Gestion de la sécurité d'un Cloud OpenStack

Vincent LEGOLL <vincent.legoll@idgrilles.fr>
Jérôme PANSANEL <jerome.pansanel@iphc.cnrs.fr>

IPHC – Décembre 2015

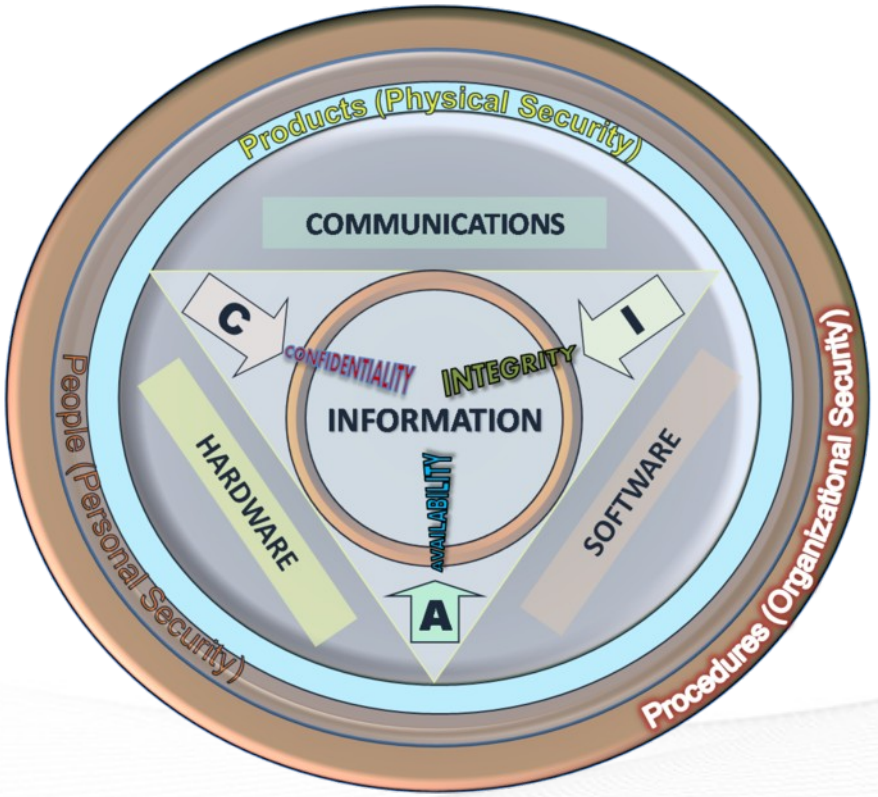
Sommaire

- Introduction
- Sécurité et Cloud
- Déployer un environnement sûr
- Sécuriser les différents composants OpenStack :
  - Dashboard / API
  - Authentification
  - Nova
  - Cinder
  - Neutron
- La sécurité des VMs

Introduction

Points clés (modèle de CIA) :

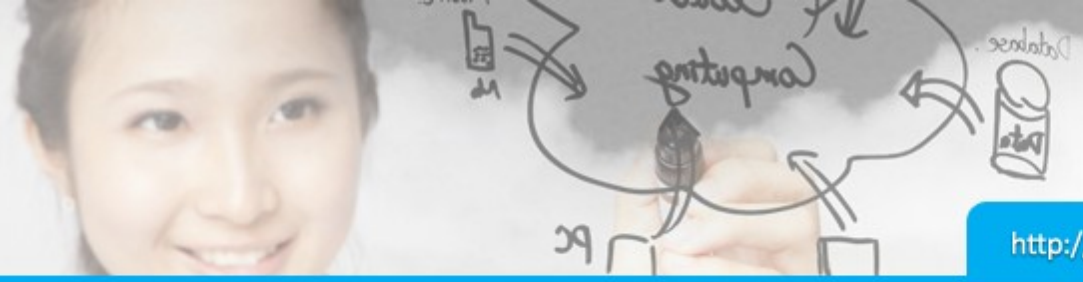
- Confidentialité
- Intégrité
- Disponibilité



Périmètre :

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

+ **Tracabilité** !!!



