lambda DAYS

28-29 JULY 2022

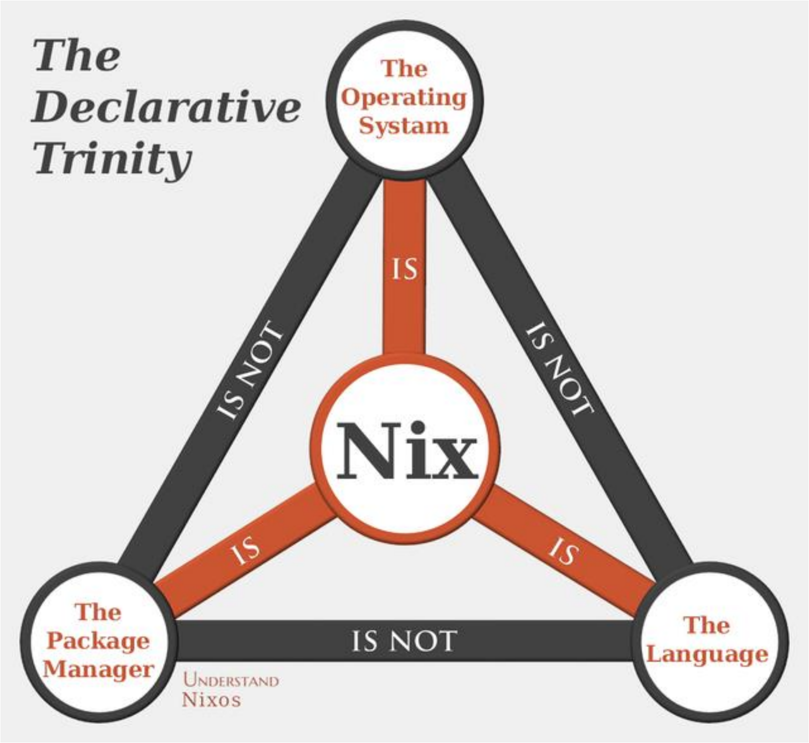
KRAKÓW | POLAND

Nix

Configure and Prosper

WHY?

What is Nix?

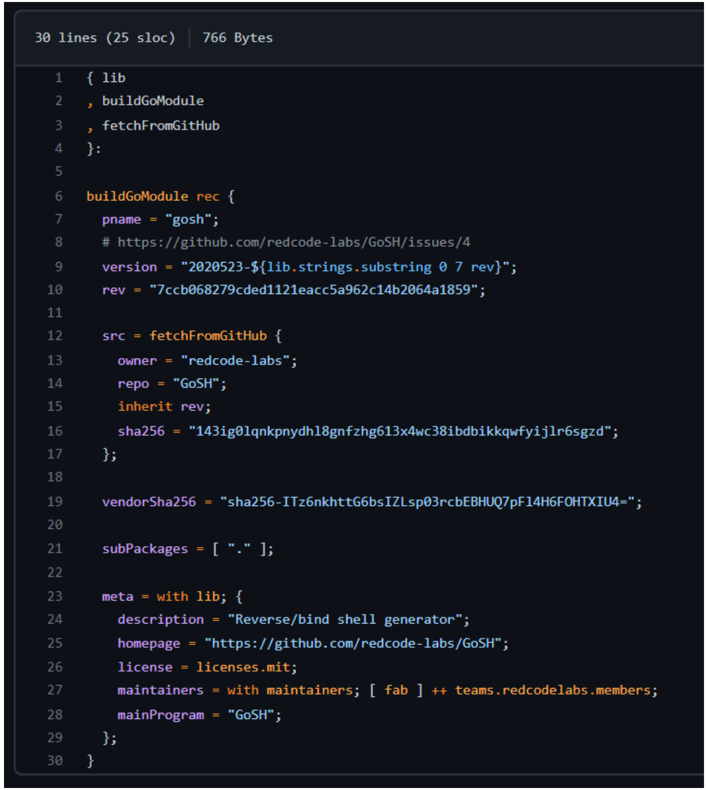

The Declarative Trinity
The Operating Systam
Nix
The Package Manager
The Language
IS
IS
IS
IS NOT
IS NOT
IS NOT
Understand Nixos

What does Nix 'ecosystem' offer?

- Reproducibility
- Immutability
- Rollbacks
- And our journey just begins...

Nix as a language

The true reason why the Tower of Babel was so messed up...

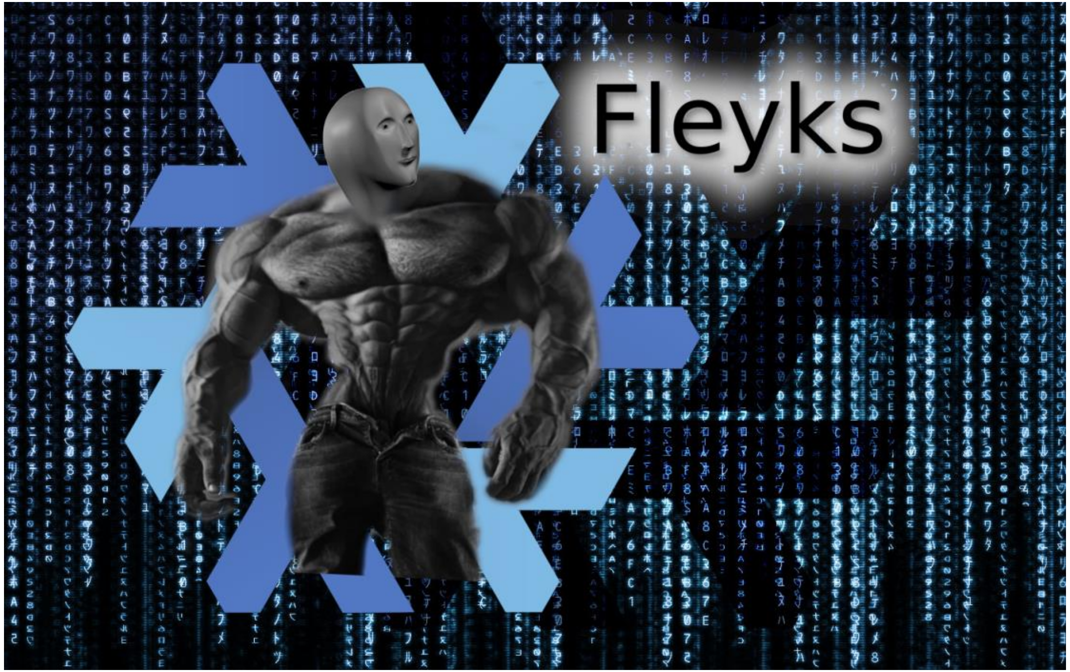


30 lines (25 sloc) | 766 Bytes

```nix
{ lib
, buildGoModule
, fetchFromGitHub
}:

buildGoModule rec {
  pname = "gosh";
  # https://github.com/redcode-labs/GoSH/issues/4
  version = "2020523-${lib.strings.substring 0 7 rev}";
  rev = "7ccb068279cded1121eacc5a962c14b2064a1859";

  src = fetchFromGitHub {
    owner = "redcode-labs";
    repo = "GoSH";
    inherit rev;
    sha256 = "143ig0lqnkpnydhl8gnfzhg613x4wc38ibdbikkqwfyijlr6sgzd";
  };

  vendorSha256 = "sha256-ITz6nkhttG6bsIZLsp03rcbEBHUQ7pFl4H6FOHTXIU4=";

  subPackages = [ "." ];

  meta = with lib; {
    description = "Reverse/bind shell generator";
    homepage = "https://github.com/redcode-labs/GoSH";
    license = licenses.mit;
    maintainers = with maintainers; [ fab ] ++ teams.redcodelabs.members;
    mainProgram = "GoSH";
  };
}
```

Flakes

here comes that snowflake...



