Guillaume PHILIPPON

SECURITY UPDATE MANAGMENT @GRIF

Outline

- Genesis of security update
- Why GRIF is (not) specific ?
- Security update procedure
- Pakiti @GRIF
- Feedback after 6 month
- And now ?

Genesis of security update

- Previously, update management was a case by case act during major security alerts
- We want a more proactive security update management
- A lot of improvement have been done on quattor about security update management

Why GRIF is (not) specific ?

- GRIF is a federation of site
  - Site have responsability of its security (not GRIF)
  - Even each GRIF admin have enough privileges to update a remote site , they have no physical access to it
  - But a desire to share security work
- This organisation have some constraints

Constraints

- Security update must be
  - Controllable by site administrator
  - Be tested to avoid issue during deployement phase
  - Quick & simple to prepare
  - Knowledge must be shared
- In fact, nothing is really specific to GRIF

Security update procedure (normal case)

- 1 update per month
- Only security update (no functionnality update)
- No kernel update
- A unschedule update is done if a critical vulnérability is found (ie glibc on CVE-2010-3847)

Why specific case for kernel ?

- Main issue is machine reboot !
- No physical access to a remote site
- Person who make update have no responsability about site production (a reboot should be planned)

Security update (normal case)

- Quattor template are created
- Tested on our testbed
  - Eventually fixed
- Tested on a production site
  - Eventually fixed
- Deploy into GRIF (new update version is defined as default)

Security update (kernel case)

- We freeze update version for all GRIF machine
- We change the default update version
- Each site admin plan the update and the reboot of there site

Pakiti : Why a GRIF pakiti ?

- To control our work
  - How to be sure that all update have been done ?
  - How not forgive a machine froze in a specific update ?
- EGI pakiti just monitor Worker Nodes
- CEs, SEs and other services are also sensitive machine

Pakiti : In practice

- 1 pakiti instance for GRIF (hosted at IRFU)
- Monitor all GRIF machine (in progress)
- 5 OS (from sl4.5 to sl5.5)
- Client configuration manage by quattor
- Server installation manage by quattor (but not configuration)
- Help us to
  - Verify if all machine is up to date
  - Verify if all package is up to date

Feedback after 6 month

- 6th monthly update in progress + 3 unschedule update
- 4 persons have made security upgrade for GRIF
- Less latency between vulnerability notify and update deployement

But nothing is perfect

- Made update take about 1 day (test & fix phase)
  - Some SL modification need to be fixed
- Kernel update need to be planned and can take a long time before been deployed on all GRIF machine
- Pakiti is 'immature'
  - Setup si pretty 'touchy'
  - Mysql issue when we increased number of monitored machine
  - But dev team is very reactive

And now ?

- Improve communication with other site to shared our work
- Deploy some trivial workaround to avoid pakiti mysql issue
- Improve communication between pakiti and quattor
- Improve quattor integration of pakiti server

Usefull links

- Pakiti : http://pakiti.sourceforge.net/
- Quattor errata documentation
  - https://trac.lal.in2p3.fr/Quattor/wiki/DOC/OS/Errata