

Products



Asked 3 years, 7 months ago Modified 3 years, 7 months ago Viewed 30k times

Log in

Sign up



Users

Companies

COLLECTIVES



0

TEAMS

Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.



Create a free Team

Why Teams?



23







We have a tool which needs to clone several Git repositories for aggregating documentation data. We want to put that tool in a Docker container for easily running it locally and with Jenkins, and enabling reproducibility.

The Git repositories are hosted on a private server requiring authentication with SSH keys. Thus the Docker container must somehow gain access to the SSH keys of the user running the container.

We have a list of constraints:

- 1. we do **not** want to embed SSH keys in the Docker image
- 2. we do **not** want users to build the Docker image. We consider a Dockerfile does not enable reproducibility whereas an already generated Docker image do
- 3. we do **not** want the container to run as the root user
- 4. we want to use the SSH keys of the host user running the container
- 5. parameters can be provided to the command starting the container (-v , -u , ...)

Question: How can we achieve this, if it is possible?



Related:

- <u>Using SSH keys inside docker container</u> (the SSH keys are passed at build time – we want run time)
- Clone private git repo with dockerfile (same problem)

By clicking "Accept all cookies", you agree Stack Exchange can store cookies on your device and disclose information in accordance with our <u>Cookie Policy</u>.

(running as root)

Accept all cookies

Customize settings



Your privacy



1 I'm curious as to why you consider that a Dockerfile does not enable reproducibility. – SiHa Jun 7, 2019 at 9:21

The Dockerfile question aside, I'd have thought that you could simply mount the local user's /home/user/.ssh folder (read-only) into the container. Then doing a git clone git@your.git/repo should use their ssh key. – SiHa Jun 7, 2019 at 9:23

@SiHa See e.g. this or this. A Docker image is a self-sufficient and self-contained snapshot – a Dockerfile is a list of instructions relying on dependencies that can change (other images, host, ...). As for your suggestion: the container's user could not read the host user's keys because of different ownership. – Jim Jun 7, 2019 at 12:00

No reason you couldn't change the membership of the user, I'd have thought. – SiHa Jun 7, 2019 at 12:06

Maybe giving a specific group for host and docker users, and giving this group permission to read the ssh keys? – Vitor Falcão Jun 7, 2019 at 12:34

Add a comment

2 Answers

Sorted by: Highest score (default)

\$



25





+100



You can use something like:

```
echo "git-user:x:$(id -u):$(id -g):Git User:/tmp:/bin/bash" > /tmp/fal
docker run \
    -u $(id -u):$(id -g) \
    -w /tmp \
    -v $HOME/.ssh:/path/to/.ssh \
    -v /tmp/fake_passwd:/etc/passwd \
    --entrypoint sh \
    -it \
    alpine/git

# commands in the container:
```

```
$ export GIT_SSH_COMMAND='ssh -i /path/to/.ssh/id_rsa -o "StrictHos"
$ git clone [path to git repo]
```

This will ensure the container runs with the same UID/GID as the host user, thus being able to read the keys without changing their permissions or using root rights. In details:

- -u \$(id -u):\$(id -g) set the container user to match the host user
- -w /tmp ensure we work in a directory we can write in (we may also mount a volume on which we have read/write permissions or build the image with such directory)
- -v \$HOME/.ssh:/path/to/.ssh mounts the local user SSH key from the host
- --entrypoint sh and -it are specific to alpine/git to have an interactive shell session, you may not need it with your image

Why mount a fake /etc/passwd file?

When you running a linux-based container (such as alpine or debian) with an unknown UID/GID (one which is not present in /etc/passwd), git clone command may result in error with a message such as:

```
Cloning into 'myrepo'...

No user exists for uid 1000
fatal: Could not read from remote repository.
```

By mounting this "fake" passwd file we ensure the OS will recognize the user running the container and allow our git clone command to work. Our password file will look like:

```
git-user:x:1000:1000:Git User:/tmp:/bin/bash
```

Which means roughly:

- git-user exists with UID 1000 and GID 1000
- it's HOME directory is /tmp (it's optional but this directory is writable and avoid some warning from git clone)

By setting /tmp (or another directory which may be created during image build) we ensure we have a writable HOME directory for <code>git-user</code> which will prevent a warning from <code>git clone</code> saying it could not created a .ssh directory

However this may have other side effects if you intend to run different tasks with your container.

Why use GIT_SSH_COMMAND ?

