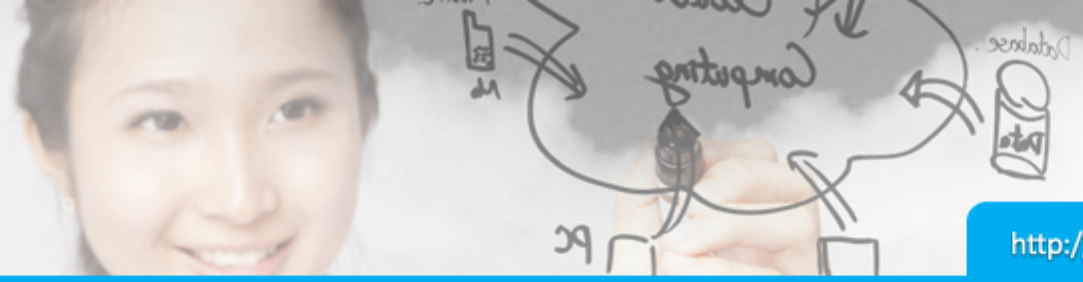
Quelle sécurité pour le Cloud fédéré ?

Jérôme Pansanel <jerome.pansanel@iphc.cnrs.fr>

Workshop Opérations France Grilles – Juin 2018



La sécurité France Grilles et EGI

Contexte européen

CSIRT EGI

- Une équipe en charge de la sécurité
- Veille active (évaluation des menaces)
- Coordonne le suivi des incidents
- Surveillance des sites
- Formation, diffusion d'information
- Contact pour les NGI et les partenaires

→ https://csirt.egi.eu/

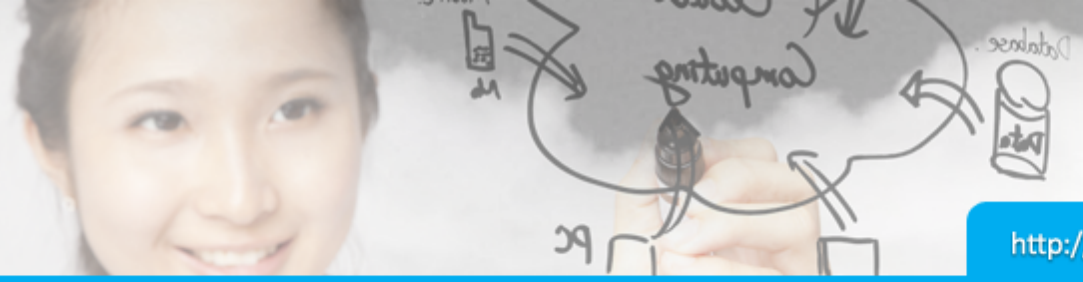
→ https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

Au niveau français

Un réseau opérationnel

- Coordinateur sécurité France Grilles
  → ngi-france-security-contact-l@france-grilles.fr
- Groupe d'administrateurs Cloud
  → cloud-admin-l@france-grilles.fr
- Liste opérations (nombreux administrateurs systèmes)
  → http://listserv.in2p3.fr/cgi-bin/wa?A0=operations-l
- Un wiki dédié
  → https://forge.in2p3.fr/projects/francegrilles-ops/wiki/Security

Attention aux informations diffusées sur les listes !



Au cas où …

En cas d'incident de sécurité

- Avertir votre correspondant sécurité local
- Contenir l'incident (p. e. snapshot / couper le réseau)
  → il faut garder des traces pour les étapes suivantes !
- Confirmer l'incident
- Avertir de la suspension du service
- Analyse de l'incident
- Debriefing
- Remise en opération

→ https://csirt.egi.eu/report-an-incident/

Déclaration d'incident

Rapidement après détection de l'incident

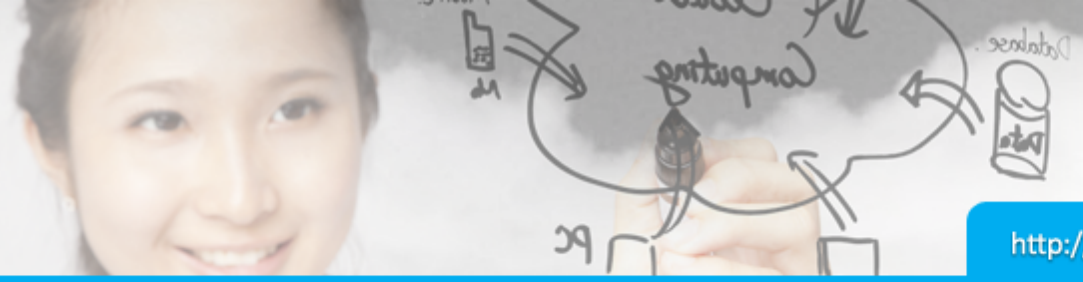
- Au niveau local : RSSI, tutelle, ...
- Au niveau français : le coordinateur sécurité France Grilles
  → ngi-france-security-contact-l@france-grilles.fr
- Au niveau européen pour les sites connectés à EGI :
  → https://csirt.egi.eu/report-an-incident/

