python-lsp-server	ruff, black, isort, flake8, mypy, pytest, hypthesis, tox, bandit, vulture, pyright, pre-commit	–
Install the dependencies for this project	requests, sqlalchemy, pydantic, fastapi, python-jose, redis, emails, reportlab, celery, pendulum	requests, sqlalchemy, pydantic, fastapi, python-jose, redis, emails, reportlab, celery, pendulum	requests, sqlalchemy, pydantic, fastapi, python-jose, redis, emails, reportlab, celery, pendulum **EXPECT THE DEPENDENCIES NOT TO BREAK OTHER DEPLOYED PROJECTS**

It works on my machine™...



The industry is trying to solve this problem with...

?

The industry is trying to solve this problem with...

But there's a catch!

Docker for development?

Some problems:

- Slower to work with in MacOS due non-native system
- You need a runtime to bundle your dependencies?
- More complex debugging
- Complex setup for GUI projects
- More complex for projects using network, you need to open ports to test
- Potential security issues (running as root)
- **Not actually reproducible!**

Docker for CI/CD?

Some problems:

- ~~Slower to work with in MacOS due non-native system~~
- You need a runtime to bundle your dependencies? **Maybe.**
- ~~More complex debugging~~
- ~~Complex setup for GUI projects~~
- ~~More complex for projects using network, you need to open ports to test~~
- Potential security issues (building as root) ← **This becomes even more important!**
- **Not actually reproducible!** ← **This becomes even more important!**

Docker for Production?

Okay, for this is actually nice.

- It's the industry standard, and there is a really nice ecosystem around it.
  - Kubernetes
  - Docker-Compose
  - Plain Docker
  - Sysdig Secure and Sysdig Monitor
  - ECS/CloudRun
  - Lambda functions
  - ...
- Once you build the image, it's immutable and you can scan it and deploy it anywhere!...

... the problem is the build of the image.

Not actually deterministic/reproducible

Dockerfile

```
1  FROM python:3.11-slim
2
3  ENV DEBIAN_FRONTEND=noninteractive
4
5  RUN apt-get update && \
6    apt-get install -y --no-install-recommends \
7      build-essential \
8      libpq-dev \
9      gcc \
10     libssl-dev \
11     libffi-dev && \
12   rm -rf /var/lib/apt/lists/*
13
14 WORKDIR /app
15
16 COPY requirements.txt .
17 RUN pip install --no-cache-dir -r requirements.txt
18
19 COPY . .
20
21 EXPOSE 8000
22
23 CMD ["python", "app.py"]
24
```

Not actually deterministic/reproducible

Dockerfile

```
1  FROM python:3.11-slim # <-- May be a different base image after some days
2
3  ENV DEBIAN_FRONTEND=noninteractive
4
5  RUN apt-get update && \ # <-- Update may retrieve a different set of deps after some days
6    apt-get install -y --no-install-recommends \
7      build-essential \ # <-- All dependencies installed here may have a different version
8      libpq-dev \
9      gcc \
10     libssl-dev \
11     libffi-dev && \
12   rm -rf /var/lib/apt/lists/*
13
14 WORKDIR /app
15
16 COPY requirements.txt .
17 RUN pip install --no-cache-dir -r requirements.txt # <-- If dependencies are not fixed with "==" here,
18                                                    #     the versions of the libraries used may change.
19 COPY . .
20
21 EXPOSE 8000
22
23 CMD ["python", "app.py"]
24
```

Vulnerable to Supply-Chain attacks!

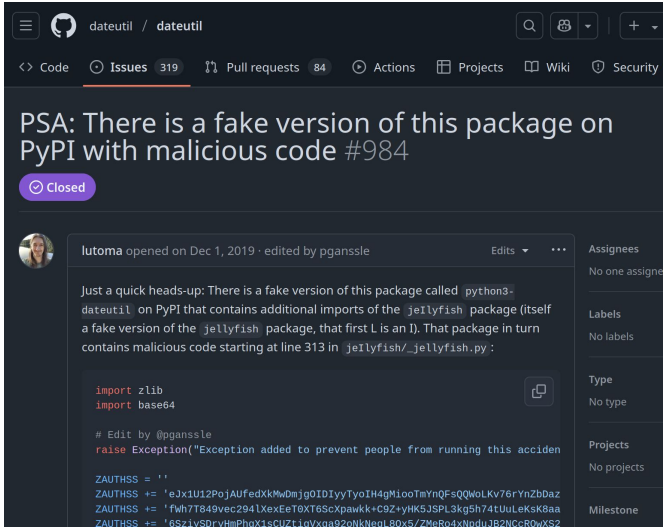
ALERT

Malware Discovered in Popular NPM Package, ua-parser-js

Last Revised: October 22, 2021

Python developers beware: This info stealing malware campaign is targeting thousands of GitHub accounts

Python developers should be wary of an information stealing malware disguised in the popular Colorama python package, which has already compromised a community of over 170,000 users



Resources > Blog > Trojanized PyPI package imitates a popular Python server ...

Trojanized PyPI package imitates a popular Python server library

February 27, 2022 By Ax Sharma

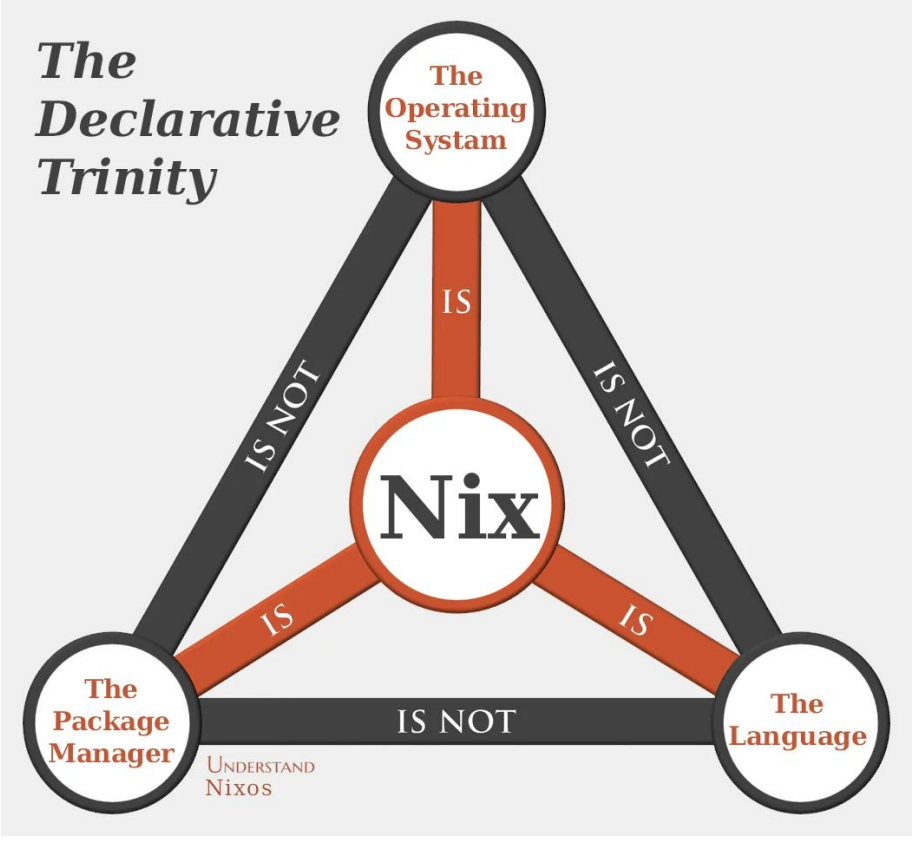
7 minute read time

Aug 24, 2023 / 5 min read / Phylum Research

Rust Malware Staged on Crates.io

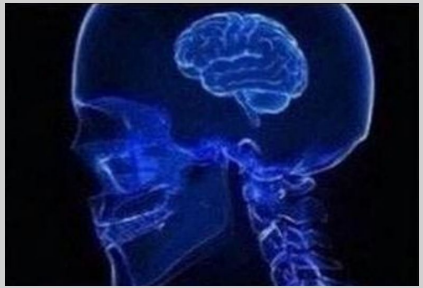
Introducing Nix

But what is Nix?



Nix: A Package Manager

- Install your programs / system libraries (Same as `apt`/`brew`/etc)
- Install your project dependencies (Same as `pip`/`poetry`/etc)
- Build your projects (Same as `cargo`/`docker`/`cmake`)
- Create temporal development environments (Same as `docker`/`virtualenv`)
- Package your project (as docker image, as `.deb`, as `.rpm`, as AppImage, etc)
- Works on GNU-Linux and MacOS
- … But for any programming language!



