

$$\text{াদু} + \text{দাবি} = \text{হাতী}$$

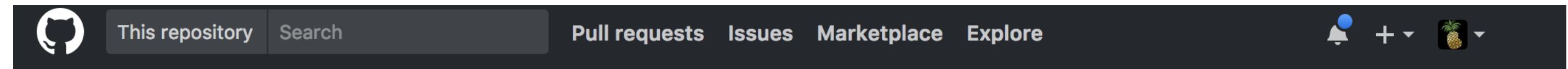
$$\text{💔} + \text{😈} = \text{💔/❤️}$$

What this talk is about

- Motivation
- History
- Purity
- Sandbox
- Ongoing challenges and future direction
- Not nix-darwin

Some motivation





Homebrew / homebrew-core

Watch ▾

121

Star

2,355

Fork

3,404

Code

Issues 25

Pull requests 82

Projects 0

Insights

First issues with macOS 10.13 High Sierra #14418

New issue

Closed

fxcoudert opened this issue on Jun 9 · 122 comments



fxcoudert commented on Jun 9 • edited by mistydemeo

Member



Assignees

No one assigned

Labels

10.13

Projects

None yet

Milestone

No milestone

This is with Developer Beta of macOS 10.13, using Xcode 9 beta, Apple LLVM version 9.0.0 (clang-900.0.22.8) .

- brew test pkg-config fails because it cannot find openssl.pc (build logs) (#15278.)
- brew test glib fails because it cannot find -lglib-2.0 (no -L is provided in the test) (#15281.)
- libunistring fails to build because make check has 28 failing tests (Illegal instruction errors) (#15174.)
- brew test python fails (build logs)

6

If the Xcode model did become the default, it's possible that would render system-protective keg_only choices like openssl on macOS 10.13 almost unimportant, although I don't expect Homebrew to make any drastic choices on that given it would cause discrepancies between the newest and older macOS versions.

mistydemeo commented on Jun 13

Contributor +1

This however isn't true when using only the CLT:

However, it *is* true when using the /usr/bin version of clang when the CLT is the active xcode_select path:

```
$ /usr/bin/clang -v
@(#)PROGRAM:ld PROJECT:ld64-301.1
configured to support archs: armv6 armv7 armv7s arm64 i386 x86_64 x86_64h armv6m armv7k arm
Library search paths:
/Library/Developer/CommandLineTools/SDKs/MacOSX.sdk/usr/lib
Framework search paths:
/Library/Developer/CommandLineTools/SDKs/MacOSX.sdk/System/Library/Frameworks/
```

DomT4 commented on Jun 13

Contributor +1

Interesting, I missed that. Nice find! I wonder if both of those exhibiting the same behaviour semi-confirms this might be an intentional choice/direction on Apple's part.

mistydemeo commented on Jun 13 • edited

Contributor +1

The behaviour between /usr/bin/clang and /Library/Developer/CommandLineTools/usr/bin/clang feels backward, which makes me wonder if it's a packaging mistake. Assuming that's the case, the intention I'm reading is:

- The Xcode version of the tool, with no headers in /usr/include, is configured only to look inside the Xcode SDK by default. This makes sense for a tool intended primarily to be used by Xcode itself, along with other software building in an Xcode-centric context.
- The /Library version of the tool is configured only to look inside its own "SDK" by analogy.
- The /usr/bin/clang version works for Unix-style CLI builds as it always did.

fxcoudert commented on Jun 13

Member +1

Other failures and links to logs:

wxmac, bison, thefuck (test failure), swiftlint, qt, swig (test failure, cannot find ruby.h).

fxcoudert commented on Jun 13

Member +1

ghc fails to build (clang preprocessor bug already reported by @mistydemeo), apache-spark test fails, midnight-commander fails to build

4

MikeMcQuaid commented on Jun 13

Owner +1

It's worth noting based on previous usage that many of the weird behaviour we're seeing now will be changed in later betas of macOS and Xcode. I don't think it's worth either worrying or fixing many of these for a while.

theeternalsw0rd commented on Jun 13

+1

I have packaged a telnet client and built a tap for it available at <https://github.com/theeternalsw0rd/homebrew-telnet> since the built-in one is mia.

I wouldn't think any package would depend on the built-in client but in case there's some obscure

```
==> ./configure --prefix=/usr/local/Cellar/lftp/4.7.7 --with-openssl=/usr/local/opt/openssl
=> make install
  /usr/local/Cellar/lftp/4.7.7: 21 files, 2.5MB, built in 1 minute 54 seconds
korni22@Erics-MBPr ~ $ lftp
lftp :~> exit
```

works fine, thanks a lot!

1

zwmwangx commented on Jul 8

Contributor +1

optipng #15419.

copumpkin commented on Jul 11 • edited

Contributor +1

The libunistring failures all come from the system's snprintf

@fxcoudert I'm seeing the exact same thing in a non-homebrew setting in 10.13, so I'm guessing something deeper has changed in 10.13.

@chapeladmin any word on the Apple bug you submitted on that illegal instruction?

Edit: just saw this, sorry!

According to Apple, the issue with bison (and I'm assuming libunistring) is %n in formatted strings that are in dynamic memory. Waiting to hear anything further from Apple, but it seems like something they are planning on fixing as they said they are continuing to work on it.

ilovezfs deleted a comment from stachowskim on Jul 11

ilovezfs deleted a comment from DomT4 on Jul 11

ilovezfs deleted a comment from stachowskim on Jul 11

ilovezfs deleted a comment from DomT4 on Jul 11

ilovezfs deleted a comment from JCount on Jul 11

68 items not shown
View more

DomT4 commented on Aug 23

Contributor +1

I'm not sure whether it impacts any formulae, but I reported this to Apple last week:

Summary:
The MobileDevice Framework seems to be absent in Xcode 9, which may well be a deliberate omission on Apple's part, but it is part of the Command Line Tools package (/Library/Developer/CommandLineTools/SDKs/MacOSX.sdk/System/Library/PrivateFrameworks/MobileDevice.framework) and after installing that also available in the usual "/System/Library/PrivateFrameworks/MobileDevice.framework" location.

However, the Xcode Developer Tools seem completely oblivious to the existence of that Framework even when passed the standard "-framework MobileDevice -F/system/Library/PrivateFrameworks" flags, and errors out with "ld: framework not found MobileDevice". If you explicitly use the Command Line Tools package's developer tools this problem does not reproduce & the executable is built & linked correctly.

Steps to Reproduce:

```
1) Create any valid C file (referenced as "test.c" below), such as:
=====
#include <stdio.h>

int main(int argc, char *argv[])
{
    printf("testSUCCESS\n");
}
=====

2) With the active developer directory set to "/Applications/Xcode-beta.app/Contents/Developer" & the Command Line Tools package installed execute "clang -Wall -framework MobileDevice -F/system/Library/PrivateFrameworks test.c"
3) Encounters the "ld: framework not found MobileDevice" failure.
4) With the Command Line Tools package installed execute "/Library/Developer/CommandLineTools/usr/bin/clang -Wall -framework MobileDevice -F/system/Library/PrivateFrameworks test.c"
5) Execute "otool -L a.out" and see the correct linkage to the MobileDevice Framework in that executable.
6) Execute ".a.out" and "testSUCCESS" is printed as expected.
```

```
refused to upgrade https://github.com/Homebrew/homebrew-core/pull/1707
Formulae affected by Homebrew/brew#2482 https://github.com/Homebrew/homebrew-core/issues/13
php: 7.1 (new formula) https://github.com/Homebrew/homebrew-core/pull/16067
hadoop 2.8.1 failed to install on 10.12.6 https://github.com/Homebrew/homebrew-core/issues/
```

Error: You are using macOS 10.13.
We do not provide support for this pre-release version.
You may encounter build failures or other breakages.
Please create pull-requests instead of filing issues.

Error: You are using macOS 10.13.
We do not provide support for this pre-release version.
You may encounter build failures or other breakages.
Please create pull-requests instead of filing issues.

DomT4 commented on Sep 5

Contributor +1

It's useful if people provide brew gist-logs of failed builds. There's a fair bit more information in there than just the failure. Also useful is a reading from xcdebuild -version if you're running a system with Xcode present.

kcoop commented on Sep 5

+1

Here's the gist for doing a brew install node directly:
<https://gist.github.com/1fc2dbabc3b0cf1484fd44cbe016818c>

and for Xcode:

```
xcdebuild -version
Xcode 9.0
Build version 9M214v
```

DomT4 commented on Sep 5 • edited

Contributor +1

@kcoop I presume you're not running a Hackintosh? (Apparently not. Your screenshot of the overview didn't load last time for some reason, apologies) The CPU: octa-core 64-bit dunno is a little odd.

@SConaway A full brew gist-logs openssl is more useful than the condensed output.