Bonnes pratiques

Pour éviter de faciliter la compromission de l'infrastructure :

- Choisir avec soin les mots de passe
- Mettre à jour régulièrement les systèmes
- Installer le minimum de logiciels
- Chiffrer les flux de données
- Gérer finement les droits d'accès

Points organisationnels :

- Veille active des exploits de sécurité dans le domaine
- Connaître la procédure de déclaration et de réponse d'incident
- Cycle d'amélioration continu
- Test et surveillance de l'infrastructure

Réf. : Guidebook on National Cyber Security Strategies (ENISA)

Procédure de réponse à un incident

- 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

Réf. : `https://wiki.egi.eu/w/images/f/f5/Site_Checklist.pdf`

Qui contacter en cas d'incident

Au niveau local :

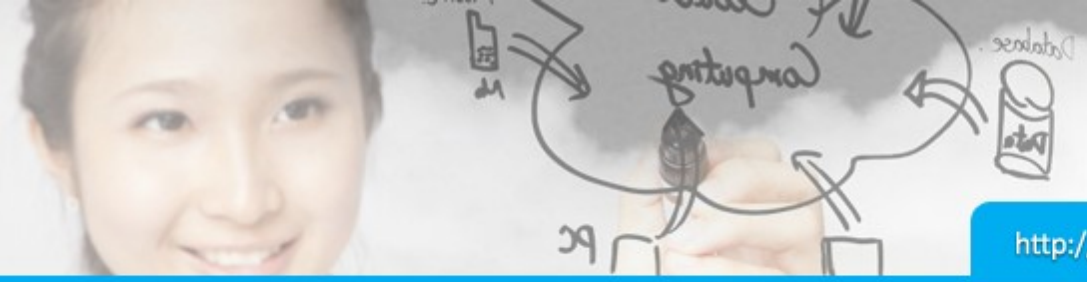
- Avertir votre correspondant sécurité local

Au niveau français :

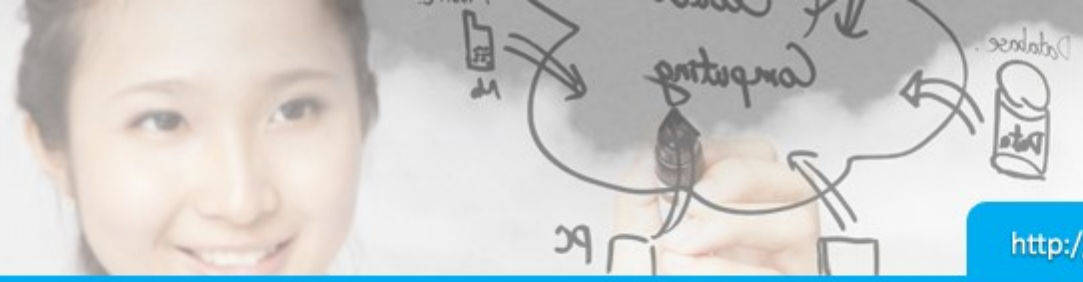
- Sophie Ferry (France Grilles)
- → ngi-france-security-contact-l@france-grilles.fr

Au niveau européen :

- CSIRT EGI
- → https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page
- → https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting
- → abuse 'at' egi.eu



- Introduction
- Sécurité et Cloud
- Déployer un environnement sûr
- Sécuriser les différents composants OpenStack :
  - Dashboard / API
  - Authentification
  - Nova
  - Cinder
  - Neutron
- La sécurité des VMs



Sécurité et Cloud

Cloud privé :

- Opéré pour une seule organisation (exemple : hébergement de services)
- Faible cloisonnement (interaction avec d'autres services du labo)
- Utilisateurs connus
- Action de sensibilisation plus facile
- Intégré plus simplement dans la PSSI de l'organisation

Cloud publique :

