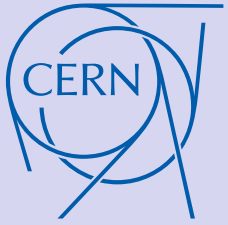
Security/traceability issues for WLCG Cloud

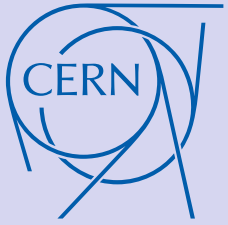
Vincent Brillault

Pre-GDB, January 2014



WLCG risk assessment

- Mostly apply to cloud (missing threats)
- Most important identified asset: Trust
- Most dangerous threat: Misused identities
- Focuses on traceability for:
  - Incident containment
  - Incident re-occurring prevention



Virtual Machine endorsement

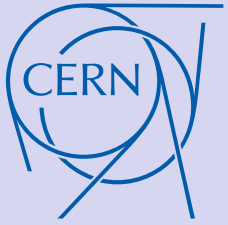
EGI policy

Security Policy for the endorsement and operation of Virtual Machine images[1]

- 2 roles:
  - Endorser: Certify VM Image
  - VM Operator: Root access on the VM
- Security requirements for both roles
- Users are not endorsers:

  An Endorser should be one of a limited number of authorised and trusted individuals appointed either by the Infrastructure Organisation, a VO or a resource centre

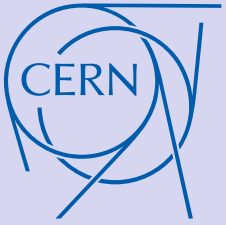
[1] https://documents.egi.eu/document/771



Virtual Machine endorsement

WLCG needs

- endorser/operator = site: current situation
- endorser = VO: could provide more flexibility
- operator = VO: could provide technical debugging
- endorser/operator = end user: not foreseen useful



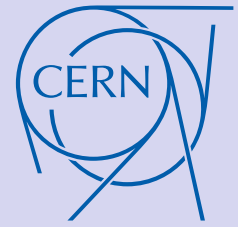
Traceability

WLCG/EGI policy

Grid Security Traceability and Logging Policy[2]

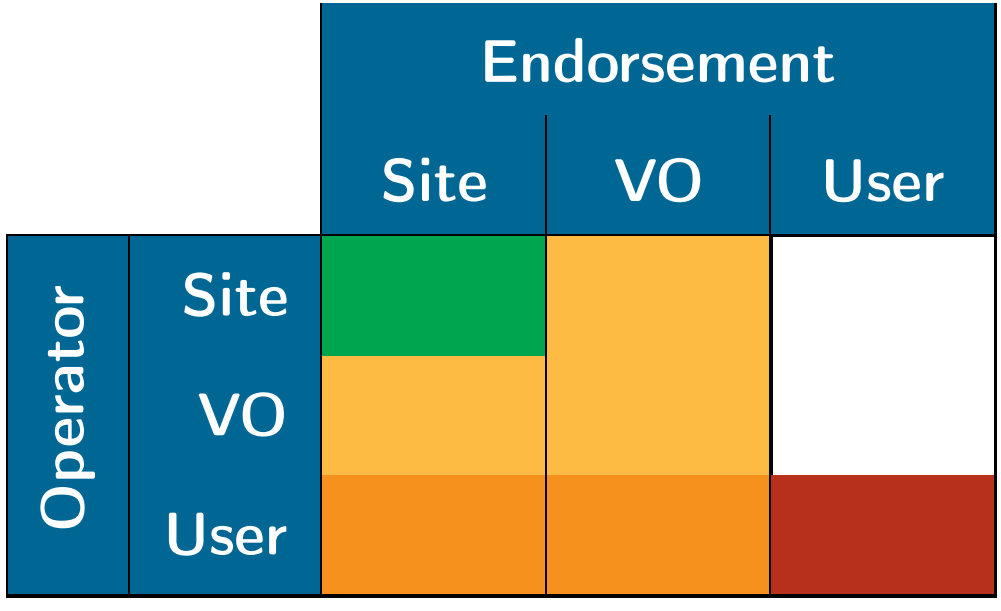
- Idea: understand and prevent incidents
- Requirements:
  - Grid software MUST produce application logs:
    - Source of any action
    - Initiator of any action
  - Logs MUST be collected centrally
  - Logs MUST be kept 90 days

