

# NIXOS

*Tristan Pinaudeau @ [Capgemini](#)*

# PRÉSENTATION

- **SRE** à Cdiscount
- **PENTESTER** à Capgemini

# INTRODUCTION

# CONSTATS

# CONSTATS

- Inexhaustivité de la cartographie

# CONSTATS

- Inexhaustivité de la cartographie
- Entropie des configurations

# CONSTATS

- Inexhaustivité de la cartographie
- Entropie des configurations
- Gestion chaotique des patchs

# CONSTATS

- Inexhaustivité de la cartographie
- Entropie des configurations
- Gestion chaotique des patchs
- Obscurité à l'audit

# CONSTATS

- Inexhaustivité de la cartographie
- Entropie des configurations
- Gestion chaotique des patchs
- Obscurité à l'audit
- Automatisation complexe

# SOLUTIONS EVENTUELLES

# SOLUTIONS EVENTUELLES

- GPO / Scripts

# SOLUTIONS EVENTUELLES

- GPO / Scripts
- Infrastructure As Code

# SOLUTIONS EVENTUELLES

- GPO / Scripts
- Infrastructure As Code
- Containerisation

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Automatisable

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Automatisable
- Versionnable

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Automatisable
- Versionnable
- Liberté de configuration

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Automatisable
- Versionnable
- Liberté de configuration
- Reproductibilité / Idempotence

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Automatisable
- Versionnable
- Liberté de configuration
- Reproductibilité / Idempotence
- Bare Metal & Env. Virtualisé

# FONCTIONNEMENT

# NPM? = NIX PACKAGE MANAGER

## The Purely Functional Software Deployment Model

Het puur functionele softwaredeploymentmodel  
(met een samenvatting in het Nederlands)

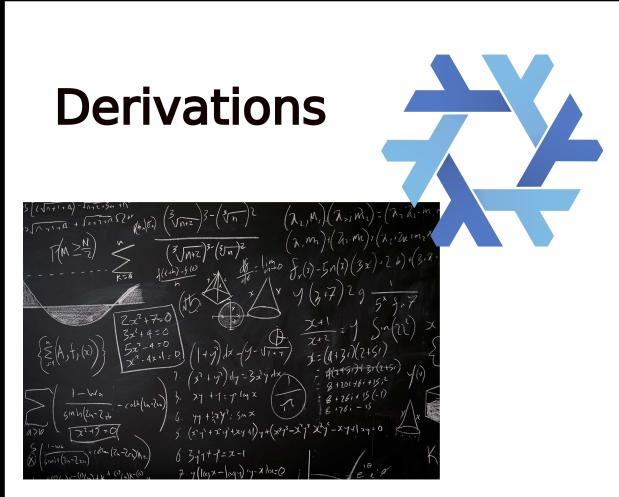
Proefschrift ter verkrijging van de graad van doctor aan de Universiteit Utrecht op gezag van de Rector Magnificus, Prof. dr. W. H. Gispen, ingevolge het besluit van het College voor Promoties in het openbaar te verdedigen op woensdag 18 januari 2006 des middags te 12.45 uur

door

Eelco Dolstra

geboren op 18 augustus 1978, te Wageningen

# ~~PACKAGE~~ DERIVATIONS



# NIX STORE

```
[tristan@master:~]$ tree /nix/store/ | head
/nix/store/
├── 0002rzpmcn4b7bq25qalw8j0v0vsl06c-ghidra.desktop.drv
├── 000iv8q3v5c9ipvq3jx2hvibnp9i9vma-source.drv
├── 001gp43bjqzx60cg345n2slzg7131za8-nix-nss-open-files.patch
├── 002jkych43y6k0y7x256hnq7vg78ijjx-lua-setup-hook.sh.drv
└── 00ix6n35smbd73xy16d0f9hkj0h7hafv-llvm-14.0.1-dev
    ├── bin
    │   └── llvm-config
    ├── include
    └── llvm
```

DERIVATION = **hash(hash(SRC) + hash(DEPENDANCES))**

# MIRROIR MON BEAU MIRROIR...

[M] 1: NixOS/nixpkgs: Nix Packages collection

The screenshot shows the GitHub repository page for 'NixOS / nixpkgs'. The repository is public and has 10.7k stars, 8.7k forks, and 292 watchers. It contains 4.1k pull requests, 5k+ issues, and 217 branches. The 'Code' tab is selected. The 'About' section describes it as a 'Nix Packages collection' and lists tags like linux, nix, nixos, nixpkgs, and hacktoberfest. The repository URL is <https://github.com/NixOS/nixpkgs>.