500

0

Number of fresh packages in repository

Number of packages in repository

1000

GNU Elpa

openSUSE science Tumblewe

MSYS2 msys2

Deb Multimedia Unstable

Gentoo overlay Pentoo

LuaRocks

HP-UX 11.31

Debian 12 Backports

OS4Depot

Open VSX

Libregamewiki

Debian Experimental

KISS Community

Terra 41

Npackd Stable

RPM Fusion Fedora Rawhide

PackMan openSUSE Leap 42.3

MPR

PackMan openSUSE Leap 15.0

openSUSE security Tumbleweed

SliTaz Current

SageMath development

KISS Community - main

Carbs Linux

WakeMeOps

RPM Fusion Fedora 39

Ubuntu 25.04 Proposed

AIX Toolbox

MX Linux MX-19 Testing

UBI 8

yiffOS Knot

MX Linux MX-23 Testing

openSUSE hardware

MX Linux MX-21 Testing

MX Linux MX-19

glaucus

openSUSE Emulators Tumbleweed

MX Linux MX-23

MX Linux MX-21

Salix 14.2

ReactOS rapps

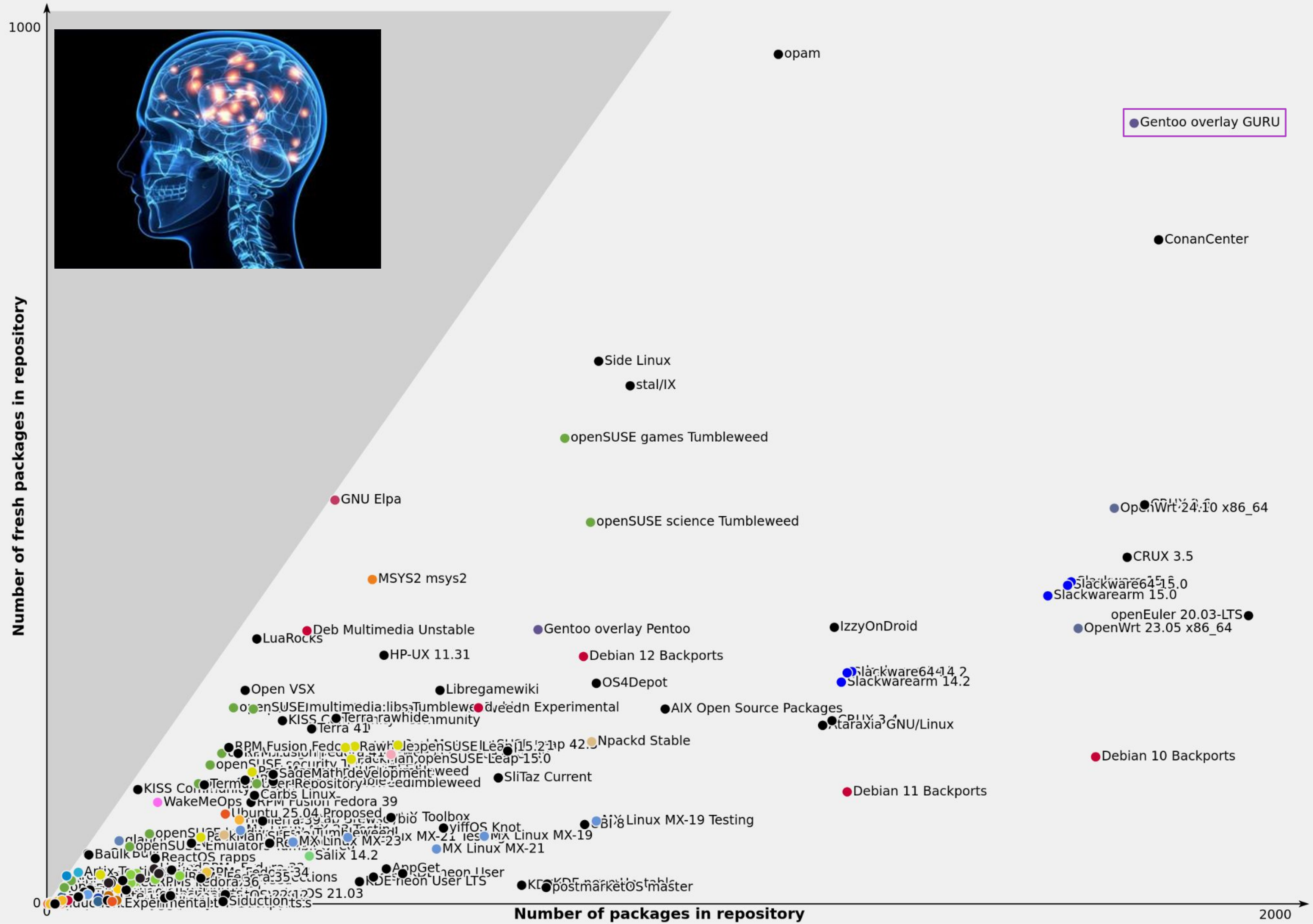
AppGet

