Tails - Feature #5630
Reproducible builds
07/18/2013 07:43 AM - Tails

Description
To ensure integrity against build machine or developer compromise, we should be able to produce identical binaries when building the same source on two different (but possibly identically configured) machines.

Team: anonym, lamby, bertagaz, u, kibi and intrigeri

Subtasks:

- Bug # 10232: Investigate vagrant-lxc for our build system
- Feature # 11966: Reproducible website build
- Feature # 11967: refresh-translations: don't update PO files unless something other POT...
- Feature # 11970: sys-subsystem-net-devices-multi-user.device/start times out
- Feature # 11971: Consider migrating some of /lib/live/config/* to systemd unit files
- Feature # 11972: Switch our Jenkins ISO build system to vagrant-libvirt
  - Feature # 12017: Update our Vagrant ISO build basebox wrt. vagrant-libvirt
  - Feature # 12327: Upgrade Lizard's memory again
- Feature # 11974: Reproducible IUK builds
- Feature # 11976: Migrate to mksquashfs that honors $SOURCE_DATE_EPOCH
- Feature # 11979: Move Vagrant's apt-cacher-ng data to a dedicated disk
- Feature # 11980: Create and provision a new Vagrant VM for every ISO build
- Feature # 11981: Delete the Vagrant VM used for an ISO build once it is finished
- Feature # 11982: Set up processes to update the Vagrant ISO build basebox
- Feature # 11983: Check if the test suite has more failures on the reproducible ISO
- Bug # 11986: Generated APT auto-removal config file encodes the build system's kernel v...
- Bug # 11987: ikiwiki includes "Posted" timestamps in some generated web pages
- Feature # 11988: Update Vagrant boxes management design doc with meeting notes
- Feature # 12002: Estimate hardware cost of reproducible builds in Jenkins
- Feature # 12032: The SquashFS creation is not deterministic
- Feature # 12051: Use ikiwiki 3.20161219+ instead of our patched one
- Bug # 12329: /usr/share/locale/*/LC_MESSAGES/tails.mo's POT-Creation-Date depends on th...
- Bug # 12330: initrd.img is not generated reproducibly
- Feature # 12338: Test ISO build reproducibility with varying number of CPU cores
- Feature # 12339: Have the ISO build reproducibility regardless of the current time
- Feature # 12345: Test ISO build reproducibility with varying CPU type
- Feature # 12348: Review'n'merge the reproducible builds branch into feature/stretch
- Feature # 12351: Test building an ISO with a fake system time set in 2018
- Feature # 12352: Error out if trying to build an ISO with a system time before SOURCE_D...
- Feature # 12409: Reconsider the need for publishing Vagrant baseboxes
- Bug # 12453: Invalid MBR ID passed to isohybrid
- Bug # 12527: Duplicate gpg-agent killing code introduced in the build-tails script