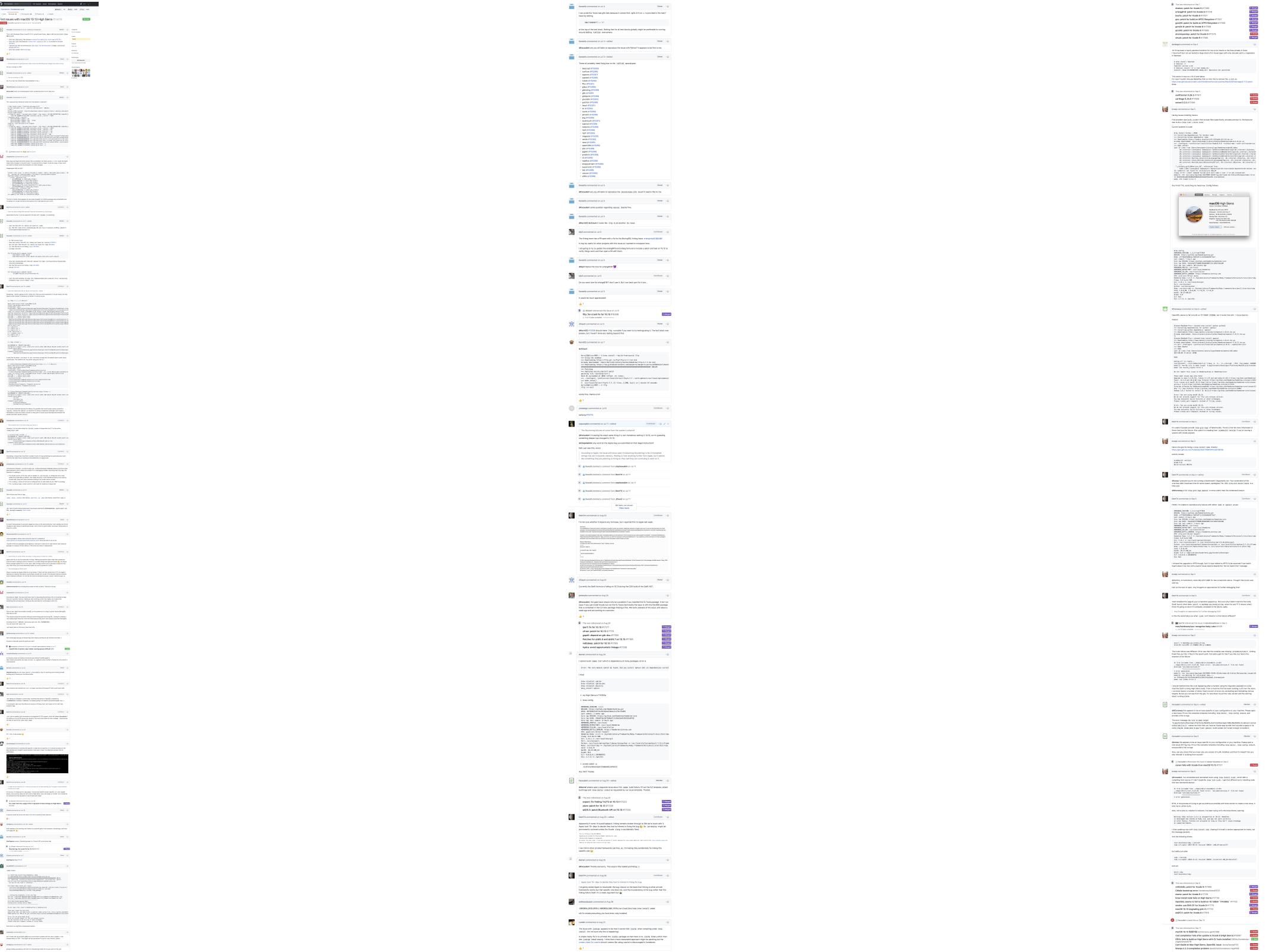
DomT4 commented on Sep 5

Contributor +1

FWIW, I'm unable to reproduce any failures with either node or openssl as per:

```
HOMEBREW_VERSION: 1.3.2-2-ge777010
ORIGIN: https://github.com/Homebrew/brew.git
HEAD: e77701075606cbcf3075d7fcc123556b63977bcf
Last commit: 8 hours ago
Core tap ORIGIN: https://github.com/Homebrew/homebrew-core
Core tap HEAD: 75d2a4a97f5e008120a603807131c185bf18dc00
Core tap last commit: 3 hours ago
HOMEBREW_PREFIX: /usr/local
HOMEBREW_REPOSITORY: /usr/local/Homebrew
HOMEBREW_CELLAR: /usr/local/Cellar
HOMEBREW_BOTTLE_DOMAIN: https://homebrew.bintray.com
CPU: octa-core 64-bit haswell
Homebrew Ruby: 2.3.3 => /System/Library/Frameworks/Ruby.framework/Versions/2.3/usr/bin/ruby
Clang: 9.0 build 990
Git: 2.14.1 => /usr/local/opt/git/bin/git
Perl: /usr/local/bin/perl => /usr/local/Cellar/perl/5.26.0/bin/perl
Python: /usr/local/opt/python/libexec/bin/python => /usr/local/Cellar/python/2.7.13_1/Frameworks/Python.framework/Versions/2.7/usr/bin/python
Ruby: /usr/local/var/rbenv/shims/ruby => /usr/local/var/rbenv/versions/2.4.1/bin/ruby
Java: 1.8.0_141
macOS: 10.13-x86_64
Xcode: 9.0 => /Applications/Xcode-beta.app/Contents/Developer
CLT: 9.0.0.0.1.1503068762
X11: N/A
```

I refused the upgrade to APFS though, but if it was related to APFS I'd be surprised if we hadn't heard about it by now with a wad of issue reports despite the "do not report this" message.



\$WORK

While attempting to compile my C program, running the following command:

442 `gcc pthread.c -o pthread`

Returns:



Agreeing to the Xcode/iOS license requires admin privileges, please re-run as root via sudo.

and my code does not compile.

Why is this happening and how can I fix this problem?

ios xcode gcc

share improve this question

edited Sep 26 '16 at 18:39



the Tin Man

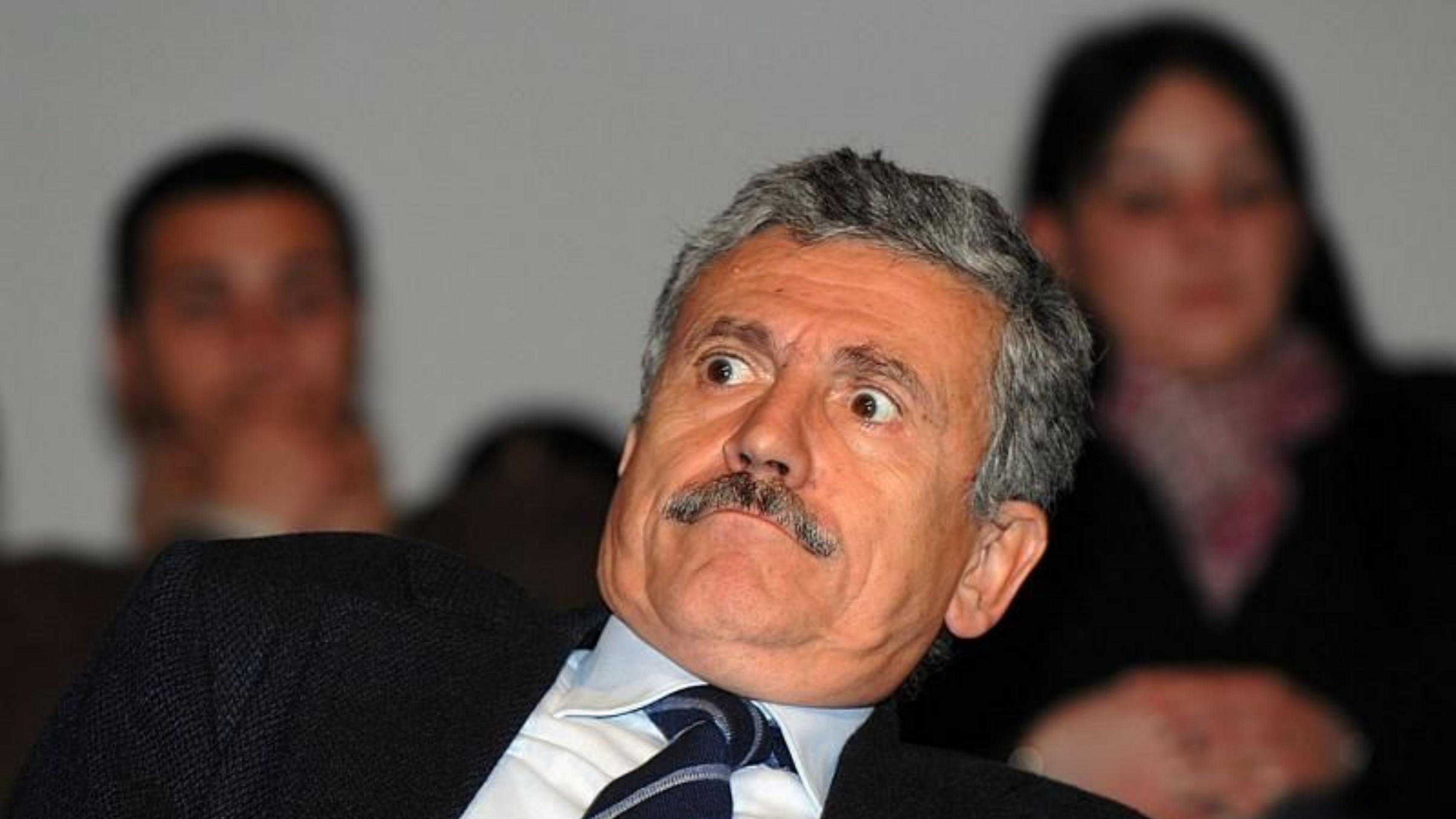
124k • 25 • 156 • 227

asked Oct 4 '14 at 21:25



coachcal

9,500 • 3 • 9 • 12



Credits¹

- @pikajude
- @gridaphobe
- @johnw
- @cstrahan
- @LnL7

¹ Among many others I couldn't fit!

Basic background knowledge

- `stdenv` is pure on Linux
- Minimal bootstrap
- Multiple stages
- Darwin public source at opensource.apple.com²

²When not missing, redacted, forgotten, etc.

History

A long, long time ago, in Q3 2014...



