Tails - Feature #11980
Feature # 5630 (Resolved): Reproducible builds
Create and provision a new Vagrant VM for every ISO build
11/21/2016 02:56 PM - intrigeri

<table>
<thead>
<tr>
<th>Status:</th>
<th>Resolved</th>
<th>Start date:</th>
<th>11/21/2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Elevated</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
<td>% Done:</td>
<td>100%</td>
</tr>
<tr>
<td>Category:</td>
<td>Build system</td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td>Tails_3.0~rc1</td>
<td>Spent time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Feature Branch:</td>
<td>feature/11980-static-build-env</td>
<td>Starter:</td>
<td></td>
</tr>
<tr>
<td>Type of work:</td>
<td>Code</td>
<td>Affected tool:</td>
<td></td>
</tr>
<tr>
<td>Blueprint:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description
---
... using the basebox encoded in the build branch + a set of APT snapshots derived from what's encoded in Git.

First of all: benchmark how much it slows down the build, to ensure this is a viable option.

The branch this VM is made for must be encoded in the VM itself, and Vagrant should abort if one tries to reuse it to build another branch (rationale: that other branch may point to an older set of APT snapshots, and then the Vagrant provisioning will try to downgrade the entire system, which won't work reliably enough for our needs). With this sanity check in, we can add an option to keep the VM running and not delete it (#11981), for faster development builds when one works on a branch.

Related issues:
Blocked by Tails - Feature #11979: Move Vagrant's apt-cacher-ng data to a ded... Resolved 11/21/2016
Blocks Tails - Feature #11981: Delete the Vagrant VM used for an ISO build on... Resolved 11/21/2016
Blocked by Tails - Feature #11972: Switch our Jenkins ISO build system to vag... Resolved 12/04/2016

Associated revisions
Revision aea46312 - 11/30/2016 01:20 PM - bertagaz
Get serial from the basebox name, use it in VM creation script.
This implements the first step of using APT snapshots in our vagrant VM, by starting to use them in the vmdebootstrap step.
Will-fix: #11980

Revision 24b6aac6 - 11/30/2016 01:20 PM - bertagaz
Respect the http_proxy environment variable if set.
Will-fix: #11980

Revision f8a01032 - 11/30/2016 01:20 PM - bertagaz
Import Tails APT repo signing key.
Will-fix: #11980

Revision 9b43319e - 12/01/2016 11:31 AM - bertagaz

05/04/2020
Check that the VM has been created to build the branch/tag/commit it is asked to.

Will-fix: #11980

**Revision 2efc291a - 12/01/2016 11:31 AM - bertagaz**

Remove useless and time consuming zeroing of filesystem.

Vmdebootstrap already does that at the end of its process.

Will-fix: #11980

**Revision 86961cda - 12/01/2016 11:40 AM - bertagaz**

Force upgrading with debian-security APT repo activated.

Otherwise each generated basebox will already be behind some security upgrades when it is created, and the creation of the vagrant builder based on this basebox is delayed by applying this security upgrades. Let save a bit of time on VM creation by including the latest security upgrade when creating a basebox.

Will-fix: #11980

**Revision 2d300a30 - 12/02/2016 12:37 PM - bertagaz**

Ship all build dependencies in the basebox.

They take quite some time to install every time a new vagrant builder is provisioned. Shipping them reduce the time it takes to build an ISO, and grow the final basebox image of around 30MB. It's probably fastest to download this in the basebox than installing them each time.

Will-fix: #11980

**Revision 6a637631 - 03/15/2017 01:54 AM - anonym**

Vagrant: update basebox to tails-builder-amd64-jessie-2017011203+feature-11980.

This box is prepared for the wip/feature/11980-per-branch-vagrant-build-vm Git branch.

Refs: #11980
Will-fix: #12017
Revision 5b2a3af4 - 03/15/2017 02:10 AM - anonym

Vagrant: provision a new Vagrant VM for every ISO build.

Well, at least when there are only successes; on failure the VM is kept and a new ‘rake build’ will start an immediate build, reusing the cached wiki from last time. This should be a nice trade-off between making it fast to rebuild a branch after a failure, and maintaining the “staticness” and “up-to-dateness” of the build environment.

