
Guide pratique de l'administrateur système/réseau

Rémi FUSSIEN – administrateur système & réseau

Sommaire

1 Avant-propos.....	4
2 Présentation de l'entreprise.....	5
2.1 Présentation de l'entreprise.....	5
2.2 Plan du site.....	6
3 Présentation du poste d'admin.....	7
3.1 Compétences requises/souhaitables.....	7
3.1.1 OS utilisés.....	7
3.1.2 Logiciels utilisés.....	7
4 Bilan de l'existant.....	8
4.1 Le réseau local.....	8
4.2 La téléphonie.....	8
4.3 Les salles de cours.....	9
4.4 Les imprimantes.....	9
4.5 Hébergement.....	10
4.5.1 Le datacenter.....	10
4.5.1.1 Adresse.....	10
4.5.1.2 Contacts.....	10
4.5.1.3 Interface de gestion Netcube.....	10
4.5.2 Les noms de domaine et les mails.....	10
4.6 Les serveurs.....	11
4.7 Descriptif détaillé des serveurs importants.....	12
4.7.1 Le serveur de production.....	12
4.7.1.1 Détails matériel.....	12
4.7.1.2 Interfaces réseau.....	12
4.7.1.3 Services en place.....	12
4.7.1.3.1 SSH.....	12
4.7.1.3.2 Apache.....	13
4.7.1.3.3 PostgreSQL.....	13
4.7.1.3.4 MySQL.....	13
4.7.1.3.5 Samba.....	13
4.7.1.4 Outils.....	14
4.7.2 Le serveur en ligne.....	15
4.7.2.1 Détail du matériel.....	15
4.7.2.2 Interfaces réseau.....	15
4.7.2.3 Services en place.....	15
4.7.2.3.1 SSH.....	15
4.7.2.3.2 Apache.....	16
4.7.2.3.3 PostgreSQL.....	16
4.7.2.4 Outils.....	16
4.8 Les outils utilisés (par moi, et juste pour info).....	16

4.8.1 Logiciels.....	16
4.8.2 Matériel.....	16
5 Les tâches courantes.....	17
5.1 Déploiement des salles.....	17
5.2 Veille et conseils.....	17
5.3 La documentation.....	17
5.4 Le maintien des serveurs.....	18
6 Les tâches à venir.....	19
6.1 Restructuration du réseau local.....	19
6.1.1 Les aménagements physiques.....	19
6.1.2 Reconfiguration du réseau.....	19
6.1.2.1 Schéma.....	19
6.1.2.2 Explications.....	20
6.1.2.3 Un adressage dynamique.....	20
6.1.2.4 Politique antivirale.....	20
6.2 La téléphonie.....	21
6.3 Modification de l'architecture du serveur en ligne.....	21
6.3.1 Le Firewall.....	21
6.3.2 La restructuration des espaces client.....	22
6.3.2.1 L'existant.....	22
6.3.2.2 Un nouveau mode de fonctionnement.....	22
6.3.2.2.1 Pourquoi changer le fonctionnement en place ?.....	22
6.3.2.2.2 Mise en place.....	22
6.3.2.2.3 Arborescence.....	23
7 Le mot de la fin.....	23

1 Avant-propos

Bonjour,

Ce document est destiné à mon successeur pour le poste d'administrateur système et réseau. Il devrait s'en servir comme guide pour commencer, et le compléter à mesure de l'évolution de son poste et de son profil, afin que celui qui lui succédera puisse en bénéficier également. Au cours de ce document, je vais essayer de décrire le plus précisément possible le fonctionnement du système d'information de l'entreprise, sa philosophie en matière de choix de système d'information, l'existant et les perspectives d'avenir.

Le poste d'administrateur est un des postes clés de l'entreprise. D'une part parce que les problèmes auxquels doit faire face un admin peuvent être très gênant, voir bloquant pour les autres (services production, administratif, stagiaires, clients), et d'autre part car c'est lui qui a la maîtrise de l'outil de communication et d'information de l'entreprise, véritable nerf de guerre pour la stratégie d'entreprise. C'est pourquoi il doit être réactif et dynamique.

