Emergency Suspension List

Vincent Brillault, CERN/EGI-CSIRT

Status update

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Overview

- How it works
- Near miss in October 2015
- Current status
- Future

How it works

Automated DN (un-)suspension mechanism

- (Un-)suspending user DNs *immediately* and reliably
- Maintained by EGI-CSIRT & WLCG Security Officer
- Hierarchical Argus servers: CERN, NGIs, Sites

Near miss: the cause

- One predictable DN banned every day for monitoring
- 2015/10/28:
  - Global puppet change at CERN (secret handling)
  - Unexpected change: DN template → empty string
- 2015/10/29 early night:
  - Daily update: pap-admin ban subject “”
  - CERN_PROD’s Argus server:

```
ERROR [AuthorizationRequestServlet] - Error evaluating policy
  java.lang.IndexOutOfBoundsException: Index: 0, Size: 0
```

Near miss: the impact

- 2015/10/29 morning:
  - Synchronization script killed
  - pap-admin un-ban not working
  - Rules manually edited to remove empty rule
  - Surprised to not receive tickets/complains
- 2015/10/29 EGI OMB:
  - Error reported, asking NGI to clean their cache
  - Surprised again: nobody seems affected!

Near miss: lesson learned

- Incident impact:
  - Expected result: the whole grid taken down
  - Observed result: only CERN lost jobs

→ Nobody was enforcing the suspension list!

→ Better monitoring of suspension framework needed

- Synchronization script hardened:
  - More configuration checks
  - Reject empty DNs

Current status

- Central Argus server stable & safe again
- NGIs have deployed NGI Argus servers
- EGI monitoring NGI Argus servers
- EGI-CSIRT designing tests for sites (submitting jobs)

Current status
NGI servers monitoring

- 4 NGI server OK
- 6 NGI servers UNKNOWN (connection error timed out)
- 19 NGI servers WARNING (ACL issues)
- 1 NGI server CRITICAL (daily DN missing)

→ Discussed at the last EGI OMB, getting better...

Future
Deployment at sites

- Trivial if you are already using Argus
- Less effective without glExec
- We should concentrate on protecting data/services
- EGI-CSIRT plans to test suspension efficiency

→ Feedback welcome, please contact me
(esp. if you have successfully deployed it!)

Future
VMs & Opaque pilot jobs

- VMs: EGI possible solution (EGI FedCloud):
  - Using *Perun*, only OpenNebula supported for now
  - (Un-)suspending VM owners

    → Limited benefits for WLCG
- Suspension rules consumed by VO frameworks?
  - Automatically? (via Argus or other format (e.g. yaml))
  - By email with the VO CSIRT?

Summary

- Suspension probably not working right now
- NGI servers being fixed (since last OMB)
- @Sites: Please deploy and share experience
- VO integration more effective for WLCG?