openQA Infrastructure - action #62666

Move openqa.opensuse.org into opensuse private network

2020-01-24 19:46 - lrupp

Status:	New	**Start date:**	2020-01-24
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	future		

Description

Dear openQA admins

We are currently working towards a better separation of SUSE and openSUSE machines. This should finally allow more community contributors to be able to jump in and either help with the current infrastructure or deploy and develop new stuff - independent from any SUSE influence.

There are just a few machines left to finish this migration - and your openQA setup is one of it.

So it like to ask if you could consider to move your current admin machine (ariel) from the "SUSE owned" private network 192.168.254.0/24 into the "openSUSE Heroes owned" network 192.168.47.0/24?

Details:

Current situation:

- 192.168.254.15 is the current IP of your host in this network
- traffic to your webservice https://openqa.opensuse.org/ gets routed via a HAproxy pair from the internet to this interface
- your machine currently reaches out to other networks ("the internet") via a gateway in this network
- you access this machine (and the machines behind it) via a port forwarding rule

New, proposed situation:

1. 47.78 will be the new IP of your host in the new network (this might change if you wait too long, but don't worry, we have enough IP addresses at the moment ;-)
2. traffic to your webservice https://openqa.opensuse.org/ gets routed via another HAproxy pair from the internet to this interface
3. your machine will reach out to other networks ("the internet") via another gateway in this network
4. you access this machine (and the machines behind it) via a dedicated openVPN, which is reachable from everywhere

Especially the last point might be interesting for you, as all the others are more or less just cosmetic.

This openVPN is the "openSUSE heroes" openVPN, which has in general nothing to do with anything you might currently use. The openSUSE Heroes try to have security in mind with everything they do - and therefor decided to trust only themselves and their loved distribution. So they setup an own authentication provider and a this dedicated VPN to combine security, maintainability and effectiveness. The result are dedicated accounts for everyone who works on openSUSE related infrastructure - while including the ability to work from wherever he is at the moment. All you need is your account and the openVPN certificates for this. If you agree to get switched, I currently see two possible solutions to work on the infrastructure for openQA:

1. use a jumphost, which has to be inside the SUSE network
2. get dedicated accounts and VPN credentials and use them

Both options might be used in parallel (while - from a security point - only using the 2nd option would be preferred), which hopefully will not become too complicated for you.

Benefit: if there will be community members, who like to help and work on openQA, they could easily be allowed to do so.

Alternatively, you can decide to "stay on the SUSE side", which will imply no change of your current workflows. You might be the only openSUSE infrastructure project staying under SUSE-IT umbrella in this case - but this option clearly exists.

With kind regards,
Lars *on behalf of the openSUSE heroes*

PS: I tried to add everyone as "watcher" to this ticket, who has currently an account on ariel. I clearly missed some and apologize for

this, but I could not really figure out everyone's "ariel login" <-> "bugzilla login" mapping.

History

#1 - 2020-01-24 20:13 - dimstar

Just my first thought:

you have seen that ariel also has an interface into 192.168.7.0/24, to directly reach OBS backends? (eth2) Is that interconnect from the heroes network into the actual SUSE infra considered and 'acceptable'?

#2 - 2020-01-24 20:37 - lrupp

dimstar wrote:

> you have seen that ariel also has an interface into 192.168.7.0/24, to directly reach OBS backends? (eth2) Is that interconnect from the heroes network into the actual SUSE infra considered and 'acceptable'?

Yes, it is. This is the so called "publisher network", which is also available to pontifex.infra.opensuse.org aka download.opensuse.org. ...and this machine is in the heroes network since a long time (2 years?) already.

#3 - 2020-01-24 20:40 - okurz

lrupp wrote:

> […] If you agree to get switched, I currently see two possible solutions to work on the infrastructure for openQA:
>
> 1. use a jumphost, which has to be inside the SUSE network
> 2. get dedicated accounts and VPN credentials and use them
>
> Both options might be used in parallel (while - from a security point - only using the 2nd option would be preferred), which hopefully will not become too complicated for you.

In general I am in favor of option 2. I would be happy to give trusted, non-SUSE persons access to a ressource why by name clearly belongs to openSUSE. Thank you for investing the effort to also find all relevant persons now as ticket watchers. Following your proposal I think it is feasible if everyone still interested in having access requests an openSUSE heroes VPN access, some have it already, e.g. me. I guess potentially a "jumphost" could be kept in parallel for a transition period if necessary.

