# Compte-rendu de réunion ResEl

26 mai 2007

par Florent Fourcot

*Membres présents*
*Membres du CA* : Antoine Bernardeau, Benoît Fontaine, Florent Fourcot, Bertrand Grelot, François Lazarus, Grégoire Péan, Thomas Péteul, Thomas Villaren.
*Membre actif* : Nicolas Aupetit

## Ordre du Jour



## 1 Bilan des activités

### Anniversaire d'Antoine

Aujourd'hui c'est l'anniversaire de notre président, vive lui. Nous lui avions caché, mais nous sommes prêts à lui installer plan9 sur l'une des machines sun qui ne sert plus à rien. Nous sommes certains que cela lui fera plaisir.

### Switchs écoles

Toujours pas de bonnes nouvelles pour les switchs prêtés par l'école, il va falloir attendre encore un peu. On espère pouvoir les installer avant la rentrée.

### Architecture du ResEl

#### Rennes

Nicolas a fait un petit point sur l'architecture du ResEl de Rennes, qui depuis l'installation de la nouvelle machine est totalement virtualisée. L'intérêt de la virtualisation là-bas est de supprimer les interactions entre les services (pas d'autres machines physiques de remplacement, si elle tombe le

réseau tombe), des machines plus simples à administrer et enfin une certaine facilité pour uniformiser les deux campus (et permettant le transfert direct de machines virtuelles notamment).

Ce qui consomme le plus de machines virtuelles à Rennes est la multitude de *Pessac*, machines placées uniquement pour faire la jonction entre les différents Vlans. Auparavant, il y avait une machine centrale (Lily à Brest par exemple), qui contenait une liste de règles de chaque Vlan vers un autre Vlan. On remarque vite la complexité du script en somme de 1 à n, un petit carré la taille augmente vite.

Comme on peut le voir sur le schéma 1 une machine a été placée entre chaque Vlan, et le Vlan 993, qui lui permet la transition entre chaque partie du réseau et le reste du monde. Chaque Pessac n'a ainsi que deux interfaces à gérer ; la gestion des adresses IP selon les zones est dynamique avec un plan d'adressage signalé par du RIP. Les scripts sont ainsi bien plus simples, et l'architecture peut-être plus compréhensible. Quand on veut modifier une règle, on est pas obligé de chercher dans le script global du firewall, globalement illisible. L'inconvénient est bien sûr la multiplication des machines.

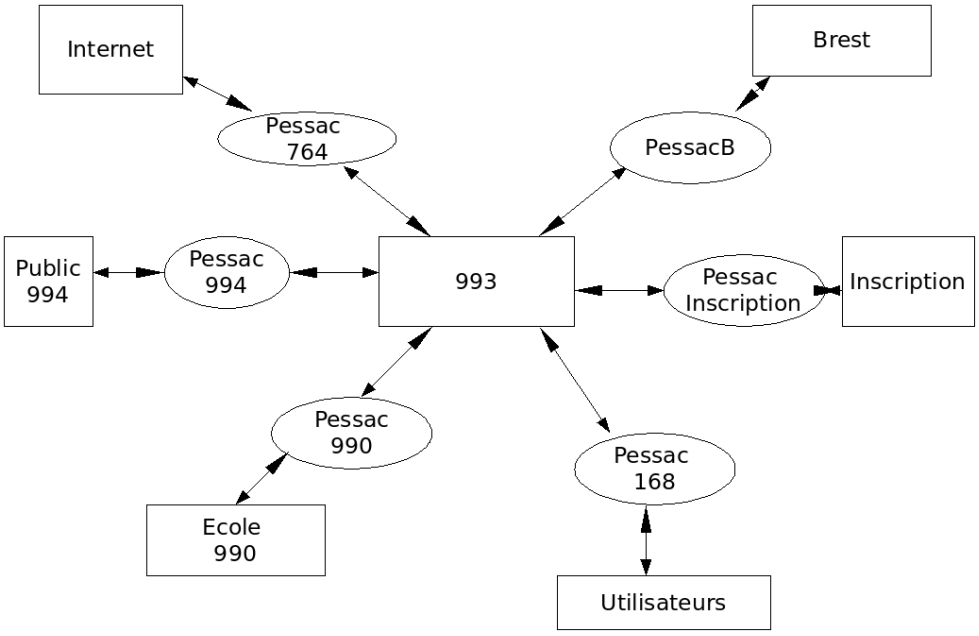


Fig. 1 – Structure réseau de Rennes

Niveau administration, chaque Pessac a une patte dans le Vlan switch, mais il n'y a pas de port 22 ouvert entre elles.

