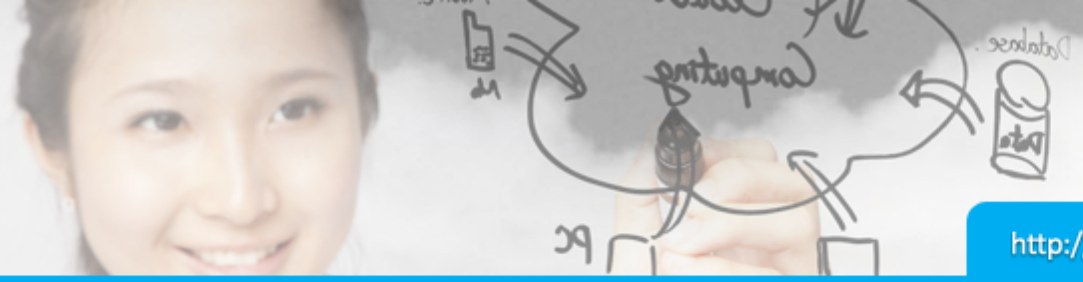
Going the extra mile

France Grilles : la sécurité dans une infrastructure distribuée

Jérôme PANSANEL

Crédits : V. Breton et G. Romier



France Grilles

Le GIS France Grilles

- Créé en 2010 par 8 partenaires
- Une fédération de ressources distribuées (grille de calcul, Cloud Computing, stockage) pour la recherche scientifique
- Renouvelé fin 2016 pour deux ans
- En pleine mutation pour relever les nouveaux défis et s'accorder à la nouvelle feuille de route du numérique en France
- Une communauté d'experts
- Un ensemble de services (FG-DIRAC, FG-iRODS, formation, …)
- Liens avec les communautés européennes (EGI, ...)
- Porté par un Master Projet IN2P3 : France Grilles Initiative depuis janvier 2017

→ **http://www.france-grilles.fr**

Dimension nationale

Projets scientifiques

- IFB
- LCG-France
- Phénome
- Préservation des logiciels
- Systèmes complexes

France Grilles Infrastructure de Recherche labellisée par le MENESR

- Démarrage de la préparation de la prochaine feuille de route édition 2018 en novembre 2016 → nouvelle infrastructure T2 France

Mise en place des groupes de travail (GT) pour implémenter la feuille de route des infrastructures numériques

- Été – automne 2016
- Participation au GT2 (Cloud) → offre(s) de services Cloud en terme de systèmes d'information et de calcul scientifique pour l'enseignement supérieur et la recherche

Dimension Européenne

Des relations privilégiées avec EGI

- P.-E. Macchi membre de l'Executive Board de EGI depuis décembre 2016
- V. Beckmann représentant français au Council d'EGI
- J. Pansanel correspondant pour les opérations en France et membre du Cloud Technical Coordination Board depuis octobre 2016

Démarrage du projet pilote du projet European Open Science Cloud

- Kick-off le 1er janvier
- France très présente (CEA, CNRS, INRA, RENATER)

Coordination du projet EINFRA-12 pour la France

- Démarrage janvier 2018

Catalogue de services 1/2

FG-Cloud
- Instanciation de VMs et de solutions (Cluster, Hadoop) multisites (SlipStream, DIRAC)
- Formation et documentation
- Aide aux administrateurs
- Accès au Cloud EGI

FG-DIRAC
- Instance nationale DIRAC
- Remplaçant du WMS / accès à la grille de calcul
- Formation
- Hébergement multi-VOs

