The Nix project

Sander van der Burg

Delft University of Technology, EEMCS,
Department of Software Technology

June 24, 2013
Software deployment

Sander van der Burg

The Nix project
Software deployment

All of the activities that make a software system available for use.
Modern applications
Modern systems are rarely *self-contained*:

- **Systems are composed** of many software components
- **Dependencies must be present and correct**, both at build-time and run-time
- **Non-functional requirements must be met:**
  - Reliability
  - Privacy
  - Component licenses
Software deployment

Challenges

- Systems are becoming *bigger*, more distributed and more complicated
- Deployment takes a lot of *effort* and *time*
- Difficult to *reproduce* a configuration elsewhere
- *Upgrading* may break a system and may introduce significant downtimes
Deployment failures

Sander van der Burg

The Nix project
Challenges

- **Complexity.** Many steps must be performed, in the right order.

- **Reliability.** Dependencies may break, files get overwritten, modified or removed. Upgrades may yield different results as fresh installations.

- **Agility.** In order to quickly deliver value, systems must be deployed faster and on-demand.

- **Genericity.** Most existing deployment solutions only support specific component-types and environments.

Sander van der Burg

The Nix project
NixOS

A GNU/Linux distribution using the Nix package manager
Main idea: store all packages in isolation from each other:

```
/nix/store/rpdxnilb0cg...-firefox-3.5.4
```

Paths contain a 160-bit **cryptographic hash** of all inputs used to build the package:

- Sources
- Libraries
- Compilers
- Build scripts
- ...

```
/nix/store
  └── 19w6773m1msy...-openssh-4.6p1
        └── bin
              └── ssh
                    └── sbin
                          └── ssdh

        └── smkabrbibqv7...-openssl-0.9.8e
                └── lib
                        └── libssl.so.0.9.8

    └── c6jbqm2mc0a7...-zlib-1.2.3
            └── lib
                    └── libz.so.1.2.3

    └── im276akmsrhv...-glibc-2.5
                    └── lib
                            └── libc.so.6
```
Nix expressions

openssh.nix

{ stdenv, fetchurl, openssl, zlib }:

stdenv.mkDerivation {
    name = "openssh-4.6p1";
    src = fetchurl {
        url = http://.../openssh-4.6p1.tar.gz;
        sha256 = "0fpjlr3bfjnd0y94bk442x2p...";
    };
    buildCommand = ''
        tar xjf $src
        ./configure --prefix=$out --with-openssl=${openssl}
        make; make install
    '';
}
Nix expressions

all-packages.nix

```nix
openssl = import ../tools/networking/openssh { inherit fetchurl stdenv openssl zlib; };
openssl = import ../development/libraries/openssl { inherit fetchurl stdenv perl; };

stdenv = ...;
openssl = ...;
zlib = ...;
perl = ...;
```

- `nix-env -f all-packages.nix -iA openssh`
- Produces a `/nix/store/l9w6773m1msy...-openssh-4.6p1` package in the Nix store.
Users can have different sets of installed applications.
- Users can have different sets of installed applications.
- `nix-env` operations create new **user environments** in the store.

```
(nix-env -u opensshh)
```
Users can have different sets of installed applications.

nix-env operations create new user environments in the store.

(nix-env -u openssh)
Users can have different sets of installed applications. nix-env operations create new user environments in the store.

(nix-env -u openssh)
- Users can have different sets of installed applications.
- `nix-env` operations create new **user environments** in the store.
- We can atomically switch between them.

```
(nix-env -u openssh)
```
User environments

- Users can have different sets of installed applications.
- `nix-env` operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the **garbage collector**.

```
(nix-env --remove-generations old)
```
User environments

- Users can have different sets of installed applications.
- `nix-env` operations create new **user environments** in the store.
- We can atomically switch between them.
- These are roots of the garbage collector.
$ nix-build --run-env -A openssh

$ openssl version
OpenSSL 1.0.1e 11 Feb 2013

$ nix-build --run-env -A hello

$ openssl version
The program 'openssl' is currently not installed.
You can install it by typing:
    nix-env -i openssl
In NixOS, all packages including the Linux kernel and configuration files are managed by Nix.

