Focus on Cloud Security at IPHC

Jérôme Pansanel
jerome.pansanel@iphc.cnrs.fr

Amsterdam – November 2016

Network Traffic Monitoring

ZNetS

- Tool for monitoring and recording machines trafic
- Acquisition and conservation of inbound and outbound traffic (post-incident analysis)
- Anomaly detection
- Data are replicated in two locations (IPHC and CC-IN2P3)
- → http://www.znets.net/

IP Address Traceability

MySQL trigger

- Hard to find the VM that was using a public IP once the IP has been disassociated
- A simple triggler log all IP association / disassociation
- Source available on GitHub: https://github.com/FranceGrilles/openstack-triggers

Tools

- Front-end to the OpenStack triggers
- Source available on GitHub: https://github.com/Pansanel/openstack-user-tools

device id	user name	associating date	disassociating date
3e2767b0-c0f7-43e6-a1aa-c92e0e016190	/C=IT/O=INFN/OU=Personal Certificate/L=Bari/CN=Vincenzo Spinoso	2015-11-30 14:11:24	2015-11-30 14:19:03
bca349ba-a3cb-4311-8722-797600630090	/O=GRID-FR/C=FR/O=ISCPIF/CN=Seyyedmaziyar Shariatpanahi	2016-02-02 11:58:45	2016-02-11 10:34:01
431e52c2-9141-48fd-b7e3-c1d59646ff0a	fg_formation_user20	2016-04-28 16:01:47	2016-04-29 09:44:50

Nova VM Isolation

Nova VM isolation

- By default, a user can interact with any other VMs in its tenant (VO), including VMs belonging to other users. Since v2.1 of the Nova API, this behaviour cannot be restricted anymore.
- Vincent Gatignol (France Grilles) maintains a set of patches (based on RDO Nova release) to give us the possibility to define the right authorisation policies.
- Available on GitHub: https://github.com/FranceGrilles/cloud-security
- Starting with Mitaka, available as RPM package (work in progress)

What about the other OS modules ?

- Snapshot a VM or a persistent storage → ability to access data of other users
- Possibility to restrict this behaviour by limiting this feature to a specific role
- Interactions between two users in the same tenant are monitored by a specific tempest test by the French NGI – problematic as we don't have the expeceted usage of a tenant
- We suggest the users to use encrypted storage.

https://blueprints.launchpad.net/nova/+spec/user-id-based-policy-enforcement
https://pdfs.semanticscholar.org/af46/9a71e17ad74a74496d59b8c412633587eabf.pdf

Questions ?