**openSUSE admin - tickets #94375**

**SSH access to code.opensuse.org isn't working**

2021-06-21 15:06 - Pharaoh_Atem

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Pharaoh_Atem</td>
</tr>
<tr>
<td>Category:</td>
<td>Git(lab)/Pagure</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Start date:</td>
<td>2021-06-21</td>
</tr>
<tr>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>% Done:</td>
<td>90%</td>
</tr>
<tr>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
</tbody>
</table>

**Description**

I noticed yesterday that SSH push to code.opensuse.org hosted Git repos wasn't working. I am getting the following error:

```
ngompa@Belldandy-Slimbook ~/S/c/P/osvc21-centoslinux-to-opensuseleap-examples (main)> git push ssh://git@code.opensuse.org/Pharaoh_Atem/osvc21-centoslinux-to-opensuseleap-examples.git
ssh: connect to host code.opensuse.org port 22: Network is unreachable
fatal: Could not read from remote repository.
```

Please make sure you have the correct access rights and the repository exists.

Maurizio also reports that cloning via the SSH address isn't working:

```
mau@tumbleweed:GIT$ git clone ssh://git@code.opensuse.org/xfce/xfce4-branding-openSUSE.git
Cloning into 'xfce4-branding-openSUSE'...
kex_exchange_identification: read: Connection reset by peer
Connection reset by 195.135.221.140 port 22
fatal: Could not read from remote repository.
```

I've checked the VM itself and it looks like sshd_config settings are fine?

```
Match User git #git_user
    AuthorizedKeysCommand /usr/lib/pagure/keyhelper.py "%u" "%h" "%t" "%f"

AuthorizedKeysCommandUser git

Match Address 192.168.47.4,192.168.47.101,192.168.47.102 #proxy
    AllowUsers git
```

Anyone have any idea what's going on here?

**History**

**#1 - 2021-06-21 15:06 - Pharaoh_Atem**

- Private changed from Yes to No

**#2 - 2021-06-22 20:10 - cboltz**

- Assignee set to lrupp

Lars, the comment in the haproxy.cfg says that you should know more about this ;)

**#3 - 2021-06-22 22:03 - lrupp**

cboltz wrote:

```
Lars, the comment in the haproxy.cfg says that you should know more about this ;)
```

Yes, the comment is from me as I did the changes there.

Simple answer: I was asked by SUSE-IT Security to close the port - and I agree with them that this service on 3 different IP addresses is not needed.
More complex: as SUSE is still responsible for the IP-range, SUSE-IT is monitoring and scanning actively for changes and potential security risks. This will happen in a more regular base starting in the next weeks.

I have to admit that my action sounds a bit unfair in the first run, but I was somehow 'elected' by SUSE-IT Security as contact person for openSUSE related infra topics - as there was/is currently nobody else inside SUSE who wants to do it. As I'm volunteering since years for openSUSE and build up a big stack of the current infra in the past, I guess it was just logical for them (and me) to contact me directly instead of trying to figure out via (for them so far unknown) mailing lists, IRC or Matrix or Forum or Discord or ... channels, whom to contact in special cases. I agreed with them that I will stay their primary contact for openSUSE related topics and will try my best to secure our community infrastructure. I will try to act as proxy under normal conditions, but I have to admit that their request about this "telnet port" was a bit demanding. Might be that their scanner classified this port (not the service) as very high risk (or because they were themselves audited at that time)?...

Anyway: I have to admit that I was surprised when I was confronted with the list of open ports in the opensuse.org ranges and agree with SUSE-IT, that we are not doing best practice here. Looks like our open minded "those, who do, decide" Mantra is not good when it comes to security.

While an SSH behind a Telnet port is not a high risk, it's another open port on three public IP addresses (and attack vector) that can easily be avoided. As there was no documentation available in the wiki or in salt about the urgent need for this port (and I also found out that the machine is neither monitored nor has the latest security updates installed) I agree with IT-Security that we should look for better alternatives.

Solution: We have openVPN for incoming traffic up and running. Please use this instead.

Regards,
Lars

PS: I initially tried to explain that it's "just SSH on a special port, even with 'prohibit-password' ('without-password' is deprecated, btw) config", but with no luck. To reduce the overall stress-level during that time and as I also do not really see the reason for this open port, I decided to disable the port at 2021-06-15 and left a note in the config and on IRC (might be freenode or libera, I have to admit that I don't remember which network).