Nixpkgs on Darwin was very impure

Code

Issues 1,994

Pull requests 499

Projects 9

Insights

Let's compile the Mac OS X SecurityTool ourselves #4326

Edit

Merged

shlevy merged 1 commit into NixOS:master from copumpkin:mac-purity on Oct 1, 2014

Conversation 8

Commits 1

Files changed 4

+95 -0



copumpkin commented on Sep 30, 2014

Member



This allows us to compile SecurityTool ourselves. There are several more Apple opensource projects that can be compiled this way that I'll slowly add.

Remaining sources of impurity:

- Reference to absolute path to Xcode. This should be integrated with the xcode derivation (and the iOS wrapper chain that exists under mobile development) but it's not obvious how to do that yet.
- Absolute reference to `xcodebuild`.

Adding this should make it possible for #3629 to work reasonably cleanly.

Reviewers



No reviews—request one

Assignees



No one—assign yourself

Labels



0.kind: enhancement

6.topic: darwin

Projects



None yet



copumpkin referenced this pull request on Sep 30, 2014

Code

Issues 1,994

Pull requests 499

Project Insights

Let's compile the Mac OS X Security Tool ourselves #4326

Merged

shlevy merged 1 commit into NixOS:master from:mac-purity

Conversation 8

Commits 1

Files changed

+95 -0



copumpkin commented on Sep 30, 2014

I had something in mind...
This allows us to compile Security Tool ourselves. There are several more Apple opensource projects that can be compiled this way that I'll slowly add.

Remaining sources of impurity:

- Reference to absolute path to Xcode. This should be integrated with the xcode derivation (and the iOS wrapper chain that exists under mobile development) but it's not obvious how to do that yet.
- Absolute reference to `xcodebuild`.

Adding this should make it possible for #3629 to work reasonably cleanly.

Reviewers

No reviews · request one

Assignees

No one—assign yourself

Labels

0.kind: enhancement

6.topic: darwin

Projects

None yet

copumpkin referenced this pull request on Sep 30, 2014

Add Apple command-line tools #4365

[Edit](#)**Closed**copumpkin wants to merge 1 commit into [NixOS:master](#) from [copumpkin:adcpkgs](#)[Conversation 4](#)[Commits 1](#)[Files changed 5](#)[+107 -9](#)

copumpkin commented on Oct 2, 2014

Member



This should add a sensible "SDK" and precompiled command-line tools from ADC, possibly suitable for bootstrapping nix on darwin someday. You'll need to configure an `adc_user` and `adc_pass` to download it. Even if we don't use the binary tools for bootstrapping, having the SDK in the store will be quite valuable when automating calls to `xcodebuild`, which will be necessary for building all sorts of nice packages from opensource.apple.com.

@shlevy, wanna check it out?



cstrahan and 1 other commented on an outdated diff on Oct 2, 2014



Show 2 comments

Reviewers



No reviews—request one

Assignees



No one—assign yourself

Labels



None yet

Projects



None yet

Milestone



No milestone



cstrahan commented on the diff on Oct 2, 2014

[pkgs/os-specific/darwin/command-line-tools/default.nix](#)[View full changes](#)

Add Apple command-line tools #4365

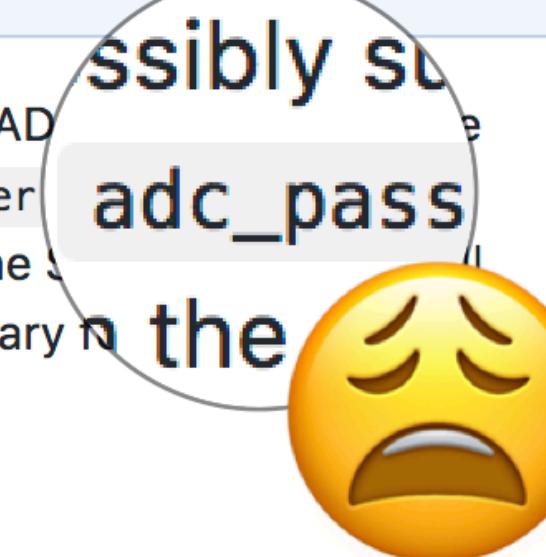
[Edit](#)[Closed](#)copumpkin wants to merge 1 commit into [NixOS:master](#) from [copumpkin:adcpkgs](#)[Conversation 4](#)[Commits 1](#)[Files changed 5](#)[+107 -9](#)

copumpkin commented on Oct 2, 2014

[Member](#) + 

This should add a sensible "SDK" and precompiled command-line tools from AD for bootstrapping nix on darwin someday. You'll need to configure an `adc_user` download it. Even if we don't use the binary tools for bootstrapping, having them be quite valuable when automating calls to `xcodebuild`, which will be necessary to get lots of nice packages from opensource.apple.com.

@shlevy, wanna check it out?



cstrahan and 1 other commented on an outdated diff on Oct 2, 2014

Show 2 comments

cstrahan commented on the diff on Oct 2, 2014

[pkgs/os-specific/darwin/command-line-tools/default.nix](#)

[View full changes](#)

Reviewers



No reviews—request one

Assignees



No one—assign yourself

Labels



None yet

Projects



None yet

Milestone



No milestone

Code

Issues 1,994

Pull requests 499

Projects 9

Insights

Suitable clang stdenv for Darwin #3661

Edit

Closed

pikajude wants to merge 16 commits into NixOS:master from pikajude:darwin-stdenv

Conversation 59

Commits 16

Files changed 69

+642 -118



pikajude commented on Aug 18, 2014

Member



Doesn't involve GCC at any point. This will be necessary once 10.10 comes around.



jwiegley commented on Aug 18, 2014

Member



+1 from me in concept; I haven't built using it yet.



gridaphobe commented on the diff on Aug 21, 2014

pkgs/stdenv/darwin/default.nix

View full changes

```
2 +
3 +import ../../generic rec {
4 +  inherit config;
5 +
6 +  preHook =
7 +
8 +    export NIX_ENFORCE_PURITY=
9 +    export NIX_IGNORE_LD_THROUGH_GCC=1
10 +   export NIX_DONT_SET_RPATH=1
11 +   export NIX_NO_SELF_RPATH=1
12 +   dontFixLibtool=1
13 +   stripAllFlags="" # the Darwin "strip" command doesn't know "-s"
14 +   xargsFlags=""
15 +   export MACOSX_DEPLOYMENT_TARGET=10.6
16 +   export SDKROOT=$(/usr/bin/xcrun --show-sdk-path 2>/dev/null || true)
17 +   export NIX_CFLAGS_COMPILE+=" --sysroot=/var/empty -idirafter $SDKROO"
```

Reviewers

No reviews—request one

Assignees

No one—assign yourself

Labels

2.status: work-in-progress

6.topic: darwin

Projects

None yet

Milestone

No milestone

Notifications

[Unsubscribe](#)

You're receiving notifications because you were mentioned.

17 participants



Code

Issues 1,994

Pull requests 499

Projects 9

Insights

Suitable clang stdenv for Darwin #3661

Closed

pikajude wants to merge 16 commits into NixOS:master from pikajude:darwin-stdenv

Edit

Conversation 59

Commits 16

Files changed 69

+642 -118



pikajude commented on Aug 18, 2014

Member



Doesn't involve GCC at any point. This will be necessary once 10.10 comes around.



jwiegley commented on Aug 18, 2014

Member



+1 from me in concept; I haven't built using it yet.

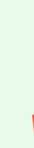


gridaphobe commented on the diff on Aug 21, 2014

pkgs/stdenv/darwin/default.nix

View full changes

```
2 +
3 +import ../../generic rec {
4 +  inherit config;
5 +
6 +  preHook =
7 +
8 +    "export NIX_ENFORCE_PURITY=
9 +    export NIX_IGNORE_LD_THROUGH_GCC=1
10 +   export NIX_DONT_SET_RPATH=1
11 +   export NIX_NO_SELF_RPATH=1
12 +   dontFixLibtool=1
13 +   stripAllFlags="" # the Darwin "strip" command doesn't know "-s"
14 +   xargsFlags=""
15 +   export MACOSX_DEPLOYMENT_TARGET=10.6
16 +   export SDKROOT=$(/usr/bin/xcrun --show-sdk-path 2>/dev/null || true)
17 +   export NIX_CFLAGS_COMPILE+=" --sysroot=/var/empty -idirafter $SDKROO"
```



Reviewers

No reviews—request one

Assignees

No one—assign yourself

Labels

2.status: work-in-progress

6.topic: darwin

Projects

None yet

Milestone

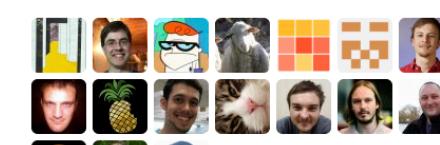
No milestone

Notifications

[Unsubscribe](#)

You're receiving notifications because you were mentioned.

17 participants



Code

Issues 1,994

Pull requests 499

Projects 9

Insights

Suitable clang stdenv for Darwin #3661

Closed

pikajude wants to merge 16 commits into NixOS:master from pikajude:darwin-stdenv

Edit

Conversation 59

Commits 16

Files changed 69

+642 -118



pikajude commented on Aug 18, 2014

Member



Doesn't involve GCC at any point. This will be necessary once 10.10 comes around.



jwiegley commented on Aug 18, 2014

Member



+1 from me in concept; I haven't built using it yet.

gridaphobe commented on the diff on Aug 21, 2014

pkgs/stdenv/darwin/default.nix

View full changes

```
2 +  
3 +import ../../generic rec {  
4 +  inherit config;  
5 +  
6 +  preHook =  
7 +    ''  
8 +      export NIX_ENFORCE_PURITY=  
9 +      export NIX_IGNORE_LD_THROUGH_GCC=1  
10 +     export NIX_DONT_SET_RPATH=1  
11 +     export NIX_NO_SELF_RPATH=1  
12 +     dontFixLibtool=1  
13 +     stripAllFlags="" # the Darwin "strip" command doesn't know "-s"  
14 +     xargsFlags=""  
15 +     export MACOSX_DEPLOYMENT_TARGET=10.6  
16 +     export SDKROOT=$(/usr/bin/xcrun --show-sdk-path 2>/dev/null || true)  
17 +     export NIX_CFLAGS_COMPILE+=" --sysroot=/var/empty -idirafter $SDKROO"
```

Reviewers

No reviews—request one

Assignees

No one—assign yourself

Labels

2.status: work-in-progress

6.topic: darwin

Projects

None yet

Milestone

No milestone

Notifications

Unsubscribe

You're receiving notifications because you were mentioned.