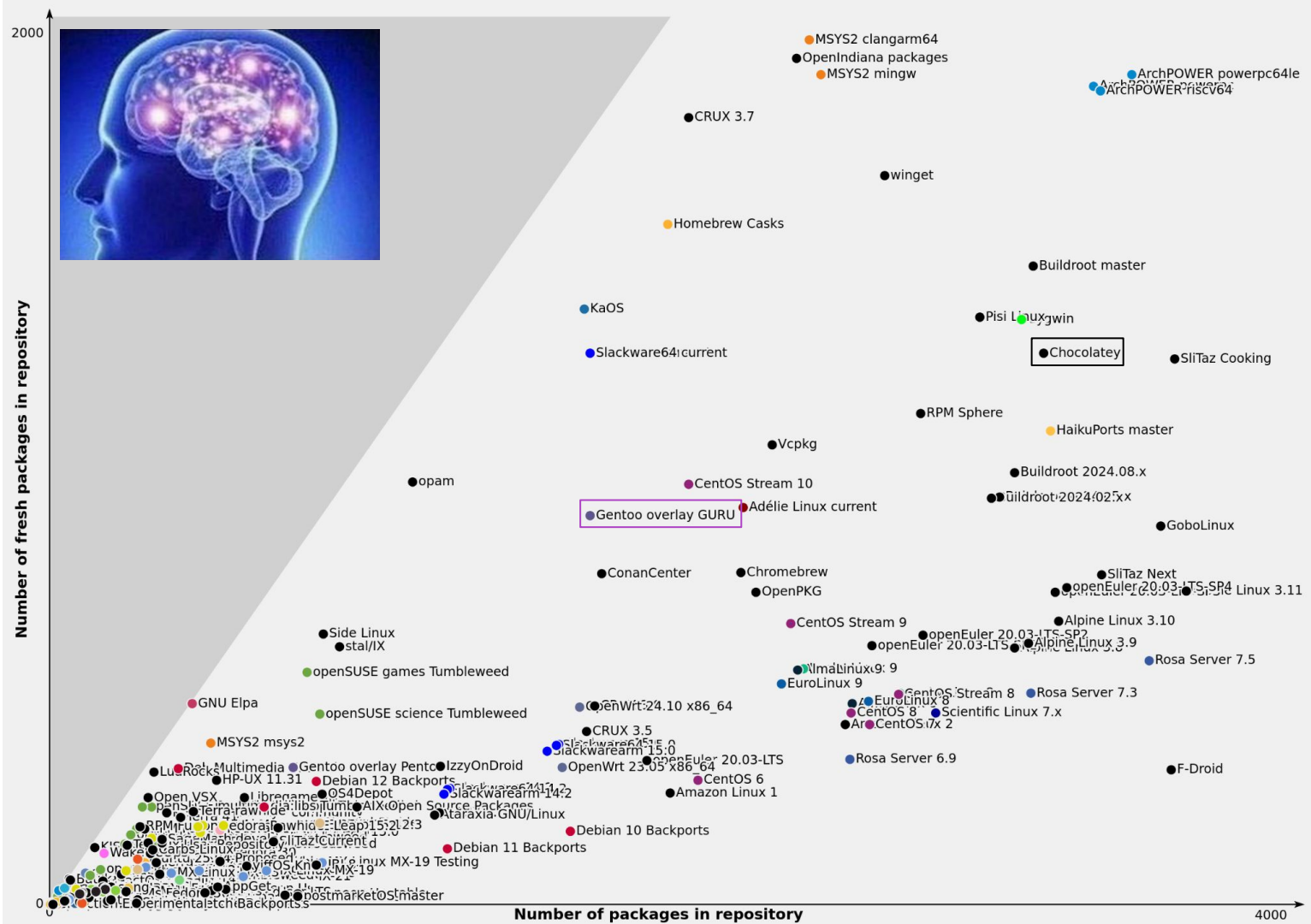
KDE neon User

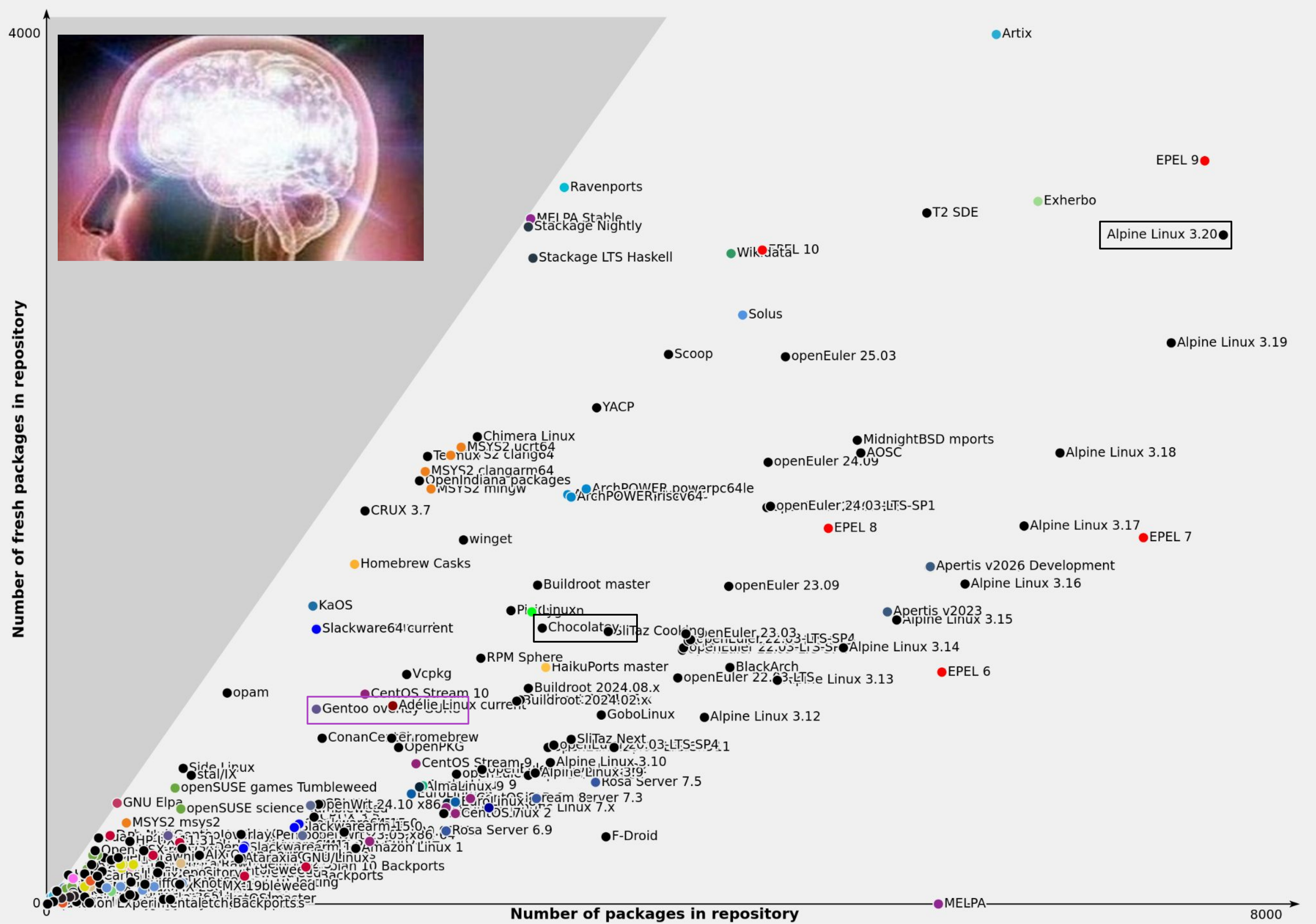
KDE neon User LTS

postmarketOS master

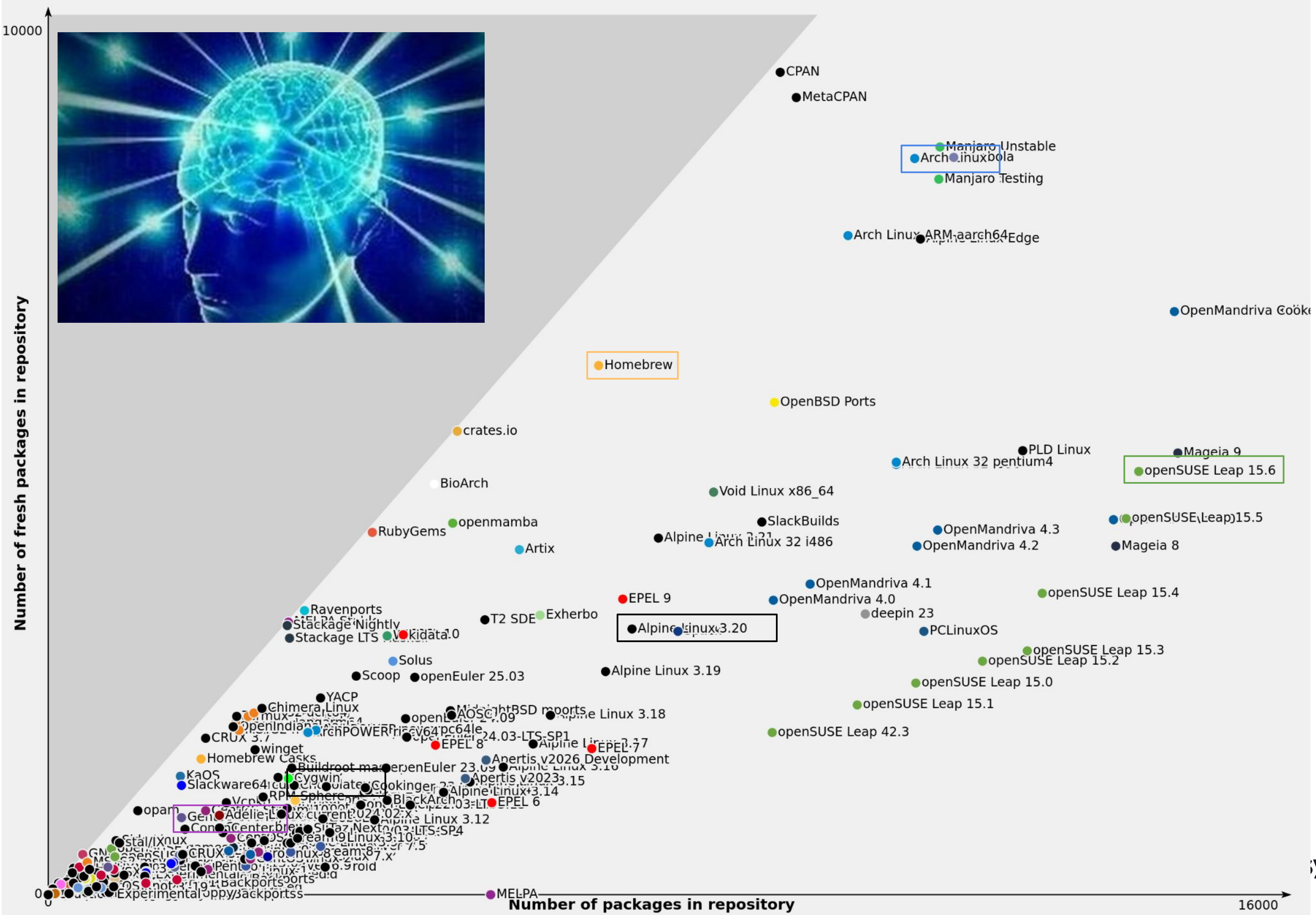
Siduction

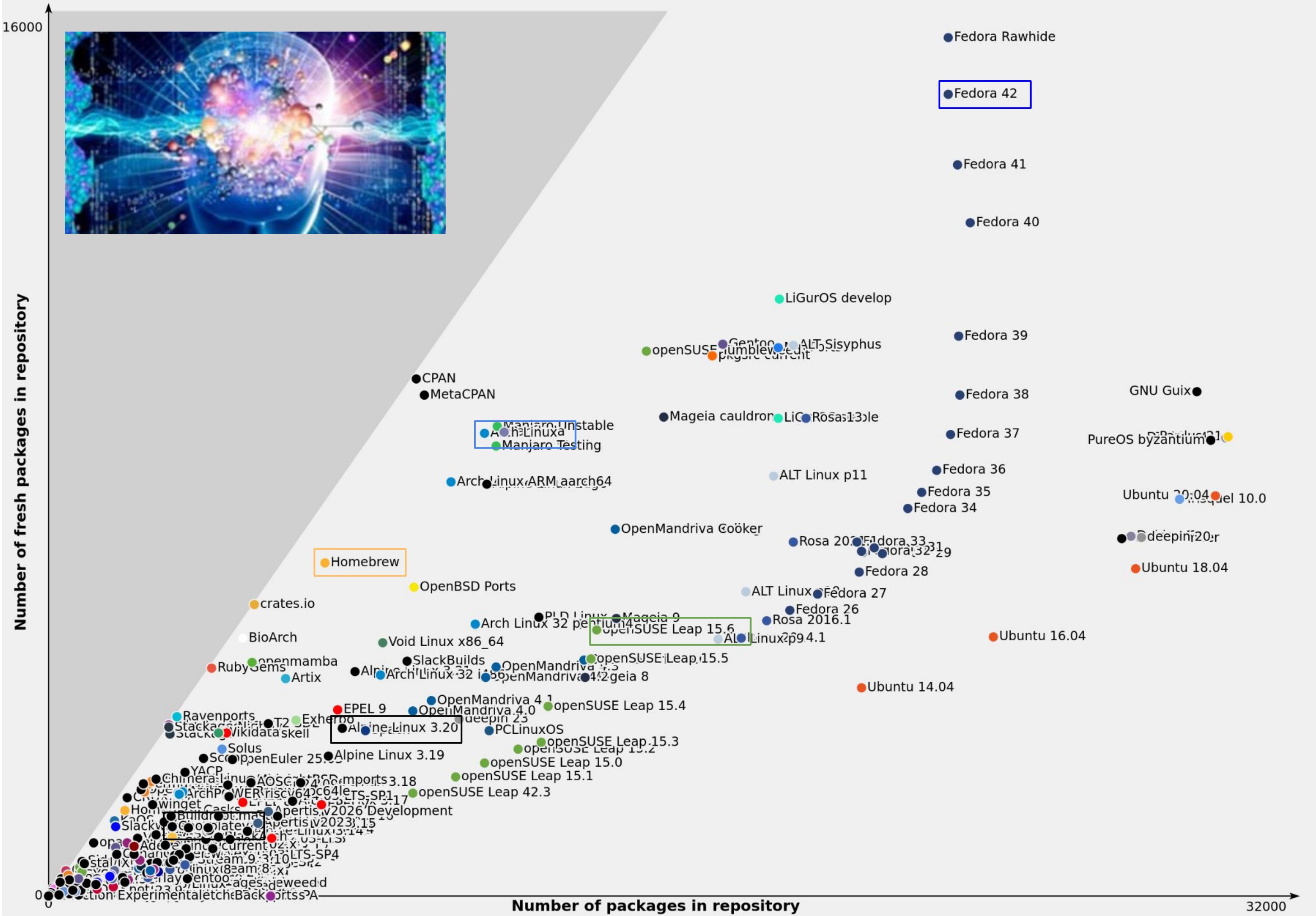

1000
0
0
2000
Number of fresh packages in repository
Number of packages in repository
opam
Gentoo overlay GURU
ConanCenter
Side Linux
stal/IX
openSUSE games Tumbleweed
GNU Elpa
openSUSE science Tumbleweed
OpenWrt 24.10 x86_64
CRUX 3.5
MSYS2 msys2
Slackware64 15.0
Slackwarearm 15.0
openEuler 20.03-LTS
Deb Multimedia Unstable
Gentoo overlay Pentoo
IzzyOnDroid
OpenWrt 23.05 x86_64
LuaRocks
HP-UX 11.31
Debian 12 Backports
Slackwarearm 14.2
Open VSX
Libregamewiki
OS4Depot
AIX Open Source Packages
Ataraxia GNU/Linux
Terra 41
Npackd Stable
Debian 10 Backports
SliTaz Current
WakeMeOps
Carbs Linux
Debian 11 Backports
MX Linux MX-19 Testing
yiffOS Knot
MX Linux MX-19