#4 - 2020-01-24 21:01 - lrupp

okurz wrote:

> Following your proposal I think it is feasible if everyone still interested in having access requests an openSUSE heroes VPN access, some have it already, e.g. me.

Requesting a openSUSE heroes account/VPN is normally done via email to admin@opensuse.org

I would shorten that, if either everyone who wants just adds a comment here - or someone gives me a list of those who volunteer.

#5 - 2020-01-27 06:20 - SLindoMansilla

lrupp wrote:

> okurz wrote:
>
> > Following your proposal I think it is feasible if everyone still interested in having access requests an openSUSE heroes VPN access, some have it already, e.g. me.
>
> Requesting a openSUSE heroes account/VPN is normally done via email to admin@opensuse.org
>
> I would shorten that, if either everyone who wants just adds a comment here - or someone gives me a list of those who volunteer.

I don't have an openSUSE VPN account, but I would like to have it.
Until now, I was using ariel as my jump host to openSUSE network.
Should I then request it via admin@opensuse.org?

#6 - 2020-01-27 08:29 - okurz

SLindoMansilla wrote:

> lrupp wrote:
>
> > okurz wrote:
> >
> > > Following your proposal I think it is feasible if everyone still interested in having access requests an openSUSE heroes VPN access, some have it already, e.g. me.
> >
> > Requesting a openSUSE heroes account/VPN is normally done via email to admin@opensuse.org
> >
> > I would shorten that, if either everyone who wants just adds a comment here - or someone gives me a list of those who volunteer.
>
> I don't have an openSUSE VPN account, but I would like to have it.
> Until now, I was using ariel as my jump host to openSUSE network.
> Should I then request it via admin@opensuse.org?

As suggested by lrupp everyone with a "vpn4me plz" comment here should suffice

#7 - 2020-01-27 08:38 - dheidler

vpn4me plz - even though I would like to keep the jumphost in parallel as it doesn't require me to setup vpn when I'm in the suse network.

#8 - 2020-01-27 08:46 - andriinikitin

vpn4me

#9 - 2020-01-27 08:59 - cdywan

vpn4me plz

#10 - 2020-01-27 15:46 - mkittler

vpn4me plz

#11 - 2020-01-28 09:54 - tinita

vpn4me plz

#12 - 2020-04-30 16:09 - lrupp

- Checklist set to [x] anikitin, [ ] cdywan, [ ] dheidler, [x] dimstar, [ ] mkittler, [ ] SLindoMansilla, [ ] tinita, [x] okurz

Update:

1. ariel is now reachable also via

```
ssh -p 2213 gate.opensuse.org
```

This should obsolete the internal way to access ariel. So please do NOT use proxy-opensuse any longer. We will shut down this old interface in the next days, to allow access to ariel for community members.

2. VPN accounts will be created during the next days. With point 1, there is not need to hurry here. But: once we equipped everyone in the list above successfully with an account, we will shut down the SSH port forwarding from 1 to increase security. So please check, if you have scripts or transfers running that will not work any longer, once we finally only allow VPN access to the machine.

VPN status: see checklist. Please ping here, if I forgot someone.

#13 - 2020-04-30 17:07 - favogt

vpn4me plz

I use it mainly for debugging issues in running tests over VNC, a privilege which I hope can be used by a wider set of people in the future.

#14 - 2020-04-30 20:55 - okurz

lrupp wrote:

> […] we will shut down the SSH port forwarding from 1 to increase security. So please check, if you have scripts or transfers running that will not work any longer, once we finally only allow VPN access to the machine.

One thing came to mind. I am running some scripts for example in a gitlab CI pipeline on gitlab.suse.de, e.g. https://gitlab.suse.de/openqa/auto-review/pipelines . Done properly these scripts *would* rely on the external API accessible over https however for

some statistics and monitoring currently I am still using ssh into o3 to access the database with read-only access. If you do not have a good idea how to keep that connected I think would need to find a better way, just saying :)

#15 - 2020-05-09 17:44 - okurz

After o3 is (temporarily?) available over gate.opensuse.org I changed sshd to not allow root anymore with PermitRootLogin no and installed and enabled "sshguard" to block off some malicious login attempts.