03/22/2020
<table>
<thead>
<tr>
<th>Bug #</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>12529</td>
<td>Vagrant box creation needlessly downloads Linux from debian-security</td>
<td>Resolved</td>
</tr>
<tr>
<td>12530</td>
<td>Vagrant box creation fails: can't unmount chroot that's busy</td>
<td>Resolved</td>
</tr>
<tr>
<td>12531</td>
<td>ISO builds on Jenkins are fragile since the migration to vagrant-libvirt</td>
<td>Resolved</td>
</tr>
<tr>
<td>12577</td>
<td>Aborted Jenkins ISO builds can cause next ones on the same isobuilder to fail</td>
<td>Resolved</td>
</tr>
<tr>
<td>12578</td>
<td>Abort if Vagrant create box fails</td>
<td>Resolved</td>
</tr>
<tr>
<td>12599</td>
<td>/var/lib/libvirt/images gets filled on isobuilders</td>
<td>Resolved</td>
</tr>
<tr>
<td>12618</td>
<td>Retrieving ISO build artifacts sometimes fails on Jenkins</td>
<td>Resolved</td>
</tr>
<tr>
<td>13302</td>
<td>/var/lib/libvirt/images sometimes gets filled on isobuilders, take 2</td>
<td>Resolved</td>
</tr>
<tr>
<td>12541</td>
<td>isobuilders memory check keeps switching between OK and WARNING since the ...</td>
<td>Resolved</td>
</tr>
<tr>
<td>12565</td>
<td>Test failures on Jenkins due to lack of disk space</td>
<td>Resolved</td>
</tr>
<tr>
<td>12566</td>
<td>ikiwiki image size specification makes the ISO build unreproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>12567</td>
<td>fontconfig cache is not generated reproducibly even with patch from Debian...</td>
<td>Resolved</td>
</tr>
<tr>
<td>12574</td>
<td>isobuilders system_disks check keeps switching between OK and WARNING since...</td>
<td>Resolved</td>
</tr>
<tr>
<td>12575</td>
<td>Fix basebox:clean_old</td>
<td>Resolved</td>
</tr>
<tr>
<td>12576</td>
<td>Have Jenkins use basebox:clean_old instead of basebox:clean_all</td>
<td>Resolved</td>
</tr>
<tr>
<td>12579</td>
<td>reproducibly_build_Tails_ISO_* Jenkins job are broken</td>
<td>Resolved</td>
</tr>
<tr>
<td>12595</td>
<td>Not enough space in /var/lib/jenkins on isobuilders</td>
<td>Resolved</td>
</tr>
<tr>
<td>12606</td>
<td>Better balance our isobuilders' I/O load over all available SSDs</td>
<td>Resolved</td>
</tr>
<tr>
<td>12608</td>
<td>Analyze what's still not reproducible on current testing branch</td>
<td>Resolved</td>
</tr>
<tr>
<td>12616</td>
<td>Document our vagrant based build setup in Jenkins</td>
<td>Resolved</td>
</tr>
<tr>
<td>12619</td>
<td>/usr/share/doc/tails/website/torrents/rss.html is not reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>12620</td>
<td>/usr/local/lib/tor-browser/omni.js embeds build timestamp</td>
<td>Resolved</td>
</tr>
<tr>
<td>12625</td>
<td>Make ikiwiki resize images deterministically</td>
<td>Resolved</td>
</tr>
<tr>
<td>12626</td>
<td>Report back to the reproducible builds community about how we did it</td>
<td>Resolved</td>
</tr>
<tr>
<td>12628</td>
<td>Draft a &quot;user&quot; (aka. RM) story for the reproducible release process</td>
<td>Duplicate</td>
</tr>
<tr>
<td>12630</td>
<td>Document how users can verify a reproducibly built ISO/IUK</td>
<td>Resolved</td>
</tr>
<tr>
<td>12633</td>
<td>Lower the workload caused by reproducible builds Jenkins jobs</td>
<td>Resolved</td>
</tr>
<tr>
<td>12637</td>
<td>Deploy rake libvirt volumes clean up task on all Jenkins build jobs</td>
<td>Resolved</td>
</tr>
<tr>
<td>12641</td>
<td>Comment changes in POT files make ISO builds non-reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>12654</td>
<td>Introduce more variations in our reproducibility CI tests</td>
<td>Resolved</td>
</tr>
<tr>
<td>12681</td>
<td>reproducibly_build_Tails_ISO_* Jenkins jobs are buggy when building from a...</td>
<td>Resolved</td>
</tr>
<tr>
<td>12715</td>
<td>Decide what builds we will try to reproduce in Jenkins</td>
<td>Resolved</td>
</tr>
<tr>
<td>12725</td>
<td>Sort out the apt-snapshots-disk partition situation on apt.lizard</td>
<td>Resolved</td>
</tr>
<tr>
<td>12726</td>
<td>There should be a date on the notes in the News section of the website</td>
<td>Resolved</td>
</tr>
<tr>
<td>12735</td>
<td>live/initrd.img not reproducible in some environments</td>
<td>Resolved</td>
</tr>
<tr>
<td>12736</td>
<td>live/vmlinuz not reproducible in some environments</td>
<td>Duplicate</td>
</tr>
<tr>
<td>12738</td>
<td>Remove gconf</td>
<td>Resolved</td>
</tr>
<tr>
<td>12737</td>
<td>utilities not reproducible in some environments</td>
<td>Duplicate</td>
</tr>
<tr>
<td>12739</td>
<td>Metadata for directories inside the squashfs not reproducible in some environments</td>
<td>Rejected</td>
</tr>
<tr>
<td>12740</td>
<td>Various .cache files not reproducible in some environments</td>
<td>Resolved</td>
</tr>
<tr>
<td>12909</td>
<td>/var/cache/cracklib/src-dicts not reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>13439</td>
<td>mimeinfo.cache not reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>13440</td>
<td>GTK immodules.cache not reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>13441</td>
<td>giomodule.cache not reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>13442</td>
<td>gdk-pixbuf's loaders.cache not reproducible</td>
<td>Resolved</td>
</tr>
<tr>
<td>12741</td>
<td>/lib/modules/&quot;modules.&quot; not reproducible in some environments</td>
<td>Resolved</td>
</tr>
<tr>
<td>13436</td>
<td>Have Jenkins jobs that reproduce ISOS when a branch ticket is Ready for...</td>
<td>Resolved</td>
</tr>
<tr>
<td>13504</td>
<td>Rebase our custom squashfs-tools package on 1:4.3-3+deb9u1</td>
<td>Rejected</td>
</tr>
<tr>
<td>13531</td>
<td>Use ikiwiki 3.20161219+, again</td>
<td>Duplicate</td>
</tr>
<tr>
<td>13623</td>
<td>Executable bits of /etc/hostname not set deterministically</td>
<td>Resolved</td>
</tr>
<tr>
<td>13624</td>
<td>Analyze results of Tails 3.1 call for reproduction</td>
<td>Resolved</td>
</tr>
<tr>
<td>14512</td>
<td>Send second email call to test reproducibility of Tails 3.2alpha1</td>
<td>Resolved</td>
</tr>
<tr>
<td>14520</td>
<td>Prepare &amp; publish a blog post about testing Tails ISO reproducibility</td>
<td>Resolved</td>
</tr>
</tbody>
</table>
Feature # 14607: Analyze results of Tails 3.2-alpha1 call for reproduction (Resolved)