MX Linux MX-21
MX Linux MX-23
Salix 14.2
ReactOS rapps
AppGet
KDE neon User LTS
postmarketOS master


2000
Number of fresh packages in repository
0
0
Number of packages in repository
4000
MSYS2 clangarm64
OpenIndiana packages
MSYS2 mingw
ArchPOWER powerpc64le
ArchPOWER riscv64
CRUX 3.7
winget
Homebrew Casks
Buildroot master
KaOS
Chocolatey
SliTaz Cooking
RPM Sphere
HaikuPorts master
Vcpkg
Buildroot 2024.08.x
opam
CentOS Stream 10
Adélie Linux current
Gentoo overlay GURU
GoboLinux
ConanCenter
Chromebrew
SliTaz Next
OpenPKG
Alpine Linux 3.10
CentOS Stream 9
Side Linux
openSUSE games Tumbleweed
Rosa Server 7.5
EuroLinux 9
Rosa Server 7.3
GNU Elpa
openSUSE science Tumbleweed
CentOS 8
Scientific Linux 7.x
CRUX 3.5
MSYS2 msys2
Rosa Server 6.9
F-Droid
HP-UX 11.31
Debian 12 Backports
CentOS 6
Amazon Linux 1
Debian 10 Backports
Debian 11 Backports
MX-19 Testing
postmarketOS master

