Working Group on Logging

TCB Action 06/04

Michel Drescher

e-infrastructure

Harmonised logging

- Very easy when:
  - Dealing with monolithic systems
  - Only one programming language is used
  - Only one platform is used
- Not so easy when
  - Systems are distributed
  - Many different languages & libraries are used
  - Many different platforms are used
  - Developers are fairly autonomous

“Organic” logging

- Many non-matching logging levels
- Many different ways to configure logging
- Many different log message formats
  - Message metadata, i.e. timestamp, level, target
- Many different logging infrastructures
  - UN*x Syslog, Java platform, …
- Admins must know the union of all!

Logging for infrastructure management

- Records a system's health and state
- Is required for system audits
- Needs to be configurable for changing environments or incidents
- Needs to integrate with existing logging persistence infrastructures

Working Group proposal (1)

- Examine infrastructure management aspects
- Define a commonly used logging ontology
  - Logging levels
  - Logging domains (e.g. security, access, management, debug)
  - Message metadata
  - Persistence infrastructure
- Examine uniform configuration approaches
  - Configuration file formats?
  - Integrated with fabric management solutions?
  - Sensible default values (policy?)

Working Group proposal (2)

- Short term topics
  - Define ontologies
  - Any issues that can be handled as GGUS tickets (based on the ontologies)
- Medium/Long term topics
  - Harmonised configuration files vs. default configuration (by policy)
  - Harmonised configuration interface
  - Integration with fabric management solutions
  - Will results in TCB level requirements
- Mandate proposal
  - Define scope
  - Lifetime 6 months
  - Outputs
    - Reach short term goals
    - Reach harmonisation in configuration files and interface
    - Develop requirements to be submitted to the TCB
    - Reports to the TCB on activities, executive for each TCB meeting