- Opéré pour un ensemble d'utilisateurs / organisations
- Ouvert sur l'extérieur
- La communication vers les utilisateurs peut être compliquée
- Réputation du fournisseur de ressource
- Impact sur les autres activités du laboratoire

Étude de la sécurité

- Quelles sont les procédures pour maintenir les services opérationnels et à jour, en particulier concernant les patchs de sécurité ?
- Est-ce que les différents réseaux sont séparés ? Quels sont les outils utilisés pour surveiller l'activité du (des) réseau(s) ?
- Êtes-vous en contact avec les responsables sécurité ? Sont-ils au courant qu'une infrastructure de type Cloud est déployée ?
- Comment sont sauvegardés les logs ? Sont-ils stockés de manière à ce qu'ils ne soient pas modifiables en cas de compromission ?
- Qui peut accéder au Cloud ? Comment est géré cet accès ?
- Est-ce que les services Cloud fonctionnent sur du matériel dédié ?
- Pouvez-vous simplement suspendre un utilisateur / groupe ?

Étude de la sécurité

- Est-ce que différents rôles sont définis dans vos tenants ?
- Comment sont installées les images virtuelles ? Est-ce qu'une procédure d'endossement existe ?
- Est-ce que vous avez une procédure pour surveiller le réseau des VMs (en particulier savoir où est-ce que ce se connecte chaque VM) ?
- Les VMs d'un tenant sont-elles disponible depuis d'autres tenants ?
- Si l'utilisateur peut se connecter en tant que 'root' sur la VM, est-ce que ses connexions sont surveillées ?
- Savez-vous réaliser des snapshots ?
- Est-ce que les conditions d'utilisation de votre Cloud sont disponibles pour tous les utilisateurs ?
- Combien de temps garder vous les informations (utilisateurs, …) ?

Introduction

Machines virtuelles

OpenStack

Keystone | Glance | Cinder | Nova | Neutron

OS
(http, ssh, mysql, libvirt, ...)

Sommaire

- Introduction
- Sécurité et Cloud
- Déployer un environnement sûr
- Sécuriser les différents composants OpenStack :
  - Dashboard / API
  - Authentification
  - Nova
  - Cinder
  - Neutron
- La sécurité des VMs

Principaux services

Service	Protocols	Ports	Purpose	Used by	Security domains(s)
beam.smp	AMQP	5672/tcp	AMQP message service	RabbitMQ	MGMT
tgtd	iSCSI	3260/tcp	iSCSI initiator service	iSCSI	PRIVATE(data network)
sshd	ssh	22/tcp	allows secure login to nodes and guest VMs	Various	MGMT, GUEST, and PUBLIC as configured
mysqld	mysql	3306/tcp	MySQL database service	Various	MGMT
apache2	http	443/tcp	Dashboard	Tenants	PUBLIC
dnsmasq	dns	53/tcp	DNS services	Guest VMs	GUEST

AMQP

- Est-ce que votre configuration AMQP est protégée par un mot de passe ?
- Est-ce que votre serveur AMQP n'écoute que sur le réseau dédié ?
- Est-ce que votre serveur AMQP utilise un chiffrage SSL ?
- Est-ce que l'utilisateur Guest a été supprimé ?

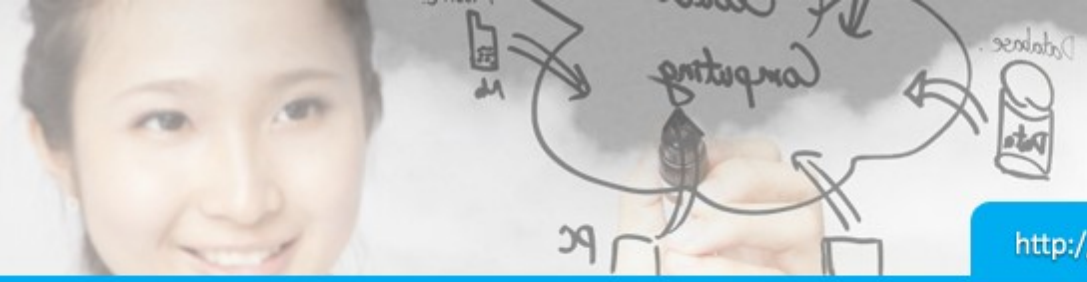
→ `http://docs.openstack.org/security-guide/messaging/security.html`