Will-fix: #11980, #11981

Revision 79b7f9ca - 05/09/2017 12:03 PM - bertagaz

Merge remote-tracking branch 'origin/wip/11972-use-vagrant-in-jenkins' into stable

Fix-committed: #11972, #11979, #11980, #11981, #11006

History

#1 - 11/21/2016 02:56 PM - intrigeri
- Blocked by Feature #11979: Move Vagrant's apt-cacher-ng data to a dedicated disk added

#2 - 11/21/2016 02:57 PM - intrigeri
- Subject changed from Provision a new Vagrant VM at every build to Create and provision a new Vagrant VM for every ISO build

#3 - 11/21/2016 02:58 PM - intrigeri
- Blocks Feature #11981: Delete the Vagrant VM used for an ISO build once it is finished added

#4 - 11/21/2016 03:00 PM - intrigeri
- Description updated

#5 - 11/21/2016 03:01 PM - intrigeri
- Description updated

#6 - 12/02/2016 06:05 PM - bertagaz
- Status changed from Confirmed to In Progress

Applied in changeset aea46312bde1605cd89f079ffe4b1e0af1804621.

#7 - 12/03/2016 09:43 AM - bertagaz
- Assignee set to anonym
- Target version set to Tails_2.9.1
- % Done changed from 0 to 50
- QA Check set to Ready for QA
- Feature Branch set to wip/feature/11980-per-branch-vagrant-build-vm

Implemented in the linked branch.

I've made some bold moves: for example all the build dependencies are now installed in the basebox. This leads to faster VM creation and updates,
but at the cost of longer initial basebox download. The resulting basebox image is 30MB bigger than one with only the security updates. But I think in the end it's better this way: one only download the basebox once only, while the build VM is provisioned each time one build.

One way to test this branch (once #11972 and #11979 are reviewed):

- merge it in stable, making sure #11972 and #11979 are also included.
- Set whatever extproxy in $http_proxy if needed.
- Start rake basebox:create.
- Install the new basebox with:

        cd vagrant && 
        vagrant box add 
        --name tails-builder-amd64-jessie-2016112802_default 
        definitions/tails-builder/tails-builder-amd64-jessie-2016112802.box

• rake build  
• checkout devel && merge stable  
• rake build should fail because your vm was created for stable  
• rake vm:destroy && rake build should work.

I tried to build from a 2.7 tag, but the build failed because of xorriso installation problems. It may be worth to locally build from a new 2.7.1 tag which includes this branch.

Same review policy, if happy, please don't merge this branch. I'll take care of it. We'll also have to decide about baseboxes hosting, but this should probably not block the merge of this branch.

#8 - 12/03/2016 10:49 AM - intrigeri
  - Blocked by Feature #11972: Switch our Jenkins ISO build system to vagrant-libvirt added

#9 - 12/07/2016 02:43 PM - anonym
  - Assignee changed from anonym to bertagaz
  - QA Check changed from Ready for QA to Dev Needed

The following is also about #11979 and its feature branch:

On Sid rake basebox:create is broken:

install-mbr:tails-builder-amd64-jessie-2016112802.qcow2: Probable detection of modern MBR format which is currently incompatible with install-mbr. Installing will probably break Windows installations on this system. Use --force to override.

05/04/2020
Whatever. Let’s only block on Jessie support for now.

The snapshot serial you picked has expired. I don’t want to merge this before we have a solid process that gives some guarantees about the snapshots not expiring before the basebox is retired, like happened now. Regarding retirement, that’s related to how long we want releases to be buildable, especially once we have reproducibility. IIRC we thought six months was good enough.

Any way, for now I just locally used the to 2016120601 snapshot so I could proceed (and I succeeded, in a Jessie VM), but for the next round of review, please upload your .box and make sure the APT snapshot it uses won’t expire soon.

