Contribution ID: **164** Type: **oral presentation**

Using Nagios for intrusion detection

Wednesday, 29 September 2004 14:40 (20 minutes)

Implementing strategies for secured access to widely accessible clusters is a basic requirement of these services, in particular if GRID integration is sought for. This issue has two complementary lines to be considered: security perimeter and intrusion detection systems. In this paper we address aspects of the second one.

Compared to classical intrusion detection mechanisms, close monitoring of computer services can substantially help to detect intrusion signs. Having alarms indicating the presence of an intrusion into the system, allows system administrators to take fast actions to minimize damages and stop diffusion towards other critical systems.

One possible monitoring tool is Nagios (www.nagios.org), a powerful GNU tool with capacity to observe and collect information about a variety of services, and trigger alerts.

In this paper we present the work done at CIEMAT, where we have applied these directives to our local cluster.We have implemented a system to monitor the hardware and system sensitive information. We describe the process and show through different simulated security threads how does our implementation respond to it.

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

Presenter: CARDENAS MONTES, M. (CIEMAT)

Session Classification: Grid Security

Track Classification: Track 4 - Distributed Computing Services