17 participants



 Code

 Issues 25

 Pull requests 2

 Projects 0

 Wiki

 Insights

 Settings

WIP

[Browse files](#)

 broken-stuff + broken-stuff-bootstrapped



copumpkin committed on Oct 5, 2014

1 parent e20bdeb

commit 4469e42c21d9cf4f3fce357e4e6ff4fbbf3f23b

 Showing 6 changed files with 207 additions and 130 deletions.

[Unified](#) [Split](#)

 pkgs/os-specific/darwin/command-line-tools/default.nix

+46 -17 

 pkgs/os-specific/darwin/command-line-tools/sdk.nix

+0 -25 

 pkgs/os-specific/darwin/command-line-tools/tools.nix

+0 -25 

 pkgs/stdenv/darwin/default.nix

+113 -47 

 pkgs/stdenv/darwin/trivialBootstrap.sh

+47 -0 

 pkgs/stdenv/default.nix

+1 -16 

```
... ... @@ -0,0 +1,47 @@
1 +
2 +# Building bootstrap tools
3 +echo Building the trivial bootstrap environment...
4 +$mkdir -p $out/bin
5 +
6 +$ln -s $ln $out/bin/ln
7 +
8 +PATH=$out/bin/
9 +
10 +cd $out/bin
11 +
12 +ln -s $mkdir
13 +ln -s /bin/sh
14 +ln -s /bin/cp
15 +ln -s /bin/mv
16 +ln -s /bin/rm
17 +ln -s /bin/ls
18 +ln -s /bin/cat
19 +ln -s /bin/echo
20 +ln -s /bin/expr
21 +ln -s /bin/test
22 +ln -s /bin/chmod
23 +
24 +ln -s /usr/bin/tr
25 +ln -s /usr/bin/wc
26 +ln -s /usr/bin/sed
27 +ln -s /usr/bin/tar
28 +ln -s /usr/bin/xar
29 +ln -s /usr/bin/awk
30 +ln -s /usr/bin/env
31 +ln -s /usr/bin/comm
32 +ln -s /usr/bin/cpio
33 +ln -s /usr/bin/curl
34 +ln -s /usr/bin/grep
35 +ln -s /usr/bin/gzip
36 +ln -s /usr/bin/tail
```

Fake, but a start

Actual derivation references!!

```
53 + preHook = ''
54 + export NIX_ENFORCE_PURITY=
55 + export NIX_IGNORE_LD_THROUGH_GCC=1
56 + export NIX_DONT_SET_RPATH=1
57 + export NIX_NO_SELF_RPATH=1
58 + dontFixLibtool=1
59 + stripAllFlags="" # the Darwin "strip" command doesn't know "-s"
60 + xargsFlags=" "
61 + export MACOSX_DEPLOYMENT_TARGET=10.6
62 + export SDKROOT=
63 + export SDKROOT_X=${buildTools.sdk} ←
64 + export NIX_CFLAGS_COMPILE+=" --sysroot=/var/empty -idirafter $SDKROOT_X/usr/include -F$SDKROOT_X/System/Library/Frameworks"
65 + export NIX_LDFLAGS_AFTER+=" -L$SDKROOT_X/usr/lib"
66 + '';
44 67
45 - stdenv.fetchurlBoot ←
68 - stage1 = rec {
69 -   stdenv = import ./generic;
70 -   inherit system config fetchable;
71 + inherit (stage0.stdenv) name shell initialPath fetchurlBoot; ←
46 72
47 - overrides = pkgs_:
48 -   inherit gcc;
49 -   inherit (gcc bin);
50 -   inherit (pkgs)
51 -   gzip bzip2 xz bash coreutils diffutils findutils gawk
52 -   gnumake gnused gnutar gnugrep gnupatch perl;
73 + gcc = import ../../build-support/clang-wrapper { ←
74 +   nativeTools = true;
75 +   nativePrefix = "${buildTools.tools}/Library/Developer/CommandLineTools/usr";
76 +   nativeLibc = true;
77 +   stdenv = stage0.stdenv;
78 +   libcxx = "/";
79 +   shell = "/bin/sh";
80 +   clang = {
81 +     name = "clang-9.9.9";
82 +     gcc = "/no-such-path";
83 +     outputPath = "${buildTools.tools}/Library/Developer/CommandLineTools/usr";
84 +   };
85 + };
```

WIP

[Browse files](#)

↳ broken-stuff + broken-stuff-bootstrapped



copumpkin committed on Oct 12, 2014

1 parent 1531c61

commit 652ed3f889820fab9ffa7cf47301af6a6acdb7a7

Showing 7 changed files with 210 additions and 65 deletions.

Unified Split

- pkgs/os-specific/darwin/cctools-port/default.nix

+0 -64

→ pkgs/os-specific/darwin/{cctools-port → cctools}/ld-ignore-rpath-link.patch

0

→ pkgs/os-specific/darwin/{cctools-port → cctools}/ld-rpath-nonfinal.patch

0

+ pkgs/os-specific/darwin/cctools/port.nix

+70 -0

+ pkgs/stdenv/darwin/README.md

0

+ pkgs/stdenv/darwin/make-bootstrap-tools.nix

+137 -0

● pkgs/top-level/all-packages.nix

+3 -1

```
... ... @@ -0,0 +1,137 @@
1 +{system ? builtins.currentSystem}:
2 +
3 +with import ../../top-level/all-packages.nix {inherit system;};
4 +
5 +rec {
6 +  # We want coreutils without ACL support.
7 +  coreutils_ = coreutils.override (orig: {
8 +    aclSupport = false;
9 +    stdenv = overrideInStdenv stdenv [ libiconv ];
10 +  });
11 +
12 +  diffutils_ = diffutils.override (orig: {
13 +    stdenv = overrideInStdenv stdenv [ libiconv ];
14 +  });
15 +
16 +  gnutar_ = gnutar.override (orig: {
17 +    stdenv = overrideInStdenv stdenv [ libiconv ];
18 +  });
19 +
20 +  bash_ = bash.override (orig: {
21 +    stdenv = overrideInStdenv stdenv [ libiconv ];
22 +  });
23 +
24 +  curl = import ../../tools/networking/curl {
25 +    inherit fetchurl;
26 +    zlibSupport = false;
27 +    sslSupport = false;
28 +  };
29 +
30 +  busyboxStaticSh = busybox.override {
31 +    extraConfig = ''
32 +      CLEAR
33 +      CONFIG_STATIC y
34 +
35 +      CONFIG_ASH y
36 +      CONFIG_BASH_COMPAT y
37 +      CONFIG_ASH_ALIAS y
```

🤔 I don't work on darwin

Branch: **broken-stuff** ▾

Commits on Oct 15, 2014



libc++ build purity

pikajude committed on Oct 15, 2014



124dce1



when -nostdlib is present, stop linking with c++abi

pikajude committed on Oct 15, 2014



5711f41



cc rename

pikajude committed on Oct 15, 2014



7b9de44



Commits on Oct 14, 2014



fix libc++{,abi} builds

pikajude committed on Oct 14, 2014



f570a08



Tell llvm explicitly not to target i386 on darwin

copumpkin committed on Oct 14, 2014



61157b5



Don't need fetchadc for command-line tools

copumpkin committed on Oct 14, 2014



e23e739



This should fix our llvm builds, I hope

copumpkin committed on Oct 14, 2014



758f688



Commits on Oct 13, 2014



This might fix the libc++abi and libc++ weirdness, and with any luck ...

copumpkin committed on Oct 13, 2014



6b1e179



Commits on Oct 12, 2014



Update cctools-port version

copumpkin committed on Oct 12, 2014



cf398cd



Replace gcc references with cc in all-packages

copumpkin committed on Oct 12, 2014



f76d340



Collaboration!

