HEPiX Virtualisation Working Group Report

Tony Cass
WLCG GDB
May 9th 2012

Background

- The HEPiX virtualisation working group was formed to facilitate the instantiation of user-generated virtual machine images at HEPiX (and WLCG) sites.
- Users were expressing such a wish in 2008/9, but sites were worried about issues such as uncontrolled root access and the maintenance of the traceability logs required by Grid security policies.

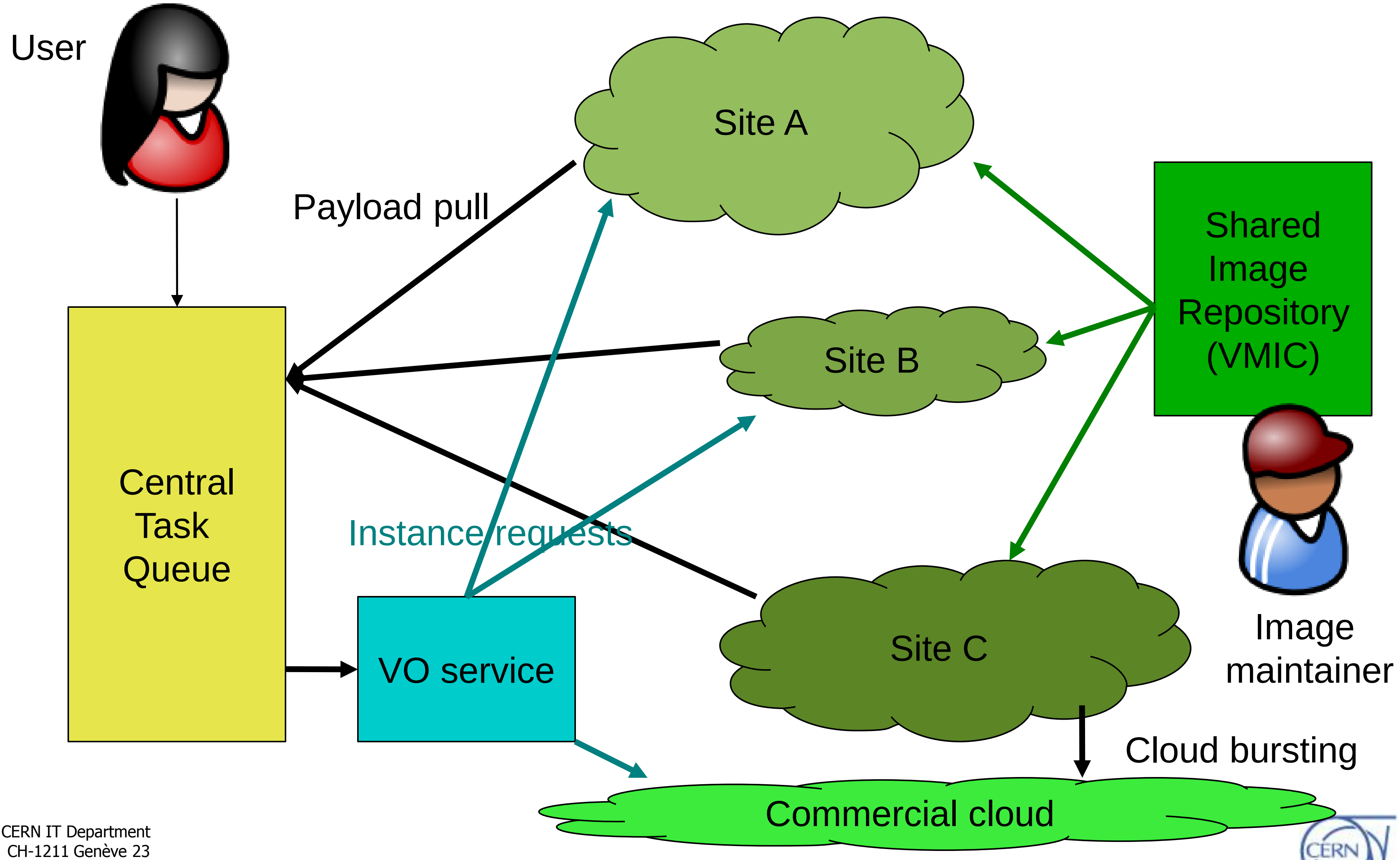
Image endorsement

- The HEPiX VWG developed a policy that introduced the concept of image “endorsers”: people who would guarantee that images they generated could be safely used at sites.
- Amongst other things, such images would
  - have no embedded user credentials, and
  - enable sites to contextualise the images to enable the required logging and make other necessary customisations.
    - Sites agree, however, not to modify the software environment of the image.
- Sites are free to trust (or not) specific image endorsers but, if they do trust someone in this role, it is expected that any images endorsed by this person can be used at that site without the need for inspection or manual approval.
- The HEPiX VWG policy became the basis of an approved JSPG policy document, “Policy Trusted Virtual Machines”.

Current Status

- The endorsement policy is agreed.
- Technical arrangements have been defined for
  - image contextualisation
    - these are compatible with EC2/OpenNebula/OpenStack
  - exchange of information between the site infrastructure and a running virtual machine
    - e.g. remaining lifetime, that the virtual machine can be terminated, …
- A framework for image endorsers to publish and distribute images has been developed.
  - This has been integrated with StratusLab’s marketplace at LAL and is being integrated with OpenStack Glance at CERN.
- CERNVM images are compatible with the HEPiX VWG policies
  - and there has been a security review of the underlying technology.

How this could be used



Slide courtesy of Ulrich Schwickerath

Summary

- It should be possible for trusted user generated images to be safely instantiated at HEPiX and WLCG sites
  - compatible with the aim of the working group…
- The contextualisation step, in addition to enabling the necessary logging, also provides a way for images to be integrated in the local batch system
  - although considerable gymnastics would be required to enable the installation of credentials allowing the download of "joblets" from an experiment-specific queue.
- The creation and use of images which connect directly to an experiment-specific pilot job framework is entirely feasible
  - and, in my view, desirable.