### Brest

La vision à court terme de Brest est d'éclater noboot, et de mettre en place les Vlans. Nicolas avait fait un plan des services de Brest, en les regroupant par activité. (une machine de scan par exemple) La DMZ sera supprimée, une machine internet en entrée redirigera les bon ports vers la zone publique.

### Plan de migration

L'objectif des migrations est d'apprendre des erreurs de Collector, et de ne pas recommencer de telles interruptions de services. Que Garbage soit inacessible est déjà relativement problèmatique, alors pour les autres services, ce serait encore moins bien. Voici une petite liste des erreurs à méditer :

- Mise en production trop tôt
- Pas de bonnes connaissances des services à virtualiser
- Système de fichiers incorrect, elle n'est pas en LVM.
- La réplication avec Rennes buggait, ne pas oublier les interactions avec le monde extérieur.
- La méthode de scan a changé, ne pas oublier de surveiller les petits détails ...

## 2 Travaux en cours

### Serveur de logs

La grande question du jour était de savoir s'il était utile de logguer toutes les machines, et si oui lesquels. Les logs doivent rester courts, et utiles, donc uniquement sur les machines du ResEl critiques. Il est en revanche utile d'avoir toutes les commandes sudo pour remonter ce qu'il s'est passé. De cette question en découle une autre, faut-il séparer Brest et Rennes dans l'envoi de mails ? Les administrateurs de Rennes ne sont pas forcément interessés par les activités de Brest, et inversement.

Nicolas propose que l'on développe le Nirvana en terme de choix et de gestion de ces priorités. Il propose une interface sur laquelle chaque administrateur pourrait s'abonner aux machines qu'il souhaite, et définir un ordre de priorité d'apparition dans le mail (anima en premier pour l'ircop par exemple). Cela permettra notamment aux débutants de ne pas être submergés par la quantité d'informations l'année prochaine.

L'avantage c'est que les gens que cela n'intéresse pas ne les liront pas comme c'est le cas avant, mais qu'au moins ce sera clair entre qui les lit et qui ne les lit pas. Comme parfois les administrateurs sont, de plus, un peu plus spécialisés dans un service que dans un autre, la présentation sera meilleure qu'un choix arbitraire de priorité des machines. L'interface serait dans l'idéal intégrée à RA2, et hop ce serait parfait, on pourrait tout faire (mais bon, cela va demander un peu de temps à *Benoît* pour le faire.).

### État de Padova

Petit point de résumé : Padova est réinstallée (avec des belles partitions en plus), tous les fichiers de configuration sont là. Il a juste fallu modifier le home de backuppc qui par défaut n'est pas idéal. (pas dans le /srv) Les clefs ssh ont également été rapatriées, mais toujours pas de sauvegarde...

Nicolas signale que l'interface web de backuppc est très pratique pour localiser les erreurs, pour cela il ne reste qu'une erreur au lancement d'apache, il faudrait activer le module apache pour le LDAP.

A plus long terme, il est bon de réfléchir à l'utilité de backuppc. Comment concrètement sauvegarder une machine virtuelle, qui par défaut est simplement une grosse image, pas facile de gérer un historique. En revanche backuppc permet lui de tracer les modifications, de choisir ce qui doit être sauvegardé ou pas (par exemple le site web étant bientôt sous total contrôle de version dans le svn, une sauvegarde semble superflue).
Les deux ont leurs avantages et leurs inconvénients, et l'on restera certainement sur un système avec sauvegarde des images à court terme (inférieure à 7 jours) et sur le long terme sauvegarde par backuppc. On pourra ainsi relancer les machines rapidement (C'est après tout le but de la virtualisation...) sans perdre pour autant en qualité de sauvegardes. La sauvegarde des images complètes ne pose normalement aucun soucis à chaud avec du LVM.

