Mise en place d'un proxy SSH

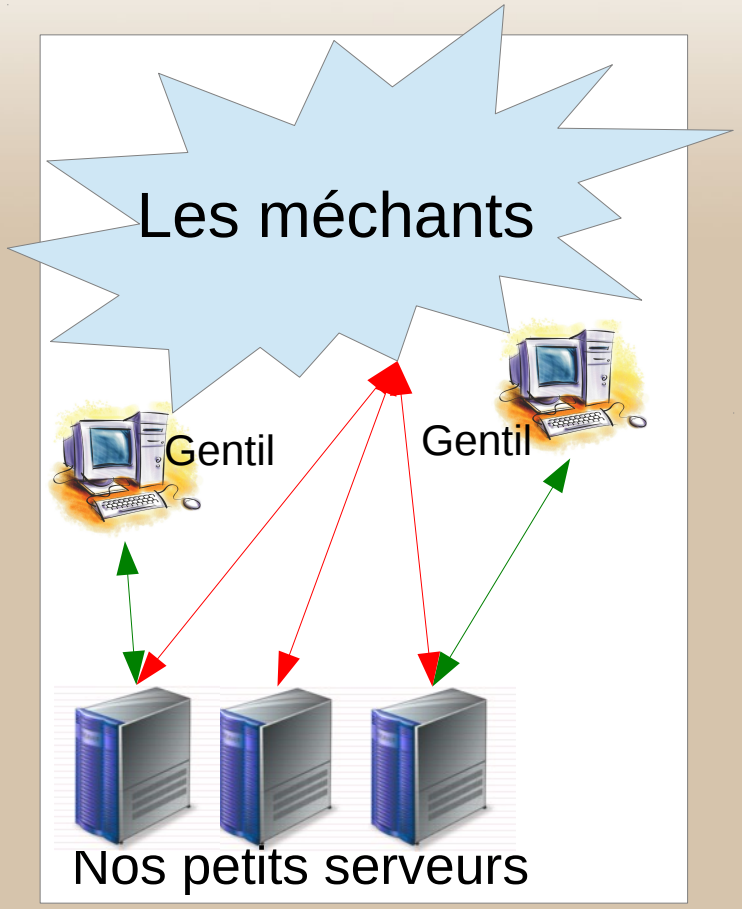
→ Bonus : ansible

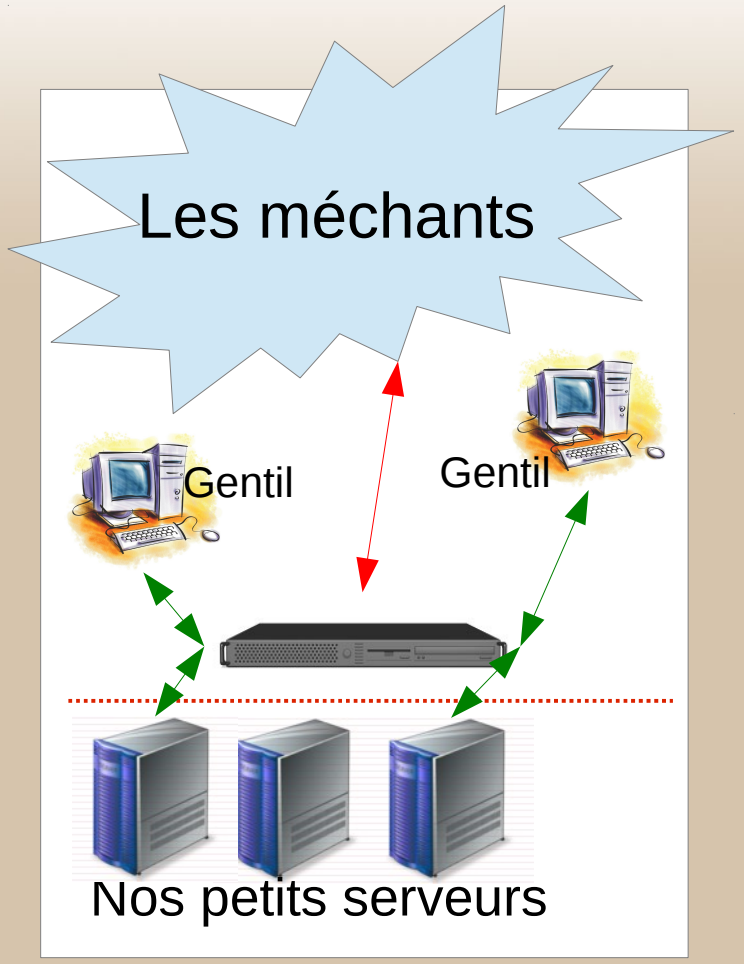
François Legrand

JI 2014

Objectifs

- **Limiter la surface d'attaque à 1 (ou 2) machines**
- **Proxy ssh**





SSH Proxy

LPNHE PARIS

rbash est mon ami

- rbash pour « restricted bash » → on définit les commandes accessibles dans /usr/rbin en créant des liens logiques vers les commandes souhaitées

```
ln -s /usr/bin/ssh /usr/rbin/ssh
ln -s /usr/bin/scp /usr/rbin/scp
ln -s /bin/nc /usr/rbin/nc
```

- **Protection « naturelle » contre les failles de bash** (car les commandes env ou bash ne sont pas accessibles) !
- On force les « users normaux » à rbash et on autorise le bash standard aux admins (dans /etc/ldap.conf et /etc/profile)

→ Détails dans le poster dynamique

ANSIBLE

LPNHE PARIS

Qu'est-ce que c'est ?

- « radically simple IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and many other IT needs. »
- Alternative à Puppet
- Courbe d'apprentissage très rapide (2 heures suffisent)
- Basé sur ssh (pas de d'agent ou de client à installer, une clé ssh suffit)
- Templates YAML
- Mode push

ANSIBLE

LPNHE PARIS

Comment ça marche : les hosts

- Un fichier « hosts » qui liste vos machines à administrer

```
[proxmox-servers]
lpnhevirt1.in2p3.fr location=1222-SS-09
lpnhevirt2.in2p3.fr location=1222-2-10

[physical-debian-servers]
lpnauth2.in2p3.fr location=1222-SS-09
lpnhevirt1.in2p3.fr location=1222-SS-09

[physical-servers:children]
proxmox-servers
physical-debian-servers
```

ANSIBLE

LPNHE PARIS

Comment ça marche : les playbooks

- Des fichies « playbook » qui listent les actions à réaliser

```
- hosts: debian-like-servers:lpnclaude.in2p3.fr
  tasks:

  - name: install fail2ban
    apt: pkg=fail2ban state=present

  - name: push config
    copy: src=jail.local-debian dest=/etc/fail2ban/jail.local
mode=0644 owner=root group=root

  - name: start fail2ban
    command: /etc/init.d/fail2ban restart
```

ANSIBLE

LPNHE PARIS

Comment ça marche : push

- On pousse la config en lançant le playbook

```
$ ansible-playbook -s -K fail2ban.yml

TASK: [install fail2ban]
*****************************************************
ok: [lpnhevirt1.in2p3.fr]
ok: [lpnhevirt2.in2p3.fr]

TASK: [push config]
*****************************************************
changed: [lpnhevirt1.in2p3.fr]
ok: [lpnhevit2.in2p3.fr]
```