Nix Packages collection

linux nix nixos nixpkgs  
hacktoberfest

About

Readme

MIT license

Security policy

10.7k stars

292 watching

8.7k forks

<https://github.com/NixOS/nixpkgs> [top] [1/1]

File	Description	Time
tpwrules	and Mindavi zfp: 0...	30 minutes ago
.github	Merge pull request #200289 from fricklerhan...	2 days ago
doc	doc/vim: Clarify buildVimPlugin/buildVimPlu...	2 days ago
lib	licenses: add bsd2WithViews	15 hours ago
maintainers	maintainers: add lightquantum	16 hours ago
nixos	Merge pull request #201396 from ElvishJerri...	2 hours ago
pkgs	zfp: 0.5.5 -> 1.0.0, fix issues	30 minutes ago
.editorconfig	.editorconfig: disable for Apple nib files	3 months ago

# VOUS FAITES LE LIEN ?

```
1 [tristan@demo:~]$ gcc --version
2 gcc (GCC) 11.3.0
3
4 [tristan@demo:~]$ which gcc
5 /home/tristan/.nix-profile/bin/gcc
6
7 [tristan@demo:~]$ ls -l /home/tristan/.nix-profile/bin/gcc
8 /home/tristan/.nix-profile/bin/gcc -> /nix/store/ykcrnkiicqg
```

# VOUS FAITES LE LIEN ?

```
1 [tristan@demo:~]$ gcc --version
2 gcc (GCC) 11.3.0
3
4 [tristan@demo:~]$ which gcc
5 /home/tristan/.nix-profile/bin/gcc
6
7 [tristan@demo:~]$ ls -l /home/tristan/.nix-profile/bin/gcc
8 /home/tristan/.nix-profile/bin/gcc -> /nix/store/ykcrnkiicqg
```

# VOUS FAITES LE LIEN ?

```
1 [tristan@demo:~]$ gcc --version
2 gcc (GCC) 11.3.0
3
4 [tristan@demo:~]$ which gcc
5 /home/tristan/.nix-profile/bin/gcc
6
7 [tristan@demo:~]$ ls -l /home/tristan/.nix-profile/bin/gcc
8 /home/tristan/.nix-profile/bin/gcc -> /nix/store/ykcrnkiicqg
```

# CAS PRATIQUE

# SITUATION INITIALE

```
└── docker-compose.yml  
└── Makefile  
└── template.env
```

# "TALK IS CHEAP,..."

```
1 {pkgs, fetchFromGitHub, ...}:
2 let
3   argProjectName = "--project-name '$name'";
4   argComposeFile = "--file '$src/docker-compose.yml'";
5   dockerCmd = "compose ${argProjectName} ${argComposeFile}"
6 in
7 derivation {
8   name = "docker-nextcloud";
9
10  system = builtins.currentSystem;
11
12  src = fetchFromGitHub {
13    owner = "0b11stan";
14    repo = "docker-nextcloud";
15    rev = "main".
```

# "TALK IS CHEAP,..."

```
1 {pkgs, fetchFromGitHub, ...}:
2 let
3   argProjectName = "--project-name '$name'";
4   argComposeFile = "--file '$src/docker-compose.yml'";
5   dockerCmd = "compose ${argProjectName} ${argComposeFile}"
6 in
7 derivation {
8   name = "docker-nextcloud";
9
10  system = builtins.currentSystem;
11
12  src = fetchFromGitHub {
13    owner = "0b11stan";
14    repo = "docker-nextcloud";
15    rev = "main".
```

