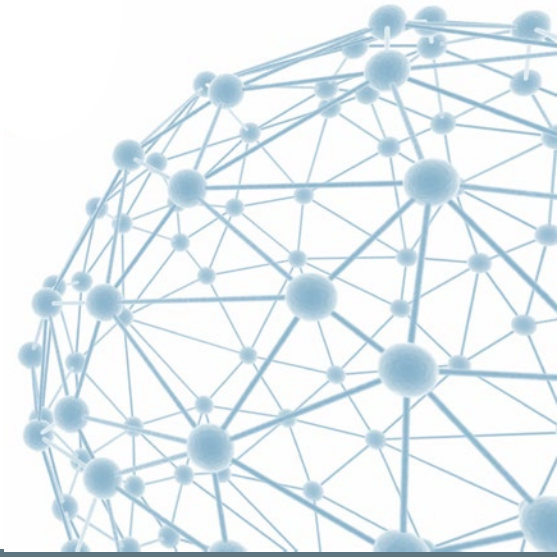
OpenSSL and Java 7 vs. 512-bit proxy keys

Maarten Litmaath
CERN

GDB, 2014-01-15



Prologue

- Nov 18 – GGUS:98964 opened by DESY-HH admin Dmitry Ozerov
  - WMS delegates proxies with 512-bit keys that are refused by Java 7 used by dCache
  - /usr/lib/jvm/jre/lib/security/java.security:
    - jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024
  - Workaround: remove second clause, or change 1024 to 512
  - GridSite developers accepted the bug

Meetings and forums

- Dec 9 – WLCG ops meeting ATLAS report
  - not working: openssl-1.0.1e-16.el6_5 (SL6.5)
  - last version working ok: openssl-1.0.0-27.el6
- Long thread on LCG-Rollout started Dec 12 by DESY-ZN admin Andreas Haupt
  - CREAM failures fully understood on Jan 9
- Updates in ops meetings and ops coordination meeting on Dec 19
  - Try to stay on the old openssl during the break

Analysis (1)

- Simon Fayer of Imperial College concluded:
  - If both endpoints are running the newest openssl, they negotiate TLS1.2 which doesn't support 512-bit keys...
  - This is why only pairs of fully upgraded machines fail (if either end is older, TLS1.1 is used instead).
- And Java 7 by default refuses such keys
  - Possibly affecting instances of Argus, BeStMan (including EOS), CREAM, dCache, StoRM, …

Analysis (2)

- Delegations with 512-bit keys are coming from GridSite libraries
  - Used by WMS, CREAM, UI, FTS-3, PanDA, …
- New GridSite rpms available as of Dec 16
  - EMI-2 Update 21
  - EMI-3 Update 12
- EGI broadcast sent Dec 16
  - https://operations-portal.egi.eu/broadcast/archive/id/1066

Which node types need the fix?

- WMS
  - Both SL5 and SL6
  - CERN WMS (e.g. for SAM): Jan 21
- FTS-3
  - CERN production instance re-installed with SLC6.4 before the break
  - Other production instances?
  - Pilot instance updated last Fri → all OK now
    - ATLAS functional tests had been moved back to the FTS-2 temporarily after lots of errors during the break
- PanDA → done
- CREAM?
  - EMI-2 CREAM on SL6 may be affected if proxy delegation bug workaround was not undone
    - https://wiki.italiangrid.it/twiki/bin/view/CREAM/KnownIssues#EMI_2_CREAM_CE_delegates_bad_pro
- More?

More fall-out

- OSG have done an emergency release to fix Globus components (gatekeeper) affected by the OpenSSL change
- Fixed upstream in Globus Toolkit 5.2.5
  - Fixed packages in EPEL as of Dec 20
    - https://admin.fedoraproject.org/updates/FEDORA-EPEL-2013-12307/
- Failures for 512-bit-key proxies may (re)appear as services get updated or upgraded to SL6.5
  - We need to get rid of such proxies by updating GridSite on the relevant intermediary services