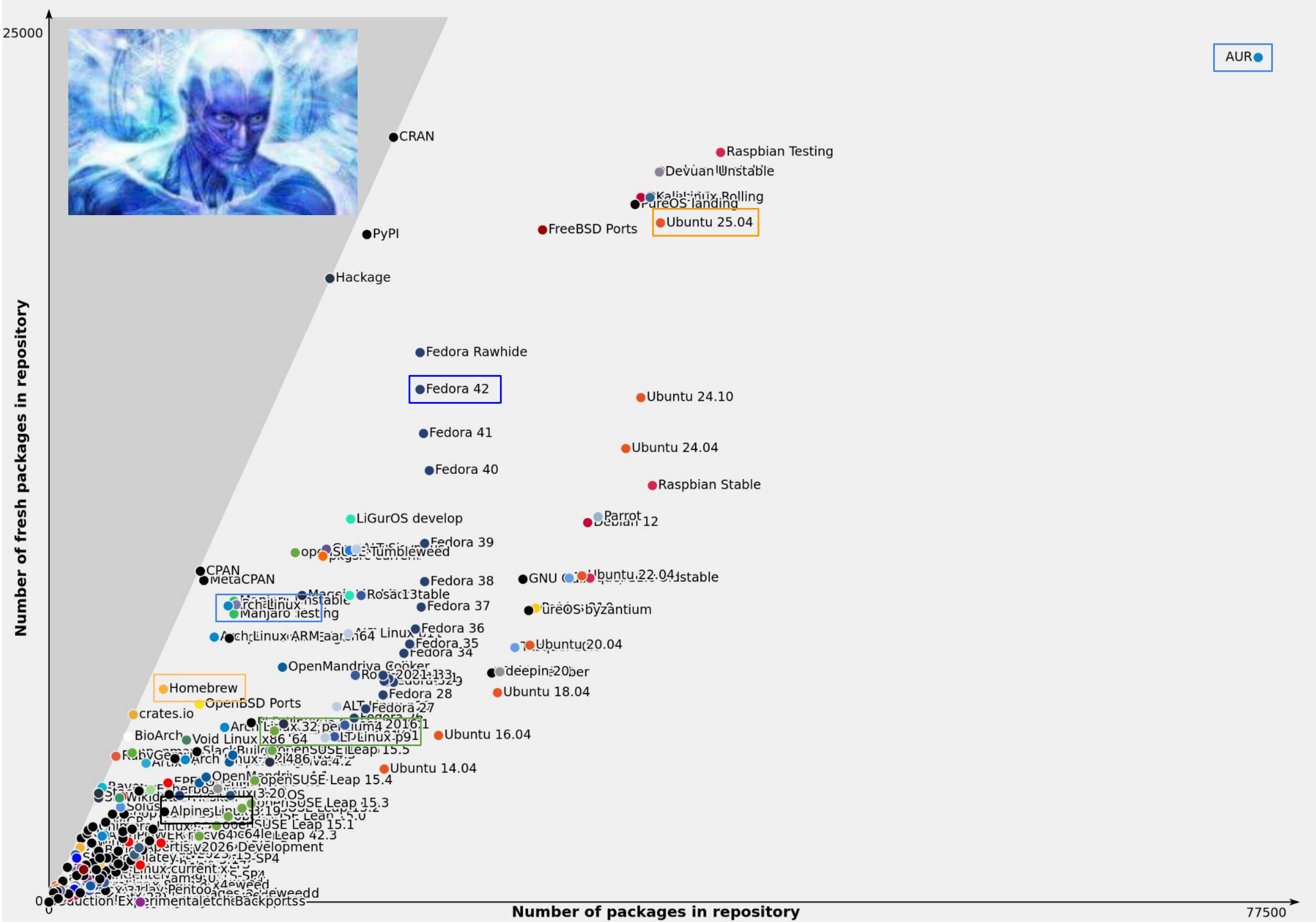


Number of fresh packages in repository
Number of packages in repository
4000
8000
0
Artix
EPEL 9
Exherbo
T2 SDE
Alpine Linux 3.20
Ravenports
Stackage Nightly
Stackage LTS Haskell
EPEL 10
Solus
Alpine Linux 3.19
Scoop
openEuler 25.03
YACP
Chimera Linux
MSYS2 ucrt64
MSYS2 clangarm64
OpenIndiana packages
MidnightBSD mports
AOSC
openEuler 24.09
Alpine Linux 3.18
ArchPOWER powerpc64le
CRUX 3.7
openEuler 24.03-LTS-SP1
EPEL 8
Alpine Linux 3.17
EPEL 7
winget
Homebrew Casks
Apertis v2026 Development
Buildroot master
openEuler 23.09
Alpine Linux 3.16
KaOS
Apertis v2023
Alpine Linux 3.15
Slackware64 current
Chocolatey
SliTaz Cooking
openEuler 23.03
Alpine Linux 3.14
RPM Sphere
HaikuPorts master
BlackArch
Vcpkg
EPEL 6
Alpine Linux 3.13
opam
CentOS Stream 10
Buildroot 2024.08.x
Gentoo overlay GURU
Adélie Linux current
GoboLinux
Alpine Linux 3.12
ConanCenter
SliTaz Next
OpenPKG
CentOS Stream 9
Alpine Linux 3.10
openSUSE games Tumbleweed
Rosa Server 7.5
AlmaLinux 9
GNU Elpa
openSUSE science
OpenWrt 24.10 x86_64
MSYS2 msys2
Rosa Server 6.9
F-Droid
Amazon Linux 1
MX 19 backports
MELPA


10000
0
16000
Number of fresh packages in repository
Number of packages in repository
CPAN
MetaCPAN
Manjaro Unstable
Manjaro Testing
Arch Linux ARM aarch64
Edge
OpenMandriva Cooker
Homebrew
OpenBSD Ports
crates.io
BioArch
PLD Linux
Arch Linux 32 pentium4
Mageia 9
openSUSE Leap 15.6
Void Linux x86_64
RubyGems
openmamba
SlackBuilds
Artix
Arch Linux 32 i486
OpenMandriva 4.3
OpenMandriva 4.2
openSUSE Leap 15.5
Mageia 8
OpenMandriva 4.1
OpenMandriva 4.0
openSUSE Leap 15.4
EPEL 9
deepin 23
Ravenports
Stackage Nightly
Stackage LTS
T2 SDE
Exherbo
PCLinuxOS
openSUSE Leap 15.3
openSUSE Leap 15.2
Solus
Scoop
openEuler 25.03
Alpine Linux 3.19
openSUSE Leap 15.0
openSUSE Leap 15.1
YACP
Chimera Linux
openSUSE Leap 42.3
winget
Homebrew Casks
EPEL 8
EPEL 7
Apertis v2026 Development
KaOS
Slackware64
Cygwin
BlackArch
EPEL 6
Alpine Linux 3.12
MELPA



16000
Number of fresh packages in repository
Number of packages in repository
0
32000
Fedora Rawhide
Fedora 42
Fedora 41
Fedora 40
LiGurOS develop
Fedora 39
ALT Sisyphus
CPAN
MetaCPAN
GNU Guix
Fedora 38
Mageia cauldron
Manjaro Unstable
Manjaro Testing
Fedora 37
PureOS byzantium
Fedora 36
ALT Linux p11
Fedora 35
Fedora 34
Ubuntu 18.04
OpenMandriva Cooker
Homebrew
OpenBSD Ports
Fedora 28
crates.io
ALT Linux
Fedora 27
Fedora 26
Rosa 2016.1
Ubuntu 16.04
BioArch
Void Linux x86_64
openSUSE Leap 15.6
openSUSE Leap 15.5
SlackBuilds
Artix
Ubuntu 14.04
OpenMandriva 4.1
openSUSE Leap 15.4
EPEL 9
OpenMandriva 4.0
Alpine Linux 3.20
PCLinuxOS
openSUSE Leap 15.3
Solus
Alpine Linux 3.19
openSUSE Leap 15.0
openSUSE Leap 15.1
openSUSE Leap 42.3
Apertis v2026 Development


25000
Number of fresh packages in repository
Number of packages in repository
0
77500
AUR
CRAN
Raspbian Testing
Devuan Unstable
Ubuntu 25.04
FreeBSD Ports
PyPI
Hackage
Fedora Rawhide
Fedora 42
Ubuntu 24.10
Fedora 41
Ubuntu 24.04
Fedora 40
Raspbian Stable
LiGurOS develop
Debian 12
Fedora 39
CPAN
MetaCPAN
Fedora 38
Ubuntu 22.04
Fedora 37
Fedora 36
Fedora 35
Fedora 34
Ubuntu 20.04
OpenMandriva Cooker
Ubuntu 18.04
Homebrew
Fedora 28
OpenBSD Ports
Fedora 27
crates.io
Ubuntu 16.04
BioArch
Void Linux
Ubuntu 14.04
openSUSE Leap 15.4
openSUSE Leap 15.3
openSUSE Leap 15.1
openSUSE Leap 42.3

70000

Number of fresh packages in repository

0

Number of packages in repository

110000

nixpkgs unstable

nixpkgs stable 24.11

nixpkgs stable 24.05

nixpkgs stable 23.11

nixpkgs stable 23.05

nixpkgs stable 22.11

nixpkgs stable 22.05

nixpkgs stable 21.11

AUR

CRAN

PyPI

Hackage

FreeBSD

Raspbian Testing

Ubuntu 25.04

Fedora Rawhide

Fedora 42

Fedora 41

Fedora 40

Ubuntu 24.10

Ubuntu 24.04

Raspbian Stable

Parrot 12

LiGurOS,develop

openSUSE Tumbleweed

CPAN

Rosa

PureOS byzantium

Ubuntu 20.04

Ubuntu 18.04

Ubuntu 16.04

Ubuntu 14.04

Experimental

Backports

Nix: A Package Manager

https://determinate.systems/nix-installer/

```
root@bfa62626c80c:/# curl --proto '=https' --tlsv1.2 -sSf -L https://install.determinate.systems/nix | sh -s -- install
info: downloading installer https://install.determinate.systems/nix/tag/v3.3.1/nix-installer-x86_64-linux
 INFO nix-installer v3.3.1
 INFO Step: Create directory `/nix`
 INFO Step: Provision Nix
 INFO Step: Create build users (UID 30001-30032) and group (GID 30000)
 INFO Step: Configure Nix
 INFO Step: Create directory `/etc/tmpfiles.d`
 INFO Step: Configure upstream Nix daemon service
 INFO Step: Remove directory `/nix/temp-install-dir`
 WARN SelfTest([ShellFailed { shell: Sh, command: "\"sh\" \"-lc\" \"nix build --option substitute false --option post-bu
\"; builder = \\\"/bin/sh\\\"; args = [\\\"-c\\\" \\\"echo hello > \\\\$out\\\"]; }\\'\"", output: Output { status: Exit
     at <nix/derivation-internal.nix>:37:12:\n           36|\n           37|   strict = derivationStrict drvAttrs;\n
whose name attribute is located at «string»:1:14\n\n       error: cannot connect to socket at '/nix/var/nix/daemon-socke
 substitute false --option post-build-hook \\'\\' --no-link --expr \\'derivation { name = \\\"self-test-bash-17454330565
\'\"", output: Output { status: ExitStatus(unix_wait_status(256)), stdout: "", stderr: "error:\n       … while calling t
t = derivationStrict drvAttrs;\n             |             ^\n           38|\n\n       … while evaluating derivation 'sel
o socket at '/nix/var/nix/daemon-socket/socket': No such file or directory\n" } }])
Nix was installed successfully!
To get started using Nix, open a new shell or run `. /nix/var/nix/profiles/default/etc/profile.d/nix-daemon.sh`
```

Nix: A Package Manager

- Unique paths
- Multiple versions
- Complete dependencies
- Multi-user support
- Atomic upgrades / Rollbacks
- Use without install / Temporal shells
- Declarative
- Reproducible
- Garbage collection

```
[user@host ~]$ find /nix/store -type f -name node
/nix/store/4bgg8j8275adawqbc5rkm4fv48dgg2i3-nodejs-18.18.2/bin/node
/nix/store/3k43a25ijnmfpkkyg94npv85ksc8nhly-nodejs-20.11.1/bin/node
/nix/store/71r8n7ckcpvav9qwshlr12hjd5nlchds-nodejs-20.12.2/bin/node
/nix/store/74a6mmrgxzcg9axl1gmdz3j2y1bjd13f-nodejs-20.12.2/bin/node
/nix/store/v14k93caffbf0xz2g7bqr964grxxqlmj-nodejs-20.15.1/bin/node
```

```
root@336200137c8b:/# nix profile history
Version 1 (2025-04-23):
  nix: ∅ -> 2.28.1
  nss-cacert: ∅ -> 3.107

Version 2 (2025-04-23) <- 1:
  flake:nixpkgs#legacyPackages.x86_64-linux.helix: ∅ -> 25.01.1

Version 3 (2025-04-23) <- 2:
  flake:nixpkgs#legacyPackages.x86_64-linux.neovim: ∅ -> 0.10.2

Version 4 (2025-04-23) <- 3:
  flake:nixpkgs#legacyPackages.x86_64-linux.python3: ∅ -> 3.12.8

Version 5 (2025-04-23) <- 4:
  flake:nixpkgs#legacyPackages.x86_64-linux.neovim: 0.10.2 -> 0.11.0
  flake:nixpkgs#legacyPackages.x86_64-linux.python3: 3.12.8 -> 3.12.9

Version 6 (2025-04-23) <- 5:
  flake:nixpkgs#legacyPackages.x86_64-linux.neovim: 0.11.0 -> ∅
```