# "TALK IS CHEAP,..."

```
1 {pkgs, fetchFromGitHub, ...}:
2 let
3   argProjectName = "--project-name '$name'";
4   argComposeFile = "--file '$src/docker-compose.yml'";
5   dockerCmd = "compose ${argProjectName} ${argComposeFile}"
6 in
7 derivation {
8   name = "docker-nextcloud";
9
10  system = builtins.currentSystem;
11
12  src = fetchFromGitHub {
13    owner = "0b11stan";
14    repo = "docker-nextcloud";
15    rev = "main".
```

# "TALK IS CHEAP,..."

```
1 {pkgs, fetchFromGitHub, ...}:
2 let
3   argProjectName = "--project-name '$name'";
4   argComposeFile = "--file '$src/docker-compose.yml'";
5   dockerCmd = "compose ${argProjectName} ${argComposeFile}"
6 in
7 derivation {
8   name = "docker-nextcloud";
9
10  system = builtins.currentSystem;
11
12  src = fetchFromGitHub {
13    owner = "0b11stan";
14    repo = "docker-nextcloud";
15    rev = "main";
```

# "TALK IS CHEAP, ..."

```
8     name = "docker-nextcloud";
9
10    system = builtins.currentSystem;
11
12    src = fetchFromGitHub {
13        owner = "0b11stan";
14        repo = "docker-nextcloud";
15        rev = "main";
16        sha256 = "sha256-Sh+9Apb71QJHeShgaUbqLXQJMEjrBfkY/tW4Pi
17    };
18
19    builder = "${pkgs.bash}/bin/bash";
20
21    args = [ "-c"
```

# "TALK IS CHEAP,..."

```
16      sha256 = "sha256-5f1e58fb71931e09a094e801e7fb1f77c47d  
17  };  
18  
19  builder = "${pkgs.bash}/bin/bash";  
20  
21  args = [ "-c"  
22    ''  
23    "${pkgs.coreutils}/bin/mkdir $out \  
24    && echo "${pkgs.docker}/bin/docker ${dockercmd}" \  
25    > $out/$name.sh \  
26    && ${pkgs.coreutils}/bin/chmod +x $out/$name.sh  
27    ''  
28  ];  
29 }
```

# "TALK IS CHEAP,..."

```
16      sha256 = "sha256-51f3e58b714931e09a094e801e7fb1f77c47d  
17  };  
18  
19  builder = "${pkgs.bash}/bin/bash";  
20  
21  args = [ "-c"  
22    ''  
23    "${pkgs.coreutils}/bin/mkdir $out \  
24    && echo "${pkgs.docker}/bin/docker ${dockercmd}" \  
25    > $out/$name.sh \  
26    && ${pkgs.coreutils}/bin/chmod +x $out/$name.sh  
27    ''  
28  ];  
29 }
```

# "TALK IS CHEAP,..."

```
16      sha256 = "sha256-5f1e58fb714931e09a094e80e7fb1f77c47d  
17  };  
18  
19  builder = "${pkgs.bash}/bin/bash";  
20  
21  args = [ "-c"  
22    ''  
23    "${pkgs.coreutils}/bin/mkdir $out \  
24    && echo "${pkgs.docker}/bin/docker ${dockercmd}" \  
25    > $out/$name.sh \  
26    && ${pkgs.coreutils}/bin/chmod +x $out/$name.sh  
27    ''  
28  ];  
29 }
```

# CONFIGURATIONS

```
###      /etc/nixos/configuration.nix      ###

{config, lib, pkgs, ...}:
let
  secretMySQLRootPassword = builtins.getenv "MYSQL_ROOT_PASSWORD";
  secretMySQLPassword = builtins.getenv "MYSQL_PASSWORD";
in {
  imports = [./hardware-configuration.nix];

  ...
  system.stateVersion = "22.05";
}
```