Commits on Oct 28, 2014



libclosure's Block.h in libSystem. Starting work on a libunwind
copumpkin committed on Oct 28, 2014



d84e299



Don't fix libtool in our final stage
copumpkin committed on Oct 28, 2014



331ca6d



Add a simple TargetConditionals.h
copumpkin committed on Oct 28, 2014



b0736d0



Add architecture and disable Carbon stuff in python
copumpkin committed on Oct 28, 2014



9789d15



Stuff seems to be working
copumpkin committed on Oct 28, 2014



8a1511c



Sorta kinda starting to come together
copumpkin committed on Oct 28, 2014



268815b



cctools cleanup + headers
copumpkin committed on Oct 28, 2014



3381ead



Commits on Oct 27, 2014



Update cctools
copumpkin committed on Oct 27, 2014



5183ad0



Commits on Oct 23, 2014



Lots of Apple packages, mostly not complete builds but enough to
make... ...
copumpkin committed on Oct 23, 2014



fcdc0bb



Commits on Oct 17, 2014



Add bootstrap_cmds
copumpkin committed on Oct 17, 2014



5f32976



Commits on Oct 15, 2014



Update darwin's bootstrap-tools (WIP)
copumpkin committed on Oct 15, 2014



2a78260



Add a primitives package for darwin
copumpkin committed on Oct 15, 2014



1a5e27f



Add csu
copumpkin committed on Oct 15, 2014



932c3ac



Darwin headers

226 pkgs/stdenv/darwin/default.nix

View ▾

```
diff --git a/pkgs/stdenv/darwin/default.nix b/pkgs/stdenv/darwin/default.nix
--- a/pkgs/stdenv/darwin/default.nix
+++ b/pkgs/stdenv/darwin/default.nix
@@ -7,132 +7,36 @@
 7   7   rec {
 8   8     allPa
 9   9       l-packages.nix;
+10  + com
+11  + e
+12  + e
+13  + ex
+14  + exp
+15  + stripNNT_SET_RPATH=1 ip" command doesn't know "-s"
+16  + xargsFlag
+17  + export MACOSX_DEPLOYMENT_TARGET=10.7
+18  + export SDKROOT=
+19  + export CMAKE_OSX_ARCHITECTURES=x86_64
+20  + export NIX_CFLAGS_COMPILE+=" --sysroot=/var/empty -Wno-multichar -Wno-deprecated-declarations"
+21  + '';
+22  +
+23  10  bootstrapTools = derivation {
+24  11  - inherit system;
+25  12  name = "bootstrap-tools";
+26  13  - name = "trivial-bootstrap-tools";
+27  14  builder = "/bin/sh";
+28  15  - args = [ ./trivialBootstrap.sh ];
+29  16  -
+30  17  - mkdir = "/bin/mkdir";
+31  18  - ln = "/bin/ln";
+32  19  - };
+33  20  args = [ ./unpack-bootstrap-tools.sh ];
+34  21  #
+35  22  # The simplest stdenv possible to run fetchadc and get the Apple command-line tools
+36  23  stage0 = rec {
+37  24  - fetchurl = import ../../build-support/fetchurl {
+38  25  -   inherit stdenv;
+39  26  -   curl = bootstrapTools;
+40  27  - };
+41  28  tarball = "/Users/copumpkin/bootstrap-tools.cpio.bz2";
+42  29  stdenv = import ../generic {
+43  30  -   inherit system config;
+44  31  -   name = "stdenv-darwin-boot-0";
+45  32  -   shell = "/bin/bash";
+46  33  -   initialPath = [ bootstrapTools ];
+47  34  -   fetchurlBoot = fetchurl;
+48  35  -   cc = "/no-such-path";
+49  36  - };
+50  37  - };
+51  38  - };
+52  39  - };
+53  40  - };
+54  41  - };
+55  42  - };
+56  43  - };
+57  44  - };
+58  45  - };
+59  46  - };
+60  47  - };
+61  48  - };
+62  49  - };
+63  50  - };
+64  51  - };
+65  52  - };
+66  53  - };
+67  54  - };
+68  55  - };
+69  56  - };
+70  57  - };
+71  58  - };
+72  59  - };
+73  60  - };
+74  61  - };
+75  62  - };
+76  63  - };
+77  64  - };
+78  65  - };
+79  66  - };
+80  67  - };
+81  68  - };
+82  69  - };
+83  70  - };
+84  71  - };
+85  72  - };
+86  73  - };
+87  74  - };
+88  75  - };
+89  76  - };
+90  77  - };
+91  78  - };
+92  79  - };
+93  80  - };
+94  81  - };
+95  82  - };
+96  83  - };
+97  84  - };
+98  85  - };
+99  86  - };
+100 87  - };
+101 88  - };
+102 89  - };
+103 90  - };
+104 91  - };
+105 92  - };
+106 93  - };
+107 94  - };
+108 95  - };
+109 96  - };
+110 97  - };
+111 98  - };
+112 99  - };
+113 100  - };
+114 101  - };
+115 102  - };
+116 103  - };
+117 104  - };
+118 105  - };
+119 106  - };
+120 107  - };
+121 108  - };
+122 109  - };
+123 110  - };
+124 111  - };
+125 112  - };
+126 113  - };
+127 114  - };
+128 115  - };
+129 116  - };
+130 117  - };
+131 118  - };
+132 119  - };
+133 120  - };
+134 121  - };
+135 122  - };
+136 123  - };
+137 124  - };
+138 125  - };
+139 126  - };
+140 127  - };
+141 128  - };
+142 129  - };
+143 130  - };
+144 131  - };
+145 132  - };
+146 133  - };
+147 134  - };
+148 135  - };
+149 136  - };
+150 137  - };
+151 138  - };
+152 139  - };
+153 140  - };
+154 141  - };
+155 142  - };
+156 143  - };
+157 144  - };
+158 145  - };
+159 146  - };
+160 147  - };
+161 148  - };
+162 149  - };
+163 150  - };
+164 151  - };
+165 152  - };
+166 153  - };
+167 154  - };
+168 155  - };
+169 156  - };
+170 157  - };
+171 158  - };
+172 159  - };
+173 160  - };
+174 161  - };
+175 162  - };
+176 163  - };
+177 164  - };
+178 165  - };
+179 166  - };
+180 167  - };
+181 168  - };
+182 169  - };
+183 170  - };
+184 171  - };
+185 172  - };
+186 173  - };
+187 174  - };
+188 175  - };
+189 176  - };
+190 177  - };
+191 178  - };
+192 179  - };
+193 180  - };
+194 181  - };
+195 182  - };
+196 183  - };
+197 184  - };
+198 185  - };
+199 186  - };
+200 187  - };
+201 188  - };
+202 189  - };
+203 190  - };
+204 191  - };
+205 192  - };
+206 193  - };
+207 194  - };
+208 195  - };
+209 196  - };
+210 197  - };
+211 198  - };
+212 199  - };
+213 200  - };
+214 201  - };
+215 202  - };
+216 203  - };
+217 204  - };
+218 205  - };
+219 206  - };
+220 207  - };
+221 208  - };
+222 209  - };
+223 210  - };
+224 211  - };
+225 212  - };
+226 213  - };
+227 214  - };
+228 215  - };
+229 216  - };
+230 217  - };
+231 218  - };
+232 219  - };
+233 220  - };
+234 221  - };
+235 222  - };
+236 223  - };
+237 224  - };
+238 225  - };
+239 226  - };
+240 227  - };
+241 228  - };
+242 229  - };
+243 230  - };
+244 231  - };
+245 232  - };
+246 233  - };
+247 234  - };
+248 235  - };
+249 236  - };
+250 237  - };
+251 238  - };
+252 239  - };
+253 240  - };
+254 241  - };
+255 242  - };
+256 243  - };
+257 244  - };
+258 245  - };
+259 246  - };
+260 247  - };
+261 248  - };
+262 249  - };
+263 250  - };
+264 251  - };
+265 252  - };
+266 253  - };
+267 254  - };
+268 255  - };
+269 256  - };
+270 257  - };
+271 258  - };
+272 259  - };
+273 260  - };
+274 261  - };
+275 262  - };
+276 263  - };
+277 264  - };
+278 265  - };
+279 266  - };
+280 267  - };
+281 268  - };
+282 269  - };
+283 270  - };
+284 271  - };
+285 272  - };
+286 273  - };
+287 274  - };
+288 275  - };
+289 276  - };
+290 277  - };
+291 278  - };
+292 279  - };
+293 280  - };
+294 281  - };
+295 282  - };
+296 283  - };
+297 284  - };
+298 285  - };
+299 286  - };
+300 287  - };
+301 288  - };
+302 289  - };
+303 290  - };
+304 291  - };
+305 292  - };
+306 293  - };
+307 294  - };
+308 295  - };
+309 296  - };
+310 297  - };
+311 298  - };
+312 299  - };
+313 300  - };
+314 301  - };
+315 302  - };
+316 303  - };
+317 304  - };
+318 305  - };
+319 306  - };
+320 307  - };
+321 308  - };
+322 309  - };
+323 310  - };
+324 311  - };
+325 312  - };
+326 313  - };
+327 314  - };
+328 315  - };
+329 316  - };
+330 317  - };
+331 318  - };
+332 319  - };
+333 320  - };
+334 321  - };
+335 322  - };
+336 323  - };
+337 324  - };
+338 325  - };
+339 326  - };
+340 327  - };
+341 328  - };
+342 329  - };
+343 330  - };
+344 331  - };
+345 332  - };
+346 333  - };
+347 334  - };
+348 335  - };
+349 336  - };
+350 337  - };
+351 338  - };
+352 339  - };
+353 340  - };
+354 341  - };
+355 342  - };
+356 343  - };
+357 344  - };
+358 345  - };
+359 346  - };
+360 347  - };
+361 348  - };
+362 349  - };
+363 350  - };
+364 351  - };
+365 352  - };
+366 353  - };
+367 354  - };
+368 355  - };
+369 356  - };
+370 357  - };
+371 358  - };
+372 359  - };
+373 360  - };
+374 361  - };
+375 362  - };
+376 363  - };
+377 364  - };
+378 365  - };
+379 366  - };
+380 367  - };
+381 368  - };
+382 369  - };
+383 370  - };
+384 371  - };
+385 372  - };
+386 373  - };
+387 374  - };
+388 375  - };
+389 376  - };
+390 377  - };
+391 378  - };
+392 379  - };
+393 380  - };
+394 381  - };
+395 382  - };
+396 383  - };
+397 384  - };
+398 385  - };
+399 386  - };
+400 387  - };
+401 388  - };
+402 389  - };
+403 390  - };
+404 391  - };
+405 392  - };
+406 393  - };
+407 394  - };
+408 395  - };
+409 396  - };
+410 397  - };
+411 398  - };
+412 399  - };
+413 400  - };
+414 401  - };
+415 402  - };
+416 403  - };
+417 404  - };
+418 405  - };
+419 406  - };
+420 407  - };
+421 408  - };
+422 409  - };
+423 410  - };
+424 411  - };
+425 412  - };
+426 413  - };
+427 414  - };
+428 415  - };
+429 416  - };
+430 417  - };
+431 418  - };
+432 419  - };
+433 420  - };
+434 421  - };
+435 422  - };
+436 423  - };
+437 424  - };
+438 425  - };
+439 426  - };
+440 427  - };
+441 428  - };
+442 429  - };
+443 430  - };
+444 431  - };
+445 432  - };
+446 433  - };
+447 434  - };
+448 435  - };
+449 436  - };
+450 437  - };
+451 438  - };
+452 439  - };
+453 440  - };
+454 441  - };
+455 442  - };
+456 443  - };
+457 444  - };
+458 445  - };
+459 446  - };
+460 447  - };
+461 448  - };
+462 449  - };
+463 450  - };
+464 451  - };
+465 452  - };
+466 453  - };
+467 454  - };
+468 455  - };
+469 456  - };
+470 457  - };
+471 458  - };
+472 459  - };
+473 460  - };
+474 461  - };
+475 462  - };
+476 463  - };
+477 464  - };
+478 465  - };
+479 466  - };
+480 467  - };
+481 468  - };
+482 469  - };
+483 470  - };
+484 471  - };
+485 472  - };
+486 473  - };
+487 474  - };
+488 475  - };
+489 476  - };
+490 477  - };
+491 478  - };
+492 479  - };
+493 480  - };
+494 481  - };
+495 482  - };
+496 483  - };
+497 484  - };
+498 485  - };
+499 486  - };
+500 487  - };
+501 488  - };
+502 489  - };
+503 490  - };
+504 491  - };
+505 492  - };
+506 493  - };
+507 494  - };
+508 495  - };
+509 496  - };
+510 497  - };
+511 498  - };
+512 499  - };
+513 500  - };
+514 501  - };
+515 502  - };
+516 503  - };
+517 504  - };
+518 505  - };
+519 506  - };
+520 507  - };
+521 508  - };
+522 509  - };
+523 510  - };
+524 511  - };
+525 512  - };
+526 513  - };
+527 514  - };
+528 515  - };
+529 516  - };
+530 517  - };
+531 518  - };
+532 519  - };
+533 520  - };
+534 521  - };
+535 522  - };
+536 523  - };
+537 524  - };
+538 525  - };
+539 526  - };
+540 527  - };
+541 528  - };
+542 529  - };
+543 530  - };
+544 531  - };
+545 532  - };
+546 533  - };
+547 534  - };
+548 535  - };
+549 536  - };
+550 537  - };
+551 538  - };
+552 539  - };
+553 540  - };
+554 541  - };
+555 542  - };
+556 543  - };
+557 544  - };
+558 545  - };
+559 546  - };
+560 547  - };
+561 548  - };
+562 549  - };
+563 550  - };
+564 551  - };
+565 552  - };
+566 553  - };
+567 554  - };
+568 555  - };
+569 556  - };
+570 557  - };
+571 558  - };
+572 559  - };
+573 560  - };
+574 561  - };
+575 562  - };
+576 563  - };
+577 564  - };
+578 565  - };
+579 566  - };
+580 567  - };
+581 568  - };
+582 569  - };
+583 570  - };
+584 571  - };
+585 572  - };
+586 573  - };
+587 574  - };
+588 575  - };
+589 576  - };
+590 577  - };
+591 578  - };
+592 579  - };
+593 580  - };
+594 581  - };
+595 582  - };
+596 583  - };
+597 584  - };
+598 585  - };
+599 586  - };
+600 587  - };
+601 588  - };
+602 589  - };
+603 590  - };
+604 591  - };
+605 592  - };
+606 593  - };
+607 594  - };
+608 595  - };
+609 596  - };
+610 597  - };
+611 598  - };
+612 599  - };
+613 600  - };
+614 601  - };
+615 602  - };
+616 603  - };
+617 604  - };
+618 605  - };
+619 606  - };
+620 607  - };
+621 608  - };
+622 609  - };
+623 610  - };
+624 611  - };
+625 612  - };
+626 613  - };
+627 614  - };
+628 615  - };
+629 616  - };
+630 617  - };
+631 618  - };
+632 619  - };
+633 620  - };
+634 621  - };
+635 622  - };
+636 623  - };
+637 624  - };
+638 625  - };
+639 626  - };
+640 627  - };
+641 628  - };
+642 629  - };
+643 630  - };
+644 631  - };
+645 632  - };
+646 633  - };
+647 634  - };
+648 635  - };
+649 636  - };
+650 637  - };
+651 638  - };
+652 639  - };
+653 640  - };
+654 641  - };
+655 642  - };
+656 643  - };
+657 644  - };
+658 645  - };
+659 646  - };
+660 647  - };
+661 648  - };
+662 649  - };
+663 650  - };
+664 651  - };
+665 652  - };
+666 653  - };
+667 654  - };
+668 655  - };
+669 656  - };
+670 657  - };
+671 658  - };
+672 659  - };
+673 660  - };
+674 661  - };
+675 662  - };
+676 663  - };
+677 664  - };
+678 665  - };
+679 666  - };
+680 667  - };
+681 668  - };
+682 669  - };
+683 670  - };
+684 671  - };
+685 672  - };
+686 673  - };
+687 674  - };
+688 675  - };
+689 676  - };
+690 677  - };
+691 678  - };
+692 679  - };
+693 680  - };
+694 681  - };
+695 682  -
```