Bug # 14729: Fix gdk-pixbuf vulnerability (CVE-2017-2862) (Resolved)

Feature # 14756: Drop update-ca-certificates.service (Resolved)

Feature # 14757: Final report for SponsorT 2016 (Resolved)

Bug # 14767: ikiwiki does not order news items deterministically (Resolved)

Bug # 14924: reproducibly_build_Tails_ISO_stable Jenkins job always fails (Resolved)

Bug # 14933: stable branch is not reproducible: differences in some .fa.html website files (Resolved)

Bug # 14944: jenkins-data-disk is running out of disk space (Resolved)

Bug # 14946: Topic branches that lag behind their base branch don’t build reproducibly ... (Resolved)

Bug # 15141: reproducibly_build_Tails_ISO_stable job erroneously fails when build repro... (Resolved)

Related issues:

- Related to Tails - Feature #8511: Have all Debian packages we use build in a ...
  Confirmed 01/01/2015

- Related to Tails - Feature #7100: Decide what to do with machine-id
  Confirmed 04/16/2014

- Blocked by Tails - Bug #8125: Self-host the Tor Browser tarballs we need
  Resolved 10/15/2014

- Blocked by Tails - Bug #9416: Stop shipping ssl-cert-snakeoil in the ISO
  Resolved 05/17/2015

- Blocked by Tails - Bug #9419: eatmydata is not being used in the build chroot
  Resolved 05/17/2015

- Blocked by Tails - Bug #11273: clean up libdvd-pkg build files
  Resolved 03/21/2016

Associated revisions

Revision 4dd6fe78 - 11/20/2016 09:22 AM - intrigeri
Export last changelog entry's timestamp as SOURCE_DATE_EPOCH (refs: #5630).

Revision d52e4e9e - 11/20/2016 09:33 AM - intrigeri
Don't include /var/cache/ldconfig/aux-cache in the ISO (refs: #5630).

It causes reproducibility issues, and is not needed strictly speaking.

