Contribution ID: **25** Type: **not specified**

A scheme for defining and deploying trusted Virtual Machines to Grid Sites using Configuration Management Systems

Monday, 1 November 2010 14:30 (30 minutes)

Sites (service providers) and VOs (service users/functionality providers) are debating how to define trusted VO-provided VM images. We present an alternative scheme that, using a Configuration Management System (CMS), does not require Sites to trust VO-provided images. It gives VO the freedom to design and customize functionalities, while letting Sites retain full control over instances.
Configuration Management Systems (CMS, such as Puppet/Cfengine, have been widely used in computing centers to automatically manage resources. They provide high level languages to define desired states of target systems, such as installing software packages, running services, enforcing firewall, etc.
We propose a two level scheme. Both VO and Site start from a well trusted base image (e.g. base installation of SL5 with no customization). At the VO-level, VO experts customize the base image to perform VO specific tasks (e.g. ATLAS Condor Worker). These customizations are not committed to the image, instead, they are defined in CMS language and stored in a SVN repository. At the Site-level, site experts define site-specific configurations and security policies in CMS language.
When deploying, VO needs no privileged access in instances. Site manager starts the base-images that contains CMS clients, which apply VO-level definitions then Site-level definitions. At this time, the instance is ready to perform VO defined tasks. Since Site-level definitions are applied at last, the VMs are ensured to comply with Site policies.
This scheme eliminates the problem of trusting VM images. It is more flexible, more reliable, and more secure.

Summary

Comments to Reviewers:
The approach is based on the fact that, with the help of Configuration management systems, the VM can be customized/contexualized to meet the requirements of both VO and Site at boot time. So that root access is not required for VOs on deployed instances.
Benefits of this approach:
1. Eliminate the need for sites to trust an image provided by an individual.
2. VO needs no root access on deployed VMs (running instances).
3. Easier to expire, revoke or catalog a set of definitions than a VM image.
4. Versioning control of VO customizations and Site policies.
5. Give VO the freedom to customize to meet their needs
6. Give Sites the ease to enforce security policies

Primary author: YAO, Yushu (Lawrence Berkeley National Lab. (LBNL))

Presenter: YAO, Yushu (Lawrence Berkeley National Lab. (LBNL))

Session Classification: Virtualization