Compte-rendu de réunion ResEl

15 avril 2007

par Florent Fourcot

Membres présents
Membres du CA : Antoine Bernardeau, Raphaël Bissauge, Benoît Fontaine, Florent Fourcot, Hugo Geissmann, Jean-Edouard Babin (Jeb) en vidéo conférence depuis Rennes.
Membres actifs sans droit de vote : Jérémy Rizzoli, Jérémie Soria.

Ordre du Jour

1 Bilan des activités

1.1 Minute de silence pour Jeb à Rennes

Rapidement effectué (en moins d'une minute par exemple), à bientôt Jeb. :)

1.2 Point sur la virtualisation

Petit rappel : selon les services, les modifications des fichiers de configuration entre les machines actuelles et les futures machines virtualisée sont plus ou moins compliquée. Dans le cadre d'une migration réfléchie, les services les moins critiques (mais loin d'être les moins utilisés, comme garbage) seront virtualisés en premier, afin d'acquérir de l'expérience avant de poursuivre.
Niveau sécurité : certaines machines virtuelles auront besoin d'envoyer sur différentes Vlan, cela peut-être gênant car la seule solution fiable actuelle et de permettre à la dom0 de le faire. Si la dom0 est attaquée, l'envoi sur n'importe quelle Vlan sera très simple.
Il est cependant très simple de restreindre la dom0 à un Vlan particulier, et hop ça devrait aller mieux.

1.3 Vlan « 666 »

Pour éviter la propagation des virus sur le réseau, placer automatiquement des machines infectées sur un Vlan particulier, avec encore possibilité d'accéder à des anti-virus sur une page contenant des explications/instructions, mais ni d'internet ni courriel, pourrait être une solution. (même si en pratique, le numéro du Vlan ne sera pas 666, car numéro réservé par l'école...)

Bientôt nous n'aurons plus de switch 3com sur le campus, c'est donc une solution totalement envisageable. L'avantage par rapport à arpkiller qui coupait automatiquement les machines au port de la machine, est de fournir des informations à l'utilisateur sur les raisons de cette coupure automatiquement (renvoi automatique sur une page du site).

Comme le dit Jeb, il faudra créer par exemple une VM 'décontamination', contenant le site web avec des pages d'explications. Il faudra également un DCHP, la redirection de l'ensemble des requêtes sur le port 80 en local, le blocage des autres ports, etc ... L'IP de la VM doit être la même que grandours dans le Vlan utilisateur pour que les utilisateurs en IP fixe puissent quand même voir le site "spécial". Comme le Vlan n'est pas routé, le fait d'utiliser la meme ip que grandours ne pose pas de problème.

Critiques internes : est-il vraiment utile de monter une vlan exclusivement pour cela ? Est-il réellement bon de placer toutes les machines infectées sur la même Vlan, pour qu'elles s'auto-contaminent entre elles ? Et enfin, perdre une Vlan sur le nombre limité que l'on peut utiliser est-ce vraiment raisonnable ?

1.4 Sondage pour le satellite

Le sondage est prêt, il ne manque plus qu'à le placer sur baal pour le mettre à disposition de tous. Comme François n'est pas là, il faudra en reparler avec lui rapidement.

1.5 Livraison de la dernière commande

La commande devrait bientôt arriver au courrier de l'école.

1.6 Refonte W3

Vincent Larrat est prêt à s'occuper du CSS, le projet avance. Cependant le BdE ne répond pas vraiment aux courriels, donc pas très simple... Pour le ResEl la priorité n'est pas la CSS, mais bien la migration sur le serveur, et la mise à jour de spip effectuée par Nicolas Aupetit. Normalement la version comprend toutes les options du cahier des charges du BdE, hormis les demandes particulières du BdS.

2 Décisions prises

2.1 Achat matériel

2.1.1 Renouvellement matériel Rennes

Il faudrait une nouvelle machine pour Rennes, un seul serveur fonctionne là bas et regroupe l'ensemble des services. Pour rajouter des services et fiabiliser un peu le réseau, il faudrait une nouvelle machine. (installation de la TNT sur la nouvelle machine) Jeb a estimé les besoins, et fait faire un devis pour l'achat du matériel. Au total, les dépenses s'élèveraient à environ 800 euros. Voici la liste détaillée des demandes de Jeb :

- Silverstone SST-FP53S (5 exemplaires) à 114,52 €
- Enermax ECA-3070B (2 exemplaires) 149,91 €

- Intel DG965RY 108,99 €
- Intel Pentium D - 915 (Boîte) 95,99 €
- G.Skill Kit Extreme2 2 x 512 Mo PC6400 PK 96,95 €
- Cooler Master Hyper L3 32,90 €
- Hitachi Deskstar 7K160 - 160 Go - 8 Mo 99,99 €
- Hitachi Deskstar 7K160 SATA - 160 Go - 8 Mo 48,99 €
- Western Digital Caviar SE S-ATA 160 Go - 8 Mo 53,99 €
- Zalman ZM-F3 (4 exemplaires) 35,59 €

Conclusion du vote : 6 voix pour. La commande définitive peut-être effectuée.