Pour que ce travail puisse se faire dans les meilleures conditions, l'admin doit instaurer une relation de confiance avec les autres. Les utilisateurs auxquels il fournit des outils doivent sentir qu'ils peuvent compter sur lui en cas de problème.

Voilà deux ans que j'ai hérité des fonctions d'administrateur système et réseau d'Afide. Ayant un profil de développeur, j'ai également contribué au développement de la plate-forme, aux outils actuellement utilisés par la production et réalisé quelques développements web comme le front-office du site Afide ou le site du serveur de production. Ne sachant pas si la personne qui me remplacera aura des capacités en développement, je n'aborderais pas cette facette de mon poste.

Au fil de mon expérience à Afide, j'ai mis en place certaines choses, j'en ai maintenu d'autres, mais il reste encore beaucoup de choses à faire.

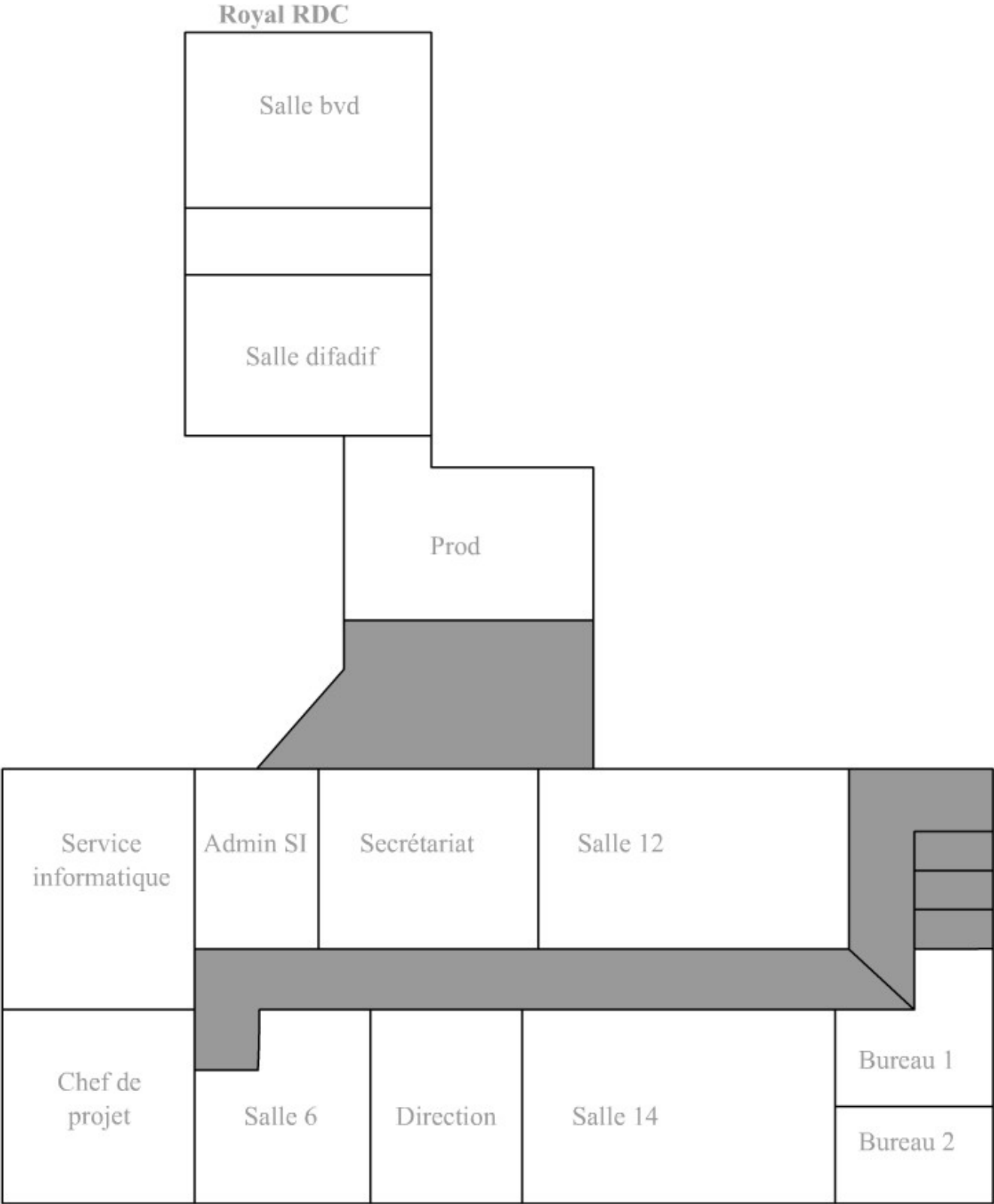
2 Présentation de l'entreprise

2.1 *Présentation de l'entreprise*

AFIDE est une entreprise de taille humaine (entre 10 et 20 personnes). Cela implique une certaine polyvalence de l'administrateur.

L'entreprise s'axe selon trois pôles d'activités. Les formations (multimédia, bureautique, ...), le conseil/audit (exercé par les consultants en ressources humaines) et la production dont la principale tâche est le développement de la plate-forme (framework) d'Afide. Nous sommes contraint pour les formations d'utiliser des logiciels propriétaires, mais en général, la philosophie première et surtout pour la production est d'utiliser des logiciels open source. En générale, les tâches demandées viennent de M. Stern (directeur), et du chef de projet en ce qui concerne la production.

2.2 Plan du site



3 Présentation du poste d'admin

3.1 Compétences requises/souhaitables

Par rapport à l'existant, plusieurs compétences sont indispensables, et certaines sont appréciables.

Au niveau des systèmes d'exploitation, le parc d'Afide est un environnement hétérogène et certaines machines sont vieillissantes, et donc pénibles à entretenir.

