Sécurité sur la Grille

M. Jouvin (LAL-Orsay)

Tutorial Utilisateur Grille

MRM Grille Paris Sud, LAL

2 Juin 2010

Agenda

- Les besoins et les contraintes
- Les différents composants
- Les certificats
- Les Virtual Organizations
- Les proxies

Système(s) de sécurité

- La grille est un système largement distribué :
  - Des milliers d'utilisateurs
  - Plus de 300 sites dans le monde
- Le système de sécurité doit permettre d'établir des relations de confiance entre les différents acteurs
  - Les administrateurs de sites
  - Les utilisateurs

Contraintes

- Evolutif :
  - Les personnes ne peuvent pas connaître toutes les autres
  - Performance doit être acceptable
  - Permettre l'accès de personnes de différents pays
- Utilisation doit être « simple » :
  - Sinon, les gens ne l'utilisent pas
  - Equilibre difficile entre sécurité et utilisation simple
  - Doit permettre une délégation des droits utilisateurs à certains services (soumission de jobs, transfert de fichiers…)

Fonctionnalités Essentielles

- Authentification
  - Qui est qui ?
- Autorisation
  - Qui a le droit ?
- Audit sécurité
  - Qui fait quoi et quand ?
- Comptabilité
  - Combien de ressources sont utilisées par un utilisateur ?

Grid Security Infrastructure

- GSI : un standard pour les logiciels de grille de calcul
  - Conçu par le projet Globus aux U.S.A.
  - Utilisé par (presque) toutes les grandes grilles
- Basé sur « Public Key Infrastructure »
  - Chaque entité a une clé publique et une clé privée
  - Format : X509v3
- Principales fonctionnalités :
  - Single sign-on : le mot de passe n'est donné qu'une seule fois
  - Délégation : une personne (ou un service) peut autoriser un autre service à agir en son nom
    - ✓ Autorise une autre entité à utiliser son authentification et ses autorisations
  - Authentification mutuelle : le destinataire et l'émetteur s'authentifient

Certificat = Passeport Grille

- Un certificat n’est qu’une pièce d’identité !
  - Ne donne aucun droit en soi
- Un certificat X509v3 peut être émis pour
  - Une personne physique (certificat personnel)
  - Une machine (certificat de hôte)
  - Un programme (certificat de service) : pas (encore) utilisé
- La clé publique (certificat)
  - Signée après vérification de l'identité du destinataire
  - Publiée sur le réseau
- La clé privée : chiffrée et protégée par un mot de passe
  - Conservée sur le poste de l’utilisateur ou sur la machine

Autorités de Certfication (CA)

- Rôle essentiel dans l'établissement de la confiance
  - En charge de « signer » les certificats utilisateurs /machines
  - Doit vérifier le droit de l'utilisateur à utiliser la grille avant de signer un certificat
    - Travail de « préfecture » si on prend l'analogie des passeports
- Une ou plusieurs par pays ou groupe de pays (~90)
  - Etablit des relations de confiance avec les autres CAs
  - Coordonne les activités au niveau de chaque pays
- Pour la France, seuls les certificats de la CA « GRID-FR » sont acceptés sur la grille.

Authentification = Certificats

- Principales informations :
  - Le sujet ou DN du certificat identifiant de façon unique un utilisateur ou une machine
    - Equivalent du username dans la grille
  - La période de validité du certificat (en général une année)
  - Des extensions X509v3
    - Les utilisations autorisées du certificat, email…
- 2 Formats différents
  - PKCS12 : un seul fichier pour la clé privée ET la clé publique
  - PEM : deux fichiers, 1 pour la clé privé, 1 pour la clé publique
  - Tous les outils grille acceptent le format PKCS12 mais Globus et gLite utilisent un nom de fichier différent…
    - usercert.p12 pour gLite, usercred.p12 pour Globus
    - Possibilité de faire un symlink

Organisations Virtuelles

- Organisations Virtuelles (VOs)
  - Ensemble d'individus ayant des buts communs
  - Membres de la VOs répartis en sous-groupes
    - 1 membre peut aussi avoir 1 *rôle* dans le groupe
  - Appartenance à 1 VO détermine les ressources accessibles
    - Groupes et rôles peuvent modifier les droits d'accès aux ressources
  - 1 utilisateur peut appartenir à plusieurs VOs
- Les utilisateurs sont regroupés par :
  - Expériences : biomed, alice, atlas, esr, …
  - Projets : embrace, gridpp, auvergrid, …
  - Laboratoires : vo.lal.in2p3.fr, vo.u-psud.fr, cppm, …
- Liste des VOs existantes :
  - http://cic.gridops.org/index.php?section=home&page=volist

Autorisation

- Autorisation = droits par service et par site sur la base de :
  - La VO à laquelle appartient l'utilisateur
  - Le groupe de la VO auquel appartient l'utilisateur
  - L'identité de l'utilisateur
- L'administrateur d'une VO :
  - Décide qui peut être un membre de cette VO
  - Repartit les membres dans des groupes et sous-groupes
  - Définit les « rôles » de ses membres
- L'administrateur d'un site :
  - Décide quelles VOs le site supporte
  - Met en place le contrôle d'accès défini par la VO
- 1 service orienté « autorisation » : ARGUS
  - Permet un contrôle central (mapping, banissement)

Délégation

- Les utilisateurs ne peuvent pas autoriser chaque transaction dans la grille :
  - Trop de jobs dans la grille
  - Les jobs ne sont pas forcément localisés sur un seul site
  - Un job peut avoir besoins d'utiliser d'autres services
- Doit être possible de déléguer les droits d'accès aux jobs et aux services grilles :
  - Certains services (WMS, FTS, CREAM CE) ont besoin d'agir au nom de l'utilisateur avec d'autres services
  - La clé privée du certificat est une information sensible et ne peut être transmise aux services grilles
  - Création d'un clone de courte durée du certificat : « proxy »

Proxy

- Nouveau certificat :
  - Signé par le certificat d'utilisateur
  - Période de validité beaucoup plus courte que le certificat utilisateur
    - ~1/2 journée
  - Valable pour une VO avec éventuellement un groupe/rôle spécifique
    - Besoin d'un autre proxy pour agir au nom d'une autre VO…
  - Le fichier contenant le proxy est envoyé avec le job et permet d'agir avec les droits de l'utilisateur
- Proxy de courte durée (12h pour la plupart des VOs)
  - *voms-proxy*-init --voms VO, -info, -destroy
- Proxy de longue durée (durée spécifiée par l'utilisateur)
  - *myproxy*-init, -info, -destroy, -get-delegation

Autres Services

- Les services grilles génèrent un « log » des actions
  - Pour comprendre qui fait quoi et quand
  - Pour comprendre le fonctionnement du système

- Comptabilité
  - Pas vraiment la sécurité mais basée sur l'authentification
  - Base des données centralisée pour l'utilisation (par VO)
    - http://www3.egee.cesga.es/gridsite/accounting/CESGA/egee_view.html
  - Le middleware ne met pas encore en place des quotas.

Récapitulatif

- Les grilles basées sur gLite utilise la « Grid Security Infrastructure » comme système de sécurité.
- Authentification
  - Réseau des CAs signent les certificats des entités
  - Le certificat est le « passeport grille » pour les utilisateurs
- Autorisation
  - Gérée par les Organisations Virtuelles
  - Mise en place par les administrateurs des sites
- « Proxies »
  - Contiennent les VOs, groupes, et rôles de l'utilisateur
  - Permettent une délégation de droits aux services grilles et aux jobs