2.1.2 Brest

L'achat d'un serveur NAS pourrait être utile pour l'installation des machines virtuelles, ainsi que pour divers stockage. Il faut tout d'abord décider si oui ou non, sur le principe, nous achetons ou pas une machine, puis savoir quel type de machine on commande. (entre serveur pro, ou machine montée avec des pièces détachées.)
Résultat du vote pour le principe de l'achat : 5 pour, une abstention.
Résultat du vote pour le type de matériel : 5 pour un serveur pro, et une abstention.
La commande exacte sera définie sur la mailing liste gestion@resel.fr, il reste à discuter notamment sur le nombre et la taille des disques durs. Jeb est notamment en contact avec IBM et Dell pour obtenir des devis.

3 Tâches à accomplir

3.1 Sécurité

3.1.1 Gérer les machines inactives

Eviter la réapparition de machines avec des fausses adresses MAC qui n'ont pas été utilisée depuis longtemps devient nécessaire, les moyens de surveillance actuels ne sont pas suffisants.
Une idée bien plus simple que d'installer de l'identification forte en 802.1x est de forcer de retaper le login/mot de passe pour une machine inactive depuis quelques jours sur le ResEl. (trois jours par exemple) Il n'est pas possible de couper l'ensemble des services du ResEl, mais uniquement l'internet. (ce qui passe par Lily en l'occurrence) C'est certainement très facile pour des personnes utilisant du DHCP, un petit poil moins pour ceux qui se placent en ip fixe. Il faut réfléchir (en demandant des informations complémentaires aux anciens notamment) à l'installation précise de ce système. Rajouter un champ dans le ldap est certainement la solution la plus pratique. (et la plus saine)

3.1.2 Couper totalement le Wifi

Actuellement en cas de coupure d'un utilisateur, on accède encore aux services du ResEl par le WiFi, la coupure n'est qu'au niveau du firewall et non pas du serveur radius. Le seul moyen est de rajouter à la main dans le fichier de configuration un filtre pour les utilisateurs très très méchants. *Benoît* se charge d'automatiser un peu tout ça, en rajoutant un fichier contenant les utilisateurs interdits. (cette modification est uniquement pour des cas de comportement très graves, équivalent d'une coupure au port pour du filaire)

3.1.3 Bornes WiFi « pirates »

On voit de plus en plus de bornes WiFi d'utilisateurs se connecter sur le réseau. Elles sont souvent mal configurées, à savoir en DHCP (serveur DHCP pirate...), sans protection, et enfin font du NAT.

N'importe qui peut donc avoir accès par ce moyen au réseau du ResEl, et tous les services qui vont avec. Il va falloir prévoir des « rondes » sur le campus, pour évaluer proprement la situation et signaler le problème. (prévoir de communiquer également sur le sujet)
Commentaire de Jeb : pour le WiFi on va avoir un problème de Vlan aussi. Il faut regarder si les bornes sont capables de mettre un utilisateur dans un Vlan particulier (en utilisant le 802.1x) si oui c'est cool (et il devient facile de couper) si c'est pas le cas c'est un peu la merde :) Il faut regarder du coté de Kamikaze (prochaine release d'OpenWRT)
Une interdiction complète de ces bornes est à prévoir, à moins de proposer une configuration obligatoire fournie par le ResEl. (pour celles qui sont configurables) (même si vu le nombre de bornes existantes, on peut toujours rêver d'y parvenir...)

3.2 Passage en etch et UTF-8

La migration en etch doit-être prudente, les machines étant a priori les plus critiques sont Baal, Venus et Noboot. Il faudra tester sur d'autres machines le changement, et le faire vraiment proprement. Au passage, ne pas oublier de passer tout les serveurs en UTF-8, pour ceux qui ne le sont pas encore. Le passage en etch aura de nombreux avantages, suivi des paquets, actualisation des services (sympa 5 sur Venus par exemple...)

Une autre solution est de migrer directement dans les VM, en risquant de ne pas passer avant quelques temps les serveurs en etch si la virtualisation prend du retard.

3.3 PXE

Le PXE est moche, *Antoine* voudrait l'améliorer. Toutes les idées pour le rajout de distribution sur le PXE est bienvenue, il faut également changer la page d'accueil du PXE pour signaler ce qui est disponible. (actuellement la page n'est absolument pas à jour)