NixOS does not have directories such as: /lib and /usr

NixOS has a minimal /bin and /etc

But NixOS is more then just a distribution managed by Nix
NixOS configuration

/etc/nixos/configuration.nix

```nix
{pkgs, ...}:

{  boot.loader.grub.device = "/dev/sda";

  fileSystems = [ { mountPoint = "/"; device = "/dev/sda2"; } ];
  swapDevices = [ { device = "/dev/sda1"; } ];

  services = {
    openssh.enable = true;

    xserver = {
      enable = true;
      desktopManager.kde4.enable = true;
    };
  };

  environment.systemPackages = [ pkgs.mc pkgs.firefox ];
}
```
NixOS configuration

nixos-rebuild switch

- Nix package manager builds a complete system configuration
  - Includes all packages and generates all configuration files, e.g. OpenSSH configuration
- Upgrades are (almost) atomic
  - Components are stored safely next to each other, due to hashes
  - No files are automatically removed or overwritten
- Users can switch to older generations of system configurations not garbage collected yet
The Nix project

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, ’e’ to edit the
commands before booting, or ’c’ for a command-line.

GNU/Linux
Nix/NixOS advantages

- **Reliability.** Dependencies are always complete, present and correct. No files overwritten, modified or removed.

- **Reproducibility.** Because side-effects are removed, build functions always yield same result, regardless on what machine they are executed.

- **Generic.** We can invoke arbitrary build processes in Nix functions. Nix is supported on many operating systems: Linux, FreeBSD, Mac OS X, Windows (Cygwin)

- **Efficient.** Only components that must be built are build. Nix store serves as a cache.

- Scope is *limited* to packages on local machines.
Nix applications
$ disnix-env -s services.nix -i infrastructure.nix -d distribution.nix
{distribution, system}:

let pkgs = import ../top-level/all-packages.nix {
  inherit distribution system;
}; in
{
  mobileeventlogs = {
    name = "mobileeventlogs";
    pkg = pkgs.mobileeventlogs;
    type = "mysql-database";
  };
  MELogService = {
    name = "MELogService";
    pkg = pkgs.MELogService;
    dependsOn = {
      inherit mobileeventlogs;
    };
    type = "tomcat-webapplication";
  };
  SDS2AssetTracker = {
    name = "SDS2AssetTracker";
    pkg = pkgs.SDS2AssetTracker;
    dependsOn = {
      inherit MELogService ...
    };
    type = "tomcat-webapplication";
  };
...}
Infrastructure model

{  
    test1 = {
        hostname = "test1.net";
        tomcatPort = 8080;
        mysqlUser = "user";
        mysqlPassword = "secret";
        mysqlPort = 3306;
        targetEPR = http://test1.net/.../DisnixService;
        system = "i686-linux";
    }
    test2 = {
        hostname = "test2.net";
        tomcatPort = 8080;
        ...
        targetEPR = http://test2.net/.../DisnixService;
        system = "x86_64-linux";
    }
}

Captures machines in the network and their relevant properties and capabilities.
{infrastructure}:

{
    mobileeventlogs = [ infrastructure.test1 ];
    MELogService = [ infrastructure.test2 ];
    SDS2AssetTracker = [ infrastructure.test1 infrastructure.test2 ];
    ...
}

Maps services to machines
Deployment process

Specifications are used to derive deployment process:

- **Building** services from source code
- **Transferring** services to target machines
- **Deactivating** obsolete services and **activating** new services
Welcome to Trac 0.11.7

Trac is a **minimalistic** approach to **web-based** management of **software projects**. Its goal is to simplify effective tracking and handling of software issues, enhancements and overall progress.

All aspects of Trac have been designed with the single goal to **help developers write great software** while **staying out of the way** and imposing as little as possible on a team's established process and culture.