#16 - 2020-07-29 07:12 - okurz

- Priority changed from Normal to Low

#17 - 2020-10-22 13:36 - okurz

- Target version set to Ready

#18 - 2020-10-22 19:12 - okurz

- Target version changed from Ready to future

As o3 is reachable from the outside with #62666#note-12 we already benefit and I can live with the current situation for longer and wait for e.g. lrupp to follow up with the next steps at any later time.

#19 - 2020-10-23 07:28 - ybonatakis

vpn4me plz

On Thu, 2020-10-22 at 19:12 +0000, redmine@opensuse.org wrote:

> [openSUSE Tracker]
> Issue #62666 has been updated by okurz.
>
> Target version changed from Ready to future
>
> As o3 is reachable from the outside with #62666#note-12 we already
> benefit and I can live with the current situation for longer and wait
> for e.g. lrupp to follow up with the next steps at any later time.
>
> ---
>
> action #62666: Move openqa.opensuse.org into opensuse private network
> https://progress.opensuse.org/issues/62666#change-339508
>
> - Author: lrupp
> - Status: New
> - Priority: Low
> - Assignee:
> - Category:
>
> ## * Target version: future
>
> Dear openQA admins
>
> We are currently working towards a better separation of SUSE and
> openSUSE machines. This should finally allow more community
> contributors to be able to jump in and either help with the current
> infrastructure or deploy and develop new stuff - independent from any
> SUSE influence.
>
> There are just a few machines left to finish this migration - and
> your openQA setup is one of it.
>
> So it like to ask if you could consider to move your current admin
> machine (ariel) from the "SUSE owned" private network
> 192.168.254.0/24 into the "openSUSE Heroes owned" network
> 192.168.47.0/24?
>
> Details:
>
> Current situation:
>
> - 192.168.254.15 is the current IP of your host in this network
> - traffic to your webservice https://openqa.opensuse.org/ gets routed via a HAproxy pair from the internet to this interface
> - your machine currently reaches out to other networks ("the internet") via a gateway in this network
> - you access this machine (and the machines behind it) via a port forwarding rule

New, proposed situation:

1. 47.78 will be the new IP of your host in the new network (this might change if you wait too long, but don't worry, we have enough IP addresses at the moment ;-)
2. traffic to your webservice https://openqa.opensuse.org/ gets routed via another HAproxy pair from the internet to this interface
3. your machine will reach out to other networks ("the internet") via another gateway in this network
4. you access this machine (and the machines behind it) via a dedicated openVPN, which is reachable from everywhere

Especially the last point might be interesting for you, as all the
others are more or less just cosmetic.

This openVPN is the "openSUSE heroes" openVPN, which has in general
nothing to do with anything you might currently use. The openSUSE
Heroes try to have security in mind with everything they do - and
therefor decided to trust only themselves and their loved
distribution. So they setup an own authentication provider and a this
dedicated VPN to combine security, maintainability and effectiveness.
The result are dedicated accounts for everyone who works on openSUSE
related infrastructure - while including the ability to work from
wherever he is at the moment. All you need is your account and the
openVPN certificates for this. If you agree to get switched, I
currently see two possible solutions to work on the infrastructure
for openQA:

1. use a jumphost, which has to be inside the SUSE network
2. get dedicated accounts and VPN credentials and use them

Both options might be used in parallel (while - from a security point

- only using the 2nd option would be preferred), which hopefully will not become too complicated for you.

Benefit: if there will be community members, who like to help and
work on openQA, they could easily be allowed to do so.

Alternatively, you can decide to "stay on the SUSE side", which will
imply no change of your current workflows. You might be the only
openSUSE infrastructure project staying under SUSE-IT umbrella in
this case - but this option clearly exists.

With kind regards,
Lars *on behalf of the openSUSE heroes*

PS: I tried to add everyone as "watcher" to this ticket, who has
currently an account on ariel. I clearly missed some and apologize
for this, but I could not really figure out everyone's "ariel login"
<-> "bugzilla login" mapping.

#20 - 2020-10-23 07:39 - okurz

There is no VPN. And please avoid lengthy unedited quotes which make the comments harder to read.

#21 - 2021-03-16 06:43 - SLindoMansilla

- Checklist set to [x] SLindoMansilla