Commits on Nov 7, 2014
 More stuff copumpkin committed on Nov 7, 2014
 Flesh out the bootstrap tools copumpkin committed on Nov 7, 2014
Commits on Nov 6, 2014
 Better copumpkin committed on Nov 6, 2014
 No more patch-dyld copumpkin committed on Nov 6, 2014
Commits on Nov 5, 2014
 Darwin bootstrap tools copumpkin committed on Nov 5, 2014
Commits on Nov 4, 2014
 Err, how could I forget cpio copumpkin committed on Nov 4, 2014
 Update ancient headers and add more known purifying patches copumpkin committed on Nov 4, 2014
Commits on Nov 3, 2014
 Whoops, forgot these copumpkin committed on Nov 3, 2014
 Assorted purification for bootstrap purposes copumpkin committed on Nov 3, 2014
 No libc++abi tests for now, I guess copumpkin committed on Nov 3, 2014
Commits on Nov 2, 2014
 Our libunwind build is a little better, but still doesn't work copumpkin committed on Nov 2, 2014
 libc++abi now only dependd on libunwind when not on darwin copumpkin committed on Nov 2, 2014
 Add CommonCrypto headers copumpkin committed on Nov 2, 2014
 More clang wrapper stuff, and isable otool in cctools for now copumpkin committed on Nov 2, 2014

An actual bootstrap!

Branch: **pure-darwin-st...** ▾

Commits on Nov 9, 2014



Yeah, that version was broken too

copumpkin committed on Nov 9, 2014



d97d97b



Update bootstrap tools sha256

copumpkin committed on Nov 9, 2014



75f6337



Point at my new bootstrap tools

copumpkin committed on Nov 9, 2014



a3272e3



We need this header too (breaks adv_cmds and ps)

copumpkin committed on Nov 9, 2014



aa49314



No need for this

copumpkin committed on Nov 9, 2014



2143036



Pure bootstrap ...