Revision bfbfecc4 - 11/20/2016 09:40 AM - intrigeri
Don't include monkeysphere private key in the ISO (refs: #5630).

It causes reproducibility issues and should not be shared among all
Tails systems. Thankfully it is only useful when using monkeysphere
to authenticate users connecting to the Tails system, and we don't
ship SSHd, so 1. shipping that key previously was not a security issue;
2. we don't have to generate this key at boot time.

Revision a8f5383f - 11/20/2016 11:06 AM - intrigeri
Merge remote-tracking branch 'lamby/regenerate-fontconfig' into feature/5630-deterministic-builds
refs: #5630

Revision 70efd9dc - 11/20/2016 11:22 AM - intrigeri
Don't ship /etc/console-setup/cached_setup_keyboard.sh in the ISO.
refs: #5630
It's useless since it refers to a file in /tmp that won't exist anyway,
and it causes reproducibility issues.
Don't ship /var/lib/monkeysphere/authentication/ in the ISO (refs: #5630).

Same rationale as in commit:bfbfecc4a3e0979c862525fa81abe431c9bdecfe.

Don't ship /root/.gnupg/trustdb.gpg in the ISO: it's not needed and causes reproducibility issues (refs: #5630).

Pretend that tails-keyring.gpg is created at $SOURCE_DATE_EPOCH, to make its content deterministic (refs: #5630).

Empty /etc/machine-id instead of deleting it (Closes: #11970, refs: #5630, refs: #7100).

Ensure the SquashFS creation time is $SOURCE_DATE_EPOCH (refs: #5630).

Drop mtme clamping: lb_chroot_reproducible does that for us already (refs: #5630).

Don't pass -mkfs-fixed-time to mksquashfs, instead rely on having it honor $SOURCE_DATE_EPOCH (refs: #5630).

This reverts commit 0f56eea534f6cde1bee912cc51ceeb435790df80.

Don't include root's gpg-agent socket files in the SquashFS (refs: #5630).

Normalize timestamps of files in config/chroot_local-includes before building.

Ensure /etc/resolv.conf is owned by root:root in the SquashFS.

lb_chroot_resolv will "cp -a" it from the source tree, so it inherits its ownership from the whoever cloned the Git repository. This has two problems. First, this results in unsafe permissions on this file (e.g. a Vagrant build results in the 'amnesia' user having write access to it). Second, building with a different user results in a non-deterministic SquashFS.

refs: #5630
Pass a fixed MBR ID to isohybrid (refs: #5630).

Otherwise, a random one is used, that makes the build unreproducible even when
the content of the ISO filesystem matches.

Revision dbc479a8 - 03/29/2017 12:34 PM - intrigeri
Reproducible builds post-processing: don't try deleting /etc/ssl/certs/java/cacerts that's not shipped anymore (refs: #5630).

Revision bd43b818 - 03/29/2017 03:12 PM - intrigeri
Reproducible builds post-processing: don't try deleting /usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64/server/classes.jsa, that's not shipped anymore (refs: #5630).

Revision ababdf9 - 05/20/2017 08:40 AM - intrigeri
Revert "Ship the fontconfig cache in the ISO again, after making it reproducible"

This reverts commit d7dae73111ea2521ff98010b5ebd62a11e5cb3ef.
refs: #5630

History

#1 - 07/19/2013 01:47 AM - intrigeri
- Type of work set to Code

Type of work: Code

#2 - 06/09/2014 12:15 PM - BitingBird
- Description updated
- Category set to Build system
- Starter set to No

#3 - 11/01/2014 08:34 PM - intrigeri
- Blocked by Bug #8125: Self-host the Tor Browser tarballs we need added

#4 - 01/01/2015 10:58 PM - intrigeri
- Related to Feature #8511: Have all Debian packages we use build in a deterministic way added

#5 - 05/17/2015 09:52 AM - intrigeri
- Feature Branch set to feature/5630-deterministic-builds

#6 - 05/17/2015 09:55 AM - intrigeri
Requires our tails/debian-old-2.0-faketime branch of live-build, otherwise faketime has no effect on the commands run in the chroot set up by live-build.