Procédures

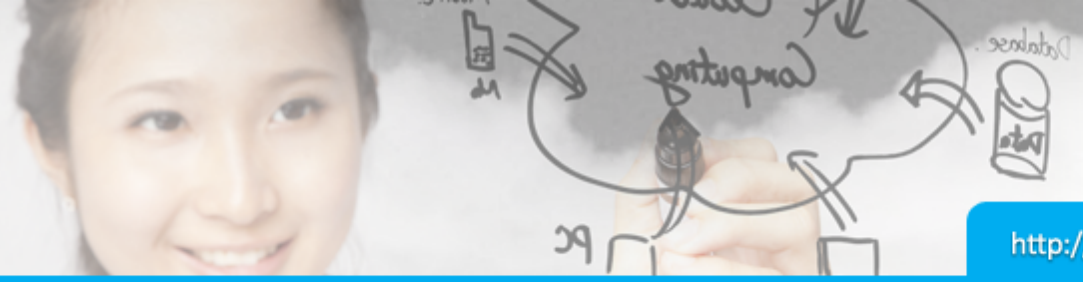
Pour éviter d'agir dans l'urgence

- Avoir des procédures testées
- Suivi d'activité d'un utilisateur / traçabilité
- Suspension d'un utilisateur
- Snapshot d'une VMs
- Informer les partenaires et les tutelles
- …

Des procédures standards → mise en commun ?



