Contribution ID: **163**   Type: **poster**

Using Tripwire to check cluster system integrity

Wednesday 29 September 2004 10:00 (1 minute)

Expansion of large computing fabrics/clusters throughout the world would create a need for stricter security. Otherwise any system could suffer damages such as data loss, data falsification or misuse.

Perimeter security and intrusion detection system (IDS) are the two main aspects that must be taken into account in order to achieve system security.

The main target of an intrusion detection system is early detection in the previously mentioned cases, as a way to minimize any damage in data contained in the system.

Tripwire is one of the most powerful IDSs and is widely used as a security tool by the community of network administrators. Tripwire is oriented to monitor the status of files and directories, being able to detect the lightest change suffered by them.

At Ciemat, Tripwire has been used to monitor our local clusters, involved in GRID projects such as implementation of LCG prototypes, to guarantee the integrability of data generated, and stored there. It is used as well to monitor any modificacion of operating system files and any other scientific core software.

Primary authors: PEREZ-CALLE, E. (CIEMAT); RODRIGUEZ CALONGE, F.J. (CIEMAT); CARDENAS MONTES, M. (CIEMAT)

Presenter: PEREZ-CALLE, E. (CIEMAT)

Session Classification: Poster Session 2

Track Classification: Track 4 - Distributed Computing Services