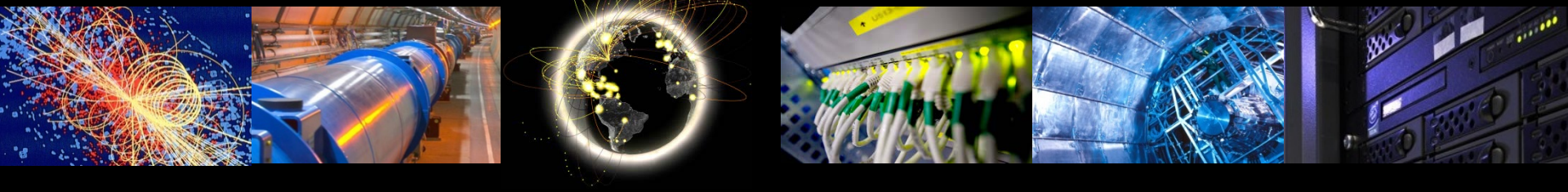
Emergency Suspension list

Vincent BRILLAULT

HEPiX Spring 2014, Annecy



WLCG
Worldwide LHC Computing Grid

CERN

Emergency suspension

- Suspended DN can't submit jobs to sites
- Automated Suspension:
  - "Fast": Delays configurable & known in advance
  - Completely automated:
    - No human communication delays
    - Works outside working hours
    - Uniform response guaranteed
- Unbanning also automated:
  - False positive cost controlled
  - Uniform state, no suspension left behind

Suspension procedures

- Old procedure:
  - Detect something (e.g. BitCoin mining)
  - Forensics & Analysis of incident
  - Escalate with other sites if needed
  - Contact the user & the VO
  - If malicious activity confirmed, not from user:
    - Ask all sites to ban the DN
    - Notify the CA of the potential Certificate compromise

Suspension procedures

- New procedure:
  - Detect something
  - Rapid analysis (check for false positive)
  - Add the user to the emergency suspension list
  - Forensics & Analysis of incident
  - Escalate with other sites if needed
  - Contact the user & the VO
  - Remove from suspension list if user recognize activity (e.g. Bitcoin “testing”) or false positive

Suspension new procedure

- Faster response:
  - Smaller resource losses
  - Reduce propagation & escalation risks
- Potential false positive:
  - Initial analysis decreases the probability
  - Cost:
    - Depends on list diffusion delays
    - Configurable/controllable

Suspension Infrastructure

- Hierarchical infrastructure:
  - Central servers hosted by CERN
  - (EGI) Relays hosted by each NGI
  - (EGI) sites contact only their own NGI
- Hierarchical rules:
  - Central rules: WLCG/EGI/OSG security officers
  - NGI rules: NGI security officers
  - Sites rules: Site adminitrators

Argus

- Old EGEE project
- gLExec integration (Argus-PEP)
- Argus-PAP:
  - Local ACLs
  - Pulls remote rules
- Support:
  - Authors have dropped the project
  - Future support by INFN

Suspension Infrastructure

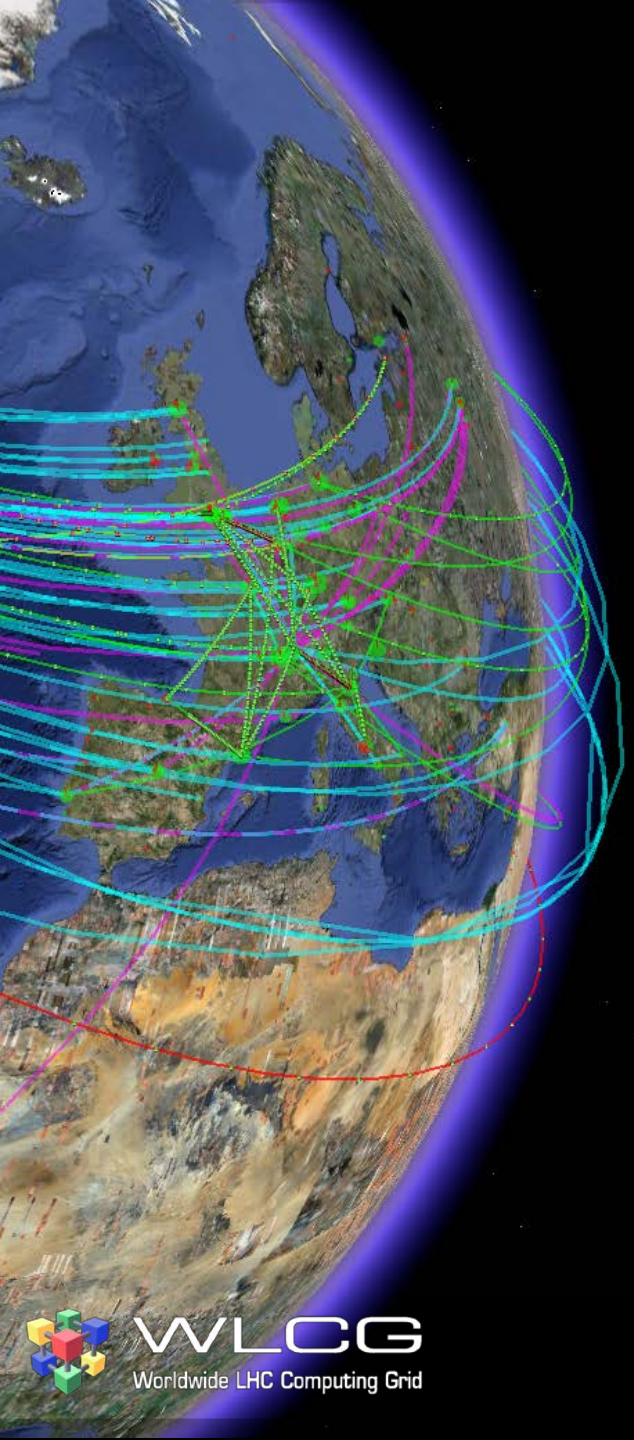
- Privacy (on central list):
  - x509 authentication
  - Only accredited clients can get the suspension list
- Interoperability:
  - Argus: soap interface, can be fetched by curl!
  - Raw YAML list available at CERN (ACL on demand)

Monitoring

- Delay propagation to Argus nodes:
  - Special (invalid) DN banned every day
  - Nagios probe
  - EGI will monitor NGI Argus nodes
- Suspension testing ?
  - Would require a valid banned DN
  - Not foreseen in close future

Future Potential Evolutions

- Propagate Emergency Suspension list to VOs:
  - Simultaneous automatic suspension on VO side
  - Protects resources managed by VOs
  - Redundancy
- Kill jobs of suspended users?
  - Running malicious jobs are currently not killed!
  - No easy solution with current infrastructure…



Questions ?

Fetching the list

- Curl:

```
curl --cacert /etc/grid-security/certificates/CERN-TCA.pem --cert $CERT --key $KEY -H 'SOAPAction: """' -H "Content-Type: text/xml; charset=utf-8" -H "Content-type: text/xml; charset=utf-8" -H 'Soapaction:"""' -X POST -d '<?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:ns0="http://schemas.xmlsoap.org/soap/encoding/" xmlns:ns1="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns2="http://services.pap.authz.glite.org" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Header/><ns1:Body><ns2:listPolicies><papAlias>default</papAlias></ns2:listPolicies></ns1:Body></SOAP-ENV:Envelope>' 'https://lcg-argus.cern.ch:8150/pap/services/XACMLPolicyManagementService?wsdl'
```

  - XACML output (can be parsed by XML parsers)

- Python:
  - ‘Simple’ solution using soap & xml libs
  - Ask me the code ;)