Sécurité d'une infrastructure OpenStack



Côté administrateur

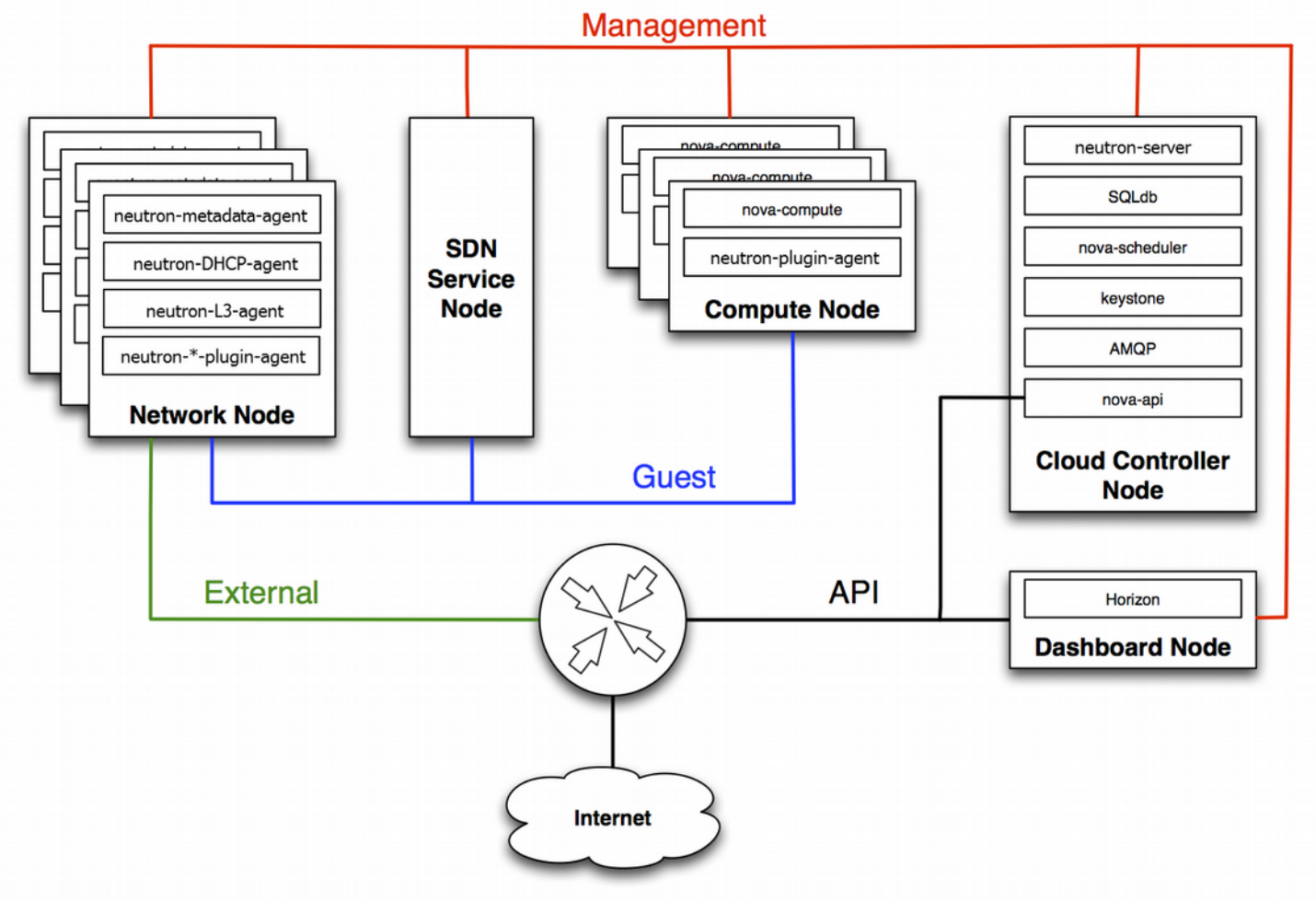
De manière générale

- Mettre à jour son infrastructure
- Faire évoluer régulièrement son infrastructure OpenStack
- Vérifier les droits du fichier de configuration :

```
$ ls -l /etc/nova/nova.conf
-rw-r----- 1 root nova 348875 févr. 20 14:27 /etc/nova/nova.conf
```

- Séparer les réseaux en fonction de leur utilisation (mgmt, public, data, …) ?
- Utiliser des points d'accès chiffrés (SSL)
- Gérer correctement les rôles et privilèges dans les fichiers `policy.json`
- Un projet == un groupe d'utilisateurs partageant le même projet
- Gestion centralisée des logs (services et réseau)

→ https://docs.openstack.org/security-guide/


Management
neutron-metadata-agent
neutron-DHCP-agent
neutron-L3-agent
neutron-*-plugin-agent
Network Node
SDN Service Node
nova-compute
nova-compute
neutron-plugin-agent
Compute Node
neutron-server
SQLdb
nova-scheduler
keystone
AMQP
nova-api
Cloud Controller Node
Guest
External
API
Horizon
Dashboard Node
Internet

Côté utilisateur

De manière générale

- Chiffrer les disques permanents
- Installer fail2ban
- Utiliser des clés pour l'authentification SSH (plutôt que des mots de passe)
- Mettre à jour les systèmes (automatiquement si nécessaire)
- Avoir conscience de la responsabilité d'un système (politique d'utilisation du Cloud)
- Éteindre les VMs quand elles ne sont plus utiles
- Uniquement ouvrir les ports nécessaires dans les *security groups*

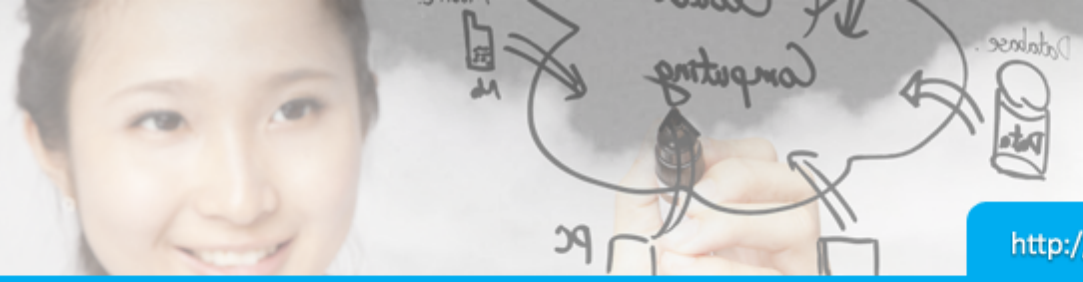
→ https://docs.openstack.org/security-guide/