Nix: A Programming Language (DSL)

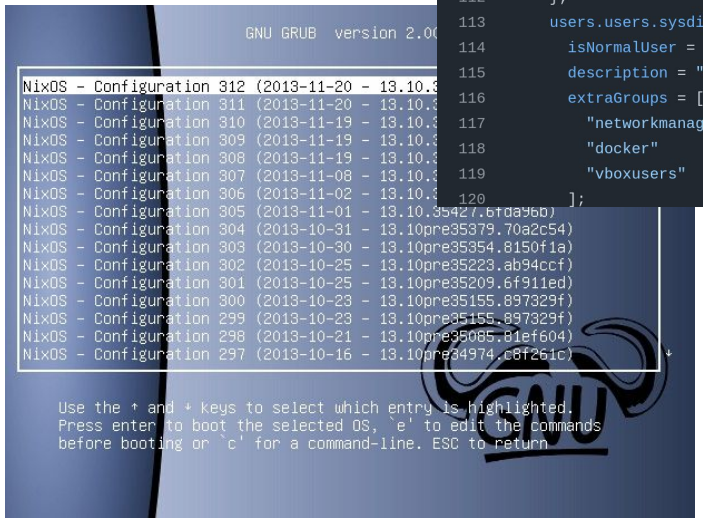
- Pure functional programming language (Same as Haskell)
- Used to define how packages are built
- Used to define the system configuration (both as single-user, or at system level with NixOS)
- It's like JSON but with functions

Nix: An Operating System

NixOS

- Base Linux distribution (not based on anything else)
- Nix is the package manager
- Everything can be configured as code, using the Nix DSL
  - Declarative
  - Reproducible
  - Atomic upgrades / Rollbacks
  - You can select which revision to boot

```
 99      users.users.fede = {
100        isNormalUser = true;
101        description = "Fede";
102        extraGroups = [
103          "networkmanager"
104          "wheel"
105          "docker"
106          "vboxusers"
107        ];
108        packages = with pkgs; [
109          calibre
110          unstable.telegram-desktop
111        ];
112      };
113      users.users.sysdig = {
114        isNormalUser = true;
115        description = "Sysdig";
116        extraGroups = [
117          "networkmanager"
118          "docker"
119          "vboxusers"
120        ];
```



Nixify your workflow

apt / rpm / homebrew / … replacement

(for user installation)

```
root@e4cdbac6f0fc:/# hx
bash: hx: command not found
root@e4cdbac6f0fc:/# nix profile install nixpkgs#helix
warning: 'install' is a deprecated alias for 'add'
root@e4cdbac6f0fc:/# which hx
/root/.nix-profile/bin/hx
root@e4cdbac6f0fc:/# hx --version
helix 25.01.1 (e7ac2fcd)
root@e4cdbac6f0fc:/# nix profile list
Name:               helix
Flake attribute:    legacyPackages.x86_64-linux.helix
Original flake URL: flake:nixpkgs
Locked flake URL:   github:NixOS/nixpkgs/18dd725c29603f582cf1900e0d25f9f1063dbf11?narHash=sha256-awS2zRgF4uTwrOKwwiJcByDzDOdo3Q1rPZbiHQg/N38%3D
Store paths:        /nix/store/iaw20cfamh885ya4sl41x2na8iq2yaf2-helix-25.01.1

Name:               nix
Store paths:        /nix/store/dpmfvjkkz3dj0ix2cpkrv3cyxryv20m9-nix-3.3.1

Name:               nss-cacert
Store paths:        /nix/store/y2zh06pccwcvz43xwgd8mr8pbqflkqww-nss-cacert-3.107
root@e4cdbac6f0fc:/# nix profile history
Version 1 (2025-04-15):
  nix: ∅ -> 3.3.1
  nss-cacert: ∅ -> 3.107

Version 2 (2025-04-15) <- 1:
  flake:nixpkgs#legacyPackages.x86_64-linux.helix: ∅ -> 25.01.1
root@e4cdbac6f0fc:/#
```

Use software without installing it!

Temporal shell

```
root@818a7b1a855c:/# cargo
bash: cargo: command not found
root@818a7b1a855c:/# rustc
bash: rustc: command not found
root@818a7b1a855c:/# nix shell nixpkgs#cargo nixpkgs#rustc
root@818a7b1a855c:/# cargo --version
cargo 1.86.0 (adf9b6ad1 2025-02-28)
root@818a7b1a855c:/# rustc --version
rustc 1.86.0 (05f9846f8 2025-03-31) (built from a source tarball)
root@818a7b1a855c:/# exit
exit
root@818a7b1a855c:/# cargo --version
bash: cargo: command not found
root@818a7b1a855c:/# rustc --version
bash: rustc: command not found
root@818a7b1a855c:/#
```

Direct execution

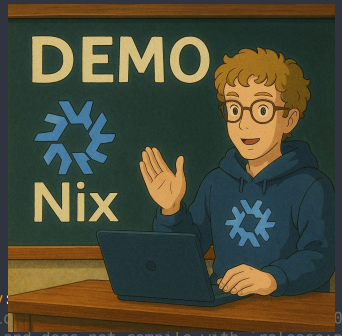
```
root@ec8b96b6365b:/# dust
bash: dust: command not found
root@ec8b96b6365b:/# nix run nixpkgs#dust
 29M             ┌── archive.ubuntu.com_ubuntu_dists_noble_universe_b..
 45M          ┌──┴ lists
 45M       ┌──┴ apt
 50M    ┌──┴ lib
 51M ┌──┴ var
 53M │           ┌── pack-01373374a93204f82078ad76caaf193a70029c8..
 56M │        ┌──┴ pack
 56M │     ┌──┴ objects
 56M │  ┌──┴ tarball-cache
 56M │  ├─ nix
 56M │  └─ .cache
 56M ├─ root
 19M │  ┌─ bin
8.3M │  │     ┌─ gconv
 51M │  │  ┌──┴ x86_64-linux-gnu
 53M │  └──┴ lib
 85M │  ┌─ usr
```

Unified Dev Environment

- Just one command: `nix develop`
- Integrates with `direnv`!

```
devShells.default =
  with pkgs;
  mkShell {
    packages = [
      cargo
      rustc
      rustfmt
      cargo-audit
      cargo-watch
      cargo-nextest
      cargo-expand
      clippy
      just
      rust-analyzer
      lldb
      pre-commit
    ];

    inputsFrom = [ sysdig-lsp ];

    shellHook = ''
      pre-commit install
      export PATH="$PWD/target/debug:$PWD/target/release:$PATH"
    '';

  };
```

```
inputs = {
  nixpkgs.url = "github:NixOS/nixpkgs/nixpkgs-unstable";
  nixpkgs-graalvm8.url = "github:NixOS/nixpkgs/3109ff5765505dbe1f7f2905ed3f54c62bd0acaa";
};
outputs =
  {
    self,
    nixpkgs,
    nixpkgs-graalvm8,
  }:
  let
    supportedSystems = [
      "x86_64-linux"
      "aarch64-linux"
      "x86_64-darwin"
      "aarch64-darwin"
    ];

    setJavaVersion = final: prev:
      # We need to use a very old
      # does not pass the tests and does not compile with `release:prepare` and `release:perform`.
      jdk = graalvm8ForSystem prev.system;
      jdt-language-server = prev.jdt-language-server.override { jdk = prev.jdk; };
    };

    graalvm8ForSystem = system: (import nixpkgs-graalvm8 { inherit system; }).graalvm8-ce;

    forEachSystem =
```




```
devShells = forEachSystem (
  pkgs: with pkgs; {
    default = mkShell {
      buildInputs = [
        jdt-language-server
        maven
        jdk
      ];
    };
  }
```