#4 - 2021-06-22 22:20 - Irupp
Pharaoh_Atem wrote:

```bash
ngompa@Belldandy-Slimbook ~/S/c/P/osvc21-centoslinux-to-opensuseleap-examples (main)> git push ssh://git@code.opensuse.org
:Pharaoh_Atem/osvc21-centoslinux-to-opensuseleap-examples.git
ssh: connect to host code.opensuse.org port 22: Network is unreachable
fatal: Could not read from remote repository.
```

This is, btw, an interesting setup:

- accept all external traffic via IPTables rules from 195.135.221.140 (note: no IPv6!) and redirect them from port 22 to port 23
- via haproxy from port 23 to 192.168.47.84, port 22

I know that the sshd on the local machines (anna/elsa) was blocking you from using the port directly. The sshd there is "last resort" for SUSE-IT, if something goes wrong with the openVPN on scar. For this, the firewall rules only allow connections to port 22 from the SUSE IP-ranges. But your generic IPTables rule now blocks all traffic to port 22 on 195.135.221.140 anyway. Luckily, nobody needed this "last resort" fallback ...

Suggestion: as IT-Security is now happy with the quick reaction and I owe you something for my quick, uncoordinated action (sorry for this) - what about moving pagure, aka code.opensuse.org, out of the infra.opensuse.org network and equip it with an own pair of public IPs? - Would that be an acceptable "sorry" for you?

That way, we could leave anna/elsa as proxy and "last resort", while we can build up some special barricades (external ssh only allowed for the user git and surrounded with apparmor as example) for pagure on dedicated IPs... (while - the sshd on the infra-network could stay as it is).

#5 - 2021-06-22 22:28 - Pharaoh_Atem

If it can be set up to be managed by our config management, that's fine with me. As for why it wasn't applying the latest updates, I don't know why that would be the case. It's managed by Salt and I just kind of expect the Salt master to do that...

#6 - 2021-07-19 08:54 - Irupp

- Status changed from New to Closed
- % Done changed from 0 to 100

Pharaoh_Atem wrote:

If it can be set up to be managed by our config management, that's fine with me. As for why it wasn't applying the latest updates, I don't know why that would be the case. It's managed by Salt and I just kind of expect the Salt master to do that...

Expecting something to happen magically seems to be a new Religion... ;)

At least for this machine (and many others), I can proof that this is not the case and updates are not installed automatically. Please either change this in Salt - or install the updates manually...
Regards,
Lars

#7 - 2021-07-19 12:52 - Pharaoh_Atem
Irupp wrote:

Pharaoh_Atem wrote:

If it can be set up to be managed by our config management, that's fine with me. As for why it wasn't applying the latest updates, I don't know why that would be the case. It's managed by Salt and I just kind of expect the Salt master to do that...

Expecting something to happen magically seems to be a new Religion... ;-) 

No. It makes no sense to use configuration management that has an agent if we can't apply automatic update security policy.

At least for this machine (and many others), I can proof that this is not the case and updates are not installed automatically. Please either change this in Salt - or install the updates manually...

Well, I applied updates manually but now I have to pick a time to reboot the box so the new kernel takes effect. I guess I'll have to see if it's even technically possible to do automatic updates through Salt, since apparently that's not a thing on our boxes.

(At work, we use Puppet and that definitely does it.)

#8 - 2021-07-19 19:54 - cboltz
- Status changed from Closed to New

In theory the updates get installed by suse-online-update.timer.

In practise, suse-online-timer (and zypper) will refuse to work if there are conflicts - which makes sense, but should[tm] also cause an alert somewhere[tm]. (Sadly systemd timers don't send out mails on error, like cron does.)

(Off-topic: It seems pagure was updated, therefore I'll pick an unrelated example - on moodle.i.o.o there's a file conflict for /usr/sbin/clamav-milter between the installed clamav-milter package and the clamav package from the update repo which prevents the automated updates. Reported as https://bugzilla.opensuse.org/show_bug.cgi?id=1188482. Since I was already logged in, I updated everything except clamav. Oh, and I did the initial(!) highstate on that VM :) I also wonder why clamav is installed/needed on moodle.i.o.o.)

(Off-topic once more - some VMs answer a zypper lu with a request to add a new signing key for Repository: Update repository with updates from SUSE Linux Enterprise 15 - and that also blocks installing updates. This affects kubic, metrics and mirrordb2.)

That said - AFAIK the SSH port for code.o.o is still no reopened, therefore I'll reopen this ticket.

#9 - 2021-07-19 20:15 - Irupp
- Status changed from New to Feedback
- Assignee changed from lrupp to Pharaoh_Atem

cboltz wrote:

In theory the updates get installed by suse-online-update.timer.

In practise, suse-online-timer (and zypper) will refuse to work if there are conflicts - which makes sense, but should[tm] also cause an alert somewhere[tm]. (Sadly systemd timers don't send out mails on error, like cron does.)

One of the reasons, why we have additional monitoring for this.
It just does not help, if nobody looks at the monitoring...

I also wonder why clamav is installed/needed on moodle.i.o.o.)

clamav is needed, because people can upload files on moodle. These files (presentations, images, videos) should be scanned before offered back to users.

(Off-topic once more - some VMs answer a zypper lu with a request to add a new signing key for Repository: Update repository with updates from SUSE Linux Enterprise 15 - and that also blocks installing updates. This affects kubic, metrics and mirrordb2.)