As all Wiki pages, this page is editable, this means that you can modify the contents of this page simply by using your web-browser. Simply click on the "Edit this page" link at the bottom of the page. WikiFormatting will give you a detailed description of available Wiki formatting commands.

"**trac-admin yourenvdir initenv**" created a new Trac environment, containing a default set of wiki pages and some sample data. This newly created environment also contains **documentation** to help you get started with your project.

You can use **trac-admin** to configure Trac to better fit your project, especially in regard to **components**, **versions** and **milestones**.

**TracGuide** is a good place to start.

Enjoy!

*The Trac Team*
Motivating example: Trac

Trac can be deployed in a *distributed* environment:

- Subversion server
- Database server
- Web server
Distributed NixOS configuration

```nix
{ storage = {pkgs, ...}:
  {
    services.nfsKernel.server.enable = true; ...
  };

postgresql = {pkgs, ...}:
  {
    services.postgresql.enable = true; ...
  };

webserver = {pkgs, ...}:
  {
    fileSystems = [
      { mountPoint = "/repos"; device = "storage:/repos"; } ];
    services.httpd.enable = true;
    services.httpd.extraSubservices = [ { serviceType = "trac"; } ]; ...
  };

... }
```
Distributed deployment

nixops create network.nix ec2.nix
nixops deploy

- Instantiate VMs in a cloud infrastructure
- Build system configurations by the Nix package manager
- Transfer complete system and all dependencies to target machines in the network
  - Efficient: only missing store paths must be transferred
  - Safe: Existing configuration is not affected, because no files are overwritten or removed
- Activate new system configuration
  - In case of a failure, roll back all configurations
  - Relatively cheap operation, because old configuration is stored next to new configuration
Virtualization

nixos-build-vms network.nix; ./result/bin/nixos-run-vms

- Builds a network of QEMU-KVM virtual machines closely resembling the network of NixOS configurations
- We don’t create disk images
- The VM mounts the Nix store of the host system using SMB/CIFS
Welcome to Trac 0.11.5

Trac is a minimalistic approach to web-based management of software projects. Its goal is to simplify effective tracking and handling of software issues, enhancements and overall progress.

All aspects of Trac have been designed with the single goal to help developers write great software while staying out of the way and imparting as little as possible on a team's established process and culture.

As all Wiki pages, this page is editable. This means that you can modify the contents of this page simply by using your web browser. Simply click on the "Edit this page" link at the bottom of the page. WikiFormatting will give you a detailed description of available Wiki formatting commands.

Trac's wiki engine is built on dbm's Persistent, a new Trac environment, containing a default set of wiki pages and some sample data. This newly created environment also contains documentation to help you get started with your project.

You can use the wiki to configure Trac to better suit your project, especially in regard to components, versions and milestones.

TracGuide is a good place to start.

Enjoy!
The Trac Team

Starting Points
- TracGuide — Built-in Documentation
- Info/The Trac project — The Open Source Project
- WikiFAQ — Frequently Asked Questions
- WikiSupport — Wiki Support

Sander van der Burg

The Nix project
trac.nix

testScript = ''
   $postgresql→waitForJob("postgresql");
   $postgresql→mustSucceed("createdb trac");

   $webserver→mustSucceed("mkdir -p /repos/trac");
   $webserver→mustSucceed("svnadmin create /repos/trac");

   $webserver→waitForFile("/var/trac");
   $webserver→mustSucceed("mkdir -p /var/trac/projects/test");
   $webserver→mustSucceed("trac-admin /var/trac/projects/test initenv ".
      "Test postgres://root@postgresql/trac svn /repos/trac");

   $client→waitForX;
   $client→execute("konqueror http://webserver/projects/test &");
   $client→waitForWindow(qr/Test.*Konqueror/);

   $client→screenshot("screen");
   '';
Testing

nix-build tests.nix -A trac
Experience

- Distributed deployment of a Hydra build environment
- Continuous integration and testing of NixOS
  - NixOS installer
  - OpenSSH
  - Trac
  - NFS server
- Continuous integration and testing of various GNU projects
  - Install NixOS system with bleeding edge glibc
- Other free software projects
Various events may occur in a network of machines:

- Crashing machines
- Adding a new machine
- Change of a capability (e.g. increase of RAM)
- Dynamic Disnix generates infrastructure and distribution models and redeploy a system
License analysis

- We can also trace all files and processes involved in a build process.
- And we can determine the licenses of the original source files to say something about the result.

```
/usr/bin/patchelf
patchelf.cc g++ patchelf.o g++ patchelf install /usr/bin/patchelf
```
# Hydra: Nix based continuous integration and testing

Sander van der Burg

The Nix project

## Hydra queue

<table>
<thead>
<tr>
<th>#</th>
<th>P</th>
<th>Job</th>
<th>Release Name</th>
<th>System</th>
<th>Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started</td>
<td>2490518</td>
<td>gnu:mpfr-trunk:build_with_gxx</td>
<td>mpfr3.2.1-dev-3.2.0-dev</td>
<td>x86_64</td>
<td>16:32</td>
</tr>
<tr>
<td>Started</td>
<td>2490519</td>
<td>gnu:mpfr-trunk:build</td>
<td>mpfr3.2.0-dev</td>
<td>x86_64</td>
<td>16:32</td>
</tr>
<tr>
<td>Started</td>
<td>2490524</td>
<td>gnu:emacs-trunk:build</td>
<td>emacs-24.1.50</td>
<td>x86_64</td>
<td>16:33</td>
</tr>
<tr>
<td>Queued</td>
<td>2489249</td>
<td>nixpkgs:trunk:haskellPackages_ghc741_clientsession</td>
<td>haskell-clientsession-haskell-g7.4.1-0.7.5</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
<tr>
<td>Queued</td>
<td>2489250</td>
<td>nixpkgs:trunk:haskellPackages_ghc704_no_profiling_certificate</td>
<td>haskell-certificate-g7.4.4-1.2.1</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
<tr>
<td>Queued</td>
<td>2489251</td>
<td>nixpkgs:trunk:haskellPackages_ghc741_repaAlgorithms</td>
<td>haskell-repa-algorithms-haskell-g7.4.1-3.1.3.1</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
<tr>
<td>Queued</td>
<td>2489259</td>
<td>nixpkgs:trunk:haskellPackages_ghc704_profiling.RSA</td>
<td>haskell-RSA-g7.4.4-1.2.1.8-profiling</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
<tr>
<td>Queued</td>
<td>2489262</td>
<td>nixpkgs:trunk:haskellPackages_ghcHEAD_pwstoreFast</td>
<td>haskell-pwstore-fast-g7.5.20120419.2.2</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
<tr>
<td>Queued</td>
<td>2489267</td>
<td>nixpkgs:trunk:haskellPackages_ghc704_profiling.cryptohash</td>
<td>haskell-cryptohash-g7.4-0.7.5-profiling</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
<tr>
<td>Queued</td>
<td>2489271</td>
<td>nixpkgs:trunk:haskellPackages_ghc704_no_profiling.yesodStatic</td>
<td>haskell-yesod-static-g7.4.4.1.0.0.1</td>
<td>x86_64</td>
<td>15:27</td>
</tr>
</tbody>
</table>
Conclusion

- We have shown Nix, a purely functional package manager, and NixOS a Linux distribution built around Nix.
- We have briefly shown a number of Nix applications.
- They provide fully automatic, reliable, reproducible, and efficient deployment for the latest generation of systems.
NixOS website: http://nixos.org

- *Nix*. A purely functional package manager
- *Nixpkgs*. Nix packages collection
- *NixOS*. Nix based GNU/Linux distribution
- *Hydra*. Nix based continuous build and integration server
- *Disnix*. Nix based distributed service deployment
- *NixOps*. NixOS-based multi-cloud deployment tool

Software available under free and open-source licenses (LGPL/X11)
Nix package manager can be used on any Linux system, FreeBSD, OpenSolaris, Darwin and Cygwin.

Virtualization features can be used on any Linux system running the Nix package manager and KVM.