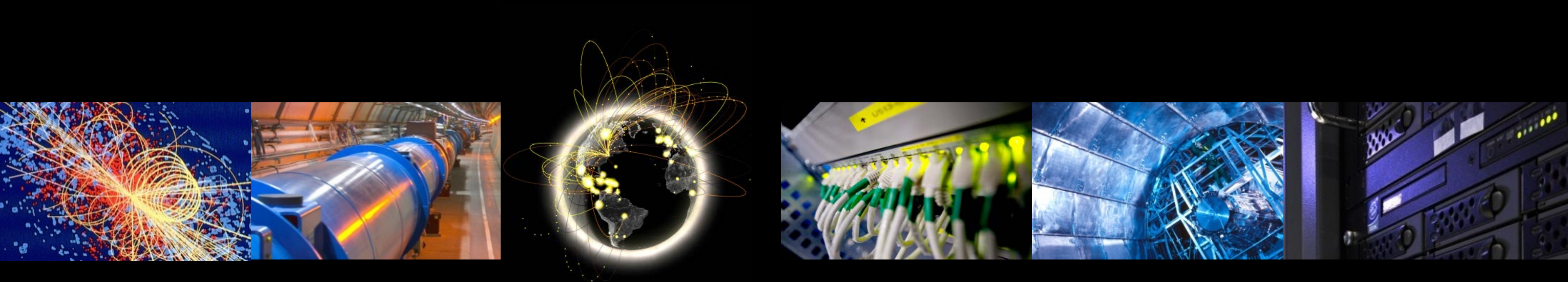
Traceability & Isolation WG

Vincent BRILLAULT, CERN/EGI-CSIRT

GDB April 2016, CERN



Why now?

- Emergence of new isolation technologies (cgroups, namespaces…)

- Site to VO expertise shift via virtualization:
  - VOs controlling the execution context (e.g. VM)
  - Sites unable to monitor/ensure user isolation

- Commercial clouds?

Mandate proposal

Explore new traceability and isolation paradigms, propose a new model taking advantage of new technologies and VO frameworks while keeping full trustworthy traceability and isolation of users actions.

Working Group status

- Created at the last GDB (March 2016, AMS)
- New mandate
- Call for participants open:
  - VO framework experts needed
  - Site experts needed

Initial ideas

- Split Host/Time → user/payload identification
  - Sites only identify the VO
  - VOs can identify the user & payload
- Trust the pilot job & VO framework
  - Sites should only monitor external behavior
- Protect pilot jobs from the users using container technologies (cgroup/namespaces)

First Feedback

From Brian Bockelman/OSG:

- In RHEL7 groups/namespaces still privileged
  - RHEL8? Newer kernels? Other distributions?
- Protecting pilot jobs from file interactions hard
- Existing glexec plugins:
  - lcmaps-plugins-namespace
  - lcmaps-plugins-anonymous-accounts

Next step

More people and ideas needed, please join!