Unified CI/CD Environment

```yaml
jobs:
  lint:
    name: Lint
    runs-on: ubuntu-latest
    defaults:
      run:
        shell: nix develop --command bash {0}
    steps:
      - name: Fetch code
        uses: actions/checkout@v4

      - name: Install nix
        uses: DeterminateSystems/nix-installer-action@main

      - name: Run lint
        run: |
          just lint
```

```yaml
  build-and-test:
    name: Build and test
    runs-on: ubuntu-latest
    defaults:
      run:
        shell: nix develop --command bash {0}
    steps:
      - name: Fetch code
        uses: actions/checkout@v4

      - name: Install nix
        uses: DeterminateSystems/nix-installer-action@main

      - name: Run tests
        run: |
          just test
        env:
          SECURE_API_URL: https://us2.app.sysdig.com
          SECURE_API_TOKEN: ${{ secrets.SECURE_API_TOKEN }}
```

Nix as a build tool

```
pkgs.stdenv.mkDerivation {
  name = "my-program";
  src = ./main.c;
  nativeBuildInputs = [];
  buildInputs = [];
  dontUnpack = true;
  buildPhase = ''
    clang $src -o my-program
  '';
  installPhase = ''
    mkdir -p $out/bin
    cp my-program $out/bin
  '';
}
```

```
pkgs.buildNpmPackage {
  name = "my-project";
  src = ./.;
  # ...
}
```


```
pkgs.rustPlatform.buildRustPackage rec {
  name = "my-rust-crate";
  src = ./.;
  cargoLock = {
    lockFile = "${src}/Cargo.lock";
  };
```

```
pkgs.buildDartApplication {
  name = "my-project";
  src = ./.;
  # ...
}
```

```
pkgs.buildDotnetPackage
  name = "my-project";
```

```
pkgs.buildRubyGem {
  name = "my-project";
  src = ./.;
  # ...
}
```

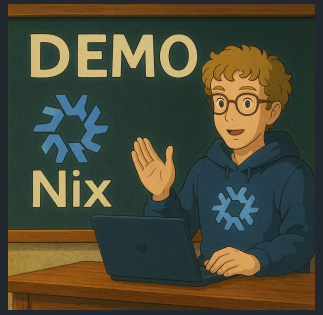
```
pkgs.buildGoModule {
  name = "my-project";
  src = ./.;
  # ...
}
```

Nix as a build tool

```
packages = with pkgs; {
  inherit sysdig-lsp;
  default = sysdig-lsp;

  sysdig-lsp-linux-amd64 = pkgsCross.gnu64.pkgsStatic.sysdig-lsp;
  sysdig-lsp-linux-arm64 = pkgsCross.aarch64-multiplatform.pkgsStatic.sysdig-lsp;
  sysdig-lsp-darwin-amd64 = pkgsCross.x86_64-darwin.sysdig-lsp;
  sysdig-lsp-darwin-arm64 = pkgsCross.aarch64-darwin.sysdig-lsp;
  sysdig-lsp-windows-amd64 = pkgsCross.mingwW64.sysdig-lsp;
};
```

```
steps:
  - name: Checkout code
    uses: actions/checkout@v4

  - name: Install Nix
    uses: DeterminateSystems/nix-installer-action@main

  - name: Configure Nix cache
    uses: DeterminateSystems/flakehub-cache-action@main

  - name: Build LSP for ${{ matrix.os }}-${{ matrix.arch }}
    run: nix build -L .#sysdig-lsp-${{ matrix.os }}-${{ matrix.arch }}

  - name: Copy binary built
    run: cp -a ./result/bin/sysdig-lsp /tmp/sysdig-lsp-${{ matrix.os }}-${{ matrix.arch }}

  - name: Upload binary
    uses: actions/upload-artifact@v4
    with:
      name: sysdig-lsp-${{ matrix.os }}-${{ matrix.arch }}
      path: /tmp/sysdig-lsp-${{ matrix.os }}-${{ matrix.arch }}
      if-no-files-found: error
      retention-days: 1
```

```
1   {
2     rustPlatform,
3     pkgsStatic,
4     lib,
5     stdenv,
6     pkg-config,
7     openssl,
8   }:
9   let
10    cargoFile = builtins.fromTOML (builtins.readFile ./Cargo.toml);
11  in
12  rustPlatform.buildRustPackage {
13    pname = cargoFile.package.name;
14    version = cargoFile.package.version;
15    src = ./.;
16    cargoLock = {
17      lockFile = ./Cargo.lock;
18    };
19
20    nativeBuildInputs = [
21      pkg-config
22    ];
23
24    buildInputs = [
25      openssl.dev
26    ] ++ lib.optionals stdenv.hostPlatform.isDarwin (with pkgsStatic; [ libiconv ]);
27
28    doCheck = false;
29    meta.mainProgram = "sysdig-lsp";
30  }
```



Nix Everything Everywhere All at Once

Build docker images with Nix

- Same experience in production, for K8s, docker-compose or whatever executes containers
- But with nix benefits:
  - Reproducible
  - Declarative

```nix
{ dockerTools, sysdig-lsp }:
dockerTools.buildLayeredImage {
  name = "sysdig-lsp";
  tag = sysdig-lsp.version;

  contents = [ sysdig-lsp ];
  config.Entrypoint = [ "sysdig-lsp" ];
}
```

```nix
13      overlays.default = final: prev: {
14        sysdig-lsp = prev.callPackage ./package.nix { };
15        sysdig-lsp-docker = prev.callPackage ./docker.nix { };
16      };
17
18      flake = flake-utils.lib.eachDefaultSystem (
19        system:
20        let
21          pkgs = import nixpkgs {
22            inherit system;
23            config.allowUnfree = true;
24            overlays = [ self.overlays.default ];
25          };
26        in
27        {
28          packages = with pkgs; {
29            inherit sysdig-lsp;
30            default = sysdig-lsp;
31
32            sysdig-lsp-linux-amd64 = pkgs
33            sysdig-lsp-linux-arm64 = pkgs
34            sysdig-lsp-darwin-amd64 = pkg
35            sysdig-lsp-darwin-arm64 = pkg
36            sysdig-lsp-windows-amd64 = pk
37
38            inherit sysdig-lsp-docker;
39          };
```

```
sysdig-lsp on  master [$+] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-e
❯ nix build .#sysdig-lsp-docker
warning: Git tree '/home/fede.barcelona/Documents/sysdig-lsp' is dirty

sysdig-lsp on  master [$+] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-e
❯ docker load -i ./result
5dd93e74baad: Loading layer [==================================================>]  2.079MB/2.079M
809dae97e4fc: Loading layer [==================================================>]  399.4kB/399.4k
04ded239e74e: Loading layer [==================================================>]    215kB/215kB
f57664dcc45e: Loading layer [==================================================>]  30.78MB/30.78M
e4f606e0c2d8: Loading layer [==================================================>]    215kB/215kB
0d8befe6684f: Loading layer [==================================================>]  10.02MB/10.02M
ac351887713a: Loading layer [==================================================>]  8.264MB/8.264M
3823867c8392: Loading layer [==================================================>]  12.05MB/12.05M
0b97ada0e8c8: Loading layer [==================================================>]  10.24kB/10.24k
Loaded image: sysdig-lsp:0.4.1

sysdig-lsp on  master [$+] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-e
❯ docker images
REPOSITORY   TAG       IMAGE ID       CREATED        SIZE
sysdig-lsp   0.4.1     fa2ad1137c48   55 years ago   63.1MB

sysdig-lsp on  master [$+] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-e
❯
```

Package DEB files with Nix

```
sysdig-lsp on  master [$!+] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️ impure (nix-shell-env) on
❯ nix bundle --bundler bundlers#toDEB .#sysdig-lsp
warning: Git tree '/home/fede.barcelona/Documents/sysdig-lsp' is dirty

sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️ impure (nix-shell-env) o
❯ ls -al ./deb-single-sysdig-lsp/sysdig-lsp_1.0_amd64.deb
.r--r--r-- 22M root  1 Jan  1970 ./deb-single-sysdig-lsp/sysdig-lsp_1.0_amd64.deb

sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️ impure (nix-shell-env) o
❯
```

Package DEB files with Nix

```
❯ docker run --rm -it -v $PWD:/lsp ubuntu:24.04
root@8406c2fa285f:/# apt install /lsp/sysdig-lsp_1.0_amd64.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'sysdig-lsp' instead of '/lsp/sysdig-lsp_1.0_amd64.deb'
The following NEW packages will be installed:
  sysdig-lsp
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/21.7 MB of archives.
After this operation, 63.1 MB of additional disk space will be used.
Get:1 /lsp/sysdig-lsp_1.0_amd64.deb sysdig-lsp amd64 1.0 [21.7 MB]
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package sysdig-lsp.
(Reading database ... 4381 files and directories currently installed.)
Preparing to unpack /lsp/sysdig-lsp_1.0_amd64.deb ...
Unpacking sysdig-lsp (1.0) ...
Setting up sysdig-lsp (1.0) ...
root@8406c2fa285f:/# sysdig-lsp --help
LSP implementation that integrates vulnerability and IaC scanning directly into your editor

Usage: sysdig-lsp

Options:
  -h, --help     Print help
  -V, --version  Print version
root@8406c2fa285f:/# which sysdig-lsp
/usr/bin/sysdig-lsp
root@8406c2fa285f:/# ls -al /usr/bin/sysdig-lsp
lrwxrwxrwx 1 root root 75 Jan  1  1980 /usr/bin/sysdig-lsp -> /nix/store/k47lfj3fysc0vxhmc6wyikrm576yvr42-sysdig-lsp-0.4.1/bin/sysdig-lsp
root@8406c2fa285f:/#
```

