# CHEP'07 et Sécurité

- Morceaux choisis...
- www.chep2007.org

# Présentations

- Security Incident Management in a Grid environment (Marcus Schulz)
- Identity Management (Alberto Pace)
- Power and Air Conditioning Challenges in Computing Centers (Amber Boehnlein)
- gLexec: glueing grid computing jobs to the Unix world (David Groep)
- The Gridsite Security Architecture (Andrew McNab)
- Adressing the Pilot Jobs seccurity problem withj gLexec (Igor Sfiligoi)

# ISSeG training session

- Session pratique mise en oeuvre de la sécurité selon ISSeG
- ISSeG = Integrated Site Security for Grids
- Une approche pragmatique de la sécurité issue du CERN
- Voir plus loin ...

# Security Incident Management in a Grid environment

- Les Grilles de Calcul sont une cible intéressante
  (Nb de machines, disponibilité, bande passante)
- Elles sont aussi très exposées
  (propagation entre sites via relations de confiance, homogénéité des OS, niveaux de sécurité inhomogènes)
- Cependant, jusqu'à présent pas d'incident spécifiquement lié aux techno Grilles

CHEP'2007:Security Incident Management in a Grid env. (Marcus Schulz)

# Politique de Sécurité Grille

- LCG/EGEE Incident Handling and Response Guide (JSPG, 28/11/2005)
  - Traitement des incidents en lien avec le ROC Security Contact
  - EGEE Operational Security Coordination Team
  - Annonce via projetct-egee-security-csirts@cern.ch
  - Intégration avec la Politique Locale
- Bonnes Pratiques et entrainement
  - Voir le CIC Portal

CHEP'2007:Security Incident Management in a Grid env. (Marcus Schulz)

# Sécurité Grilles : Conclusion

- Des procédures établies
- Renforcer la confiance entre sites et  diminuer les différence de niveau de sécurité
- La sécurité repose fortement sur les sites et les règles de bases restent le plus important
- Il reste beaucoup à faire en matière de prévention et détection

CHEP'2007:Security Incident Management in a Grid env. (Marcus Schulz)

# Identity Management

- Les dispositifs classiques de renforcement de la sécurité (pare-feu, DMZ, proxies,etc.) ne suffisent pas
- Il faut prendre en compte :
  - Le Facteur Humain (education, sensibilisation,...)
  - La gestion des identités et des accès
- Authentication, Authorization, Accounting (AAA)
  - Trois composants indépendants en théorie

CHEP'2007 : Identity Management (Alberto Pace)

# Identity Management

- Authentication
  - Pouvoir mobiliser plusieurs techniques
- Authorization
  - Traduction des rôles avec les mécanismes natifs des OS
- Accounting (Traçabilité)
  - Who, When, Where, What
  - Une contre-partie de l'augmentation de privilèges ?

CHEP'2007 : Identity Management (Alberto Pace)

# Identity Management : Conseils

- Un compte unique (SSO) pour chacun (ne donne accès à rien sans autorisation)
- Création de compte automatique
- Opérations privilégiées via un mécanisme d'élévation de type « su » avec traçabilité des actions
- Interface pour la gestion des identités utilisable par l'administration et par les utilisateurs eux-même pour certaines informations
- Autorisations uniquement par l'intermédiaire de groupes (permet de gérer des communautés)

CHEP'2007 : Identity Management (Alberto Pace)

# Power and Air Conditioning Challenges

- Les batiments et salles machines ont une durée de vie bien supérieure à celles des équipements informatiques
- On prévoit une demande toujours plus forte d'espace et de puissance
- Il faut consommer 330 Watts pour fournir 100Watts à un équipement électronique
- Il n'existe pas de solution unique
-

CHEP'2007:Power and Air Conditioning Challenges in Computing Centers (Amber Boehnlein)

# Power and Air Conditioning Challenges

- Niveaux à considérer : processeur, boitiers, racks, salles.
- Au niveau rack, il faut penser à l'évacuation de la chaleur. Des dispositifs existent (cheminées, refroidissement à eau)
- L'alimentation des rack en courant continu est envisagée
- La planification des espaces (salles ou portions de salles) est importante

CHEP'2007:Power and Air Conditioning Challenges in Computing Centers (Amber Boehnlein)

# Power and Air Conditioning Challenges

- Stratégies :
- Swing spaces : (espaces tampon ?)
- Fallowing : vider totalement une partie de salle, ré-équiper en électricité et en clim de manière adaptée aux nouveaux équipements
- Espaces selon usage :
  - avec ou sans UPS
  - secouru par un générateur
  - besoin de clim réduits (bandothèques)
- Rechercher les économies à tous les niveaux

CHEP'2007:Power and Air Conditioning Challenges in Computing Centers (Amber Boehnlein)

# gLexec

- Un mécanisme similaire à apache suExec permettant d'associer un DN Grid à un identifiant Unix
- Une librairie unique pour plusieurs services grille (LCAS, LCMAPS, GUMS)
- Permet à certains de ces processus de tourner sur une identité non-root
- Permet d'utiliser des « pilot-jobs » et de tourner sous l'identité de l'utilisateur, non celle qui lance les pilot-jobs
- Nécessite un moyen sûr de diffuser la politique pour gLexec.

CHEP'2007:gLexec: glueing grid computing jobs to the Unix world (David Groep)

# The Gridsite Security Architecture

- A l'origine : gestion des certificats Grille pour Apache
- Un module Apache : mod_gridsite
- Une librairie d'authentification capable d'utiliser un grand nombre de technologies : Certificats X509, Listes de DNs, VOMS, Client DNS hostname, <plus à venir>
- API en C mais des interfaces sont prévues pour C++, Python, Perl

CHEP'2007:The Gridsite Security Architecture (Andrew McNab)

# ISSeG

http://isseg.web.cern.ch/ISSeG/03_About_IsseG/Aims/Aims.htm

- Pour prendre en compte les nouveaux problèmes de sécurité liés aux Grilles de Calcul
- Complémentaire à EGEE Grid Security
- Se concentre sur la sécurité au niveau d'un site
- Aborde simultanément les aspects administratifs, techniques et éducationnel

# ISSeG Training Site

http://isseg-training.web.cern.ch/ISSeG%2Dtraining/default.htm

- En cours de développement ...
- Un ensemble de documents décrivant :
- Des menaces et des risques par catégories
- Des recommandations selon la taille des sites
- Des recommandations pour chaque communauté concernée :
  - Utilisateurs
  - Administrateurs de sites
  - Développeurs
  - Responsables (Managers)