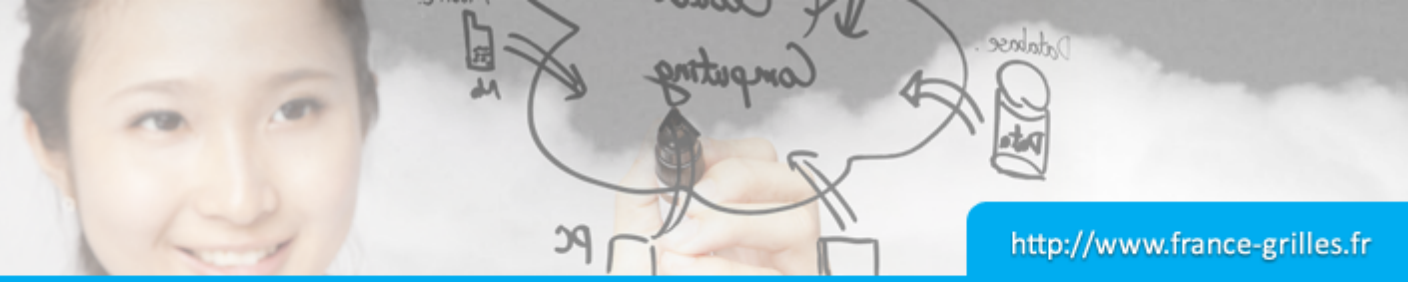
FG-iRODS
- Accès à une zone de stockage iRODS (100 TB) pour les données scientifiques
- Accessible depuis les infrastructures de grille et de Cloud (et au-delà)
- Formation

Catalogue de services 2/2

Formation
- Cadre pour les formations
- VO spécifique – vo.formation.idgrilles.fr
- Certificats temporaires dédiés
- Réseau de formateurs

Certificats robot GRID2-FR
- Mise en place de service utilisant des ressources Grille / Cloud
- RENATER

FG-SOL
- Nouveau service pour la préservation des logiciels
- Présentation pendant les journées SUCCES : **https://succes2017.sciencesconf.org/**



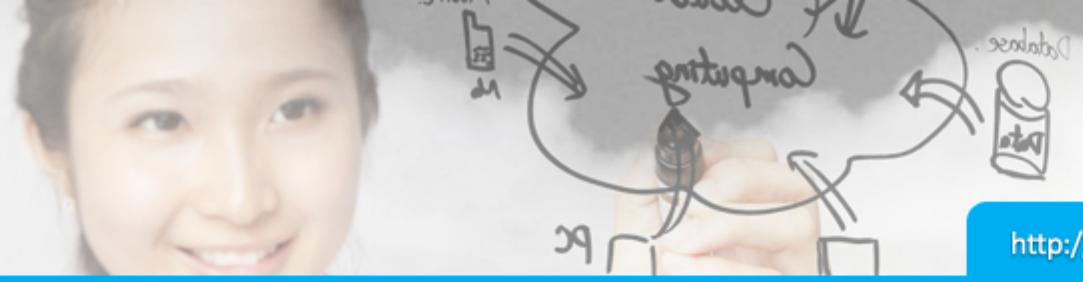
Prochaines formations

FG-Cloud
- Formation Utilisateur OpenStack – Novembre 2017 à Strasbourg
- Formation Administrateur OpenStack Neutron – Décembre 2017 à Clermont