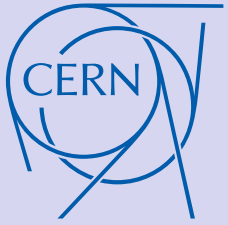
[2] https://edms.cern.ch/document/428037 & https://documents.egi.eu/document/81



Traceability

Applicability with potential scenarios



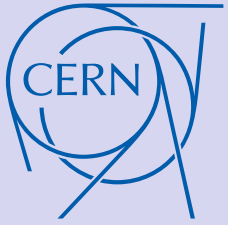


Traceability

Site/VO endorser/operator

Virtualization only introduces new possibilities:

- Logging requirements not changed/impacted:
  - Every action/every user
  - Forwarded to a central server
- New logs required (policy extension?):
  - Which endorsed VM is running?
  - Who is operating it (Site/VO) ?
- User compartmentalization:
  - Similar to glexec? (one UID per user)
  - Re-instantiate VM for each user (not job)
    - Perfect easy compartmentalization
    - High impact for unique short jobs



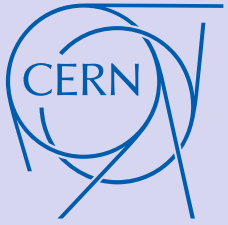
Traceability

Site/VO endorser, User operator

Complete root access for user is dangerous:

- Endorsed VM:
  - Contains up-to-date software (by policy)
  - Contains secured configuration (by policy)
  - Can include protections/logging...
- User in full-power:
  - Can break configuration (maliciously or by error)
  - Can disable logging (maliciously or by error)
  - Can falsify data (non-trusted logs)
- Simple accountability/traceability: user responsible
- Difficult detailed incident analysis
- VM cannot be re-used by different users

No identified reason for such situation: highly discouraged



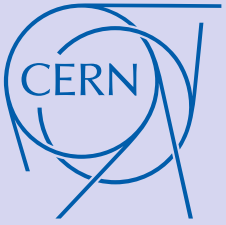
Traceability

User endorser & operator

Complete user control: no security

- Unknown VM:
  - Can be vulnerable (not patched, outdated...)
  - Can be badly configured (no logs, anonymous access...)
  - Could be fully-encrypted (no forensics possible)
- User in full-power:
  - Can falsify data (non-trusted logs)
- Simple accountability/traceability: user responsible
- Potentially impossible incident analysis
- VM cannot be re-used by different users

No identified reason for such situation: highly discouraged

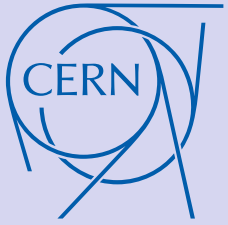


Traceability

Lost data on VM deletion

- VM creation/deletion easy (could be VO/user initialized)
- VM lifetime foreseen shorter than current WN
- If trusted operator/endorser:
  - Application logs centrally kept
  - More system logs probably needed
  - Unknown/modified file preservation would help forensics
- If non-trusted operator/endorser:
  - Application logs (central) not trustworthy
  - System logs (central) not trustworthy
  - VM disk MUST be preserved after deletion

Policy extension required?

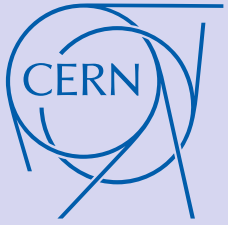


Monitoring

WN monitoring

Three evolutions possible:

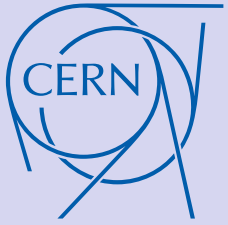
- Probe every VM for vulnerability:
  - Much more work than now (who?)
  - Extremely diverse security contacts
- Limit VM lifetime:
  - Vulnerability window restricted (automatic)
  - How long (soft/hard limits ?) ?
    - Hours ?
    - 2-3 days ?
    - Week(s) ?
    - Month(s) ?
- If Trusted endorser/operator:
  - Identify vulnerable VM in trusted VM store
  - Contact *all* VM operators (who?)
  - *Kill* switch to be implemented (who?)