- Quite advanced
- More than powerful
- Possibilities of Nix skyrocket thanks to them

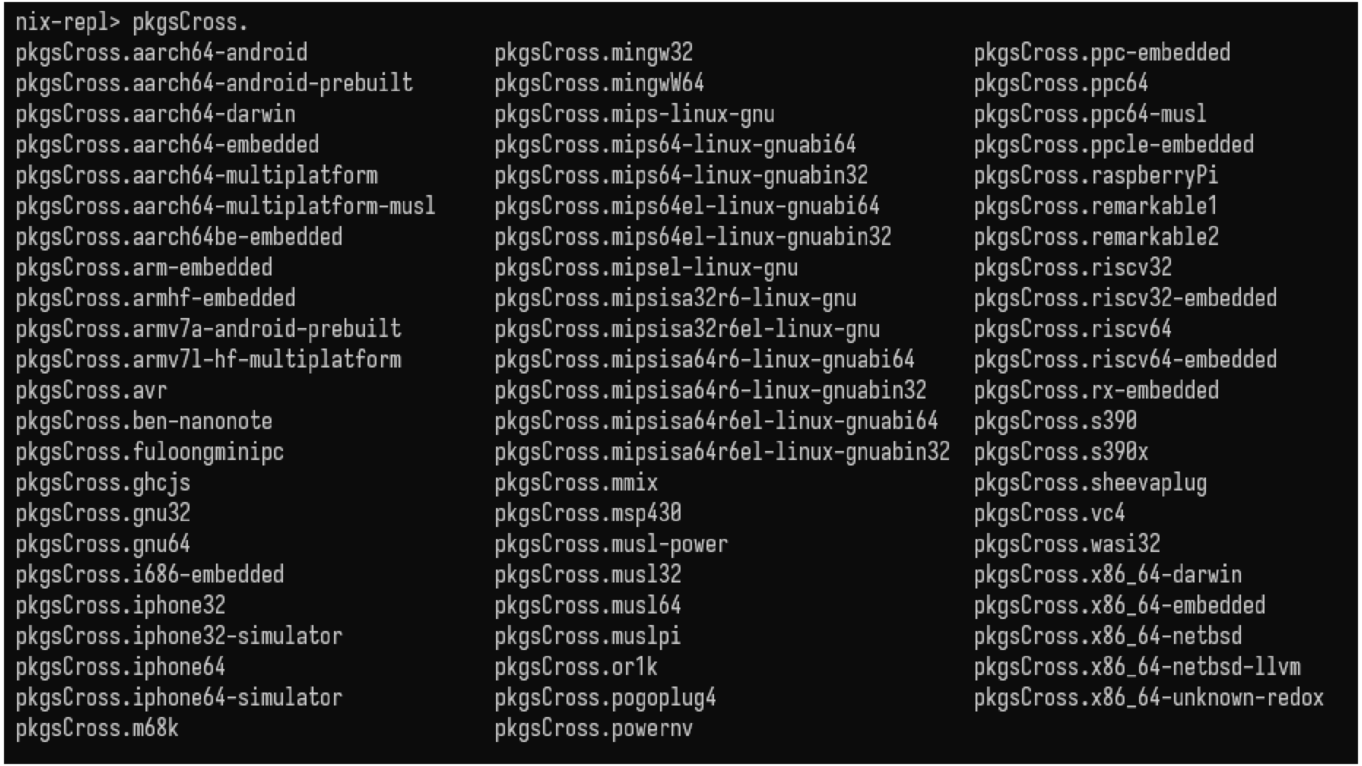
Nix as a package manager

Doom Slayer in Dependency Hell

- OOTB cross-compilation
- OOTB static compilation
- Easy to set up a binary cache
- Source-based (hack on packages without forks)
- Single package manager for different development environments

