openSUSE admin - communication #101851

2021-12-07 19:00 UTC: openSUSE Heroes meeting December 2021

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
<th>Start date</th>
<th>2021-11-02</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
<td>Due date</td>
<td></td>
</tr>
<tr>
<td>Assignee</td>
<td>opensuse-admin</td>
<td>% Done</td>
<td>100%</td>
</tr>
<tr>
<td>Category</td>
<td>Event</td>
<td>Estimated time</td>
<td>0.00 hour</td>
</tr>
</tbody>
</table>

**Description**

Where: https://meet.opensuse.org/heroes
When: 2021-12-07 19:00 UTC / 20:00 CET
Who: The openSUSE Heroes team and everybody else!

**Topics**

see/use checklist

**History**

#1 - 2021-11-02 20:39 - cboltz
- Private changed from Yes to No

#2 - 2021-11-11 07:52 - lrupp

**Status updates**

**Updates/Upgrades**

- https://moodle.opensuse.org/ -> 3.11.4 (+ DeviceDetectorCache plugin)
- https://survey.opensuse.org/ -> 5.2.1 5.2.4
- https://gitlab.infra.opensuse.org/ -> 4.14.24 4.15.0 4.15.2
- https://beans.opensuse.org/matomo/ -> 4.6.1 (+ two plugin updates)
- https://monitor.opensuse.org/icingaweb2/ -> icinga2 2.13.2, re-enabled Grafana graphs inside IcingaWeb

**Gitlab**

Enabled the automatic de-activation of dormant users.

- Dormant users are automatically de-activated after 90 days of inactivity.
- Users can reactivate their account by signing in.

**JeOS image (for Leap 15.3)**

- Update to 0.4.1:
  - add/change sysctl settings:
    - do not use the privacy extension, we disabled it anyway: net.ipv6.conf.default.use_tempaddr=0 -> disable_ipv6_autoconf.conf
    - make it easier to allow to disable/enable route verification on all interfaces via net.ipv4.conf.all.rp_filter -> rp_filter.conf
    - Disable response to broadcasts. You don’t want yourself becoming a Smurf amplifier: net.ipv4.icmp_echo_ignore_broadcasts=1 -> ignore_broadcasts.conf
  - added new nrpe check definitions:
    - check_external.cfg
    - check_private.cfg
    - check_apache_status.cfg
    - check_connections.cfg
    - check_cpi_stats.cfg
    - check_partition_var.cfg
    - check_ntp.cfg
    - check_logrotate_status.cfg
    - check_iostat_vdb.cfg
    - check_mysql.cfg
    - check_rsyslog.cfg
    - check_running_kernel.cfg
    - check_eth1.cfg They are covering some defaults of the new monitoring setup.
  - added udev rules to rename eth0 to private
  - adjust /root/bin/initial_setup.sh

2022-03-13
follow the renaming
• add interactive mode for people, that need it
• add the IP of the remote syslog server in /etc/hosts, as it might happen, that the DNS resolution comes up too late for rsyslog
• install additional packages:
  • bzip2 (needed by some scripts for tar.bz2 files)
  • xfsprogs (to create/handle xfs filesystems)
• switch from EFI boot mode to legacy boot (saves some space on the root disk of the VM. EFI is not really needed there atm.)
• enforced to clean-up config.sh from deprecated values
  • moved /etc/hosts modification from config.sh to initial_setup.sh
• use releasever variable instead of hardcoded Leap version in zypper repositories, which makes an upgrade easier
• remove check_mk from xinetd: not needed/used any longer
• be a bit more verbose in config.sh: makes debugging easier
• install nnd activate umad and tuned for performance tuning
• use systemd to enable/disable services, as baseInsertService and baseRemoveService seem not to work reliably at the moment
• disable a couple of (for a VM) unneeded services:
  • IPv4 & IPv6 DHCP
  • Network nanny
  • Raid/mdadm checks
  • lvm2 services
  • battery check timer

Adjusted our virtual machine testing wiki page, to follow the latest image changes.

SSL Configuration changes

As CVE-2002-2001 allows an attacker to DoS our SSL endpoints, I disabled Diffie-Hellman Epheremal key exchange (DHE). As this was one of the weakest ciphers that our SSL servers supported, we potentially lost only very old clients (like Safari <= 8).

Have a look at https://www.ssllabs.com/ssltest/analyze.html?d=www.opensuse.org&latest for details. We are meanwhile rated A+ :-)

Fixed Security problem on paste.o.o

Michal Hrusecky thankfully fixed a XSS security issue in https://paste.opensuse.org/ today (2021-12-07). Lars asked, if he wants to migrate the service into the openSUSE heroes infrastructure: he agreed, but want to upgrade his application first, before doing so.

External IP for code.opensuse.org

Worked a bit on the external IP part for https://code.opensuse.org/:

• dehydrated setup beautified (to be ready for Salt)
• nginx SSL settings adjusted to be "A+ conform"
• services (xinetd) bond to internal interfaces

Security scans

As we have meanwhile an internal openVAS security scanner, Lars runs scans inside the internal network from time to time. Additional people with access to the instance:

• cboltz
• pjessen

For most important issues, Lars opened/opens issues here in progress.o.o and tries to assign these tickets to the Admins of the affected servers directly (if otherwise, otherwise Group opensuse-admin is default).

Most interesting at the moment might be #102599, as it's currently not clear, if jQuery is still in use at all?

#3 - 2021-12-05 19:16 - cboltz
• Checklist item [] next meeting - Jan 4th or move to Jan 11th? added

#4 - 2021-12-07 20:59 - cboltz
2021-12-07 heroes meeting

jitsi:

• test package is building
• test installation will probably be updated next week
• meet.o.o can currently only have SUSE admins because it's used for SUSE-internal meetings
• meet-test.o.o server can have community admins (use one of the *.infra.o.o VMs as jump host for ssh login)

status reports:
we have membership management again (phpMyAdmin)

helios update prepared, waiting for a review of the salt MR

Mirrorcache will implement a redirect in the future which will redirect the user to a more local mirrorcache instance to make subsequent requests faster

Notes from Lars: https://progress.opensuse.org/issues/101851#note-2 - TODO: JeOS changes need to also go into salt

Notes from Per on the mailinglist:
https://lists.opensuse.org/archives/list/heroes@lists.opensuse.org/message/2HEUWCOGLHREQ6ZS5VSHKNJDWLUKKLA/

Neal will try to fix the 500s when creating a new issue on code.o.o

Bernhard will try to find the ticket about the jenkins for openSUSE: https://progress.opensuse.org/issues/98268

IRC/matrix bridge is broken, https://progress.opensuse.org/issues/103620

datacenter move planned for April, we should have backup instances of *.o.o in Provo or at QSC to avoid downtime

backup server is ready - and waiting for admins to back up their stuff. Please open a ticket, if you want to join the “backup party”

openSUSE Infrastructure Contributor Agreement:

- we base on trust
- should include the common openSUSE principles/guidelines
- we can not require an openSUSE hero to be an openSUSE member - as they just earn the credits to become a member by working as openSUSE hero - but we can ask to follow the member guidelines in general

next meeting:

- will be moved by a week to Jan 11th

#5 - 2022-02-09 17:43 - lrupp

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