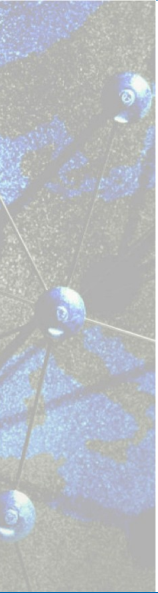


Central Emergency Suspension

Policy/Operations Implications

Sven Gabriel,

sveng@nikhef.nl, Nikhef, EGI-CSIRT

Argus Deployment

Development / Milestones

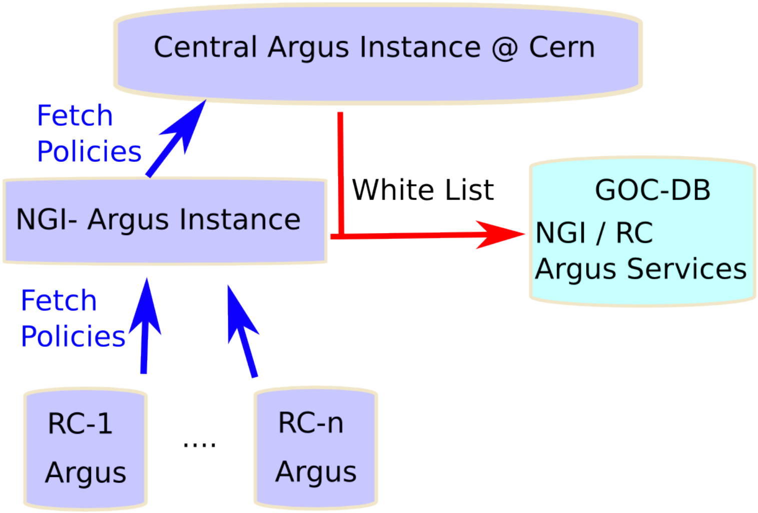
- Limit Access to the Argus instances.
- GOC-DB: Add Service Type ”NGI-ARGUS” (?)
- Service Type needs to have a host/service certificate in GOC-DB
- Central and NGI Argus Instances: ”fetch white list” from GOC-DB (?)
- NGI Argus Services can re-use the ”fetch white list”
- Monitoring: Check that the suspension information propagates down to the NGI/RC Argus instances (September, after TF)

Argus Deployment

Suspension Information Format

- The policies fetched from Argus are XACML files.
- Non Argus sites / services have to process the XACML file to meet their requirements
- Non Argus Sites should register a ”Fake Argus Server” in GOC-DB to fetch policies from the NGI-Argus
- Nikhef will provide an example to process the Argus XACML policy into Quattor

Argus Deployment



Central Argus Instance @ Cern

Fetch Policies

NGI- Argus Instance

White List

GOC-DB

NGI / RC Argus Services

Fetch Policies

RC-1 Argus

....

RC-n Argus

Argus Deployment

Next steps for NGIs

- Set-up a NGI-Argus Instance (with host/service certificate)
- Register NGI-Argus in GOC-DB
- Configure NGI Argus to fetch policies from central Argus instance at CERN
- EGI-CSIRT to test that the suspension information propagates to the NGI-Argus instances
- Within NGI: RC Argus Instances to fetch policies from NGI-Argus

Argus Deployment

NGI Argus / best practices

Argus people might have more info on that. Most obvious topics are:

- Lock down access to the NGI-Argus Instance, anyone having write access could stop all job submissions to that NGI.
- Adjust default policy refresh time (currently 4h, this means up to 12 h until suspension info is at the services)