Nix as a package manager

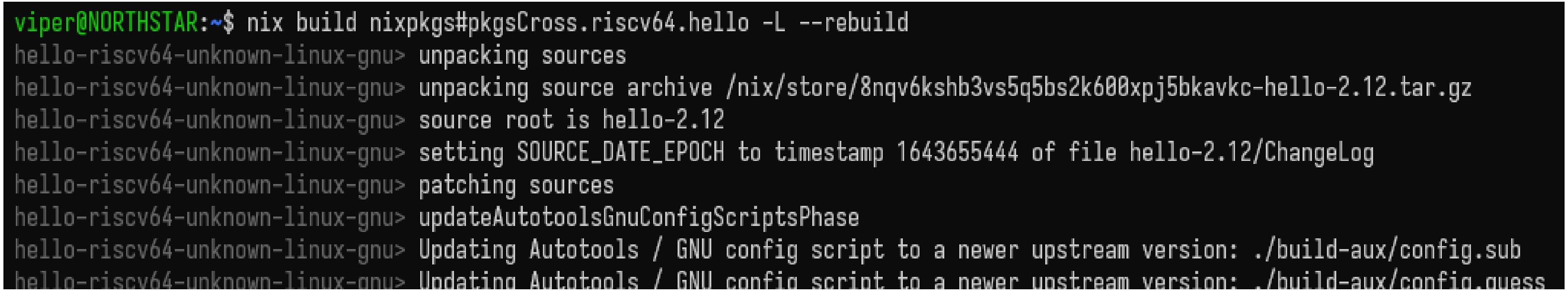
Doom Slayer in Dependency Hell



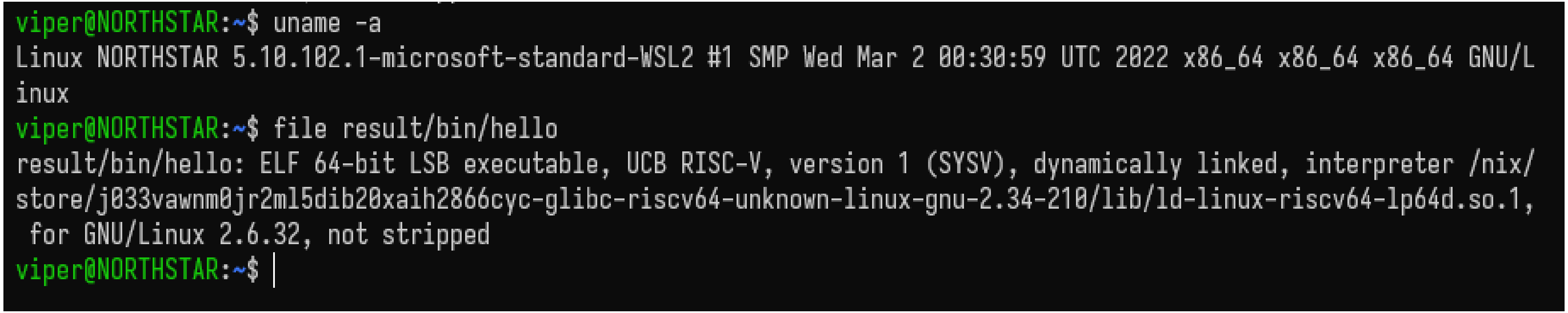
```
nix-repl> pkgsCross.
pkgsCross.aarch64-android                pkgsCross.mingw32                        pkgsCross.ppc-embedded
pkgsCross.aarch64-android-prebuilt       pkgsCross.mingwW64                       pkgsCross.ppc64
pkgsCross.aarch64-darwin                 pkgsCross.mips-linux-gnu                 pkgsCross.ppc64-musl
pkgsCross.aarch64-embedded               pkgsCross.mips64-linux-gnuabi64          pkgsCross.ppcle-embedded
pkgsCross.aarch64-multiplatform          pkgsCross.mips64-linux-gnuabin32         pkgsCross.raspberryPi
pkgsCross.aarch64-multiplatform-musl     pkgsCross.mips64el-linux-gnuabi64        pkgsCross.remarkable1
pkgsCross.aarch64be-embedded             pkgsCross.mips64el-linux-gnuabin32       pkgsCross.remarkable2
pkgsCross.arm-embedded                   pkgsCross.mipsel-linux-gnu               pkgsCross.riscv32
pkgsCross.armhf-embedded                 pkgsCross.mipsisa32r6-linux-gnu          pkgsCross.riscv32-embedded
pkgsCross.armv7a-android-prebuilt        pkgsCross.mipsisa32r6el-linux-gnu        pkgsCross.riscv64
pkgsCross.armv7l-hf-multiplatform        pkgsCross.mipsisa64r6-linux-gnuabi64     pkgsCross.riscv64-embedded
pkgsCross.avr                            pkgsCross.mipsisa64r6-linux-gnuabin32    pkgsCross.rx-embedded
pkgsCross.ben-nanonote                   pkgsCross.mipsisa64r6el-linux-gnuabi64   pkgsCross.s390
pkgsCross.fuloongminipc                  pkgsCross.mipsisa64r6el-linux-gnuabin32  pkgsCross.s390x
pkgsCross.ghcjs                          pkgsCross.mmix                           pkgsCross.sheevaplug
pkgsCross.gnu32                          pkgsCross.msp430                         pkgsCross.vc4
pkgsCross.gnu64                          pkgsCross.musl-power                     pkgsCross.wasi32
pkgsCross.i686-embedded                  pkgsCross.musl32                         pkgsCross.x86_64-darwin
pkgsCross.iphone32                       pkgsCross.musl64                         pkgsCross.x86_64-embedded
pkgsCross.iphone32-simulator             pkgsCross.muslpi                         pkgsCross.x86_64-netbsd
pkgsCross.iphone64                       pkgsCross.or1k                           pkgsCross.x86_64-netbsd-llvm
pkgsCross.iphone64-simulator             pkgsCross.pogoplug4                      pkgsCross.x86_64-unknown-redox
pkgsCross.m68k                           pkgsCross.powernv
```

Nix as a package manager

Doom Slayer in Dependency Hell



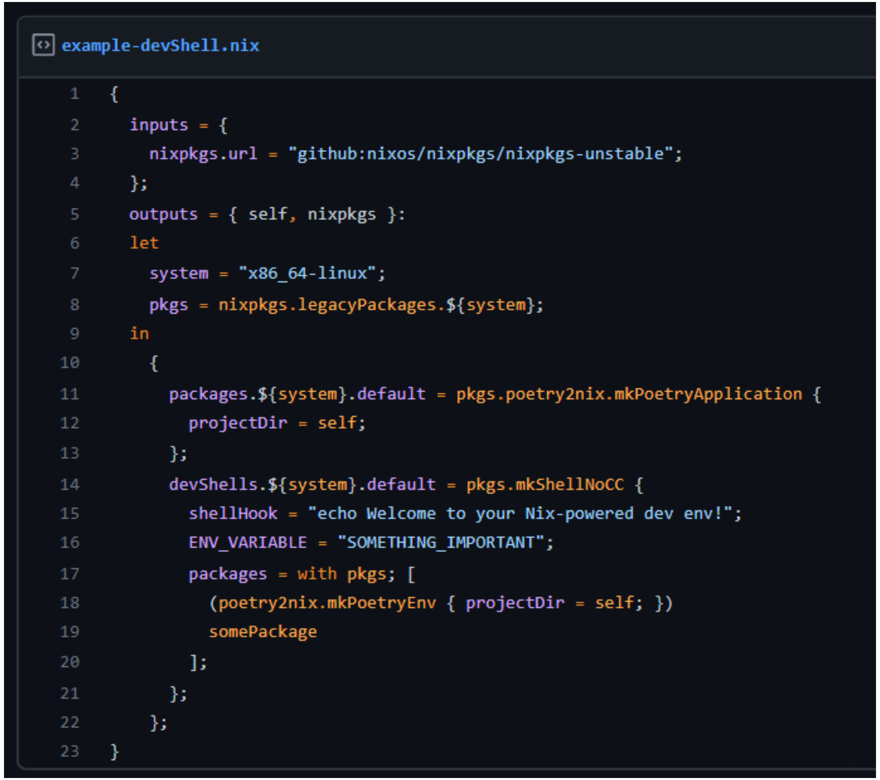
```
viper@NORTHSTAR:~$ nix build nixpkgs#pkgsCross.riscv64.hello -L --rebuild
hello-riscv64-unknown-linux-gnu> unpacking sources
hello-riscv64-unknown-linux-gnu> unpacking source archive /nix/store/8nqv6kshb3vs5q5bs2k600xpj5bkavkc-hello-2.12.tar.gz
hello-riscv64-unknown-linux-gnu> source root is hello-2.12
hello-riscv64-unknown-linux-gnu> setting SOURCE_DATE_EPOCH to timestamp 1643655444 of file hello-2.12/ChangeLog
hello-riscv64-unknown-linux-gnu> patching sources
hello-riscv64-unknown-linux-gnu> updateAutotoolsGnuConfigScriptsPhase
hello-riscv64-unknown-linux-gnu> Updating Autotools / GNU config script to a newer upstream version: ./build-aux/config.sub
hello-riscv64-unknown-linux-gnu> Updating Autotools / GNU config script to a newer upstream version: ./build-aux/config.guess
```



```
viper@NORTHSTAR:~$ uname -a
Linux NORTHSTAR 5.10.102.1-microsoft-standard-WSL2 #1 SMP Wed Mar 2 00:30:59 UTC 2022 x86_64 x86_64 x86_64 GNU/L
inux
viper@NORTHSTAR:~$ file result/bin/hello
result/bin/hello: ELF 64-bit LSB executable, UCB RISC-V, version 1 (SYSV), dynamically linked, interpreter /nix/
store/j033vawnm0jr2ml5dib20xaih2866cyc-glibc-riscv64-unknown-linux-gnu-2.34-210/lib/ld-linux-riscv64-lp64d.so.1,
 for GNU/Linux 2.6.32, not stripped
viper@NORTHSTAR:~$ 
```

