Make our SLE related tooling work with upcoming changes to build.suse.de (2FA and ssh key based authentication) size:M

2022-06-03 10:18 - okurz

Status: Feedback
Priority: Urgent
Assignee: jbaier_cz
Category: Ready

Description

Motivation

IBS is switching to 2FA and ssh key based authentication, see
https://mailman.suse.de/mlarch/SuSE/research/2022/research.2022.06/msg00003.html. We need to ensure our tools work with that.

Acceptance criteria

- AC1: All relevant projects have been updated to support 2FA and/or ssh key based authentication

Suggestions

- Update the ci template shared between qa-maintenance projects
- Relevant repositories/pipelines:
  - https://github.com/openSUSE/qem-bot/
  - https://gitlab.suse.de/qa-maintenance/bot-ng/
  - https://gitlab.suse.de/qa-maintenance/openQABot
- Use existing ssh key from GitLab and add it to IBS

History

#1 - 2022-06-08 12:23 - cdywan

The phrasing is very generic. okurz can you narrow down what tooling needs to be adapted? Or should this be an epic with that as a research task? We can't plan work items when it's unclear what workflows need to be adapted.

#2 - 2022-06-08 17:54 - okurz

cdywan wrote:

The phrasing is very generic. okurz can you narrow down what tooling needs to be adapted?

No, I can't. Identification of which tooling needs adaption is part of the work.

Or should this be an epic with that as a research task? We can't plan work items when it's unclear what workflows need to be adapted.

My assumption is that the effort is limited. Of course if we put our heads together and do find out that it's more effort than workable in a single ticket then we can extend to an epic.

#3 - 2022-06-09 09:24 - tinita

- Subject changed from Make our SLE related tooling work with upcoming changes to build.suse.de (2FA and ssh key based authentication) to Make our SLE related tooling work with upcoming changes to build.suse.de (2FA and ssh key based authentication) size:M

- Description updated

- Status changed from New to Workable

#4 - 2022-06-13 11:18 - mkittler

- Assignee set to mkittler
Ok, so that's what I've gathered so far:

1. Add SSH key `/home/teregen/.ssh/id_rsa.pub` and `qam_automation` in `/home/teregen/.ssh/authorized_keys` (both files are on qam2.suse.de) to https://idp-mfa.suse.de (not https://idp-mfa-test1.suse.de/)
   - When logging in with my personal account I can enroll a public SSH key so that looks already good. I can also enroll a totp token but that doesn't enable me to login at https://buildtest.suse.de/. It accepts my credentials but the totp is rejected with "Error : wrong otp value". Note that the totp works on https://idp-mfa-test1.suse.de/ itself instead (and can be used instead of using the mail token). I hope the SSH key will be sufficient to solve this ticket.
   - It is still strange that the SSH key shows up wrongly when viewing it later. With that I mean the SSH key shown in the row "Info" is just wrong. The same happens when adding the key once more but a different randomly wrong key shows up. Apparently normal.
   - When just pasting the key (without ssh-rsa and without trailing comment) I'm getting a 500 response but then nevertheless an empty sshkey is enrolled. A very well written web application...
2. For the production setup, I suppose I need to login via user https://build.suse.de/users/qa-maintenance
3. Who has credentials and where would a mail with TOOTP end up? asked Heiko Rommel
2. Find out what changes in the OSC config are needed
   - Locally it still asks me to put username and password into oscrc, despite having ssh-agent setup and despite having the SSH key deployed on https://idp-mfa-test1.suse.de/. So I'm still clueless what to do here to make it work. In the mail it sounds like no further configuration would be required but that is apparently not the case. Locally it works by providing user and password. The SSH key is determined automatically but could also be specified via sshkey = id_rsa.pub.
     - It supposedly works to use sshkey = id_rsa.pub as that's apparently the newly introduced option (see https://github.com/openSUSE/osc/blob/0b4158590ce5323028c744cd5ed005652c455d6/NEWS#L19) and judging by error messages one gets when just specifying e.g. sshkey = foo it is searching for files under one's .ssh directory. Still doesn't work for me though. Maybe due to 1.1.2.
     - Note that it also still wants a username and password if sshkey is present. At least the password should no longer be required so something must be wrong.
   - I've been using OSC 0.179 as provided by Tumbleweed.
     - Seems unnecessary as /home/teregen/.ssh/id_rsa.pub exists on qam2.suse.de and that key should be picked up automatically in the same way as it is already started in some steps.
   - To fix qem-bot, we might need to introduce loading a key to same ssh-agent inside the pipeline. In case some software is missing, you can also tweak the image itself: https://build.suse.de/package/view_file/QA:Maintenance/openSUSE-Leap-Container/Dockerfile
3. Ensure all steps using osc on https://gitlab.suse.de/qm-maintenance/gamops/-/blob/master/gitlab/templates.yml have ssh-agent started (in the same way as it is already started in some steps).
4. To fix qem-bot, we might need to introduce loading a key to same ssh-agent inside the pipeline. In case some software is missing, you can also tweak the image itself: https://build.suse.de/package/view_file/QA:Maintenance/openSUSE-Leap-Container/Dockerfile
5. Ensure OSC 0.178 or newer is installed on qam2.suse.de and all containers used in GitLab pipelines
   - Add repo http://download.opensuse.org/repositories/openSUSE::Tools/SLE_12_SP3/ if the necessary
   - Supposedly https://build.suse.de/package/view_file/QA:Maintenance/openSUSE-Leap-Container/Dockerfile is covering all GitLab pipelines