Base de données

- Toutes les communications avec le serveur de base de données doivent s'effectuer sur le réseau MGMT
- Les communications doivent être chiffrées par TLS
- Il faut créer un utilisateur par service et par hôte (pour faciliter l'isolation en cas de défaillance)

Sommaire

- Introduction
- Sécurité et Cloud
- Déployer un environnement sûr
- Sécuriser les différents composants OpenStack :
  - Dashboard / API
  - Authentification
  - Nova
  - Cinder
  - Neutron
- La sécurité des VMs



Dashboard et OpenStack API

Dashboard (Horizon) :

- Nécessite cookies et Javascript côté client
- Le serveur Web doit être configuré pour le chiffrement (TLS)
- Le service est ouvert sur l'extérieur ; il peut être soumis à des attaques de type DoS
- Horizon permet de gérer les groupes de sécurité pour un tenant (filtrage L3/L4)
- Vérifier que le paramètre Debug a pour valeur *False*

`http://docs.openstack.org/security-guide/dashboard/checklist.html`

API OpenStack :

- L'API doit être configurer pour utiliser le chiffrage SSL
- Le service est ouvert sur l'extérieur ; il peut être soumis à des attaques de type DoS

Sécuriser les communications : Horizon

```
<VirtualHost <ip address>:80>
  ServerName <site FQDN>
  RedirectPermanent / https://<site FQDN>/
</VirtualHost>
<VirtualHost <ip address>:443>
  ServerName <site FQDN>
  SSLEngine On
  SSLProtocol +TLSv1 +TLSv1.1 +TLSv1.2,
  SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!EXP:!LOW:!MEDIUM
  SSLCertificateFile    /path/<site FQDN>.crt
  SSLCACertificateFile  /path/<site FQDN>.crt
  SSLCertificateKeyFile /path/<site FQDN>.key
  WSGIScriptAlias / <WSGI script location>
  WSGIDaemonProcess horizon user=<user> group=<group> processes=3 threads=10
  Alias /static <static files location>
  <Directory <WSGI dir>>
    # For http server 2.2 and earlier:
    Order allow,deny
    Allow from all

    # Or, in Apache http server 2.4 and later:
    # Require all granted
  </Directory>
</VirtualHost>
```

Sécuriser les communications : API

```
<VirtualHost <ip address>:8447>
  ServerName <site FQDN>
  SSLEngine On
  SSLProtocol +TLSv1 +TLSv1.1 +TLSv1.2
  SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!EXP:!LOW:!MEDIUM
  SSLCertificateFile    /path/<site FQDN>.crt
  SSLCACertificateFile  /path/<site FQDN>.crt
  SSLCertificateKeyFile /path/<site FQDN>.key
  SSLSessionTickets Off
  WSGIScriptAlias / <WSGI script location>
  WSGIDaemonProcess osapi user=<user> group=<group> processes=3 threads=10
  <Directory <WSGI dir>>
    # For http server 2.2 and earlier:
    Order allow,deny
    Allow from all

    # Or, in Apache http server 2.4 and later:
    # Require all granted
  </Directory>
</VirtualHost>
```

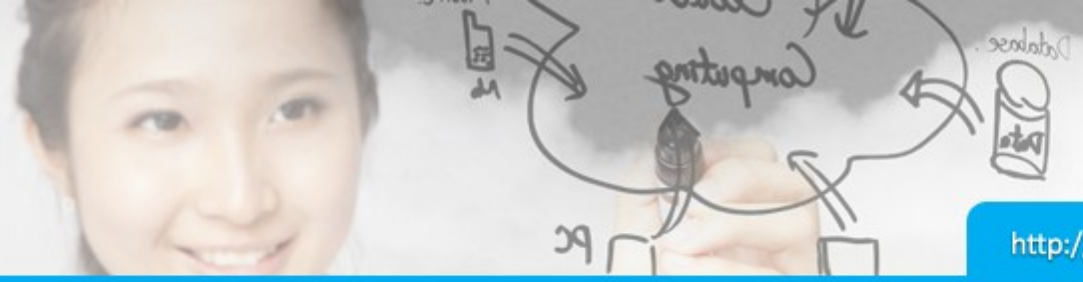
Note : possibilité de séparer AC externe et interne