#7 - 05/17/2015 10:05 AM - intrigeri
- Blocked by Bug #9416: Stop shipping ssl-cert-snakeoil in the ISO added

#8 - 05/17/2015 10:43 AM - intrigeri
- Blocked by Bug #9419: eatmydata is not being used in the build chroot added

#9 - 08/14/2015 12:14 PM - sajolida
- Description updated
- Assignee set to intrigeri
- Target version set to 2017

#10 - 09/27/2015 10:04 AM - intrigeri
- Priority changed from Low to Normal

(It's on our roadmap now.)

#11 - 09/27/2015 10:09 AM - intrigeri
- Description updated

#12 - 02/16/2016 01:17 PM - intrigeri
- Subject changed from Deterministic builds to Reproducible builds
- Blueprint set to https://tails.boum.org/blueprint/reproducible_builds/

#13 - 02/16/2016 01:22 PM - intrigeri
- Description updated

#14 - 06/27/2016 02:12 AM - BitingBird
- Status changed from Confirmed to In Progress

#15 - 06/27/2016 04:49 AM - intrigeri
- Status changed from In Progress to Confirmed
- Assignee changed from intrigeri to anonym

#17 - 11/19/2016 04:21 PM - intrigeri
- Description updated

#18 - 11/20/2016 02:06 PM - intrigeri
- Related to Feature #7100: Decide what to do with machine-id added

#19 - 11/21/2016 02:53 PM - intrigeri
- Description updated

#20 - 11/22/2016 02:01 PM - intrigeri
- Blocks Feature #11990: In 2019, try reproducing an ISO that was released in 2018 added

#21 - 03/13/2017 03:10 PM - intrigeri
- Blocked by Bug #11273: clean up libdvd-pkg build files added

#22 - 03/16/2017 07:49 AM - lamby
fontconfig issues should be resolved with: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=857892

#23 - 05/20/2017 08:53 AM - intrigeri
- Status changed from Confirmed to In Progress
#24 - 05/24/2017 07:03 AM - intrigeri
- Blocked by deleted (Feature #5926: Freezable APT repository)

#25 - 06/05/2017 09:38 AM - intrigeri
- Target version changed from 2017 to Tails_3.2
- Feature Branch deleted (feature/5630-deterministic-builds)

( 
  This branch has nothing interesting now that we generate the fontconfig cache in a reproducible manner. I've renamed it to wip/feature/5630-deterministic-builds so it doesn't eat precious cycles on our CI infra. And anyway the only non-merge commit it has on top of testing is a trivial revert.
  Setting a target version that's before the sponsor deadline.
)

#26 - 09/26/2017 12:37 PM - anonym
- Target version changed from Tails_3.2 to Tails_3.3

It seems Tails 3.2 is reproducible! Woo!

But we have some testing, documentation and communication tasks remaining so => postponed.

#27 - 10/29/2017 08:24 AM - intrigeri

(Some subtasks are meant to be done after the end of the contract.)

#28 - 11/15/2017 11:30 AM - anonym
- Target version changed from Tails_3.3 to Tails_3.5

#29 - 01/02/2018 09:12 AM - intrigeri
- Blocks deleted (Feature #11990: In 2019, try reproducing an ISO that was released in 2018)

#30 - 01/23/2018 07:52 PM -匿名
- Target version changed from Tails_3.5 to Tails_3.6

#31 - 03/14/2018 11:32 AM - bertagaz
- Target version changed from Tails_3.6 to Tails_3.7

#32 - 05/10/2018 11:09 AM - bertagaz
- Target version changed from Tails_3.7 to Tails_3.8

#33 - 05/25/2018 01:26 PM - intrigeri
- Assignee changed from anonym to intrigeri

03/22/2020
#34 - 05/26/2018 09:51 AM - intrigeri

- Assignee changed from intrigeri to bertagaz
- Target version deleted (Tails_3.8)

(Most of the work that remains to do is on bertagaz' plate so it does not make sense that this ticket is assigned to me.)

#35 - 01/09/2019 05:46 PM - intrigeri

- Status changed from In Progress to Resolved
- Assignee deleted (bertagaz)