copumpkin committed on Oct 15, 2014

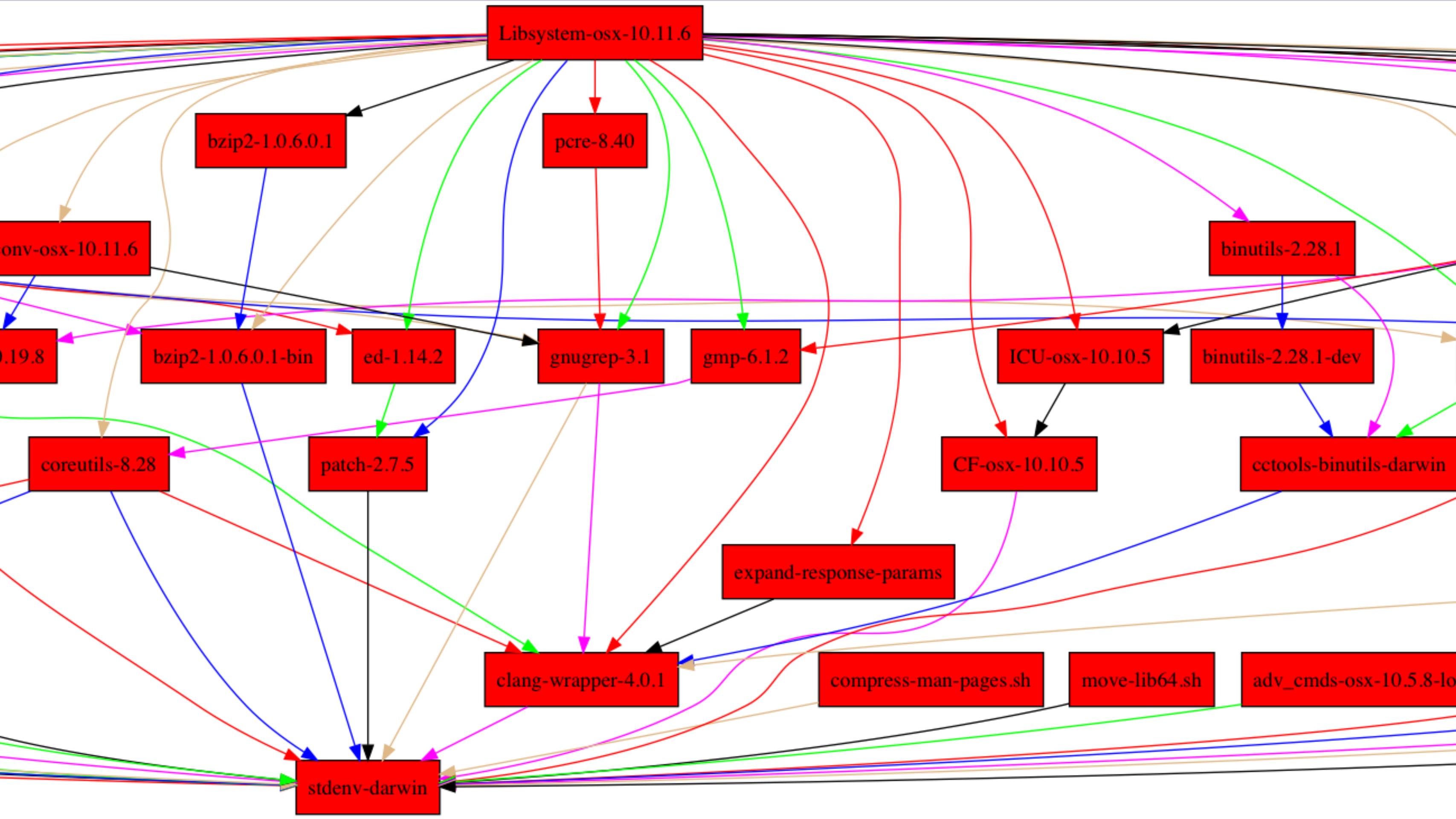


a80934b

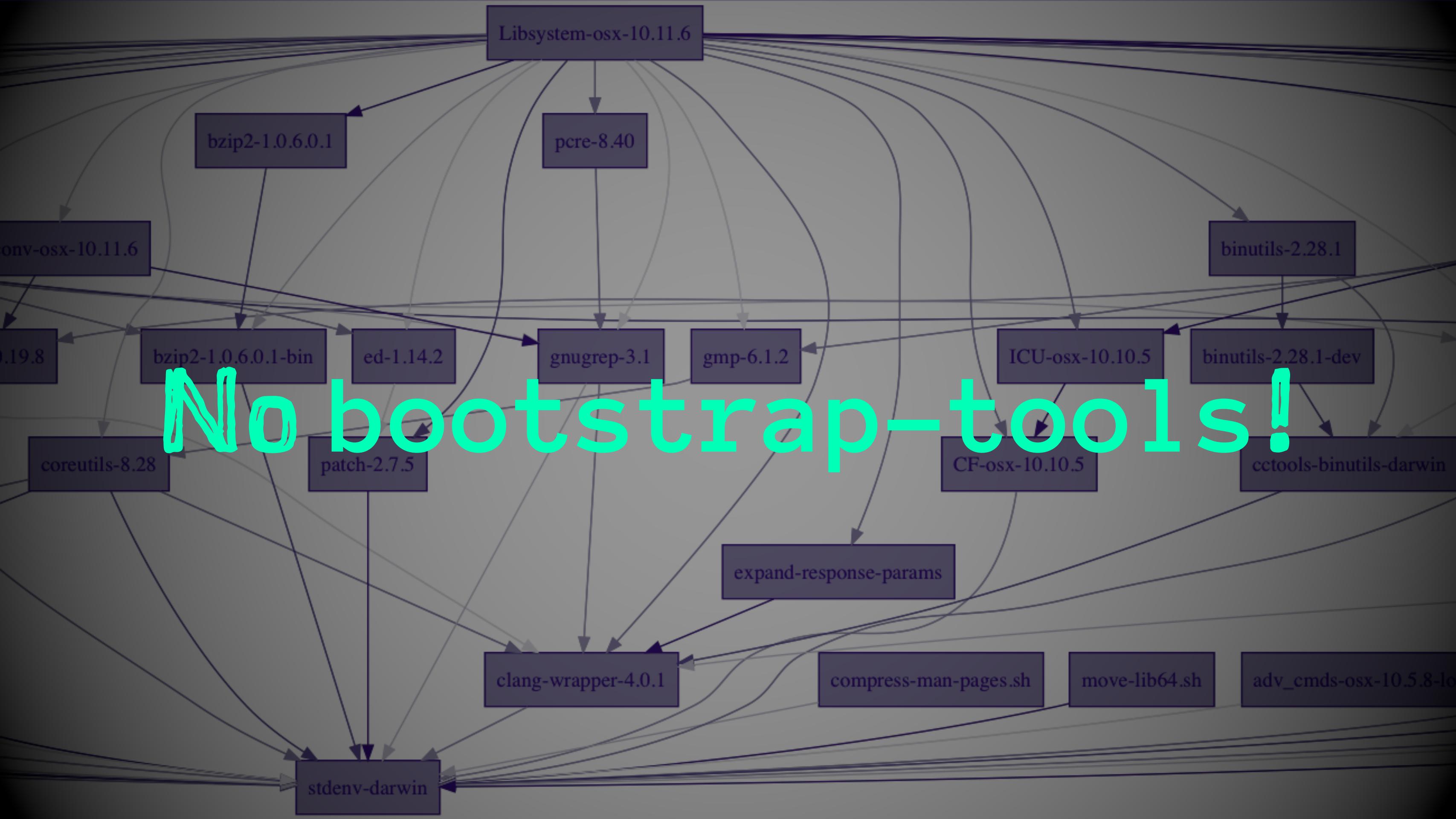


History starts forking here

Refining the stdenv



No bootstrap-tools!



```
277 278
278     -    allowedRequisites = null;
279     -/*      (with stage1.pkgs; [ darwin.dylib darwin.libSystem ]) ++
280     -      (with stage2.pkgs; [ bash libcxx libcxxabi ] ) ++
281     -      (with stage3.pkgs; [
282     -          coreutils findutils diffutils gnused gnugrep gawk gnutar gzip bzip2 gnumake bash patch xz
283     -          zlib ncurses binutils libffi libiconv pcre icu ed gmp llvmPackages.llvm llvmPackages.clang
284     -      ]);
285     -*/
286     -    overrides = _: {
299     +    allowedRequisites = (with pkgs; [
300     +        xz libcxx libcxxabi icu gmp gnumake findutils bzip2 llvm zlib libffi
301     +        coreutils ed diffutils gnutar gzip ncurses libiconv gnused bash gawk
302     +        gnugrep llvmPackages.clang patch pcre
303     +    ]) ++
304     +    (with pkgs.darwin; [
305     +        dyld libSystem corefoundation cctools
306     +    ]);
307     +    overrides = orig: persistent3 orig // {
287     308         clang = cc;
```

The sandbox

Code

Issues 25

Pull requests 2

Projects 0

Wiki

Insights

Settings

Assorted purification from running it in a sandbox

[Browse files](#)

 broken-stuff-bootstrapped



copumpkin committed on Nov 15, 2014

1 parent e75b0c5 commit bbe477ff932760d810719b1af465ae370b78dd41

Showing 9 changed files with 117 additions and 29 deletions.

[Unified](#) [Split](#)

3  pkgs/development/interpreters/python/2.7/default.nix

[View](#) ▾

```
@@ -43,6 +43,9 @@ let
43    43
44    44      ensurePurity =
45    45      ''
46 +    substituteInPlace configure \
47 +      --replace '/usr/bin/arch' 'i386'
48 +
49    # Purity.
50    for i in /usr /sw /opt /pkg; do
51      substituteInPlace ./setup.py --replace $i /no-such-path
```

7  pkgs/development/libraries/zlib/default.nix

[View](#) ▾

```
@@ -13,6 +13,13 @@ stdenv.mkDerivation rec {
13    13      sha256 = "039agw5rqvqny92cpkrfn243x2gd4xn13hs3xi6isk55d2vqqr9n";
14    14    };
15    15
16 +    postPatch = stdenv.lib.optionalString stdenv.isDarwin ''
17 +      substituteInPlace configure \
18 +        --replace '/usr/bin/libtool' 'ar' \
19 +        --replace 'AR="libtool"' 'AR="ar"' \
20 +        --replace 'ARFLAGS="-o"' 'ARFLAGS="-r"' \
21 +        '';
22 +
```

Background: macOS has an undocumented sandbox feature

- sandbox-exec tool (and related APIs)
- Like seccomp but with a much friendlier³ front-end
- TinyScheme to govern access to syscalls!
- Started for iOS app isolation, also on macOS now
- All macOS system services use it

³ Yes, an undocumented interface is friendlier than seccomp

```
;; ntpd - sandbox profile
;; Copyright (c) 2006-2009, 2014 Apple Inc. All Rights reserved.

(version 1)

(deny default)

(allow process-fork)
(allow signal (target same-sandbox))

(allow iokit-open (iokit-user-client-class "RootDomainUserClient")
        (iokit-user-client-class "AppleSMCClient"))

(allow file-read-data file-read-metadata
      (literal "/private/etc/ntp-restrict.conf")
      (literal "/private/etc/ntp_opendirectory.conf")
      (literal "/private/var/run/resolv.conf")
      (regex "^/private/etc/ntp\\.(conf|keys)$")
      (regex "^/private/etc/(services|hosts)$")
      (regex "^/private/var/run/tmpntp.conf.*"))

;
; ...
```

Add basic Apple sandbox support for "chroot" builds on darwin [WIP] #434

Edit



Closed copumpkin wants to merge 1 commit into NixOS:master from copumpkin:darwin-sandbox

Conversation 52

Commits 1

Files changed 1

+169 -17



copumpkin commented on Jan 7, 2015

Member



This uses Apple's `sandbox-exec` tool (mostly undocumented beyond its man page, but there's a bit of information on it floating around the web) to give build children very precise and limited capabilities when building. They can't talk to the network, see other processes on the system, or see any paths outside of what we explicitly include. This works through a lisp-y sandbox specification language. My change just teaches nix to construct such a specification on the fly and then feeds it into the existing Apple sandbox mechanism.

