Table of Contents

Meeting March 29, 2010

Agenda

1. Introduction of the goals of this group
2. Discussion of the IT/PES proposal to close access to lxvoadm from lxplus
3. Security recommendations
4. RPMs repositories for VOCs
5. Support for VOCs
6. AOB

Minutes

- *Attendees*:
    - ♦ **ALICE** - Patricia
    - ♦ **ATLAS** - Flavia
    - ♦ **CMS** - Peter, Patricia, Jorge
    - ♦ **LHCb** - Joel, Roberto

1. Goals of the VOC Coordination effort:
    - ♦ Find commonalities in order to avoid replication of work;
    - ♦ Present a coherent view to IT in terms of needs;
    - ♦ Create a self-supporting infrastructure with the help and the support of IT/ES and other IT groups.
2. The proposal from IT/PES to close access to lxvoadm from lxplus was discussed. Many concerns and questions were raised. Some clarifications came from IT/PES:
    1. The proposal affects **only** access to lxvoadm from lxplus through ssh.
    2. Access to lxvoadm is possible from outside CERN.
    3. The implementation plan will not start till the OK from the experiments is received. Starting from that moment, it will take about 2 weeks for the proposal to go into production.
    Specific questions:
    - ♦ Patricia (Alice) raised the issue that login to Alice VOBOXes happens through gsissh and this should continue to work.
    Answer: Access to the VOBOXes is configured by the VOCs. Therefore everything that used to work for Alice will continue to work since lxvoadm is not involved in the login process through gsissh
    - ♦ Peter (CMS) raised the issue of the need to login onto WNs from CMS VOBOXes through the generic account cmsprod for Tier-0 activities. More details are needed in order to better understand the need.
    - ♦ Joel and Roberto (LHcb) said that the proposal should be OK with LHCb since this would avoid one hop while logging onto the VOBOXes. However, they expressed some concern about the change taking place during data taking.
3. The issue about the recommendation coming from the security team to allow access to VOBOXes only through lxvoadm was discussed. ATLAS and LHCb enforce this recommendation while CMS and Alice do not. Please, check on the conclusions. VOCs expressed the need to organize a meeting on security policies and on guidelines to fill in the recent documents submitted by the CERN Security Team.
4. Existence of rpm quattor repositories per experiment:
    - ♦ Alice uses standard quattor repositories since the only dependency is from the gLite UI available in the central CERN rpm quattor repositories

  - ♦ ATLAS uses custom ATLAS quattor rpm repositories. Everything is installed through quattor, even external service packages. ATLAS spends a lot of time and man power to create rpms. In fact, the software stack ATLAS depends on is not officially supported by CERN/IT. As an example we can mention python2.5/2.6.
  - ♦ CMS does not have custom quattor rpm repositories. System rpms are taken from the standard CERN quattor repositories. Other external service packages are made available through rpms installed in user space. While this practice is really attractive also for other experiments such as ATLAS, it introduces the danger that service managers/providers do not use these distributions but install manually most of the needed software. Furthermore the VOC does not have control (security) over the services running on the vOBOXes.
  - ♦ LHCb relies on CERN quattor rpm repositories. LHCb noted that VOCs and machines are very much dependent on changes to the standard software templates. Changes must be properly announced and templates kept well in hand.
5. The question about the future of VOBox.Support was raised. This mailing list (connected to the Remedy system) will most likely be transformed in a user forum. An expert on shift will always be available to answer questions and provide adequate expertise. IT/PES is reviewing the VOC SLA. A new version of the document will soon be available and the experiments (VOCs) will be called to approve and sign again the SLA. It is important that this group provides good coordinated input to IT/PES. The new SLA will specify as well which tasks will be performed by CERN/IT and which will be under the responsibility of the VOCs. A list of concerns has been compiled to be addressed to IT/PES (see below). What will happen to ELFms.support@cernNOSPAMPLEASE.ch?

Actions

1. Flavia to follow up with the experts in IT/PES and the VOCs about point 2. A meeting can be held with the experts in case more clarifications are needed.
2. Peter to provide more details about CMS about point 2.
3. Flavia to organize a meeting on security policies and on guidelines to fill in the documents recently submitted by the CERN Security Team.

Conclusions

1. Flavia checked with the CERN Security Team and the VOCs are strongly adviced to allow access to VOBOXes only through lxvoadm. Indeed this machine runs a secure bash and therefore can log all actions. iprules templates are available for this. In the rules_vobox_prologue section of your templates you just need to include the following:

   ```
   include components/iptables/rules_lxvoadm_ssh;
   ```

   Furthermore, the policy adopted by CMS to block direct root access to VOBOXes allowing sudo access to administrators is also a recommended practice. This policy should be adopted by all VOs.
2. It was agreed that it is worth looking into the possibility of exporting the CMS tarball/rpm repository to other experiments.
3. Quite some man power is devoted by 2 experiments to produce rpms. Furthermore, all experiments are affected by changes in CERN standard templates. IT/ES will investigate on how to improve the situation. A common effort between IT/ES and the experiments should be establised.
4. List of concerns to be addressed to IT/PES:
   1. A user forum is very useful. It should be complemented by some other form of support through Remedy as it is done now.
   2. Experiments are willing to use the fabric management infrastructure offered by CERN/IT. Such an infrastructure should make the task of managing machines easier, should help saving man power and should be well supported.
   3. What will the new procedure be to submit support requests in a traceable way?

    4. The duties of CERN/IT sysadmins and the duties of the VOCs should be clearly stated in the SLA
    5. Long waiting time for hardware requests
    6. Need a way to prioritize hardware requests
    7. Training on the fabric management infrastructure for VOCs is needed.
    8. Updated and complete fabric management documentation for VOCs.
    9. Are certificate renewals handled by IT or by the VOCs?

5. The group will not hold regular meetings. Instead, focused meetings on specific topics or to discuss specific news will be called whenever the need arise. Next meeting will focus on security.

-- FlaviaDonno - 06-Apr-2010

This topic: LCG > WLCGVOC20100329
Topic revision: r2 - 2010-04-06 - unknown