I discussed this with maintenance today: looks like we ran into an issue because we upgraded the machines already in the beta-phase of Leap 15.3. Normally, all machines should have this key integrated with one of the latest updates for 15.2 - just our machines don't as they were not 15.2 any
more when this update was released.
But I'm currently going through the machines one by one and fix the problem manually (also installing the latest kernel update on this way).

That said - AFAIK the SSH port for code.o.o is still no reopened, therefore I'll reopen this ticket.

It's not so much about re-opening the SSH port: it's more about providing an external IP for this machine (including an open, secured SSH port).
I did not check the latest status of this ticket, but IMHO I set the status to feedback, when adding comment #4, which included my question.

Regards,

Lars

#10 - 2021-07-20 01:03 - Pharaoh_Atem
Irupp wrote:

Pharaoh_Atem wrote:

```
ngompa@Belldandy-Slimbook ~/S/c/P/osvc21-centoslinux-to-opensuseleap-examples (main)> git push ssh://git@code.opensuse.org
/Pharaoh_Atem/osvc21-centoslinux-to-opensuseleap-examples.git
ssh: connect to host code.opensuse.org port 22: Network is unreachable
fatal: Could not read from remote repository.
```

This is, btw, an interesting setup:

- accept all external traffic via IPTables rules from 195.135.221.140 (note: no IPv6!) and redirect them from port 22 to port 23
- via haproxy from port 23 to 192.168.47.84, port 22

I know that the sshd on the local machines (anna/elsa) was blocking you from using the port directly. The sshd there is "last resort" for SUSE-IT, if something goes wrong with the openVPN on scar. For this, the firewall rules only allow connections to port 22 from the SUSE IP-ranges. But your generic IPTables rule now blocks all traffic to port 22 on 195.135.221.140 anyway. Luckily, nobody needed this "last resort" fallback ...

Suggestion: as IT-Security is now happy with the quick reaction and I owe you something for my quick, uncoordinated action (sorry for this) - what about moving pagure, aka code.opensuse.org, out of the infra.opensuse.org network and equip it with an own pair of public IPs? - Would that be an acceptable "sorry" for you?

That way, we could leave anna/elsa as proxy and "last resort", while we can build up some special barricades (external ssh only allowed for the user git and surrounded with apparmor as example) for pagure on dedicated IPs... (while - the sshd on the infra-network could stay as it is).

Either solution is fine. We previously already did the second solution you mentioned. That's why only the git user works outside of the infra network.

#11 - 2021-09-07 19:34 - lrupp
- Status changed from Feedback to In Progress
- % Done changed from 100 to 80

pagure01.infra.opensuse.org now has:

```
3: external: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 52:54:00:c8:6e:bb brd ff:ff:ff:ff:ff:ff
inet 195.135.221.144/25 brd 195.135.221.255 scope global external
   valid_lft forever preferred_lft forever
inet6 2001:67c:2178:8::144/64 scope global
   valid_lft forever preferred_lft forever
inet6 fe80::5054:ff:feec:6ebb/64 scope link
   valid_lft forever preferred_lft forever
```

- sshd config is adjusted (not in Salt, yet)
- firewall is up and running (the external interface only allows sshd so far)
- package dehydrated is installed
- package dehydrated-nginx is installed (and configured locally in all nginx vhosts - not in Salt, yet)

ToDo:

- finally configure firewall (include ports 80,443/tcp)
- configure dehydrated (Let's encrypt)
- configure the NGINX vhosts to provide SSL
- start monitoring the machine and services

#12 - 2021-11-04 08:36 - bmwiedemann

https://gitlab.infra.opensuse.org/infra/salt/-/merge_requests/512

2022-03-13 4/5
done:
finally configure firewall (include ports 80,443/tcp) - not in salt?
configure dehydrated (Let's encrypt)
configure the NGINX vhosts to provide IPv6
configure the NGINX vhosts to provide SSL
todo:
add monitoring
configure http->https redirect in nginx
switch DNS to the :144 IPs

#13 - 2021-11-04 10:06 - bmwiedemann
- % Done changed from 80 to 90
done:
switch DNS to the :144 IPs (ev.o.o, pages.o.o, releases.o.o are all CNAMEs to code.o.o now)
configure http->https redirect in nginx

#14 - 2021-11-04 10:12 - SchoolGuy
I can confirm that SSH access indeed works from the internal network again.

```
[11:10:56] enno@bussybox /home/enno/Sources/Other/opensuse-infra-salt (1)
> ssh git@code.opensuse.org
The authenticity of host 'code.opensuse.org (2001:67c:2178:8::144)' can't be established.
ED25519 key fingerprint is SHA256:KSXBssrILtPLO3xNeVl1qKu9KSCJhZLJ9+oYkm2OXBI.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:92: 2001:67c:2178:8::144
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'code.opensuse.org' (ED25519) to the list of known hosts.
PTY allocation request failed on channel 0
Welcome SchoolGuy. This server does not offer shell access.
Connection to code.opensuse.org closed.
```