### Trolls

Tout d'abord Trolls a un seul et unique nom, stoppons les multiples alias et les changements en permanence. Ce sera *trolls*, et ceci sans discussions futures désormais. Pour faire un petit point, cinq

disques sont à l'intérieur, avec du RAID matériel. Au final, avec le disque de spare, 3 disques durs sont utiles, soit 1,5 To d'utiles. Il y a deux partitions sur chaque disque, un /boot et tout le reste en LVM.

Un noyau Xen a été installé, bien que les VM n'ont pas vocations à être lancées depuis cette machine. Le lancement est forcément bien plus rapide depuis Trolls que depuis les autres dom0, elle est clairement plus rapide. Il y a également deux interfaces réseau, une locale vers les autres Dom0 et une vers l'extérieur en trunk. Il est à noter qu'actuellement le VLan admin n'a pas d'accès vers l'internet, et n'a pas de raisons particulières de l'avoir un jour.

## 3 Décisions prises

### Mémoire à Rennes

Nicolas et Jean-Édouard voudrait racheter de la mémoire à Rennes, la machine étant un peu limitée avec ses 1Go de RAM. Le devis est de 98,16€sur `www.materiel.net`. La décision d'achat a été soumis au vote du conseil d'administration, qui a voté à 6 voix pour contre une seule contre. La commande de matériel sera donc effectuée.

## 4 Tâches à accomplir

### Référence

Il va falloir uniformiser les dom0, et réfléchir aux migrations live, qui n'est pas forcément possible avec le LVM (ce n'est pas très exportable, ce qui est tout de même un gros défaut pour une migration live). Le NFS n'est pas très sécurisé, c'est le moins que l'on puisse dire. Le NBD (Network Block Device) par contre est faisable, d'autres l'ont fait... D'après les premiers tests cela fonctionne en noyau classique, sans avoir besoin de le recompiler.

Une dernière solution est un squelette de boot qui monte en NFS certaines parties de la machine, mais bon on a connu plus propre...

Pour la gestion des Vlans dans la Dom0 : il faut à tout prix empêcher un administrateur d'une machine virtuelle d'avoir accès au trunk, on peut monter un bridge (une sorte de switch) sur la dom0 pour être tranquille.

### Certificats SSL

Les certificats SSL des sites du ResEl sont périmés : il va falloir les refaire, le plus vite étant le mieux.

### Bornes WiFi

Elles tombent toujours, sans qu'on sache bien pourquoi. On va chercher de nouveaux firmwares, en espérant que cela améliore la situation (en tout cas, ne rien faire ne risque pas d'améliorer les choses).

### Nagios

Nicolas rapelle que Nagios étant cassé, notamment par exemple un léger souci de cohérence sur le nom de trolls (mais ça c'est pas bien grave encore). Ensuite, il n'écoutait plus les switchs (switch du I11 qui tombe sans que l'on s'en aperçoive, par exemple) (et un switch, ça fait mal aux pieds en tombant). Nicolas l'a corrigé, avec une surveillance en ICMP désormais. À quand cependant l'installation sur une VM/passage en etch pour utiliser Nagios2 ? Cela permettrait notamment de reprendre une configuration plus propre. (la question des dépendances des VM est par exemple encore à définir, vu qu'elles sont par définition déplaçables...)

Il serait bon de tester également Oreon, qui doit normalement regrouper Nagios et Cacti. On est relativement septique sur l'utilité et les avantages, mais sans tests il est dur de juger. Une piste plus intéressante serait par contre de remplacer Cacti pour Munin (exemple d'utilisation de Munin sur le site du Cr@ns). Munin est plus simple à configurer et plus sympa, pour l'utilisation du ResEl ce serait bien suffisant. À réfléchir également sur quelles machines ont réellement besoin d'êtres mises sous graphe ?