Package RPM files with Nix

```
sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️  impure (nix-shell-env) o
❯ nix bundle --bundler bundlers#toRPM .#sysdig-lsp
warning: Git tree '/home/fede.barcelona/Documents/sysdig-lsp' is dirty

sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️  impure (nix-shell-env) o
❯ ls -al ./rpm-single-sysdig-lsp/sysdig-lsp-1.0-1.x86_64.rpm
.r--r--r-- 22M root  1 Jan  1970 ./rpm-single-sysdig-lsp/sysdig-lsp-1.0-1.x86_64.rpm
```

Package RPM files with Nix

```
❯ docker run --rm -it -v $PWD:/lsp fedora:42
[root@095ff609983c /]# dnf install /lsp/sysdig-lsp-1.0-1.x86_64.rpm
Updating and loading repositories:
 Fedora 42 openh264 (From Cisco) - x86_64                        100% |   5.4 KiB/s |   6.0 KiB |  00m01s
 Fedora 42 - x86_64 - Test Updates                               100% |   1.3 MiB/s |   1.2 MiB |  00m01s
 Fedora 42 - x86_64 - Updates                                    100% |   1.6 MiB/s |   2.3 MiB |  00m01s
 Fedora 42 - x86_64                                              100% |   5.2 MiB/s |  35.4 MiB |  00m07s
Repositories loaded.
Package                         Arch      Version                       Repository               Size
Installing:
 sysdig-lsp                     x86_64    1.0-1                         @commandline         60.2 MiB

Transaction Summary:
 Installing:         1 package

Total size of inbound packages is 21 MiB. Need to download 0 B.
After this operation, 60 MiB extra will be used (install 60 MiB, remove 0 B).
Is this ok [y/N]: y
Running transaction
[1/3] Verify package files                                       100% |  18.0   B/s |   1.0   B |  00m00s
[2/3] Prepare transaction                                        100% |  45.0   B/s |   1.0   B |  00m00s
[3/3] Installing sysdig-lsp-0:1.0-1.x86_64                       100% |  68.3 MiB/s |  60.4 MiB |  00m01s
Warning: skipped OpenPGP checks for 1 package from repository: @commandline
Complete!
[root@095ff609983c /]# sysdig-lsp --help
LSP implementation that integrates vulnerability and IaC scanning directly into your editor

Usage: sysdig-lsp

Options:
  -h, --help     Print help
  -V, --version  Print version
[root@095ff609983c /]# command -v sysdig-lsp
/usr/sbin/sysdig-lsp
[root@095ff609983c /]# ls -al /usr/sbin/sysdig-lsp
lrwxrwxrwx 1 root root 75 Apr 16 09:11 /usr/sbin/sysdig-lsp -> /nix/store/k47lfj3fysc0vxhmc6wyikrm576yvr42-sysdig-lsp-0.4.1/bin/sysdig-lsp
[root@095ff609983c /]#
```

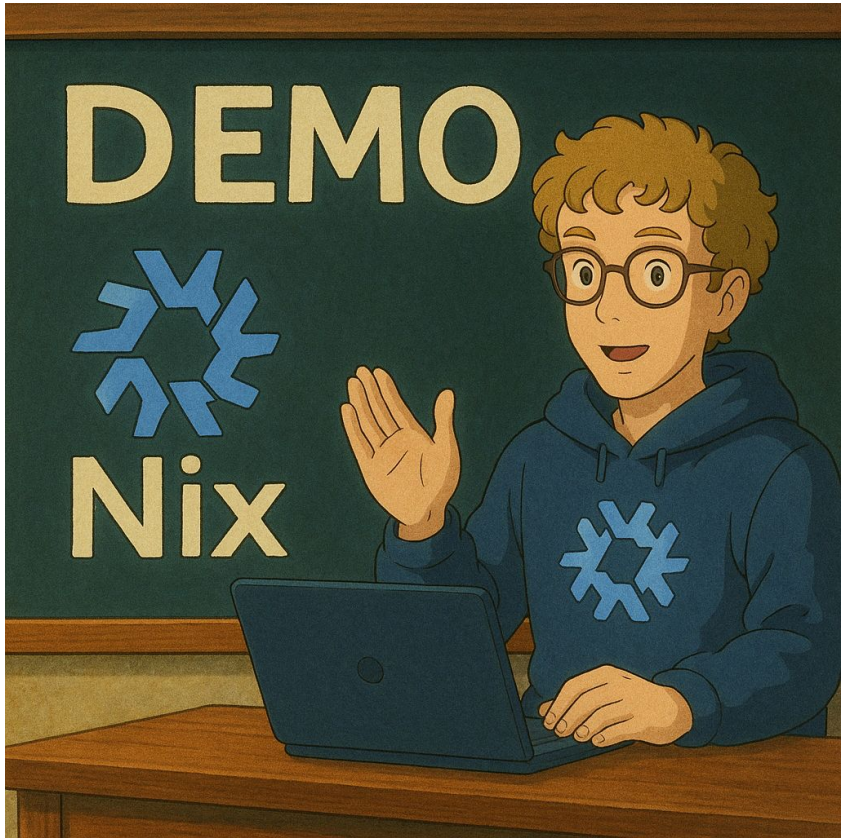
Package AppImages with Nix

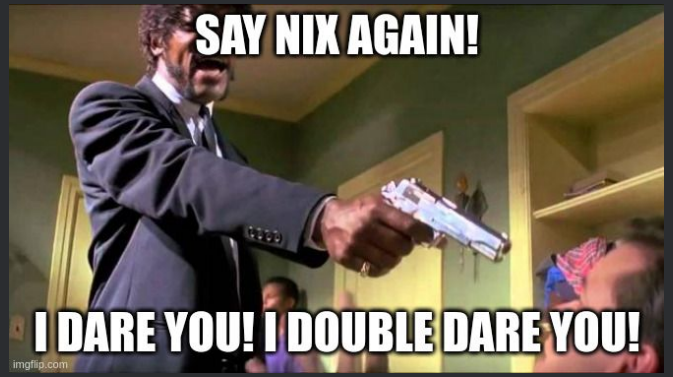
```
sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-east-1) on ☁
❯ nix bundle --bundler github:ralismark/nix-appimage .#sysdig-lsp
warning: Git tree '/home/fede.barcelona/Documents/sysdig-lsp' is dirty

sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-east-1) on ☁
❯ ls -al ./sysdig-lsp.AppImage
lrwxrwxrwx - fede.barcelona 16 Apr 11:23 ./sysdig-lsp.AppImage -> /nix/store/4391hv5hw5f397083vqyk46ghxxaaj9k-sy

sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄ impure (nix-shell-env) on ☁ (us-east-1) on ☁
❯ ls -al /nix/store/4391hv5hw5f397083vqyk46ghxxaaj9k-sysdig-lsp.AppImage
.r-xr-xr-x 23M root  1 Jan  1970 /nix/store/4391hv5hw5f397083vqyk46ghxxaaj9k-sysdig-lsp.AppImage
```

Package AppImages with Nix

```
sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️ impure (nix-shell-env) on ☁️ (us-east-1) on ☁️
❯ cp -aL ./sysdig-lsp.AppImage ./sysdig-lsp

sysdig-lsp on  master [$!+?] is 📦 v0.4.1 via 🦀 v1.85.0 via ❄️ impure (nix-shell-env) on ☁️ (us-east-1) on ☁️
❯ docker run --rm -it -v $PWD:/lsp --device /dev/fuse --cap-add SYS_ADMIN --security-opt apparmor:unconfined alp
/ # cp -a /lsp/sysdig-lsp /usr/bin/
/ # which sysdig-lsp
/usr/bin/sysdig-lsp
/ # ls -alh /usr/bin/sysdig-lsp
-r-xr-xr-x    1 30033    30001      21.9M Jan  1  1970 /usr/bin/sysdig-lsp
/ # sysdig-lsp --help
LSP implementation that integrates vulnerability and IaC scanning directly into your editor

Usage: sysdig-lsp

Options:
  -h, --help     Print help
  -V, --version  Print version
/ #
```

A self-contained Python app (bizneo)





Thank you!

Any questions?

https://determinate.systems/nix-installer/

¿Te interesa mentorizar?
¿Buscas mentoría?

https://forms.gle/ANdbgyowo1DiKELs7

¿Te apetece venir a hablarnos de Python?

Escríbenos a

zaragoza@es.python.org