GIT_SSH_COMMAND='ssh -i /path/to/.ssh/id_rsa' will ensure git clone is using our key, but this can be done using ssh-agent as well - see https://serverfault.com/questions/447028/non-interactive-git-clone-ssh-fingerprint-prompt

In the example I use -o "StrictHostKeyChecking=no" **but it may be insecure**, another solution would be to mount a known host file in the container with the git repo server host key and using -o "UserKnownHostsFile=/path/to/KnownHostFile"

ShareFollow

edited Jun 13, 2019 at 8:23

answered Jun 10, 2019 at 13:27



This does work, although cloning will spam Could not create directory '/.ssh' even when the known_hosts file is referenced with UserKnownHostsFile. It's unfortunate that all this feels like a hack – but at this point I expect all the solutions will, especially looking at issues like this. I'm curious to see other solutions though. – Jim Jun 10, 2019 at 15:21

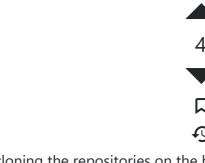
I understand, it's true the fake passwd file is a bit of a hack (I first tried without it but had to because of the issue I mentioned), however for the rest I believe it's a perfectly sane way of using git and ssh. The spam of could not create directory seems like a bug of SSH client - maybe it can be solved by setting a home directory for the user to a writable directory – Pierre B. Jun 11, 2019 at 10:12

I'm unsure how that can be done because at runtime root privileges are required for setting the home directory of a user, including self. And at build time the user is yet not known, so its home cannot be created. – Jim Jun 12, 2019 at 21:15

You may do this by setting a writable directory as home in the fake passwd file, for example: git-user:x:1000:1000:Git User:/tmp:/bin/bash which will have /tmp as home for git-user (you can also create a directory in the image during build and use it). git clone won't complain anymore (and it seems a .ssh/known_hosts file is created in set home dir), I edited answer to mention this – Pierre B. Jun 13, 2019 at 8:17

Related: <u>running git or ssh client in docker as user: No user exists for uid and docker: set running user while launch container.</u> – Jim Mar 5, 2020 at 20:24

Add a comment



Would cloning the repositories on the host machine and mounting the directories in the docker image be ok?

e.g.:

```
git clone github:repo1
git clone github:repo2
...
docker run -v repo1:/path/to/repo1 -v repo2:/path/to/repo2 ...
```

ShareFollow

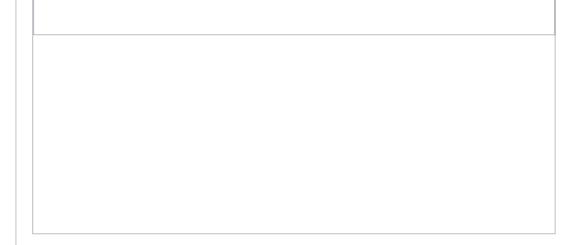
answered Jun 11, 2019 at 15:00



It would not work for a client missing Git for example. That's why we are "dockerizing" our tool, for reproducibility. – Jim Jun 12, 2019 at 21:12

Add a comment

Your Answer



Post Your Answer By clicking "Post Your Answer", you agree to our terms of service, privacy policy and cookie policy

Not the answer you're looking for? Browse other questions tagged git docker ssh-keys or ask your own question.

The Overflow Blog

- Stack Gives Back 2022!
- Commit to something big: all about monorepos (Ep. 527)

Featured on Meta

- 2022 Community-a-thon Recap
- The [shipping] tag is being burninated
- Temporary policy: ChatGPT is banned

Linked

- 461 Using SSH keys inside docker container
- 493 How to mount a single file in a volume
- Clone private git repo with dockerfile
- 52 Inject host's SSH keys into Docker Machine with Docker Compose
- 8 docker: set running user while launch container

Related

- 7867 How do I remove local (untracked) files from the current Git working tree?
- How do I undo 'git add' before commit?
- 25257 How do I undo the most recent local commits in Git?
- 9128 How do I force "git pull" to overwrite local files?
- 19843 How do I delete a Git branch locally and remotely?
- How to determine the URL that a local Git repository was originally cloned from
- 7615 How do I revert a Git repository to a previous commit?
- 11035 How do I rename a local Git branch?
- 2303 How to copy files from host to Docker container?
- 2930 From inside of a Docker container, how do I connect to the localhost of the machine?

Hot Network Questions

- Why is Ctrl-V the Paste shortcut?
- Implement a bag without replacement

What's your best practice as a DM to "protect" your awesome campaign's mystery "against" the Divination spell?

What SF story are they discussing in the book The Coward's Way of War?

Select data from a structured list

more hot questions

Question feed



STACK OVERFLOW

QuestionsHelp

PRODUCTS

Teams Advertising Collectives Talent

COMPANY

AboutPressWork HereLegalPrivacy PolicyTerms of ServiceContact UsCookie SettingsCookie Policy

STACK EXCHANGE NETWORK

TechnologyCulture & recreationLife & artsScienceProfessionalBusinessAPIData

Blog Facebook Twitter LinkedIn Instagram

Site design / logo © 2023 Stack Exchange Inc; user contributions licensed under $\underline{\text{CC BY-SA}}$. rev 2023.1.14.43159