Nix as a package manager

Doom Slayer in Dependency Hell

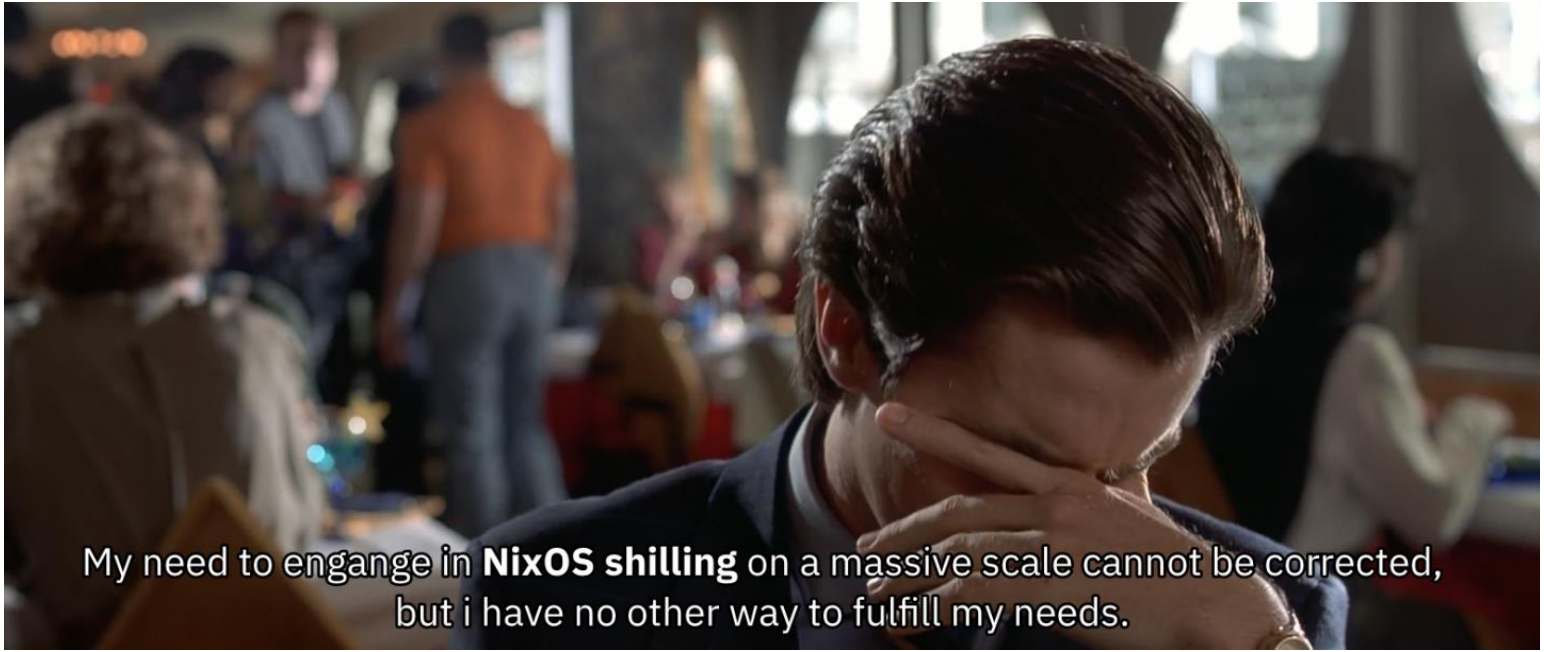


example-devShell.nix

```
{
  inputs = {
    nixpkgs.url = "github:nixos/nixpkgs/nixpkgs-unstable";
  };
  outputs = { self, nixpkgs }:
  let
    system = "x86_64-linux";
    pkgs = nixpkgs.legacyPackages.${system};
  in
    {
      packages.${system}.default = pkgs.poetry2nix.mkPoetryApplication {
        projectDir = self;
      };
      devShells.${system}.default = pkgs.mkShellNoCC {
        shellHook = "echo Welcome to your Nix-powered dev env!";
        ENV_VARIABLE = "SOMETHING_IMPORTANT";
        packages = with pkgs; [
          (poetry2nix.mkPoetryEnv { projectDir = self; })
          somePackage
        ];
      };
    };
}
```

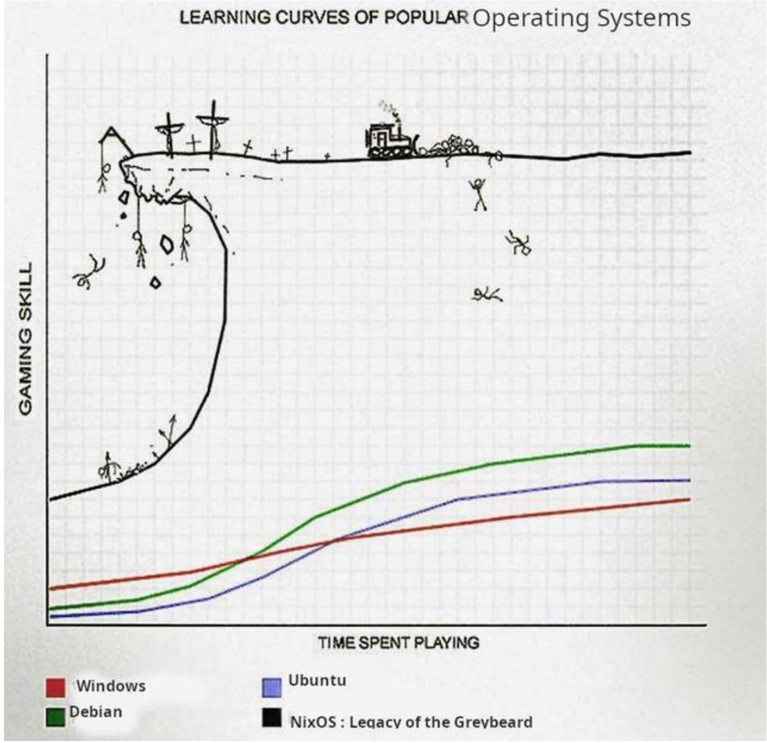
Nix as an OS

Nix philosophy to the cor... umm...kernel


My need to engange in **NixOS shilling** on a massive scale cannot be corrected,
but i have no other way to fulfill my needs.