FG-iRODS
- Formation Administrateur iRODS – Décembre 2017 à Strasbourg

FG-DIRAC
- Formation Utilisateur DIRAC – Janvier 2018 à Toulouse

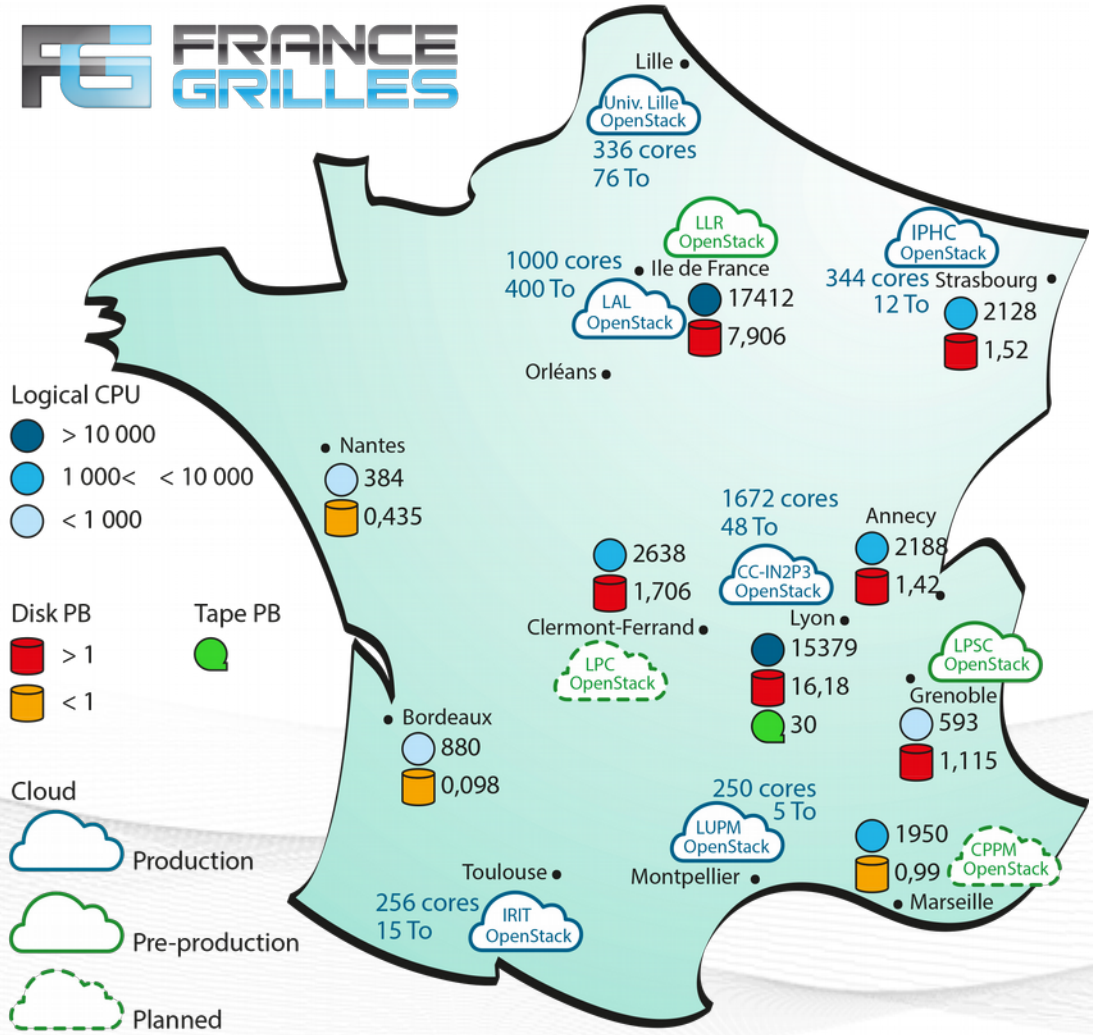
→ **http://www.france-grilles.fr**

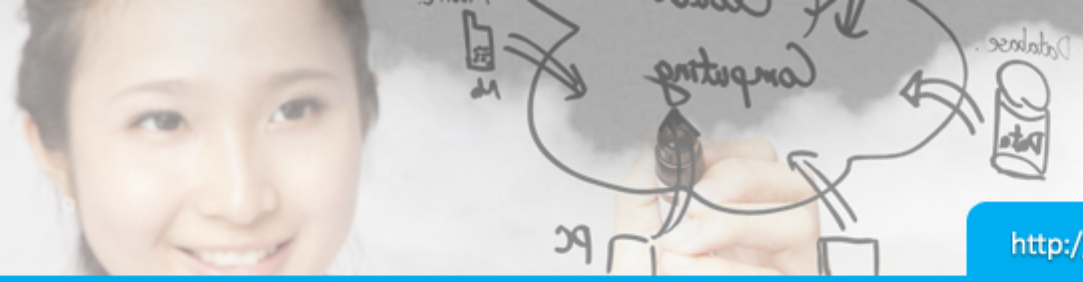


Les défis pour la sécurité

L'infrastructure

- Une infrastructure hétérogène distribuée
- Différentes entités juridiques
- Procédures site-spécifiques pour la gestion des incidents de sécurité
- Nombreux services (annuaire, framework d'authentification, soumission de jobs, stockage, ...)
- Une excellente connectivité
- Plus d'une centaine de milliers coeurs
- Plusieurs péta-octets de stockage