Incident response

Analysis

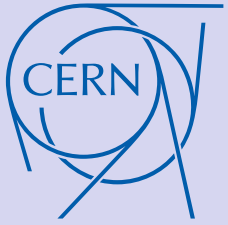
- Need well defined security contacts
- Require root access on VM for:
  - Site admin ?
  - EGI/OSG security team, WLCG security officer ?
- VM freezing/isolation (could break jobs):
  - Who is authorized to do it?
  - Procedure (under which circumstances ?) ?
- Analysis using backend services (e.g. disk providers):
  - Who is authorized to do it?
  - Procedure (under which circumstances ?) ?
  - Private data protection ?



Incident response

Response

- Need well defined security contacts
- How to ban a user:
  - From site/VO operated VM ?
  - From cloud system (user-operated VM) ?
- How to ban a cloud provider (site) ?
- How to ban a glitched VM (from the VM store):
  - For newly created VMs ?
  - *Killing* running VMs ?

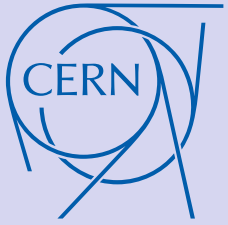


Incident response

Requirements

- Some documents may need to be revisited/extended:
  - Risk assessment (new threats)
  - Traceability requirement (new layer, VM deletion)
  - Incident procedures
- All operators and final users need to abide by a potentially extended *Acceptable Use Policy*[3] (AUP):
  - Recognizing liability
  - Allowing security teams to intervene
  - Cover other cloud specificity

[3] https://edms.cern.ch/document/428036 & https://documents.egi.eu/document/74

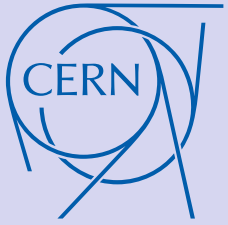


Cloud issues

Virtualization risks

Hypervisor containment might be broken:

- Require separated hypervisor clusters for:
  - Infrastructure ?
  - Worker Nodes (Site/VO operated) ?
  - Untrusted VM (End User operated) ?
- Require physical host for critical infrastucture?
- Hypervisor traceability needed:
  - VM traceability (On which hyperviser each VM is)
  - System & audit central logs



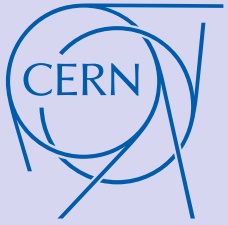
Cloud issues

External provider

- Incident response procedure?
- Abuse detection (IDS not available) ?
- Security incident costs, e.g. Amazon agreement[4]:

  If we or our affiliates are obligated to respond to a third party subpoena or other compulsory legal order or process described above, you will also reimburse us for reasonable attorneys' fees, as well as our employees' and contractors' time and materials spent responding to the third party subpoena or other compulsory legal order or process at our then-current hourly rates.

4 https://aws.amazon.com/agreement/



Next?

Questionnaire in preparation

- Describe how user proxies are handled from the moment a user submits work to the system to the moment that a user task runs, through any intermediate storage.
- How can a user or a site be blocked?
- What site security processes are applied to the machine(s) running the cloud-related services, centrally and/or at sites?
  - Who is allowed access to the machine(s) on which the service(s) run, and how do they obtain access?
  - How are authorized individuals authenticated on the machine(s)?
  - What processes exist to maintain audit logs (e.g. for use during an incident)?
  - What monitoring exists on the machine(s) to aid detection of security incidents or abuse?