3.1.1 OS utilisés

- **FreeBSD** (serveur de production, serveur en ligne, serveur de test) : la maîtrise de cet OS est très importante dans le sens où tous nos services en ligne et nos services de production sont basés dessus. Je l'ai choisi et mis en place car FreeBSD est un système extrêmement solide et bien plus structuré que Linux. Il peut assumer de fortes montées en charge et est facile à maintenir et à administrer. Un profil orienté Linux ne devrait pas éprouver de grande difficulté d'adaptation et de familiarisation avec cet OS. Évidemment, il faut maîtriser le mode console, sur le serveur en ligne il n'y a pas de serveur X.
- **GNU/Linux** (serveur de fax, routeur/passarelle, postes des développeurs) les postes des développeurs ainsi que la passerelle tournent sur Debian et le serveur de fax utilise une Mandrake.
- **Windows 2000/XP** (postes des stagiaires, postes administratifs) Windows n'est utilisé que comme poste client, mis à part le PDC qui fonctionne encore avec un vieux Windows NT.

3.1.2 Logiciels utilisés

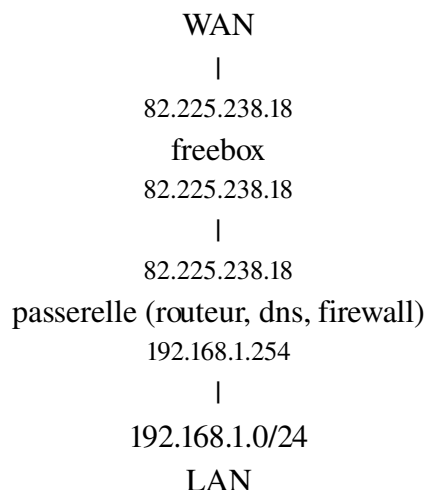
Logiciels sur lesquels repose la production et le serveur en ligne :

- **Apache** 1 et 2
- **php** 4 et 5
- **PostgreSQL** (pour exploiter PostgreSQL, l'administrateur et les développeurs utilisent **pgadmin3** et **phpPgAdmin**)
- **MySQL** (essentiellement utilisée par les outils de production : synchro, wiki, egroupeware, ...)
- **ssh** (toute l'administration et les accès au serveur en ligne se font via ssh, toute la production travaille avec ssh en export display)
- **rsync** (très utilisé pour tout ce qui touche aux synchros et aux sauvegardes)
- **samba**
- **eclipse** (principale IDE de la production)
- **Bind** (dns)
- **ipfw/iptables** et règles de routage
- **Postfix**
- **Hylafax** (serveur de fax)

4 Bilan de l'existant

4.1 Le réseau local

Le réseau local d'Afide est assez simple :



Tous les postes sont en IP statique et il n'y a aucun serveur DHCP.