Nix as an OS

Nix philosophy to the cor... umm...kernel

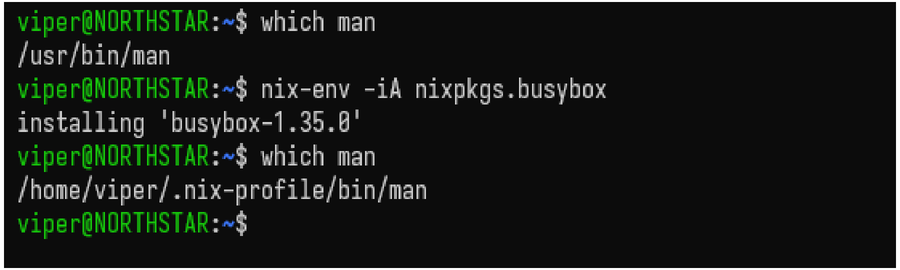


There are some cons as well but who cares, Nix is cool enough to omit all of those cons, but those are only:

- Not every binary works OOTB (requires patchelf)
- Quite slippery slope learning curve
- The biggest part of 'Nix ecosystem', can combine EVERYTHING

nix-shells

rule 'em all!



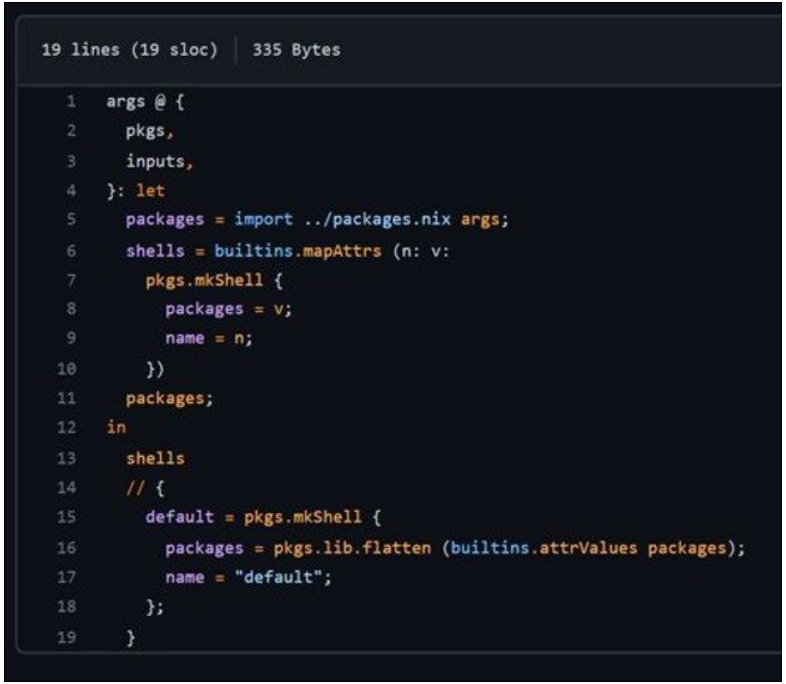
```
viper@NORTHSTAR:~$ which man
/usr/bin/man
viper@NORTHSTAR:~$ nix-env -iA nixpkgs.busybox
installing 'busybox-1.35.0'
viper@NORTHSTAR:~$ which man
/home/viper/.nix-profile/bin/man
viper@NORTHSTAR:~$
```

Nix-env is a no-no!

- Imperative (ew)
- Can 'mask' your current 'system state'

nix-shells

rule 'em all!



19 lines (19 sloc) | 335 Bytes

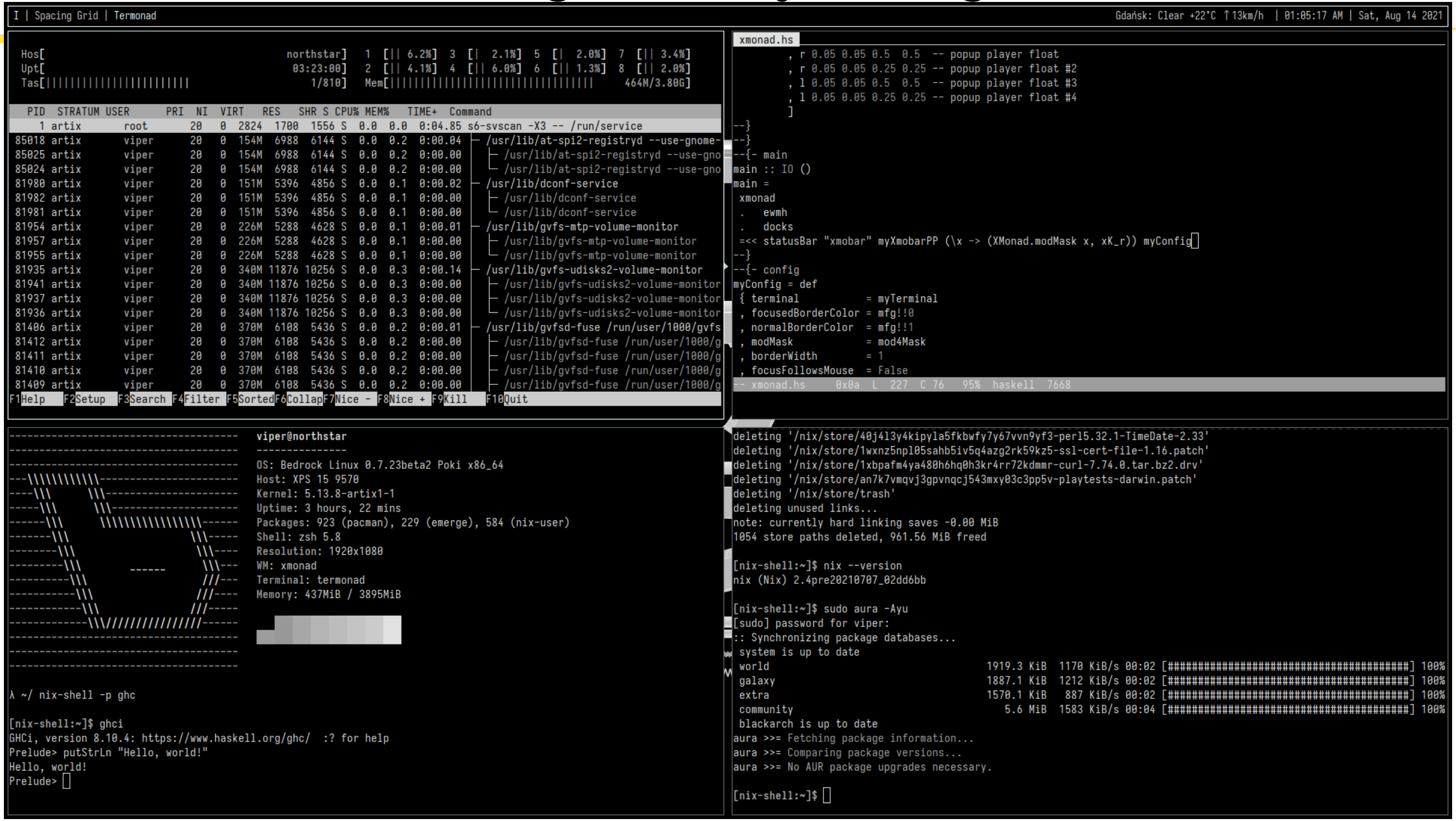
```
args @ {
  pkgs,
  inputs,
}: let
  packages = import ../packages.nix args;
  shells = builtins.mapAttrs (n: v:
    pkgs.mkShell {
      packages = v;
      name = n;
    })
  packages;
in
  shells
  // {
    default = pkgs.mkShell {
      packages = pkgs.lib.flatten (builtins.attrValues packages);
      name = "default";
    };
  }
```

nix-shells are better:

- temporary
- mix-and-match

Non-NixOS Nix

the nightmare just begins



```
I | Spacing Grid | Termonad                                  Gdańsk: Clear +22°C ↑13km/h  | 01:05:17 AM | Sat, Aug 14 2021
```

```
  Hos[                              northstar]   1  [|| 6.2%]  3  [|   2.1%]  5  [|   2.0%]  7  [|| 3.4%]
  Upt[                               03:23:00]   2  [|| 4.1%]  4  [|| 6.0%]  6  [|| 1.3%]  8  [|| 2.0%]
  Tas[||||||||||||||||||||||||        1/810]   Mem[||||||||||||||||||||||||||||||||||     464M/3.80G]

   PID  STRATUM USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
     1 artix      root      20   0  2824  1700  1556 S  0.0  0.0  0:04.85 s6-svscan -X3 -- /run/service
 85018 artix      viper     20   0  154M  6988  6144 S  0.0  0.2  0:00.04 ├ /usr/lib/at-spi2-registryd --use-gnome-
 85025 artix      viper     20   0  154M  6988  6144 S  0.0  0.2  0:00.00 │  ├ /usr/lib/at-spi2-registryd --use-gno
 85024 artix      viper     20   0  154M  6988  6144 S  0.0  0.2  0:00.00 │  └ /usr/lib/at-spi2-registryd --use-gno
 81980 artix      viper     20   0  151M  5396  4856 S  0.0  0.1  0:00.02 ├ /usr/lib/dconf-service
 81982 artix      viper     20   0  151M  5396  4856 S  0.0  0.1  0:00.00 │  ├ /usr/lib/dconf-service
 81981 artix      viper     20   0  151M  5396  4856 S  0.0  0.1  0:00.00 │  └ /usr/lib/dconf-service
 81954 artix      viper     20   0  226M  5288  4628 S  0.0  0.1  0:00.01 ├ /usr/lib/gvfs-mtp-volume-monitor
 81957 artix      viper     20   0  226M  5288  4628 S  0.0  0.1  0:00.00 │  ├ /usr/lib/gvfs-mtp-volume-monitor
 81955 artix      viper     20   0  226M  5288  4628 S  0.0  0.1  0:00.00 │  └ /usr/lib/gvfs-mtp-volume-monitor
 81935 artix      viper     20   0  340M 11876 10256 S  0.0  0.3  0:00.14 ├ /usr/lib/gvfs-udisks2-volume-monitor
 81941 artix      viper     20   0  340M 11876 10256 S  0.0  0.3  0:00.00 │  ├ /usr/lib/gvfs-udisks2-volume-monitor
 81937 artix      viper     20   0  340M 11876 10256 S  0.0  0.3  0:00.00 │  ├ /usr/lib/gvfs-udisks2-volume-monitor
 81936 artix      viper     20   0  340M 11876 10256 S  0.0  0.3  0:00.00 │  └ /usr/lib/gvfs-udisks2-volume-monitor
 81406 artix      viper     20   0  370M  6108  5436 S  0.0  0.2  0:00.01 ├ /usr/lib/gvfsd-fuse /run/user/1000/gvfs
 81412 artix      viper     20   0  370M  6108  5436 S  0.0  0.2  0:00.00 │  ├ /usr/lib/gvfsd-fuse /run/user/1000/g
 81411 artix      viper     20   0  370M  6108  5436 S  0.0  0.2  0:00.00 │  ├ /usr/lib/gvfsd-fuse /run/user/1000/g
 81410 artix      viper     20   0  370M  6108  5436 S  0.0  0.2  0:00.00 │  ├ /usr/lib/gvfsd-fuse /run/user/1000/g
 81409 artix      viper     20   0  370M  6108  5436 S  0.0  0.2  0:00.00 │  ├ /usr/lib/gvfsd-fuse /run/user/1000/g
F1Help  F2Setup  F3Search F4Filter F5SortedF6CollapF7Nice - F8Nice + F9Kill   F10Quit
```

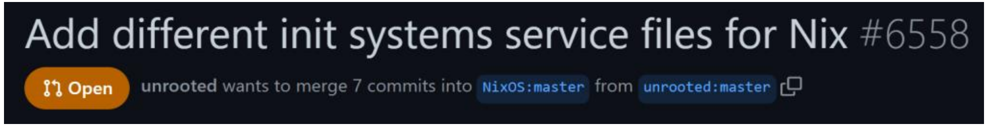
```
xmonad.hs
         , r 0.05 0.05 0.5  0.5  -- popup player float
         , r 0.05 0.05 0.25 0.25 -- popup player float #2
         , l 0.05 0.05 0.5  0.5  -- popup player float #3
         , l 0.05 0.05 0.25 0.25 -- popup player float #4
         ]
--}
--}
--{- main
main :: IO ()
main =
 xmonad
 .   ewmh
 .   docks
 =<< statusBar "xmobar" myXmobarPP (\x -> (XMonad.modMask x, xK_r)) myConfig
--}
--{- config
myConfig = def
 { terminal           = myTerminal
 , focusedBorderColor = mfg!!0
 , normalBorderColor  = mfg!!1
 , modMask            = mod4Mask
 , borderWidth        = 1
 , focusFollowsMouse  = False
-- xmonad.hs     0x0a  L  227  C 76   95%  haskell  7668
```

```
---------------------------------------   viper@northstar
---------------------------------------   ---------------
---------------------------------------   OS: Bedrock Linux 0.7.23beta2 Poki x86_64
---\\\\\\\\\\\\-----------------------   Host: XPS 15 9570
----\\\      \\\--------------------   Kernel: 5.13.8-artix1-1
-----\\\      \\\-------------------   Uptime: 3 hours, 22 mins
------\\\      \\\\\\\\\\\\\\\\\------   Packages: 923 (pacman), 229 (emerge), 584 (nix-user)
-------\\\                     \\\-----   Shell: zsh 5.8
--------\\\                     \\\----   Resolution: 1920x1080
---------\\\        ------       \\\---   WM: xmonad
----------\\\                    ///---   Terminal: termonad
-----------\\\                  ///----   Memory: 437MiB / 3895MiB
------------\\\                ///-----
-------------\\\///////////////------
---------------------------------------
---------------------------------------
---------------------------------------

λ ~/ nix-shell -p ghc

[nix-shell:~]$ ghci
GHCi, version 8.10.4: https://www.haskell.org/ghc/  :? for help
Prelude> putStrLn "Hello, world!"
Hello, world!
Prelude> 
```

```
deleting '/nix/store/40j4l3y4kipyla5fkbwfy7y67vvn9yf3-perl5.32.1-TimeDate-2.33'
deleting '/nix/store/1wxnz5npl05sahb5iv5q4azg2rk59kz5-ssl-cert-file-1.16.patch'
deleting '/nix/store/1xbpafm4ya480h6hq0h3kr4rr72kdmmr-curl-7.74.0.tar.bz2.drv'
deleting '/nix/store/an7k7vmqvj3gpvnqcj543mxy03c3pp5v-playtests-darwin.patch'
deleting '/nix/store/trash'
deleting unused links...
note: currently hard linking saves -0.00 MiB
1054 store paths deleted, 961.56 MiB freed

[nix-shell:~]$ nix --version
nix (Nix) 2.4pre20210707_02dd6bb

[nix-shell:~]$ sudo aura -Ayu
[sudo] password for viper:
:: Synchronizing package databases...
 system is up to date
 world                                  1919.3 KiB  1170 KiB/s 00:02 [######################################] 100%
 galaxy                                 1887.1 KiB  1212 KiB/s 00:02 [######################################] 100%
 extra                                  1570.1 KiB   887 KiB/s 00:02 [######################################] 100%
 community                                 5.6 MiB  1583 KiB/s 00:04 [######################################] 100%
 blackarch is up to date
aura >>= Fetching package information...
aura >>= Comparing package versions...
aura >>= No AUR package upgrades necessary.

[nix-shell:~]$ 
```