# CONFIGURATION - NEXTCLOUD

```
1 nixpkgs.overlays = [(self: super: {  
2   docker-nextcloud = super.callPackage ./docker-nextcloud.r  
3 })];  
4  
5 environment.systemPackages = [pkgs.docker-nextcloud];  
6  
7 systemd.services.nextcloud = {  
8   enable = true;  
9   restartIfChanged = true;  
10  wantedBy = ["multi-user.target"];  
11  after = ["docker.service"];  
12  bindsTo = ["docker.service"];  
13  documentation = ["https://github.com/0b11stan/docker-nextcloud"];  
14  script = "${pkgs.docker-nextcloud}/docker-nextcloud.sh";  
15  environment = {
```

# CONFIGURATION - NEXTCLOUD

```
1 nixpkgs.overlays = [(self: super: {  
2   docker-nextcloud = super.callPackage ./docker-nextcloud.r  
3 })];  
4  
5 environment.systemPackages = [pkgs.docker-nextcloud];  
6  
7 systemd.services.nextcloud = {  
8   enable = true;  
9   restartIfChanged = true;  
10  wantedBy = ["multi-user.target"];  
11  after = ["docker.service"];  
12  bindsTo = ["docker.service"];  
13  documentation = ["https://github.com/0b11stan/docker-nextcloud"];  
14  script = "${pkgs.docker-nextcloud}/docker-nextcloud.sh";  
15  environment = {
```

# CONFIGURATION - NEXTCLOUD

```
6
7 systemd.services.nextcloud = {
8     enable = true;
9     restartIfChanged = true;
10    wantedBy = ["multi-user.target"];
11    after = ["docker.service"];
12    bindsTo = ["docker.service"];
13    documentation = ["https://github.com/0b11stan/docker-nextcloud"];
14    script = "${pkgs.docker-nextcloud}/docker-nextcloud.sh";
15    environment = {
16        MYSQL_ROOT_PASSWORD = secretMySQLRootPassword;
17        MYSQL_PASSWORD = secretMySQLPassword;
18    };
19 }
```

# CONFIGURATION - NEXTCLOUD

```
4
5 environment.systemPackages = [pkgs.docker-nextcloud];
6
7 systemd.services.nextcloud = {
8     enable = true;
9     restartIfChanged = true;
10    wantedBy = ["multi-user.target"];
11    after = ["docker.service"];
12    bindsTo = ["docker.service"];
13    documentation = ["https://github.com/0b11stan/docker-nextcloud"];
14    script = "${pkgs.docker-nextcloud}/docker-nextcloud.sh";
15    environment = {
16        MYSQL_ROOT_PASSWORD = secretMySQLRootPassword;
17        MYSQL_PASSWORD = secretMySQLPassword;
18    };
}
```

# CONFIGURATION - NEXTCLOUD

```
6
7 systemd.services.nextcloud = {
8     enable = true;
9     restartIfChanged = true;
10    wantedBy = ["multi-user.target"];
11    after = ["docker.service"];
12    bindsTo = ["docker.service"];
13    documentation = ["https://github.com/0b11stan/docker-nextcloud"];
14    script = "${pkgs.docker-nextcloud}/docker-nextcloud.sh";
15    environment = {
16        MYSQL_ROOT_PASSWORD = secretMySQLRootPassword;
17        MYSQL_PASSWORD = secretMySQLPassword;
18    };
19 }
```

# CONFIGURATION - NEXTCLOUD

```
6
7 systemd.services.nextcloud = {
8     enable = true;
9     restartIfChanged = true;
10    wantedBy = ["multi-user.target"];
11    after = ["docker.service"];
12    bindsTo = ["docker.service"];
13    documentation = ["https://github.com/0b11stan/docker-nextcloud"];
14    script = "${pkgs.docker-nextcloud}/docker-nextcloud.sh";
15    environment = {
16        MYSQL_ROOT_PASSWORD = secretMySQLRootPassword;
17        MYSQL_PASSWORD = secretMySQLPassword;
18    };
19 }
```

# CONFIGURATION - DOCKER

```
virtualisation.docker.enable = true;
```

# CONFIGURATION - SSH

```
services.openssh = {  
    enable = true;  
    passwordAuthentication = false;  
    permitRootLogin = "no";  
};
```