---

*I now also asked on the mailing list because I believe my questions go under on the buildservice channel.

#7 - 2022-06-14 12:23 - toe

mkittler wrote:

(...)

Please see Adrian's mail from 2022-06-13 11:49 CET. Since yesterday, buildtest.suse.de uses the production MFA tokens which are maintained under https://idp-mfa.suse.de (VPN only)

#8 - 2022-06-14 12:30 - mkittler

Adrian has already responded. I've also already testing it locally with my personal account and everything worked. So I'm updating my previous comment.

#9 - 2022-06-14 13:33 - mkittler

- Point 2. should be resolved as well as no further config is required.
- SR to resolve point 3.: https://gitlab.suse.de/qm-maintenance/gamops/-/merge_requests/17
- That leaves point 1., 4. and 5.
Regarding 4.: It looks like qem-bot would handle the 2FA just fine as long as oscrc is configured correctly. At least in my local tests I was able to delete a comment in my home project using the following test code:

```python
from osc import conf
from openqabot.osclib.comments import CommentAPI

apiurl = "https://apitest.suse.de"
conf.get_config(override_apiurl=apiurl)
api = CommentAPI(apiurl)
api.delete("3876782")
```

I also did the opposite check. If I configure a wrong SSH key I get Couldn't load public key /home/martchus/.ssh/id_rsa.pub: No such file or directory. So it definitely reads the SSH key.

So we only need to ensure that the SSH setup is present in all pipelines where qem-bot is running. I assume I need to adjust:


I've created SR. That means there are currently 3 pending SRs:

- [https://gitlab.suse.de/qa-maintenance/qamops/-/merge_requests/17](https://gitlab.suse.de/qa-maintenance/qamops/-/merge_requests/17)
- [https://gitlab.suse.de/qa-maintenance/bot-ng/-/merge_requests/52](https://gitlab.suse.de/qa-maintenance/bot-ng/-/merge_requests/52)
- [https://gitlab.suse.de/qa-maintenance/openQABot/-/merge_requests/95](https://gitlab.suse.de/qa-maintenance/openQABot/-/merge_requests/95)

The pipelines look still good. I suppose we'll have to see whether it continues to work when 2FA actually becomes necessary.

All three [https://gitlab.suse.de/qa-maintenance/qamops/-/merge_requests/17](https://gitlab.suse.de/qa-maintenance/qamops/-/merge_requests/17), [https://gitlab.suse.de/qa-maintenance/bot-ng/-/merge_requests/52](https://gitlab.suse.de/qa-maintenance/bot-ng/-/merge_requests/52), [https://gitlab.suse.de/qa-maintenance/openQABot/-/merge_requests/95](https://gitlab.suse.de/qa-maintenance/openQABot/-/merge_requests/95) merged, please monitor pipelines in these three projects.

Small regression [https://gitlab.suse.de/qa-maintenance/openQABot/-/jobs/1029191](https://gitlab.suse.de/qa-maintenance/openQABot/-/jobs/1029191) caused by missing Gitlab variable SSH_KEY. I added it in the variable definitions (webui) and now the pipeline looks good.
None
To avoid address alert fatigue I'm dropping the "approve incidents" step from GitLab CI.

I now changed BOT_PARAMS to --dry in the approve incidents schedule. The MR was closed.

#28 - 2022-09-05 13:12 - jbaier_cz
- Status changed from Blocked to Feedback
- Assignee changed from cdywan to jbaier_cz

And we are back in business: https://gitlab.suse.de/qa-maintenance/bot-ng/-/jobs/1127130

I managed to confirm that login to https://idp-mfa.suse.de/ is possible (the OTP code will arrive via osd-admins). For some reason, we had to reset the password for the account sle-qam-openqa, the configuration is already updated. I also enrolled the necessary SSH key for the approval job and I also remove the dry parameter, so the bot actually does something. Let's hope that this will hold for some time.