Cronology

Fri, 21 Sep 2016 16:15:05 +0200:
EGI CSIRT alert 'CRITICAL' risk - gridsite impersonation vulnerability [EGI-SVG-2016-11476]. (cfr. https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2016-11476).
Affected mentioned services are: DPM, LFC, FTS, WMS. <<Cream CE turns out not to be affected.>>

No action is taken, as none of the mentioned services belongs to farming.

Fri, 30 Sep 2016 14:57:05 +0200:
Alert from EGI CSIRT notifies a number of WNs affected by the critical vulnerability of canl-c library security patch on the farm.

Fri, 30 Sep 2016 16PM:
canl-c library was updated to latest version on WNs and CREAM-CEs

Sat, 1 Oct 2016 05:17:00 GMT:
ticket from LHCb "All pilots Failed at INFN-T1"
(https://ggus.eu/index.php?mode=ticket_info&ticket_id=124174)

Sat, 1 Oct 2016 14:00 GMT:
Investigation started.

- Simple direct job submission to all the CEs works
- Jobs are dispatched to the WN, however their homedir is not created.
- Test Submission through glite WMS fails.
- Related messages in the CE log files report:
    - Cannot move ISB...
    - Problem to detect the lifetime of the proxy …
    - No such file or directory (No credentials found.)

  Other error messages are about PUT_DELEGATION failures

Actions taken
As the problems started after upgrading the canl-c library on the CEs, and all the CEs exhibit the same faulty behaviour, decision is taken to revert the upgrade on one CEs (ce08-lcg.cr.cnaf.infn.it). After a while the number of errors "Problem to detect the lifetime of the proxy" disappears, thus confirming the idea that downgrading the canl-c library to the previous version solves the problems.
[root@quattorsrv ce]# wassh -f ce 'grep "Problem to detect the lifetime of the proxy" /var/log/cream/glite-ce-cream.log| tail -1' | cut -c -35
ce01-lcg: 01 Oct 2016 22:51:57,281
ce04-lcg: 01 Oct 2016 22:52:29,392
ce05-lcg: 01 Oct 2016 22:52:05,900
ce06-lcg: 01 Oct 2016 22:52:33,140
ce07-lcg: 01 Oct 2016 22:52:06,173
ce08-lcg:

The canl-c downgrade is then performed to all the CEs
Sun, 2 Oct 2016 14:00: after a short promising period with less errors,
All the CE are again faulty. Investigation is performed on the Mysql delegation database,
Verbose logging of lcas/lcmaps is activated, no definitive results.

Mon, 3 Oct 2016:
Investigation continues.

- The problem is identified in user's proxy file being missing in the /var/cream-sandbox/<usergroup>/<userDN_user>/proxy dir of the CE. For unknown reason proxy renewal seems to fail and no recent proxies are present under the aforementioned dir.
- In the late afternoon, the problem is still ongoing and the number of active jobs on the CEs is strongly reduced. Decision is taken to reinstall the CEs to get them at a known reliable working setup.
- The operation on one CE is successful, the reinstalled CE works fine as expected.
- All other CEs but one (ce08-lcg) are reinstalled, all CEs works fine.

Tue, 4 Oct 2016, morning, further investigation and issue removal
All the CEs are faulty again.

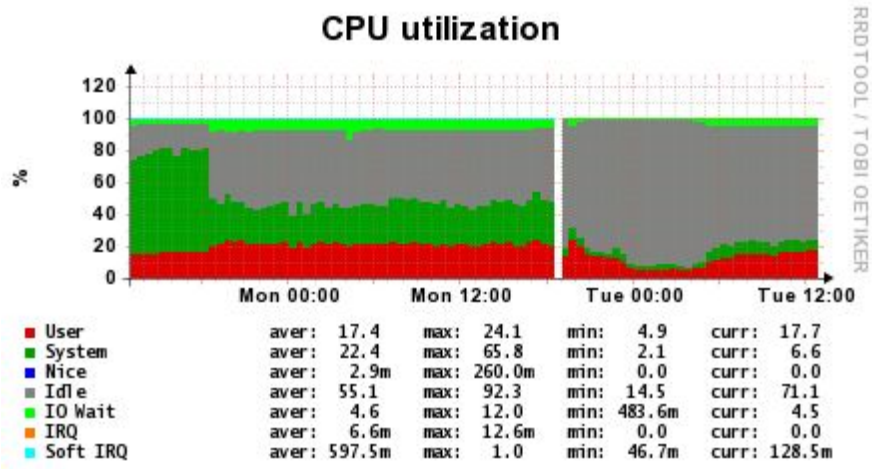
- Investigation with help from a former CREAM developer (M. Sgaravatto)
- The problem is still the same: no proxy more recent than 4AM
- The /usr/bin/glite-cream-copyProxyToSandboxDir.sh script is responsible of creating a delegated user proxy starting from the user's proxy from the cream database.
- The script is executed step by step until the root error is found and replicated:

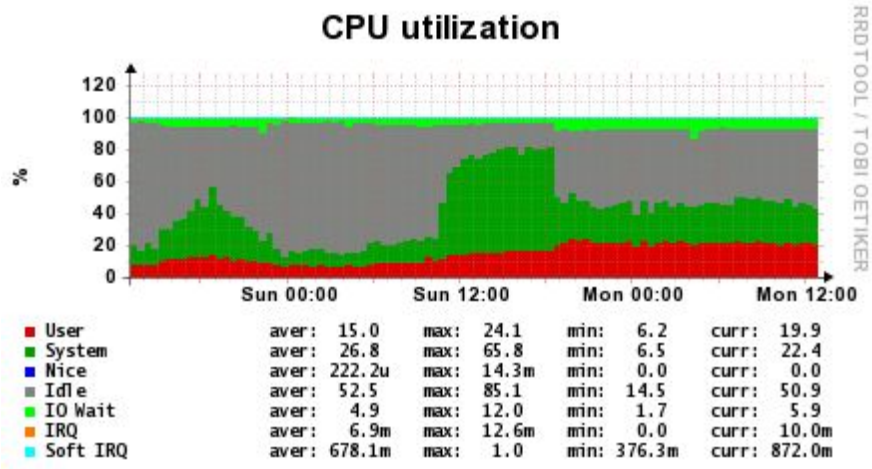
[dteam008@ce01-lcg ~]$ /usr/bin/voms-proxy-init -rfc -limited -valid 1:0 -cert /tmp/sdp_proxy.pem -key /tmp/sdp_proxy.pem -out /tmp/sdp_gu
fingerprint does not match
Function: FIPS_module_mode_set
no start line
Function: PEM_read_bio

Searching google a working solution is found: removing the dracut-fips-004-256.el6.noarch rpm fix the problem.

Still to understand what "activated" the dracut-fips , as it was present on the CEs from long time, without observable problems.

Further note: during the time of the problem, all the CEs were highly overloaded, adding one more layer of difficulty to the investigation. Reason is due to the fact that some WMS (such as glite-WMS), still used by some non-WLCG VOs, have a default ShallowRetryCount of 10, meaning that upon job failure, it gets resubmitted nine more times. In case of systematic failure, this lead to a terrible mess.





Tue, 4 Oct 2016, final analysis and problem description:
A local security expert (V. Ciaschini)

- Canl-c upgrade also triggered a security openssl upgrade: 1.0.0 → 1.0.1e
- Openssl 1.0.1e actually is 1.0.1e + openssl-fips 2.0.x (with SL 6.x)
- When the /usr/share/dracut/modules.d/01fips exists, openssl fips mode is turned on
- The /usr/share/dracut/modules.d/01fips is there, created by dracut-fips, present by default
- In fips mode, openssl looks for additional certificates into the 01fips directory, which are not there.
- The proxy renewal operation then fails because of “fingerprint does not match” error.
- Downgrading canl-c library has no effect of sort, as the openssl version is not downgraded.

Conclusion

- One minor openssl upgrade dramatically changed its behaviour, in such a way that mere existence of one directory is enough to screw system functionality.
- Urgent action at the site was requested to calm down alerts generated from pakity sensors on WNs, <<although the vulnerability is less critical on WNs>>.

- Urgent action was requested at the site on friday noon, having tuesday as local holyday. As a consequence many people were vacant until next wednesday.