Il existe dans la baie une petite borne wifi qui permet à M. Stern ainsi qu'aux formateurs de pouvoir se connecter plus facilement au réseau.

La passerelle n'est accessible via ssh que par les ip 192.168.1.203-204 (les ip que j'utilise et que je recommande d'utiliser au futur admin, au début du moins) et par le serveur en ligne.

Cette configuration a été mise en place par mon prédécesseur et correspondait au besoin d'Afide lors de sa mise en place, mais je détaillerais l'évolution du réseau que je préconise pour les nouveaux besoins d'Afide dans le chapitre sur les évolutions potentielles.

4.2 La téléphonie

Afide n'étant pas une structure assez importante pour avoir un poste dédié pour la téléphonie, c'est à l'administrateur qu'incombe la tâche de s'occuper du parc téléphonique. Le centre de Port Royal a un réseau téléphonique vieillissant et il serait une bonne chose de lui donner un petit coup de jeune. Dans la partie sur les évolutions de ce document, se trouvent mes conseils par rapport à la téléphonie.

4.3 Les salles de cours

Le pôle de formation de l'entreprise nécessite la maintenance permanente de 4 salles de cours d'une dizaine de postes chacune. Cela ne représente pas un travail énorme quand il est fait régulièrement. J'avais prévu de minimiser cette tâche au profit de mon travail en production en automatisant certaines choses, mais par manque de temps, cela n'a pas été fait.

- La salle BVD (pour boulevard), comme son nom l'indique, c'est la salle la plus proche du boulevard Port Royal. Elle est composée pour l'instant de postes DELL tout à fait récents.
- La salle 12 est composée (en théorie) de 12 postes récents DELL.
- La salle 14 est composée de 14 postes assez vieux (pIII 1000Ghz pour la plupart)
- La salle 6 est composée de 8 postes qui ont été achetés dans l'urgence chez les chinois du 12ème et montés par le fils de M. Stern et moi même. Cette salle n'est pas homogène et le matériel qui la compose n'est pas de très bonne qualité. Elle est assez pénible à gérer.
- Les formateurs ont à leur disposition deux vidéo-projecteurs.

4.4 Les imprimantes

Il y a une imprimante par salle :

- HP1320 en salle 12
- HP1320 en salle 14
- HP1320nw (en wifi) en salle 6
- HP2100tn (ethernet) en salle BVD
- DSM730 (photocopieuse du couloir reliée en réseau et servant également d'imprimante)
(code d'utilisation de la photocopieuse : **1234** (*pas génial, mais facile à retenir*))

Je conseil de conserver au maximum des imprimantes identiques pour un raison évidente de consommation de consommable identique. Des démarches pour renouveler entièrement le parc des imprimantes auprès du même fournisseur que la photocopieuse (NRG) ont déjà étaient faites. Cela permettrait d'avoir des imprimantes qui aient toutes une interface réseau (et plus besoin de poste qui partage une imprimante) et de pouvoir n'utiliser qu'un seul type de consommable (et ce avec le même coût copie que la photocopieuse).

4.5 Hébergement

4.5.1 Le datacenter

Afide loue un quart de baie dans un datacenter à Vitry/Seine à la société NetCube. Pour s'y rendre, il faut contacter M. CAMBESSEDES ou Mme GAILDRY et avoir une carte d'identité.

4.5.1.1 Adresse

Le serveur en ligne se trouve au data-center telecom italia à l'adresse :
29 Rue Edith Cavell – 94400 VITRY SUR SEINE

4.5.1.2 Contacts

Sct Netcube (prestataire pour l'hébergement)
18 bd Aristide Briand – 91600 Savigny sur orge
Pascal CAMBESSEDES (responsable projets) : 01 69 12 33 27
Christine GAILDRY (Directrice commerciale) : 01 69 12 10 50

4.5.1.3 Interface de gestion Netcube

url : <http://my.netcube.fr>
login : net3
password : net32004

4.5.2 Les noms de domaine et les mails

Tous les nom de domaines et adresses mail qui sont gérés par afide sont chez OVH. Le détail de ces derniers est dans le fichier contenant tous les mots de passes.