However, provision failed almost immediately when I tried to build from stable (with your branches merged ontop). From setup-tails-builder:

```
tag="$(git --git-dir=/amnesia.git/.git/ describe --tags --exact-match HEAD 2>/dev/null)"
```

This command can fail and hence kill the script (thanks to set -e) so I suggest adding `|| :` to allow failure.

```
if [ ! -z "${tag}" ]; then
```

There’s some strange whitespace between `*` and `]` which leads to a syntax error.

```
if ! grep -qs 'refs/' /amnesia.git/.git/HEAD; then
```

Here you make an incorrect assumption about /amnesia.git -- per the Vagrantfile, it mounts the .git subfolder, not the top-level of the Git repo checkout. In fact, you make this assumption several times in this script, and I have no idea how you managed to get the provisioning to work at the same time as building -- note that build-tails uses /amnesia.git in the other (correct) way, so both cannot possibly work at the same time.

Here I stopped for now, and I haven’t really looked at the rest of the code. I’ll do a full code review once you’ve pushed fixes so provisioning works (and preferably, uploaded a basebox, as I mentioned above).

Ah, but I did notice this problem in passing, in the Vagrantfile:

```
domain.storage :file, :size => '15G', :allow-existing => true, :cache => 'none', :path => 'apt-cacher-ng-data.qcow2'
```

The :path => 'apt-cacher-ng-data.qcow2' part is not valid Ruby, I think. Presumably you want to move the coma like so: :path => 'apt-cacher-ng-data.qcow2'.

```
domain.storage :file, :size => '15G', :allow-existing => true, :cache => 'none', :path => 'apt-cacher-ng-data.qcow2'
```

The :path => 'apt-cacher-ng-data.qcow2' part is not valid Ruby, I think. Presumably you want to move the coma like so: :path => 'apt-cacher-ng-data.qcow2'.

```
```

05/04/2020 5/12
Whatever. Let's only block on Jessie support for now.

FYI the vagrant-libvirt isobuilders will be Stretch.

if ! grep -qs 'ref:' /amnesia.git/.git/HEAD; then

Here you make an incorrect assumption about /amnesia.git -- per the Vagrantfile, it mounts the .git subfolder, **not** the top-level of the Git repo checkout.

That's because the branch for #11972 mounts the top-level Git WC, for reasons I was not able to understand (#11972#note-11); I bet there's another, much better solution to whatever problem this was meant to fix.

---

intrigeri wrote:

Whatever. Let's only block on Jessie support for now.

FYI the vagrant-libvirt isobuilders will be Stretch.

Ok. They won't need to generate baseboxes, so what I said above is not a problem for that at least.

if ! grep -qs 'ref:' /amnesia.git/.git/HEAD; then

Here you make an incorrect assumption about /amnesia.git -- per the Vagrantfile, it mounts the .git subfolder, **not** the top-level of the Git repo checkout.

That's because the branch for #11972 mounts the top-level Git WC
Wow, I somehow missed that this branch was also needed. Sorry! :S

Ok, so this branch also fixes the `path =>` issue, so with the strange whitespace removed, and the `||` I now have a build running! I'll let you know how it goes.

for reasons I was not able to understand (#11972#note-11); I bet there's another, much better solution to whatever problem this was meant to fix.

I actually like it. I was tempted to do it for importing the APT signing key during provisioning, which bertagaz now has implemented.

Unrelated: it just struck me that this ticket will make the caching of wiki builds not work any longer (this doesn't affect Jenkins, but it hits me hard). Well, or maybe they will since you can reuse the same VM if you rebuild the same branch. I'll get back about this, cause I would be extremely sad to have this caching go.

#12 - 12/07/2016 07:06 PM - anonym

I'm not thrilled about the new way of syncing the Tails sources to the work space in build-tails:

```bash
sudo rsync -a --exclude 'vagrant/.vagrant' "/amnesia.git/" "$[WORKSPACE]"
```

This will copy any build artifacts on the host to the builder VM unnecessarily (I guess it doesn't affect Jenkins, but it does affect everyone else). And other state and uncommitted changes are copied too, which perhaps could cause trouble (e.g. broken wiki build). Can't we return to how things were before using git clone + git fetch, which will only touch stuff tracked by Git? Perhaps it's even faster as well.