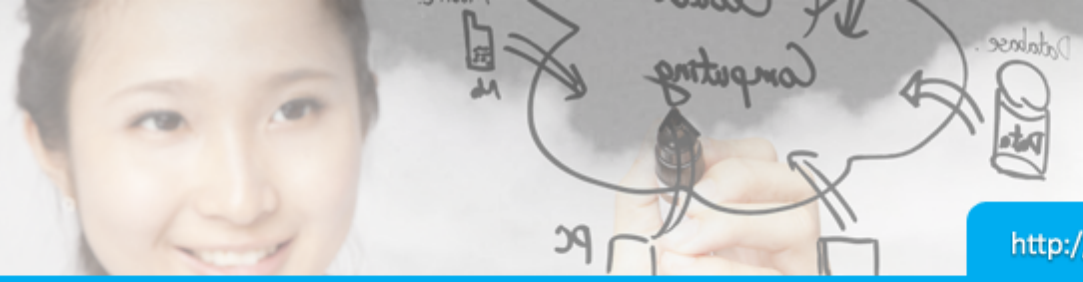


Les administrateurs

- Rarement à 100 % sur l'administration des infrastructures distribuées
- Rarement issus d'une formation en informatique (mais une passion certaine)
- Des expertises en fonction des services
- Utilisant des outils plus ou moins intégrés pour la gestion des configurations
- Travail en réseau et circulation d'information primordiaux
- Réactivité

Les utilisateurs

- Issus de nombreuses communautés scientifiques
- Des problématiques différentes dans la gestion des données (pérénité, confidentialité, volume, …)
- Compétences variables dans la gestion des soumissions, la sécurité, la mise à jour des outils, administration de machine virtuelle, ...
- Pour l'instant authentifiés d'une manière unique (certificats)
- Les communautés d'utilisateurs peuvent être prescriprices d'outils à déployer (surtout lorsqu'elles financent)
- Nous ne les connaissons pas → délégation de confiance
- Authenfication par certificat (principalement)

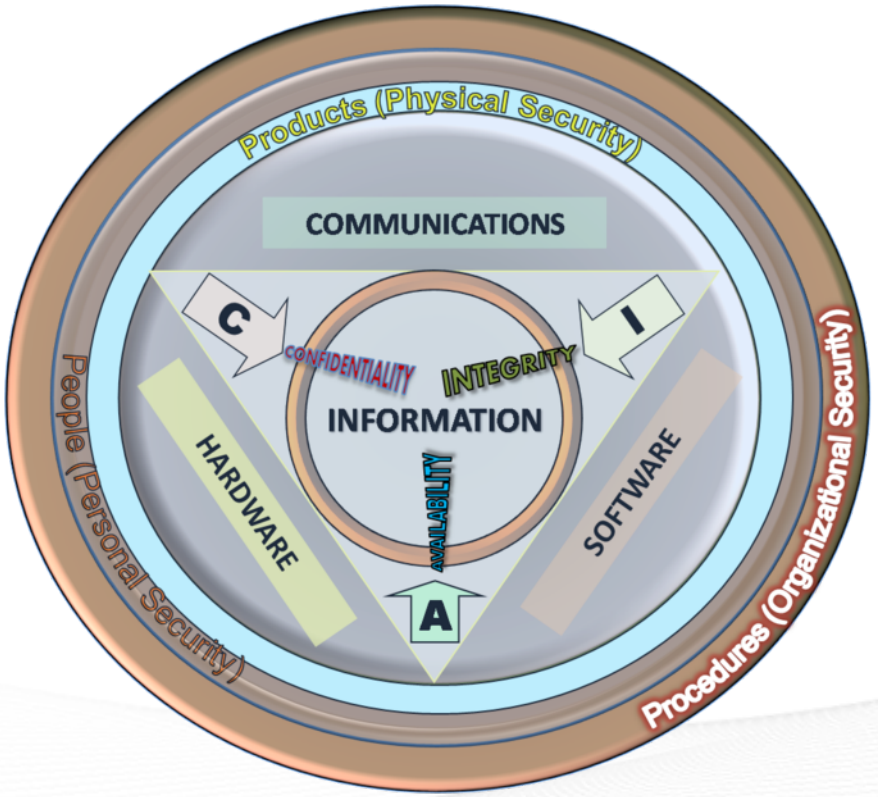


Les outils pour la sécurité

Concept

Points clés (modèle de CIA) :

- Confidentialité
- Intégrité
- Disponibilité
- *Traçabilité*



Périmètre :