Les points d'accès

Configuration des points d'accès :

- Les adresses internes et d'administration doivent être différentes de celles des adresses publiques
- Les services doivent être configurés pour utiliser les points d'accès interne (MGMT)
- Utiliser SELinux
- Dans un cas idéal, utiliser des containers pour chaque service

```
$ keystone endpoint-create \
--region RegionOne \
--service-id=1ff4ece13c3e48d8a6461faebd9cd38f \
--publicurl='https://public-ip:8776/v1/%(tenant_id)s' \
--internalurl='https://management-ip:8776/v1/%
(tenant_id)s' \
--adminurl='https://management-ip:8776/v1/%(tenant_id)s'
```



Keystone

Configuration des points d'accès :

- Souvent des tests de connexion (brute force) pour découvrir un couple identifiant / mot de passe. Identifiant les plus testés : admin et service → mot de passe conséquent et surveillance
- Possibilité d'utiliser un service externe pour forcer la complexité des mots de passe ou d'effectuer certaines actions en fonction d'attaque en force brute
- Il est conseillé d'utiliser une authentification multi-facteur pour les utilisateurs avec privilège

Keystone

- Est-ce que l'appartenance utilisateur/groupe est bien configurée pour les différents fichiers de configuraiton de Keystone ?
- Est-ce que les permissions pour les fichiers de configuration Keystone sont assez restrictives ?
- Est-ce que SSL est activé ?
- Est-ce que Keystone utilise un hash suffisamment fort pour les tokens ?
- Est-ce que le paramètre max_request_body_size a une valeur (114688) ?
- Est-ce l'authenfication *admin token* est désactivée dans /etc/keystone/keystone.conf ?

→ `http://docs.openstack.org/security-guide/identity/checklist.html`

Nova

- Est-ce que les fichiers de configuration de Nova appartiennent bien à root/nova ?
- Est-ce que les autorisations d'accès au fichier de configuration sont suffisamment restrictives ?
- Est-ce que Keystone est utilisé pour l'authentification ?
- Est-ce que le protocole d'authentification utilisé est sécurisé ?
- Est-ce que Nova communique de manière sécurisé avec Glance ?

→ `http://docs.openstack.org/security-guide/compute/checklist.html`

Rôles et privilèges

Pour chaque module, un fichier policy.json :

```
{
    "context_is_admin": "role:admin",
    "admin_or_owner": "is_admin:True or project_id:%(project_id)s",
    "default": "rule:admin_or_owner",
    "admin_api": "is_admin:True",
    "volume:create": "",
    "volume:get_all": "",
    "volume:get_volume_metadata": "",
    "volume:get_volume_admin_metadata": "rule:admin_api",
    "volume:delete_volume_admin_metadata": "rule:admin_api",
    "volume:update_volume_admin_metadata": "rule:admin_api",
    "volume:get_snapshot": "",
    "volume:get_all_snapshots": "",
    "volume:extend": "",
    "volume:update_readonly_flag": "",
    "volume:retype": "",
…
```

Par défaut, pas de différence entre owner et tenant !