I've bundled this new attribute on `darwinSystem` to allow for per-directory impurity. This is crucial for Darwin, since in a partially closed system, we're going to need to call out to many of the system APIs. We don't build ourselves—lame! The idea is to provide instructions to `sandbox-exec` to allow us to keep that impurity to a minimum.

The attribute is called `__impureHostDeps` for now, but I'm open to better names or designs. My current view is that it could even replace some of the functionality in current linux chroot builds. In my pure darwin nixpkgs, for example, I have `/bin/sh` in that list, and that makes sense on linux, too, along with some of the ubiquitous `/dev` paths.

Looking for comments, criticism, and the like. I have no automated tests for the functionality, but I'm already using the code in this branch on my pure darwin branch and it seems to work.

Relevant to #317 and #361.



jwiegley and 1 other commented on an outdated diff on Jan 7, 2015

Show 2 comments



jwiegley commented on the diff on Jan 7, 2015

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Project

None yet

Milestone

No milestone

Notifications

Unsubscribe

You're receiving notifications because you were mentioned.

5 participants



Allow edits from maintainers.

Cleanup

- dyld: Library not loaded: /usr/lib/libiconv.2.dylib** 18
#77 by datakurre was closed on Jun 23, 2015
- dyld is not supplied as argument to ccWrapper**
#68 by adnelson was closed on May 12, 2015
- aria2 fails**
#62 by jwiegley was closed on Feb 17
- erlang builds outside the sandbox, but not in**
#61 by jwiegley was closed on Feb 17
- sw_vers problem** 4
#57 by wavewave was closed on Feb 20, 2015
- Csu won't build on HEAD** 4
#54 by pikajude was closed on Feb 12, 2015
- gfortran support?** 6
#52 by wavewave was closed on Feb 17, 2015
- Can't build cmake for stdenv on HEAD** 17
#49 by pikajude was closed on Feb 7, 2015
- cc-wrapper seems to have an impure framework search path** 2
#47 by copumpkin was closed on Feb 7, 2015
- python3 won't build** 2

#43 by wmertens was closed on Feb 1, 2015
- libtool tries to run gcc as part of linking** 7
#42 by wmertens was closed on Jan 31, 2015
- Building ruby libraries fails in sandbox** 5
#38 by pikajude was closed on Feb 5, 2015
- Figure out what to do about iconv wrt GHC** 2
#37 by pikajude was closed on Jan 23, 2015
- We build llvm+clang too often in the stdenv build** 2

#35 by copumpkin was closed on Jan 19, 2015
- Can't build gmp-4.3.2 because nix can't find "a working compiler", when trying to install haskellingPackages.cabal2nix**
#33 by alpmestan was closed on Jan 17, 2015
- Break stdenv dependencies on bootstrap-tools** 2
#31 by copumpkin was closed on Jan 19, 2015
- GHC 7.8.4 won't build** 8
#30 by pikajude was closed on Feb 4, 2015
- Figure out how to pass libc = libSystem into clang-wrapper** stdenv-design 2

#28 by copumpkin was closed on Jan 19, 2015
- builder for '/nix/store/...serf-1.3.7.drv' failed with exit code 2**
#27 by henrytill was closed on Jan 11, 2015

- Wary of merging to mainline until kinks ironed out
- Opened issue-tracker on my nixpkgs fork
- Dozens of issues both on GitHub and IRC
- Hundreds of fixes from several Darwin users
- Most fixes applied to mainline, merged back to fork
- Tons of effort in general cleanups

Languishing

- Long-lived forks are miserable
- Didn't want to break existing users
- My motivation was dwindling
- Linux kept breaking us
- Very low bus factor

@pikajude saves the day

Merge pure-darwin stdenv #8363

Edit



pikajude wants to merge 4 commits into NixOS:master from pikajude:bootstrap-darwin

Conversation 49

Commits 4

Files changed 22

+871 -66



pikajude commented on Jun 17, 2015

Member



This PR contains *only* the new darwin stdenv, which is totally pure, and fixes for packages that are used during the bootstrapping process. This causes **lots of breakages**.

I'm hoping to merge this branch because it will be easier than keeping pure-darwin's PR up to date, and it's the first step to getting truly pure development on darwin going.

I have several hundred packages' worth of fixes that are ready to be cherry-picked from pure-darwin once this is in master.

Thanks to @copumpkin for doing essentially all of this. I took care of updating it for NixOS.

In master, but optional



copumpkin commented on Jun 17, 2015

Member



👍 x 1000 from me as long as people understand that Nix + Darwin will be particularly unstable immediately following this merge. There are known issues with it and I'm not sure when I'll have time to fix them. At the same time, leaving it unmerged when it touches that many things is a recipe for the whole thing just dying, so I'd be inclined to merge it.



copumpkin added **6.topic: darwin** **1.severity: mass-darwin-rebuild** labels on Jun 17, 2015



copumpkin commented on Jun 17, 2015

Member



Also, thanks @pikajude for cherry-picking all this out and keeping it alive 😊

Reviewers



No reviews—request one

Assignees



No one—assign yourself

Labels



1.severity: mass-darwin-reb...

1.severity: mass-rebuild

6.topic: darwin

Projects



None yet

Milestone



No milestone

Notifications

✖ Unsubscribe

You're receiving notifications because you were mentioned.

10 participants



switch stdenvs to pure-darwin #10187

Merged pikajude merged 1 commit into master from switch-to-pd on Oct 15, 2015

onversation 15

Commits 1

Files changed 1

+1 -1

pikajude commented on Oct 2, 2015

Member



This is to go along with my ML message requesting a default stdenv switch to pure-darwin. The reactions have been positive so far!

Default!!!

@edolstra

Reviewers

No reviews—request one

Assignees

No one—assign yourself

Labels

1.severity: mass-darwin-

6.topic: darwin

switch stdenvs

✓ df3d54e

vcunat added 6.topic: darwin

1.severity: mass-darwin-rebuild

labels on Oct 2, 2015

Projects

None yet

domenkozar referenced this pull request on Oct 3, 2015

Purer darwin stdenv #1485

Closed

More recently

- @LnL7 stepped up, many new faces in community
- Countless improvements to packages on Darwin
- @matthewbauer packaged xcbuild for us⁴
- New macOS releases required small stdenv changes
- macOS sandbox fell into disrepair⁵

⁴This is kind of a big deal

⁵But we're fixing it during the hackathon!

Ongoing challenges

- Linux users still break our stuff (not their fault!)
- Unpredictable Apple source release behavior
- Hard to find users willing to tinker with packaging

What might come next!

- Actually “take on” Homebrew
- Awesome work on a background transparent Linux VM from @puffnfresh
- Expand on ability of Linux users to use Darwin
 - Cheap Hydra workers? VM on Linux? Borg?
- @LnL7’s nix-darwin: grow & share with NixOS!
- Build GUI apps (semi-) purely?
- Improve maintainability of stdenv
- Revive sandbox and enable by default!

```
115 cp SCPreferencesKeychainPrivate.h SystemConfiguration.framework/PrivateHeaders
116 cp SCKernelSignature.h SystemConfiguration.framework/PrivateHeaders
117 cp SCNetworkSignaturePrivate.h SystemConfiguration.framework/PrivateHeaders
118 cp VPNPrivate.h SystemConfiguration.framework/PrivateHeaders
119 cp VPNConfiguration.h SystemConfiguration.framework/PrivateHeaders
120 cp VPNTunnelPrivate.h SystemConfiguration.framework/PrivateHeaders
121 cp VPNTunnel.h SystemConfiguration.framework/PrivateHeaders
122
123 mkdir derived
124
125 cat >derived/SystemConfiguration_vers.c <<EOF
126 const unsigned char SystemConfigurationVersionString[] __attribute__ ((used)) = "@(#)PROGRAM:SystemConfiguration PROJECT:c
127 EOF
128
129 mig -arch x86_64 -header derived/shared_dns_info.h -user derived/shared_dns_infoUser.c -sheader /dev/null -server /dev/null
130 mig -arch x86_64 -header derived/dns.h -user derived/dnsUser.c -sheader /dev/null -server /dev/null
131 mig -arch x86_64 -header derived/helper.h -user derived/helperUser.c -sheader /dev/null -server /dev/null
132 mig -arch x86_64 -header derived/pppcontroller.h -user derived/pppcontrollerUser.c -sheader /dev/null -server /dev/null
133
134 cc -I. -Ihelper -Iderived -F. -c SCSchemaDefinitions.c -o SCSchemaDefinitions.o
135 cc -I. -Ihelper -Iderived -F. -c SCD.c -o SCD.o
136 cc -I. -Ihelper -Iderived -F. -c SCDKeys.c -o SCDKeys.o
137 cc -I. -Ihelper -Iderived -F. -c SCDPrivate.c -o SCDPrivate.o
138 cc -I. -Ihelper -Iderived -F. -c SCDPlugin.c -o SCDPlugin.o
139 cc -I. -Ihelper -Iderived -F. -c CaptiveNetwork.c -o CaptiveNetwork.o
140 cc -I. -Ihelper -Iderived -F. -c SCDOpen.c -o SCDOpen.o
141 cc -I. -Ihelper -Iderived -F. -c SCDList.c -o SCDList.o
142 cc -I. -Ihelper -Iderived -F. -c SCDAAdd.c -o SCDAAdd.o
143 cc -I. -Ihelper -Iderived -F. -c SCDGet.c -o SCDGet.o
```

Why xcbuid is a big deal

Stdenv maintainability

- Very annoying dance to make changes to core stdenv
- Manual process to figure out best bootstrap order
- Should be possible to automate with some trickery
- xcbuild will give us much prettier build expressions for many of the stdenv components

Thanks!

Questions?