# CONFIGURATION - RÉSEAU

```
1 networking = {  
2     hostName = "nixos-harden";  
3     networkmanager.enable = true;  
4     useDHCP = true;  
5     firewall = {  
6         enable = true;  
7         allowedTCPPorts = [8080 22];  
8     };  
9 };
```

# CONFIGURATION - RÉSEAU

```
1 networking = {  
2     hostName = "nixos-harden";  
3     networkmanager.enable = true;  
4     useDHCP = true;  
5     firewall = {  
6         enable = true;  
7         allowedTCPPorts = [8080 22];  
8     };  
9 };
```

# CONFIGURATION - USER

```
1 users.users = {  
2   tristan = {  
3     isNormalUser = true;  
4     extraGroups = ["wheel" "docker"];  
5     packages = [pkgs.neovim];  
6     openssh.authorizedKeys.keyFiles = [  
7       ./ssh-keys/silver-hp.pub  
8     ];  
9   };  
10 };
```

# CONFIGURATION - USER

```
1 users.users = {  
2     tristan = {  
3         isNormalUser = true;  
4         extraGroups = ["wheel" "docker"];  
5         packages = [pkgs.neovim];  
6         openssh.authorizedKeys.keyFiles = [  
7             ./ssh-keys/silver-hp.pub  
8         ];  
9     };  
10 };
```

# CONFIGURATION - USER

```
1 users.users = {  
2     tristan = {  
3         isNormalUser = true;  
4         extraGroups = ["wheel" "docker"];  
5         packages = [pkgs.neovim];  
6         openssh.authorizedKeys.keyFiles = [  
7             ./ssh-keys/silver-hp.pub  
8         ];  
9     };  
10 };
```

# CONFIGURATION - USER

```
1 users.users = {  
2     tristan = {  
3         isNormalUser = true;  
4         extraGroups = ["wheel" "docker"];  
5         packages = [pkgs.neovim];  
6         openssh.authorizedKeys.keyFiles = [  
7             ./ssh-keys/silver-hp.pub  
8         ];  
9     };  
10 };
```

# RÉSULTATS

```
1 > wc -l src/*.nix src/*.sh
2
3   69 src/configuration.nix
4   34 src/docker-nextcloud.nix
5   42 src/hardware-configuration.nix
6     2 src/init.sh
7 147 total
```

# RÉSULTATS

```
1 > wc -l src/*.nix src/*.sh
2
3   69 src/configuration.nix
4   34 src/docker-nextcloud.nix
5   42 src/hardware-configuration.nix
6     2 src/init.sh
7 147 total
```

# RÉSULTATS

```
1 > wc -l src/*.nix src/*.sh
2
3   69 src/configuration.nix
4   34 src/docker-nextcloud.nix
5   42 src/hardware-configuration.nix
6     2 src/init.sh
7 147 total
```

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Versionnable

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Versionnable
- Automatisable

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Versionnable
- Automatisable
- Reproductibilité / Idempotence

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Versionnable
- Automatisable
- Reproductibilité / Idempotence
- Liberté de configuration

# LE SYSTÈME PARFAIT EXISTE-T-IL ?

- Versionnable
- Automatisable
- Reproductibilité / Idempotence
- Liberté de configuration
- Bare Metal & Env. Virtualisé

# SYNTHÈSE

# BONUS - ISOLATION LOGICIELLE

```
1 $ echo $PATH | tr ':' '\n'  
2  
3 /run/wrappers/bin  
4 /home/tristan/.nix-profile/bin  
5 /etc/profiles/per-user/tristan/bin  
6 /nix/var/nix/profiles/default/bin  
7 /run/current-system/sw/bin
```

# BONUS - ROOT EN READONLY

```
1 $ DERIVATION=$(ls -tp /nix/store/ | grep 'openssl.*/$')
```

```
2
```

```
3 $ ls -l /nix/store/$DERIVATION/etc/ssh/
```

```
4 total 504
```

```
5 -r--r--r-- 2 root root 505489 1 janv. 1970 moduli
```

```
6 -r--r--r-- 2 root root 1531 1 janv. 1970 ssh_config
```

```
7 -r--r--r-- 2 root root 3226 1 janv. 1970 sshd_config
```

```
8
```

```
9 $ sudo chmod +w /nix/store/$DERIVATION/etc/ssh/sshd_config
```

```
10 [sudo] Mot de passe de tristan :
```

```
11 chmod: modification des droits [...] Read-only file system
```