Non-NixOS Nix

the nightmare just begins

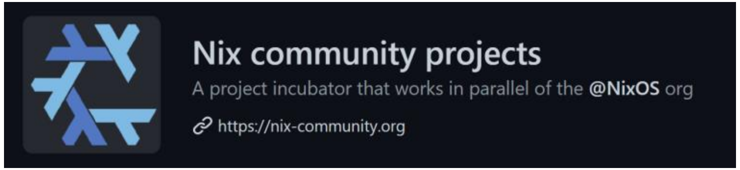


Add different init systems service files for Nix #6558

Open unrooted wants to merge 7 commits into `NixOS:master` from `unrooted:master`

Beyond Nix

if you only knew, how good things really are



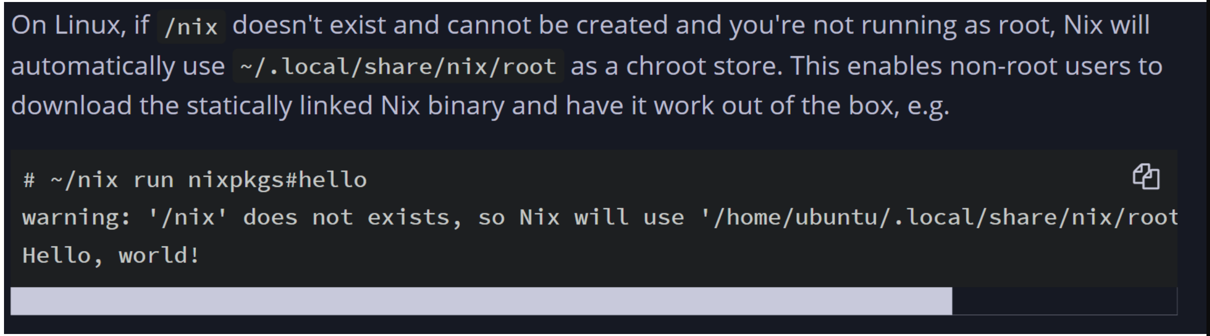
Nix community projects

A project incubator that works in parallel of the @NixOS org

https://nix-community.org

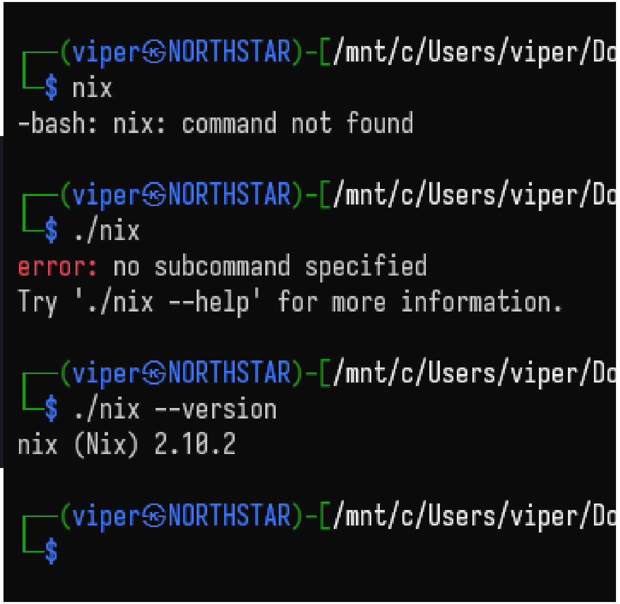
Nix portable (Nix 2.10.+)

next-gen sidearm



On Linux, if `/nix` doesn't exist and cannot be created and you're not running as root, Nix will automatically use `~/.local/share/nix/root` as a chroot store. This enables non-root users to download the statically linked Nix binary and have it work out of the box, e.g.

```
# ~/nix run nixpkgs#hello
warning: '/nix' does not exists, so Nix will use '/home/ubuntu/.local/share/nix/root
Hello, world!
```



```
┌──(viper㉿NORTHSTAR)-[/mnt/c/Users/viper/Do
└─$ nix
-bash: nix: command not found

┌──(viper㉿NORTHSTAR)-[/mnt/c/Users/viper/Do
└─$ ./nix
error: no subcommand specified
Try './nix --help' for more information.

┌──(viper㉿NORTHSTAR)-[/mnt/c/Users/viper/Do
└─$ ./nix --version
nix (Nix) 2.10.2

┌──(viper㉿NORTHSTAR)-[/mnt/c/Users/viper/Do
└─$
```

home-manager
/home, sweet /home

Think of it as of a maid:

- Manages your home
- Keeps your home tidy

lambda DAYS 28-29 JULY 2022 KRAKÓW | POLAND

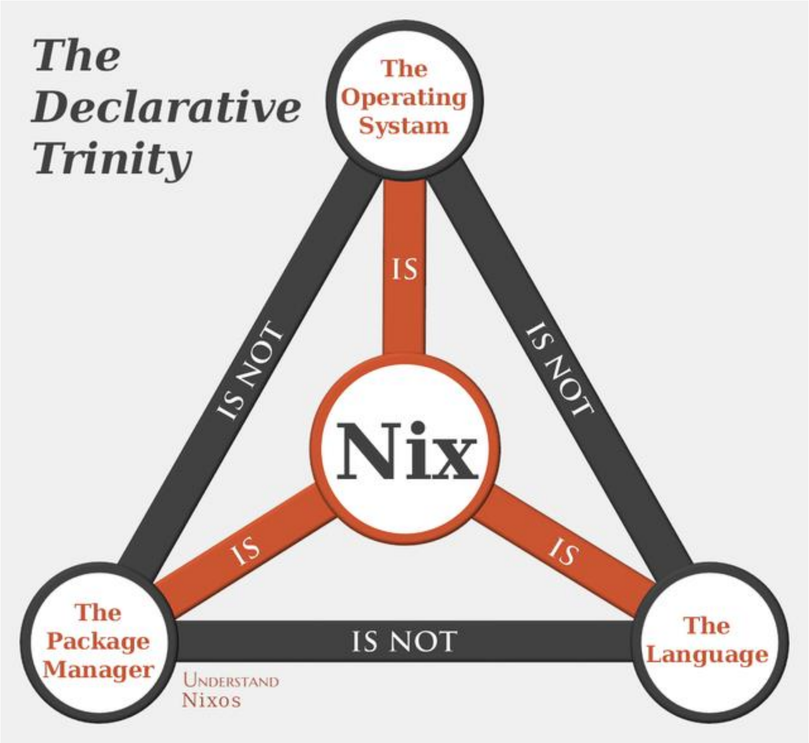
TL;DR?