Nova

Exemple pour Nova :

```
{
    "context_is_admin":  "role:admin",
    "admin_or_owner":  "is_admin:True or project_id:%(project_id)s",
    "admin_or_user":  "is_admin:True or user_id:%(user_id)s",
    "default": "rule:admin_or_user",

    "cells_scheduler_filter:TargetCellFilter": "is_admin:True",
    "compute:create": "",
    "compute:create:attach_network": "",
    "compute:create:attach_volume": "",
    "compute:create:forced_host": "is_admin:True",
    "compute:get": "rule:admin_or_owner",
    "compute:get_all": "",
    "compute:get_all_tenants": "",
    "compute:start": "",
    "compute:stop": "",
    "compute:unlock_override": "rule:admin_api",
...
```

Cinder

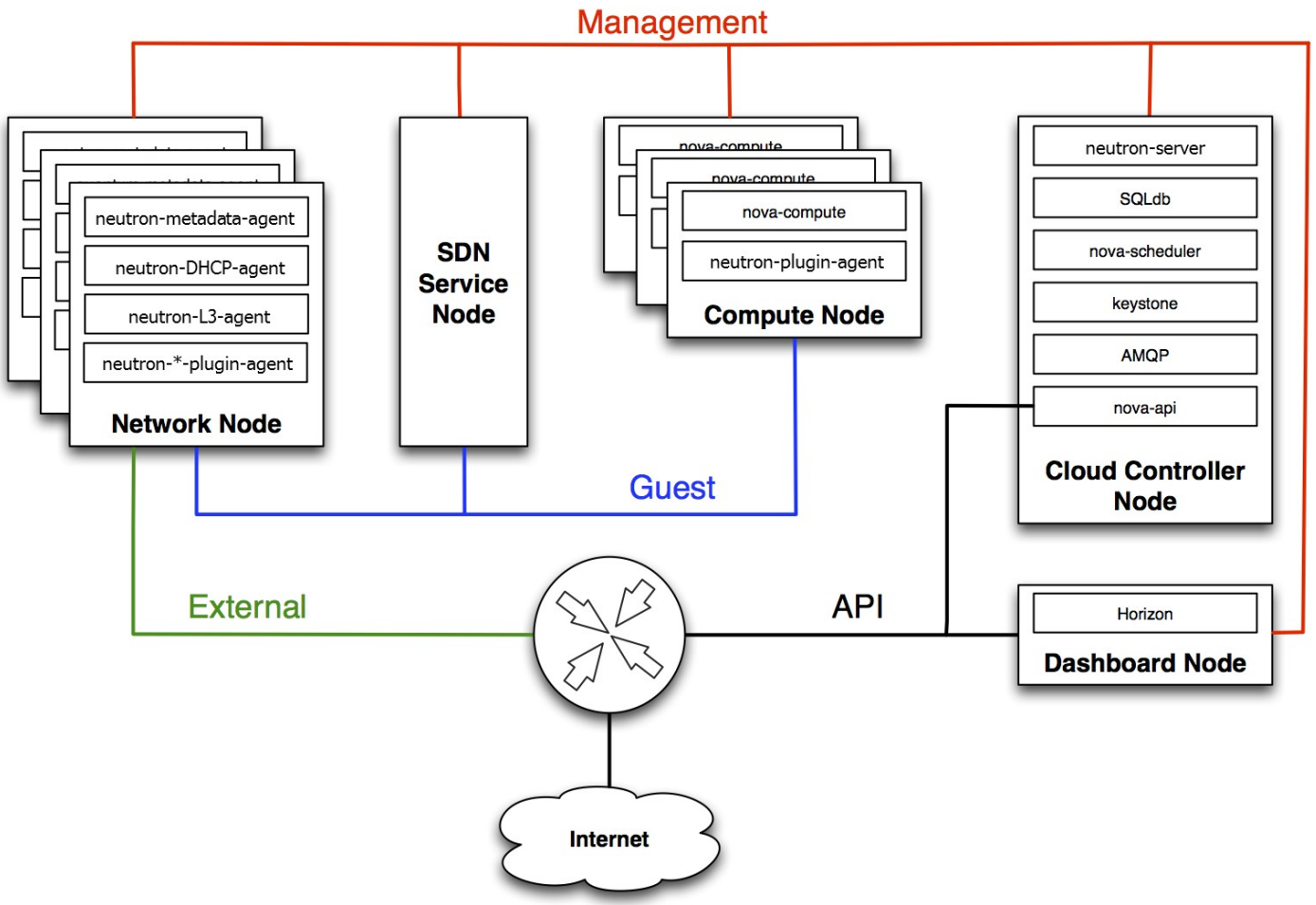
- Est-ce que les fichiers de configuration de Cinder appartiennent bien à root/cinder ?
- Est-ce que les permissions pour accéder aux fichiers de configuration de Cinder sont assez strict ?
- Est-ce que Keystone est utilisé pour l'authentification ?
- Est-ce que TLS est activé pour l'authentification ?
- Est-ce que Cinder communique avec Nova via TLS?
- Est-ce que Cinder communique avec Glance via TLS?
- Est-ce que le NAS est opéré dans un environnement sécurisé ?
- Est-ce que la valeur de la variable max_request_body_size a été définie (114688) ?
- Conseillez-vous à vos utilisateurs de chiffrer leur disque ?