#13 - 12/08/2016 02:05 PM - anonym

anonym wrote:

Can't we return to how things were before using git clone + git fetch, which will only touch stuff tracked by Git? Perhaps it's even faster as well.

FWIW, this worked fine for me:

```bash
-sudo rsync -a --exclude 'vagrant/.vagrant' "/amnesia.git/" "$[WORKSPACE]"
+if [ ! -d "$[WORKSPACE]" ]; then
  + git clone /amnesia.git/.git "$[WORKSPACE]"
+fi
+cd "$[WORKSPACE]"
+git fetch --tags origin
  sudo chown -R vagrant:vagrant "$[WORKSPACE]"
+cd "$WORKSPACE"
```
But even without that, building works! Yay! But caching of the wiki still doesn't work, which is annoying. Still, I won't block on that but rather commit to fix it when I get sufficiently sick of waiting on wiki builds. :)

So I'll do a code review now or soon. So far, the only remarks from above that are still valid are:

- What I just said above about moving from rsync to git for syncing the sources from the host to the WORKSPACE
- The weird whitespace
- The lack of "|| :

#14 - 12/08/2016 03:54 PM - anonym

Code review:

First, don't forget the three bullets from my previous comment! (BTW, I'm not sure their fixes necessarily belong in this branch, so please verify!)

    aea4631 Get serial from the basebox name, use it in VM creation script.

    -DATE_STAMP="$(date +%Y%m%d)"
    -TARGET_NAME="tails-builder-$(ARCHITECTURE)-$(DISTRIBUTION)-$(DATE_STAMP)"
    +TARGET_NAME=$(grep -Po "tails-builder-$(ARCHITECTURE)-$(DISTRIBUTION)-\d{10}" ../../Vagrantfile)
    +SERIAL=$(echo "$\{TARGET_NAME\}" | grep -Po \"\d{10}\")

I'd prefer if we passed the APT snapshot datestamp as an argument to the script, instead of extracting it from the Vagrantfile -- I rather first generate the basebox, and then update the name and digest in the Vagrantfile.

    f8a0103 Import Tails APT repo signing key.

Thanks for this commit! It has bugging me for a while that we depend on gpg --recv-keys against a key server here.

    5dd2cad Setup APT snapshots in the vagrant builder depending on what we build.

    aea4631 Get serial from the basebox name, use it in VM creation script.

I think this commit should be (possibly partially) reverted (also follow-ups in later commits). I don't understand why we ever want to switch serial for the builder VM. Please clarify!

If I am correct we can actually be so bold that we only activate the security repo. The other repos will remain the same as they were when the basebox was created so activating them will just slow down apt update and waste disk space. Right?

    86961cd Force upgrading with debian-security APT repo activated.

I think we should exclude upgrading at least the kernel. They can take quite some time, and will be completely worthless. Disabling upgrades of the initrd would also be great. Any other type of upgrade that is worthless in a one-boot VM?

One way to achieve this is to pin the exact kernel version we install when we generate the basebox.

    2d300a3 Ship all build dependencies in the basebox.
Now that we do this we can remove the two apt-get ... install from setup-tails-builder -- if there are any updates, we'll install them via apt-get -y dist-upgrade.

Also, I think we should pass --no-install-recommends to our apt-get install:s in postinstall.sh.

#15 - 12/14/2016 08:11 PM - anonym
- Target version changed from Tails_2.9.1 to Tails 2.10

#16 - 01/11/2017 07:37 AM - intrigeri
Note that while reviewing #12081, I expected rake build to automatically get the new basebox and start using it. This was not the case until I run rm -rf vagrant/.vagrant/. I guess that this needs to be fixed (if not done yet) while implementing this ticket.

#17 - 01/11/2017 07:43 AM - intrigeri
- Target version changed from Tails 2.10 to Tails_2.12

#18 - 03/15/2017 02:43 AM - anonym
- % Done changed from 50 to 60
- QA Check changed from Dev Needed to Ready for QA

I think I've got #11979, #11980 and #11980 into a quite nice shape now. I think you should start looking at it, but not merge it. Feel free to comment for all those tickets here only.

