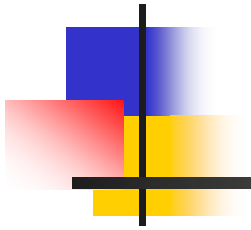


Security at The IT-ROC

Status and Plans

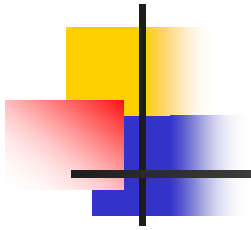
IT-ROC

- IT-ROC includes many computing sites (40) belonging to different organizations (INFN,ENEA,CNR...).
  - 1 T1
  - 9 T2
  - 30 Sites
- A (too) small working group exists for security-related activities and coordination
- Up to now, each site carried on its own activity independently.

Results of a small survey on IT-ROC sites:

- Almost 100% of the sites use some kind of firewall to limit network access to the grid resources.
  - Generally at the level of the site router (access to the LAN)
- Almost 100% of the sites monitor their grid resources
  - Nagios, Ganglia
- Very few sites use some kind of IDS or file integrity checkers to detect possible incidents.
- Very few sites have a backup policy for grid-related data.
  - √ Configurations, User data (UI)...
  - × Log files
- Few sites use an automatic upgrade system.

Interfacing with Existing policies.

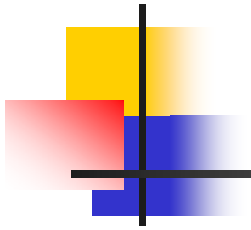


- IT-ROC Grid sites are generally hosted by some research institutions that have already some guidelines in matter of security.
- The networking infrastructure itself is managed by the GARR consortium which has its own AUP, CSIRT and incident response rules.
- What the IT-ROC security group tries to do is also to provide a “liaison” between the different entities.

GARR-CERT

- The GARR-CERT is the group responsible to manage the security incidents in the Italian research network infrastructure
- It classifies the incidents and alerts the local contacts (APM)
  - Max. response time from 1 hour to 3 days (DoS attacks – mail relay)
  - In case of no response the site/machine is filtered out on the GARR network routers
- It maintains a db of all the incidents and security alerts
- It provides support for the problems resolution.

Support and Incident Reporting



- An internal mailing list has been set up for discussion and incident reporting.

  grid-security@infn.it

- Members of this mailing list are the ROC Security Officers. Site Security Contacts can post on it
- Wiki pages with information concerning LCG/EGEE policy documents and contacts have been prepared.
- A list of Site Security Contacts is maintained and is available to all the site administrators and users registered to the IT-ROC web portal.

WIKI pages

https://grid-it.cnaf.infn.it/checklist/modules/dokuwiki/doku.php?id=cmt:security_coordination

Security Management in the Italian ROC

Table of Contents

Edit

Activities of the IT-ROC Security Group

The security group's main task is to keep contacts with the LCG/EGEE Security working groups and to provide links, references and guidelines for the italian production grid sites.
Moreover it is responsible to coordinate actions in case of a security incident occurring in one of the italian sites and to participate to the Security Service Challenge when requested by the project.

Another goal of the group is to promote best practice and discussions among site managers and resource administrators, in order to share a common knowledge concerning security monitoring, tools and procedures.

Edit

IT-ROC Contacts

- IT-ROC Security Officier : Luca Dell'Agnello
- IT-ROC Incident Response Coordination : Riccardo Brunetti
- IT-ROC Security Mailing List : grid-security **Please report incidents here**
- IT-ROC Managers: Cristina Vistoli; Luciano Gaido; Paolo Veronesi
- A list of the Security Contacts for the italian sites can be found at the section **Sites List** of the IT-ROC Web Portal

Edit

Incident Reporting Escalation and Procedures

Edit

Case 1 : An Incident is Reported by a Site Administrator

WIKI pages

https://grid-it.cnaf.infn.it/checklist/modules/dokuwiki/doku.php?id=cmt:security_coordination

Relevant Policy Documents

The italian ROC, other than following its own Security Policies (as approved by the GARR CERT or regulated by each single site administrators), admits the main security policy documents approved by the LCG/EGEE management and provided by the Joint Security Policy Group.

The Joint Security Policy Group (**JSPG**) was formed in 2004 as an extension of the LCG Security Group and mandated to advise and make recommendations to the LCG Grid Deployment Manager and the LCG Grid Deployment Board (**GDB**) on matters related to LCG/EGEE Security.

The main JSPG activity is to maintain and provide updated policy documents concerning the security of the Grid infrastructure, focusing on the formal aspects like usage rules, user/sites/VO registration, and top level requirements on the LCG/EGEE participants.

Security and Availability Policy

- Document: Security and Availability Policy
- Audience: *Resources, Users, Administrators, Developers and Virtual Organizations*
- Description: This top level document sets out the Policy regulating the activities of Grid participants which relate to the security and availability of Grid facilities and resources. It places responsibilities on each of these bodies.

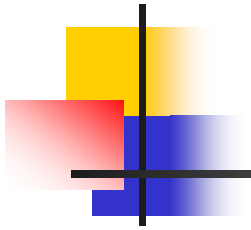
Grid Acceptable Use Policy

- Document: Grid Acceptable Use Policy
- Audience: *Every user* willing to register to a VO and to participate in some Grid related activity
- Description: This document sets out the Policy regulating the usage of the Grid infrastructure

LCG/EGEE Virtual Organization Security Policy

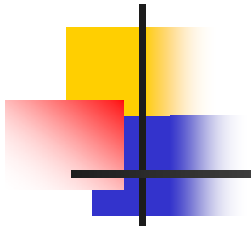
- Document: LCG/EGEE Virtual Organization Security Policy
- Audience: *VO Members and VO Managers*
- Description: This document describes a set of responsibilities placed on the members of the VO and the VO as a whole through its managers. It describes the

Incident Reporting Escalation (from site to LCG/EGEE)



- The Site Security Contact sends an Email to the grid-security mailing list. (The incident could also have been notified by the GARR-CERT to the site)
- The risk is evaluated and ROC Security Officer escalates the incident to project-lcg-security-csirts@cern.ch
- The Site Security Contact eventually notifies the incident also to GARR-CERT (if not known).
- The ROC Security Officers follow the incident and ensure that all the needed actions are taken (ban a user, remove sites from bdii ecc..). They also keep informed about actions taken by the GARR-CERT

Incident Reporting Escalation (from LCG/EGEE to Site)



- The ROC Security Officers receive notification through GGUS.
- The ROC Security Officers escalate the incident to the appropriate Site Security Contact (using mail contact and/or ticketing system) and this last eventually informs the GARR-CERT
- The ROC Security Officers follow the incident and report back to ggus and/or LCG security mailing lists.

What we plan to do

- Set up a working group with the mandate to collect experiences and propose some basic operational practices and/or requirements. We want to start from what has already been done at the sites.
  - Use of IDS and File Integrity Checkers (interesting work on hidden IDS using virtualization)
  - Backup and auditing
  - Firewalling

What we plan to do

- Prepare a template document to be periodically prepared by site administrators containing the security plans for their site.
  - Contacts and responsibilities
  - Risk analysis
  - Physical/Network access to grid farms
  - Management of user's data and personal information
  - Backup and recovery policies