



**GridPP**

UK Computing for Particle Physics

# Security Monitoring

Week 09      Week 10      Week 11

CPUS ■ Running Processes

Memory last month

Romain Wartel



- Security monitoring is one of OSCT's activities
- A Security Monitoring WG has been created:
  - Ake Sandgren (Umea University)
  - Andrew McNab (Manchester University)
  - Bob Cowles (SLAC)
  - Christine Leroy/Michael Leclerc (CEA)
  - Dimitris Zilaskos (Aristotle University of Thessaloniki)
  - Emanouil Atanassov (IPP)
  - Ian Neilson (CERN)
  - Leif Nixon (Linkoping University)
  - Miguel Cardenas Montes (CIEMAT)
  - Riccardo Brunetti (INFN)
  - Romain Wartel (RAL/CERN)



1. System-level security monitoring
  - Define a set of recommended tools for sites to deploy
  - Provide sites with documentation and/or installation mechanisms to deploy these tools
  - Search for new tools that would benefit our community
  
2. Grid-level security monitoring
  - Define what elements should be monitored in the grid
  - Design and implement the appropriate grid security monitoring tools
  - Provide sites with documentation and/or installation mechanisms to deploy these tools



Several issues have been raised:

- *Sites do not have time/resources to install and configure security monitoring tools.  
In other words, we need to make monitoring simple/centralised or nobody will use it.*
- Existing monitoring tools should are not advertised enough
- Restricting access to the monitoring reports seems to be a general concern



- May 05 - Creation of the group  
A group of LCG/EGEE members gathered to form the security monitoring WG
- Jun 05 - Initial ideas/discussions/objectives  
Several members shared their view and experience of security monitoring.  
A few objectives have been described.  
During last JSPG meeting (13-14 June 05), the following points emerged:
  - Outputs of the tools should be as centralised as possible
  - Future grid monitoring tools should be integrated in existing LCG/EGEE infrastructure
  - For a start, a simple set of important metrics should be monitored on a few critical components of the grid
- Jul/Aug/Sept 05 - Identify one or several critical components of the grid and important metrics that should be monitored
- Oct/Nov/Dec 05 - Design, develop and deploy a monitoring tool to monitor these critical components.



- SECMON Box prototype almost finished
  - DVD images Real Soon Now ...
- All local monitoring done via syslog protocol
  - Easy to integrate (already there)
  - Easy to log middleware messages to syslog
- Remote monitoring via RSS feeds
  - Can pull according to date range, message severity and/or service name ("sshd" etc)
- Remote administration via GridSite/cgi-scripts
  - Sites can delegate admin of their box to Tier2/Tier1 staff, without giving up root.
- See Andrew's talk tomorrow for technical details



**GridPP**

UK Computing for Particle Physics

# Discussion