→ `http://docs.openstack.org/security-guide/block-storage/checklist.html`

Cinder

Objectif :
Modifier le fichier policy.json pour que les utilisateurs de Cinder ne puissent pas utiliser le volume d'un autre utilisateur.

Neutron


Management
neutron-metadata-agent
neutron-DHCP-agent
neutron-L3-agent
neutron-*-plugin-agent
Network Node
SDN Service Node
nova-compute
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

Neutron

- Est-ce que les fichiers de configuration de Neutron appartiennent bien à root/neutron ?
- Est-ce que les droits d'accès à ces fichiers de configuration sont suffisamment restrictifs ?
- Est-ce que Keystone est utilisé pour l'authenfitication ?
- Est-ce que le protocol utilisé pour l'authentification est sécurisé?
- Est-ce que SSL est bien utilisé pour l'accès au serveur Neutron API ?
- Est-ce que les réseaux sont bien séparés ?
- Est-ce que l'utilisation des réseaux est traçable ?
- Est-ce que les quotas sont bien configurés ?

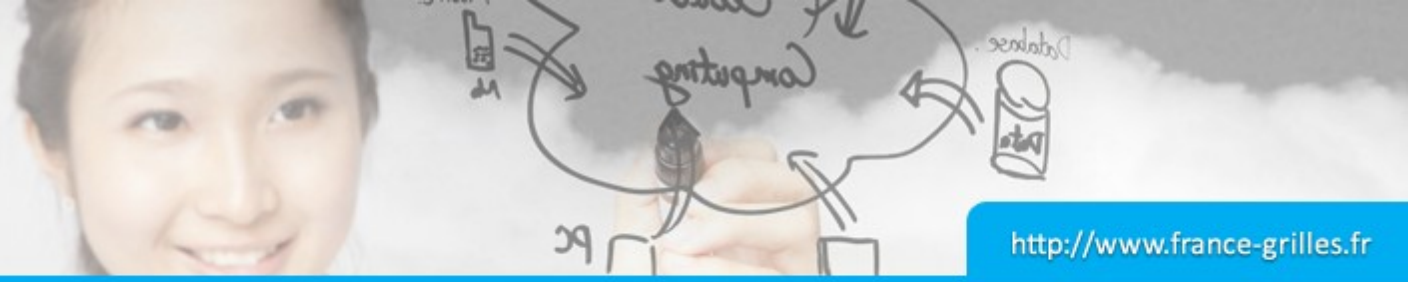
Sommaire

- Introduction
- Sécurité et Cloud
- Déployer un environnement sûr
- Sécuriser les différents composants OpenStack :
  - Dashboard / API
  - Authentification
  - Nova
  - Cinder
  - Neutron
- La sécurité des VMs

Machines virtuelles

- Activer les mises à jour automatiques
- Bonne pratique de sécurité

  → http://iase.disa.mil/stigs/Pages/index.aspx
- Fail2Ban
- Endossement des VMs
- http://docs.openstack.org/image-guide/
- Responsabilité des utilisateurs (conditions d'utilisation)
- ...



Questions ?