I haven't dealt with all concerns in the comments in this ticket, in particular #11980#note-16 seems important, and #11980#note-14 has some interesting stuff.

#19 - 03/15/2017 01:04 PM - anonym
- Feature Branch changed from wip/feature/11980-per-branch-vagrant-build-vm to feature/11980-static-build-env

#20 - 03/15/2017 02:08 PM - bertagaz
- QA Check changed from Ready for QA to Dev Needed

anonym wrote:

I think I've got #11979, #11980 and #11980 into a quite nice shape now. I think you should start looking at it, but not merge it. Feel free to comment for all those tickets here only.

I haven't dealt with all concerns in the comments in this ticket, in particular #11980#note-16 seems important, and #11980#note-14 has some interesting stuff.

Then I guess this ticket can't be set RfQA, and we'll have to do another review round once the remarks in the comments are fixed...
bertagaz wrote:

anonym wrote:

I think I've got #11979, #11980 and #11980 into a quite nice shape now. I think you should start looking at it, but not merge it. Feel free to comment for all those tickets here only.

I haven't dealt with all concerns in the comments in this ticket, in particular #11980#note-16 seems important, and #11980#note-14 has some interesting stuff.

Then I guess this ticket can't be set RfQA, and we'll have to do another review round once the remarks in the comments are fixed...

My idea was that you could review it up to the current HEAD, and when I potentially push more stuff due to the above comments then you review from that commit.

#22 - 03/15/2017 03:35 PM - anonym

- QA Check changed from Dev Needed to Ready for QA

I've gone through all comments on this ticket, and the only potentially relevant thing remaining (as of 328cd810f943df11c3b541ccc5661bab2ae2851b) is:

anonym wrote:

I think we should exclude upgrading at least the kernel. They can take quite some time, and will be completely worthless. Disabling upgrades of the initrd would also be great. Any other type of upgrade that is worthless in a one-boot VM?

I think we should do this, but I guess not block on it. Any opinions? Any implementation ideas?

So, now you can review'n'merge #12017, #11979, #11980 and #11981: let's keep all comments on this ticket, however. You probably should wait with the merge until Jenkins has successfully built from the commit I mention above. Test the shit out of it locally! :) Especially with TAILS_BUILD_OPTIONS="forcecleanup" since that is what I suggest we'll use on Jenkins.

Meanwhile I'll work on #11972.
#23 - 04/20/2017 07:15 AM - intrigeri
- Priority changed from Normal to Elevated
- Target version changed from Tails_2.12 to Tails_3.0~rc1

(The plan is to complete this early in the 3.0 cycle, so it doesn't get in the way of 3.0~rc1 and 3.0 final.)

#24 - 04/28/2017 03:31 PM - bertagaz
- % Done changed from 60 to 100
- QA Check changed from Ready for QA to Pass

anonym wrote:

  anonym wrote:

    I think we should exclude upgrading at least the kernel. They can take quite some time, and will be completely worthless. Disabling upgrades of the initrd would also be great. Any other type of upgrade that is worthless in a one-boot VM?

    I think we should do this, but I guess not block on it. Any opinions? Any implementation ideas?

With what we implemented in #12409, this is not an issue anymore.

So, now you can review'n'merge #12017, #11979, #11980 and #11981; let's keep all comments on this ticket, however. You probably should wait with the merge until Jenkins has successfully built from the commit I mention above. Test the shit out of it locally! :) Especially with TAILS_BUILD_OPTIONS="forcecleanup" since that is what I suggest we'll use on Jenkins.

I think this ticket is ready, it just needs the vagrant system to be deployed on our isobuilders to be closed.

#25 - 05/09/2017 01:57 PM - bertagaz
- Status changed from In Progress to 11

Applied in changeset 79b7f9ca5f09584bcaa4d948bff56ca2d9ffa30a.

#26 - 05/10/2017 10:05 AM - bertagaz
- Assignee deleted (bertagaz)

#27 - 05/23/2017 09:04 AM - intrigeri
- Status changed from 11 to Resolved