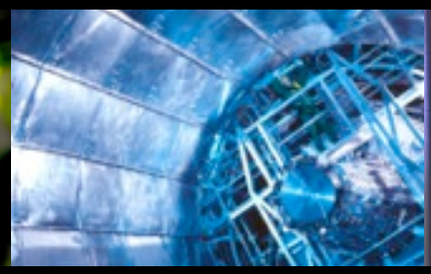
WLCG Group

# Worker Node security discussion
# Pre-GDB day

## Summary








WLCG
Worldwide LHC Computing Grid

# Security Controls

- Blocking/banning used mainly for incident response
  - Sites and a "central banning body" (central security operations) should may need to ban users
  - More rarely, the VOs may also want to ban users (in addition to VOMS removal)
  - Normally, the VOs will report incidents/malicious users to the central security operations

- Central banning needed to ensure appropriate incident response
  - Central security operations managing central banning lists
  - Banning conditions are already defined in existing security policies and procedures

# Argus

- "Authentication" cannot be used for banning
  - A user may be deemed malicious without being compromised
- "Authorization" is the appropriate way to ban users
  - Removing a user from VOMS is not sufficient due to long lived proxies.
  - Banning not really workable without central banning

- Central banning deployment proposal:
  - All WLCG sites must implement necessary mechanisms to pull central banning lists from the central Argus instance, for example by deploying Argus locally. The deployment of these solutions should be followed up in the GDB.
  - On the WN, Argus requires gLexec

# Ownership of the traceability

- Given the current job submission models chosen by several VOs, it is acknowledged that it is necessary for VOs and sites to collaborate and share information to fully resolve security incidents.

- There is a concern with traceability for data, for those cases in which the transaction with the storage element is not done with the user's proxy. There are also concerns with a number of services not using standard logging mechanisms (syslog).

# Virtualization on the WN

- Recommendations aimed at the sites should be produced to help fulfilling the logging and traceability policy on the WN (whether or not virtualization is used)

- A working group should be appointed to conduct this work

# Using external clouds

- When VOs use resources not provided by WLCG sites, or sites choose to expand by instantiating off-site cloud VMs, it is currently not possible to do so in such a way that conforms with WLCG security policies
- As specified in the WLCG risk assessment, there are significant concerns in using external cloud providers and additional work is needed to understand the policy issues it raises. There are also operational issues (including procedures and traceability)
- A working group should be appointed to conduct this work and report back to the GDB or MB as appropriate
- In the meantime VOs or sites instantiating external cloud resources should be aware of these concerns and the responsibilities they accept by using these services

# Critical proxy extension

- There are two paradigms in use at the moment. The "send a limited user proxy" model of ATLAS, LHCb, and CMS, and the "no user proxy" model of ALICE.
- ALICE can make an extension to their model to pass a "critically limited" proxy which is only valid for use by glexec. This model is much better as far as secure transport of the proxy goes, however it should be verified that there is a persistent site-level link between data and actual user.
- The model for the other three experiments requires care in transport and handling of user proxies, however these proxies can be used to provide the desired link at the storage element between file and payload owner.

# Proxy lifetime

- Can we reduce the VOMS proxy lifetimes (currently 3 to 8 days depending on the VO) back to 24h?
  - Consensus: good idea and should be a priority item of work for LS1
  - Technical implications and work needed are yet to be evaluated by each of the VOs.

# Pool account recycling

- Pool account recycling
  - Proposal: User accounts on the WN are important for security operations and pool accounts may be recycled only after they have been unused for 6 months.
  - (Unless the account is causing operational issues (too big, etc.)?)
  - It was noted that enabling gLexec on the WN will probably increase the number of necessary pool accounts.
  - VOs should publish the number of pool accounts they need in their VO Card.
  - The situation in OSG was not discussed

# Far, far away...

- A federated identity model is being considered in order to hide X509 away from end users.
- If this becomes mainstream, in the (much) longer term (LS2?) it might be useful to extend this effort to the backend services
- Explore alternative models (for example based on cryptographic signatures like Unicore, Oauth, etc.)

# Summary

- Central banning (Argus) is needed and should be deployed
  - Depends on gLexec
- Efforts needed to improve our traceability
  - Provide recommendations to the sites
  - Ensure all our software offers sufficient traceability & uses syslog
  - Sites and VOs will have to collaborate to resolve incidents
- Using external clouds brings significant concerns
  - Need to be evaluated
  - Additional policy work likely required
- Work to bring the proxy lifetime back to 24h during LS1
- Pool accounts should be recycled only after they have been unused for 6 months