Emergency Suspension List

Vincent Brillault, CERN, EGI-CSIRT

Current status update

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

Emergency Suspension List What is it?

Automated DN suspension mechanism

- Why?
  - Automatic suspension: manageable delay
  - Automatic un-suspension: manageable delay
- Suspending what? Compromised user DNs
- When? Only for Security Incident, emergency solution

Emergency Suspension List How does it work

- Using Argus 'PAP'
- EGI-CSIRT (CERN) maintains central server
- NGIs maintain NGI server
- Sites supposed to get ACLs from NGI servers

Emergency Suspension List Monitoring

- EGI monitors the NGI servers
- No central monitoring for sites
- EGI plans to run challenges

Emergency Suspension List Current status (NGI servers)

Just look at Nagios:

- 1 NGI server OK
- 8 NGI servers UNKNOWN (connection error timed out)
- 21 NGI servers WARNING (ACL issues)

Emergency Suspension List How to fix it?

- Open port 8150, at least from:
  - EGI Monitoring server: 195.251.55.111
  - The endpoint used by your sites
- Add ACLs (pap-admin add-ace), at least:
  - For CN=srv-111.afroditi.hellasgrid.gr, OU=afroditi.hellasgrid.gr, O=HellasGrid, C=GR:

    `POLICY_READ_LOCAL|POLICY_READ_REMOTE|CONFIGURATION_READ`
  - For the endpoint of your sites:

    `POLICY_READ_LOCAL|POLICY_READ_REMOTE`

Emergency Suspension List
We need your help!

- Fix NGI argus servers (firewall ACLs)
- Make sure sites use the suspension list