1. Reproducible - produces exactly the same build every time.
2. Unless early boot is broken, boots to a consistent state.
3. Can easily rollback to the previous system configuration state.
4. Declarative config FOR EVERYTHING!
5. Integration with a whole bunch of packages. Your beloved GUI rices included.
6. Cloud integration. Brilliant Docker images, also magic like NixOps
7. Portability - Nix runs on Linux and macOS, and takes 5 minutes to install (clone config and you're done).
8. Free of side effects - Actually uninstalls packages and its dependencies
9. Bleeding and stable - Can run multiple versions of the package without conflicts
10. Implicit containerization - Lorri and direnv make switching between project-local tooling easy.
11. Virtual Machines - VFIO is EASY to set up and perform declaratively (much more so than arch).
12. Kernel hacking - Kernel flags and patches are easy to add to config.
13. Use flags + source-based - each package has overrides to allow (or disallow) features to be built. Makes for a lean mean machine. Binary caching for speed.
14. OOTB rollbacks

TL;DR?

- Focus on correctness
- Reliable package storage structure
- Results are read-only
- OOTB cross-compilation support
- OOTB static compilation support
- Source-based (you can alter packages build without forking anything)
- Single package manager to rule them all! (c, python, docker, nodejs, etc)
- Great for development environment, will take care of all dependencies no matter if its postgresql or glibc
- Easy to set up a binary cache
- By default has a binary cache so you almost never need to compile anything
- Easy to set up build farm
- Super convenient for CI/CD
- Excellent testing infrastructure
- More often than not build results are bit per bit reproducible

What is Nix?


The Declarative Trinity
The Operating Systam
IS
IS NOT
IS NOT
Nix
IS
IS
The Package Manager
IS NOT
The Language
Understand Nixos

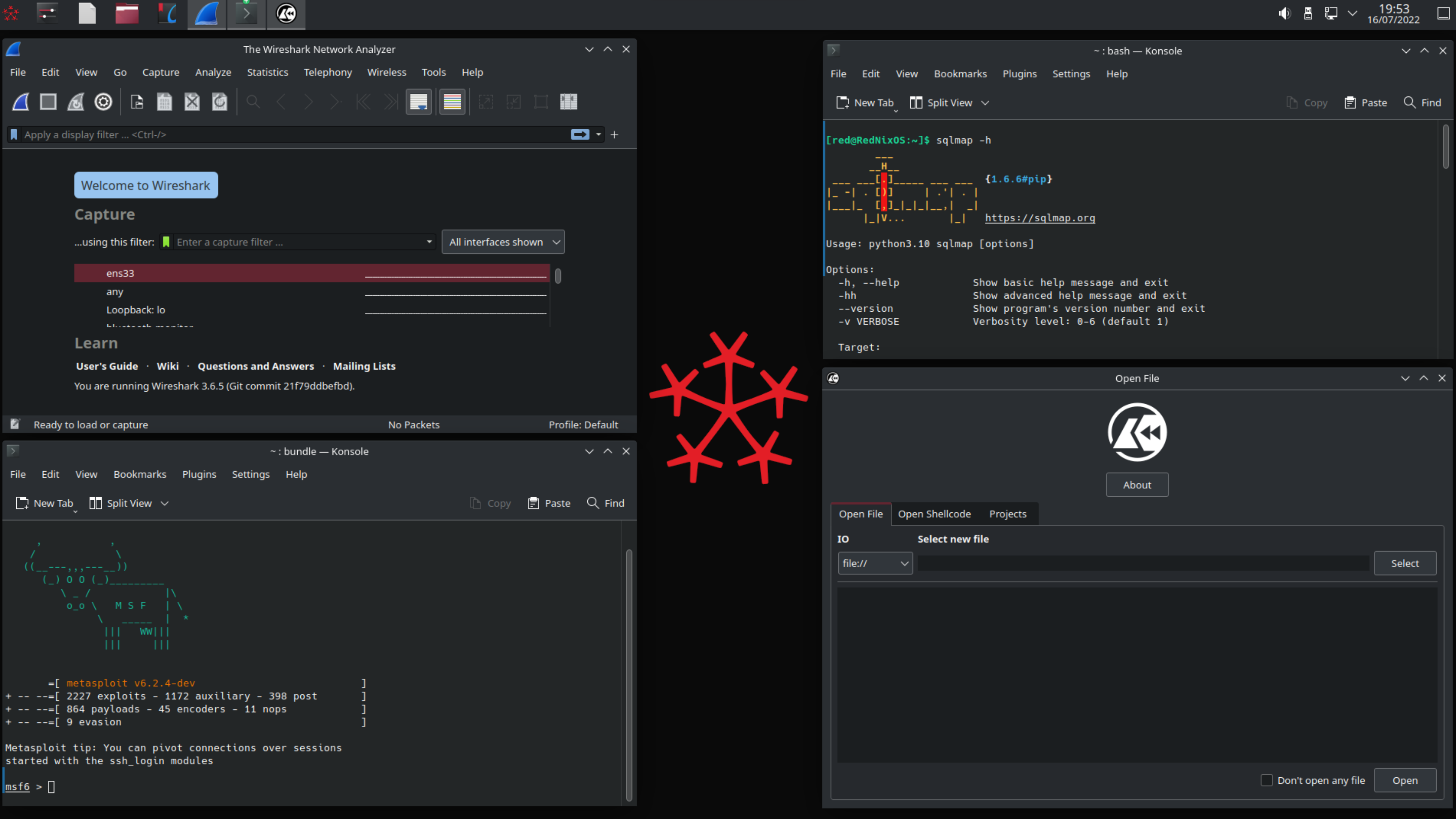
References

- NixOS - NixOS Linux
- NixOS - Nixpkgs 22.11 manual
- NixOS - Nix Pills
- Nix community projects (github.com)

Special thanks to...

[adult swim]
SHOW ME WHAT YOU GOT!

immutable yet adaptable



You are running Wireshark 3.6.5 (Git commit 21f79ddbefbd).

```
[red@RedNixOS:~]$ sqlmap -h
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.6#pip}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3.10 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
```

```
     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.2.4-dev                          ]
+ -- --=[ 2227 exploits - 1172 auxiliary - 398 post       ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > 
```

Q&A

Thanks!