# BONUS - ROOT EN READONLY

```
1 $ DERIVATION=$(ls -tp /nix/store/ | grep 'openssh.*/$')
```

```
2
```

```
3 $ ls -l /nix/store/$DERIVATION/etc/ssh/
```

```
4 total 504
```

```
5 -r--r--r-- 2 root root 505489 1 janv. 1970 moduli
```

```
6 -r--r--r-- 2 root root 1531 1 janv. 1970 ssh_config
```

```
7 -r--r--r-- 2 root root 3226 1 janv. 1970 sshd_config
```

```
8
```

```
9 $ sudo chmod +w /nix/store/$DERIVATION/etc/ssh/sshd_config
```

```
10 [sudo] Mot de passe de tristan :
```

```
11 chmod: modification des droits [...] Read-only file system
```

# BONUS - ROOT EN READONLY

```
1 $ DERIVATION=$(ls -tp /nix/store/ | grep 'openssl.*/$')
```

```
2
```

```
3 $ ls -l /nix/store/$DERIVATION/etc/ssh/
```

```
4 total 504
```

```
5 -r--r--r-- 2 root root 505489 1 janv. 1970 moduli
```

```
6 -r--r--r-- 2 root root 1531 1 janv. 1970 ssh_config
```

```
7 -r--r--r-- 2 root root 3226 1 janv. 1970 sshd_config
```

```
8
```

```
9 $ sudo chmod +w /nix/store/$DERIVATION/etc/ssh/sshd_config
```

```
10 [sudo] Mot de passe de tristan :
```

```
11 chmod: modification des droits [...] Read-only file system
```

# BONUS - ROLLBACK

```
1 [tristan@demo:~]$ ls /boot/loader/entries/ | head -n 2
2 nixos-generation-131.conf  nixos-generation-132.conf
3
4 [tristan@demo:~]$ cat /boot/.../nixos-generation-131.conf
5 title NixOS
6 version Generation 131 NixOS 22.05.4120.16f4e04658c, Linux
7 linux /efi/nixos/rax...xdm-linux-5.15.78-bzImage.efi
8 initrd /efi/nixos/846...s13-initrd-linux-5.15.78-initrd.efi
9 options init=/nix/store/4jx...17f-nixos-system-demo-22.05.4
10 machine-id b7bfdd5f273b49c6a30c4e26e84c8f21
```

# BONUS - ROLLBACK

```
1 [tristan@demo:~]$ ls /boot/loader/entries/ | head -n 2
2 nixos-generation-131.conf  nixos-generation-132.conf
3
4 [tristan@demo:~]$ cat /boot/.../nixos-generation-131.conf
5 title NixOS
6 version Generation 131 NixOS 22.05.4120.16f4e04658c, Linux
7 linux /efi/nixos/rax...xdm-linux-5.15.78-bzImage.efi
8 initrd /efi/nixos/846...sl3-initrd-linux-5.15.78-initrd.efi
9 options init=/nix/store/4jx...17f-nixos-system-demo-22.05.4
10 machine-id b7bfdd5f273b49c6a30c4e26e84c8f21
```

# LES INCONVENIENTS

# LES INCONVENIENTS

- Moins "Flexible"

# LES INCONVENIENTS

- Moins "Flexible"
- Croissances du Nix store

# LES INCONVENIENTS

- Moins "Flexible"
- Croissances du Nix store
- Systemd centric

# LES INCONVENIENTS

- Moins "Flexible"
- Croissances du Nix store
- Systemd centric
- Adoption = changement d'OS

# LES INCONVENIENTS

- Moins "Flexible"
- Croissances du Nix store
- Systemd centric
- Adoption = changement d'OS
- Surcharge de Nixpkgs

# CONCLUSION



<https://github.com/0b11stan/hackitn-nixos-slideshow>



<https://github.com/0b11stan/hackitn-nixos-demo>