- L'infrastructure
- Les procédures
- La communication vers les utilisateurs

Gestion de l'authentification et des autorisations

- Les utilisateurs s'authentifient avec un certificat
- Les services utilisent également un certificat (authentification et chiffrement)
- En France, délivré par l'autorité de certification GRID2-FR (RENATER)
- Les droits sont données en rejoignant des groupes d'utilisateurs (*Virtual Organization* – VO)
- Pilotage des autorisations à partir d'un service VOMS
- Le certificat ne voyage pas avec le job → utilisation de *proxy* (visa)
- Association au proxy d'un ensemble d'attributs indiquant ses groupes et rôles dans une VO
- Signature par le serveur VOMS de ces attributs
- Problème : nécessite un **accès** à une autorité de certification **reconnue** (IGTF)
- Mise en place du service EGI CheckIn (hub vers des fournisseurs d'identité)

Organisation au niveau européen

- CSIRT EGI
- Composé d'une dizaine de personnes
- Membre certifié de *Truster Introducer*
- 4 groupes de travail :
  - Incident Response Task Force (IRTF)
  - Security Drills Group (SDG)
  - Security Monitoring Group (SMG)
  - Training and Dissemination Group (TDG)
- Assurer les aspects opérationnels de sécurité pour parvenir à une infrastructure sûre
- Assure la coordination entre les différentes NGIs et les NRENs
- Étudie les vulnérabilités (CVE, …) et publie des recommandations
- Établit des procédures et des politiques de sécurité

→ **https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page**

Outils

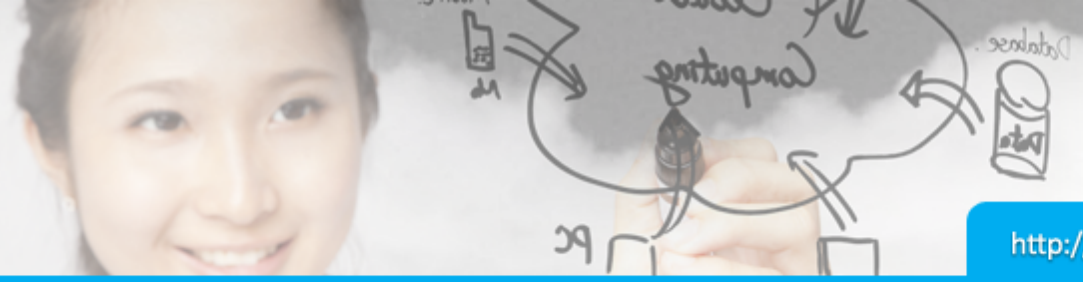
- Outil documentaire (WIKI)
- Suivi des problèmes par ticket
- Procédures de sécurité strictes (délai de réponse, action à réaliser, ...)
- Les canaux de communication sont vérifiés annuellement
- Pakiti (détection de vulnérabilité sur les sites)
- Développements logiciels pour assurer la traçabilité (OpenStack, ...)
- Développement de scénarios (*capture the flag*, attaque / défense, ...) pour la formation
- Challenges de sécurité

Coordination au niveau français

- Équipe au niveau de France Grilles piloté par le coordinateur de sécurité
- Le coordinateur est en relation étroite avec le CSIRT et les responsables des sites français
- Épaulé par le directeur technique de France Grilles et un représentant de la sécurité (chargé de mission SSI de l'IN2P3)
- Actions de formation
- Suivi des vulnérabilités et des mises à jour des sites
- Mise en place des procédures
- Développement de l'outil ZNeTS (mirroring réseau, alerte, …)
  → **http://www.znets.net/**
- Serveur Argus pour bannir centralement un utilisateur

Coordination au niveau des sites

- La coordination est propre à chaque site (en fonction des tutelles, …)
- Implique au moins un administrateur de site et le RSSI
- Le site doit appliquer les procédures de sécurité EGI et France Grilles (respect des délais de réponse, serveur ARGUS en local, ...)
- Gestion pro-active pour remonter les problèmes / utilisations inhabituelles
- Application des bonnes pratiques (centralisation et sauvegarde des logs, connaissance des procédures, gestion de l'accès aux infrastructures, mise à jour régulière, ...)



Questions ?