Analyse forensics

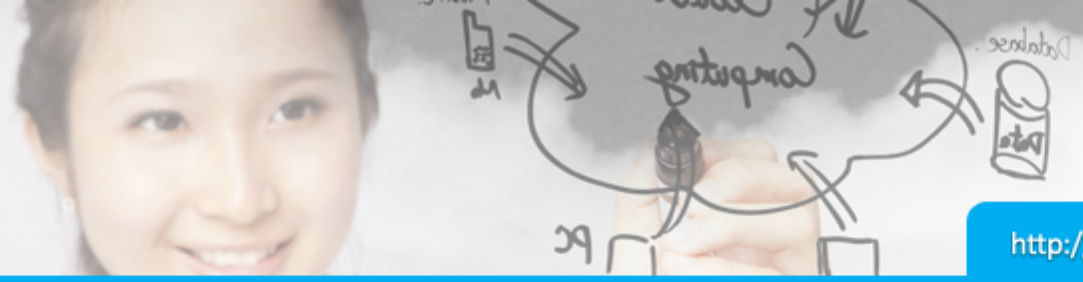
Des outils

- Images connus et génériques pour l'instant sur FG-Cloud
- Mais complexification avec l'augmentation du nombre d'utilisateurs
  → quelle stratégie à adopter ?
- Difficile de faire du *live forensics* (les administrateurs n'ont accès qu'aux flux réseau)
- Traçabilité IP -> instance → utilisateur
- Snaphsot des VMs et désactivation éventuelle
- Montage sur une machine isolée et étude

→ https://wiki.egi.eu/wiki/Forensic_Howto



Exemples d’incidents



Cas concrets d'incident

Worldwide NFS

- Lancement d'une plateforme partageant des données sur une approche multi-cloud
- Données échangées via NFS
- Export du home ouvert à tous en *rw* !
- Modification du fichier `authorized_keys` ...

Scan SSH

- VM du catalogue EGI avec un compte root protégé par un mot passe tel que *qwerty*
- Fichier de configuration SSH modifié pour autoriser la connexion par identifiant / mot de passe

Image CirrOS

- Lancement d'une image virtuelle de type CirrOS (phase de test ou formation)
- Mot de passe public : *cubswin:)*
- Détecté car trafic réseau vers un site suspect (détection NREN)

Security Challenge EGI

Le challenge

- Du 18 au 28 juillet 2017
- Organisé par le CSIRT et CESNET
- Scripts d'instanciation des VMs fournis par EGI-Ops
- Période de vacances : ressources humaines limitées

Étape 1

- Communication challenge : réponse demandée en moins de 24h
- 12 sites participants
- 80 % des sites répondent en moins d'une heure, et tous en moins de 24h
- → Les outils de communication du CSIRT sont fonctionnels
- → Les contacts de sécurité déclarés dans la GOCDB sont à jour

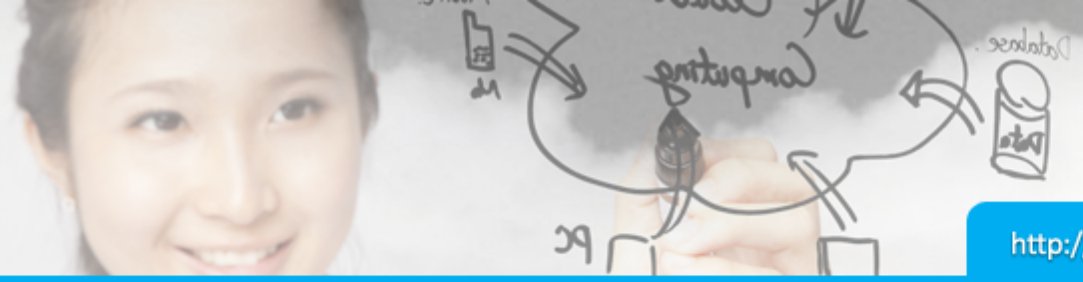
Security Challenge EGI

Étape 2

- 11 sites participants
- 21 juillet : démarrage du scénario
- 21 juillet 7h20 : démarrage de VMs avec 30h de durée de vie (traçabilité)
- 25 juillet 4h36 : démarrage des VMs qui seront compromises
- 25 juillet 14h25 : début de l'attaque DDoS / activité crypto-mining
- 25 juillet 16h58 : détection d'un trafic anormal par ReCaS-Bari
- 25 juillet 18h58 : rapport détaillé de CYFRONET-CLOUD
- 25 juillet 20h01 : diffusion d'un broadcast aux sites indiquant un incident de sécurité : délai de réponse 4h (heure de bureau)
- La moitié des sites répondent dans les délais

Conclusion

- Ligne de base sur la réponse à un incident
- Amélioration des outils pour gestion du challenge (VM, …)
- Pas de bannissement centralisé des utilisateurs
- Politique de gestion des utilisateurs par les sites n'est pas claire



Question / Discussion