Tous les mails que je reçoit concernant les tâches administratives (retour d'info des serveurs, contact avec Netcube, free, ...) me sont envoyés à l'adresse root@afide.fr. Il s'agit d'un alias, il faut juste faire pointer cet alias vers la nouvelle adresse de l'administrateur. Il ne faut pas créer de compte mais laisser cette adresse comme étant un alias, cela permet en cas de départ de ne pas avoir à contacter tout le monde pour dire qu'on a changé d'adresse et cela permet de ne pas toucher à la configuration des serveurs pour les descentes d'informations. Il ne faut pas donner cette adresse à tout le monde (pas pour les fournisseurs, pas pour les utilisateurs, pas pour les inscriptions en ligne, ...), cette adresse doit rester clean par rapport au spam.

Je ne conseille pas à l'administrateur de se faire une adresse du style admin@afide.fr, webmaster@afide.fr, etc, car il recevra forcément du spam.

4.6 Les serveurs

- **un serveur de production**, que j'ai mis à la cave car le bruit qu'il fait est insupportable (j'ai travaillé plusieurs mois à côté, et honnêtement ce n'est pas bon pour le moral). C'est un p4 2,8Ghz avec 2Go de Ram et 5 disk en RAID 5 + 1 en spare disk (géré par une carte 3ware) le tout dans un boitier rackable de 3U.
- **un serveur en ligne**, situé dans un datacenter dans le sud de paris. C'est un Bi-Xeon 3Ghz, avec 4Go de Ram et 3 disk en Raid 5 (gérés par une carte 3ware) le tout dans un boitier rackable de 2U.
- un serveur de test, situé dans la cave, à côté du serveur de production. C'est un p4 2,8Ghz avec 512Mo de Ram. Ce petit serveur me sert à faire des tests avec de mettre en place certaines choses sur les autres serveurs.
- **un serveur de fax**, situé sous le bureau du secrétariat. C'est une vieille machine avec un modem USRobotix dont la seule utilité est de recevoir les fax et de les envoyer automatiquement par mail à l'adresse fax@afide.fr et un avis de reception à FaxMaster@afide.fr. Pour que les personnes intéressées reçoivent correctement les fax, il suffit de faire une redirection par mail.
- **une passerelle**, située dans la baie. C'est une vieille machine également qui a pour rôle d'être le routeur pour la connexion ADSL, mais qui sert également de passerelle et qui servait de VPN lorsque nous avions plusieurs sites (peut-être réutilisé si on ouvre un nouveau site).

Tous les serveurs discutent entre eux et pas mal de mails (info sur les updates, les problèmes Raid, le résultat des synchros et des backups, ...) sont envoyés à l'adresse root@afide.fr

4.7 Descriptif détaillé des serveurs importants

4.7.1 Le serveur de production

4.7.1.1 Détails matériel

nom : barracuda

processeur : P4 3.8Ghz

mémoire Ram : 2048MB

cartes réseau : 3 cartes ethernet (une 3com 3c905C et deux intel Gigabit)

Contrôleur Raid : 3ware Inc 9xxx-series SATA-RAID

Disque dur : 5 disque Hitachi de 250GB en raid 5 + 1 en sparedisk

4.7.1.2 Interfaces réseau

Le serveur possède 3 interfaces :

- em0
 - ip réelle : 192.168.1.80/24
 - ip virtuelle : 192.168.1.83-110/32
- em1
 - ip réelle 192.168.1.81/24 (interface de secours)
- xl0
 - ip réelle 192.168.1.82/24 (interface de secours)

4.7.1.3 Services en place

4.7.1.3.1 SSH

sshd écoute l'ip 192.168.1.80:22

l'export X11 est autorisé

la connexion au compte root est autorisé

4.7.1.3.2 Apache

Apache est configuré avec des hôtes virtuelles le détail est le suivant :

- 192.168.1.80 : page d'accueil de la production ou l'on trouve tous les outils et renseignements utiles. L'administrateur se connecte avec l'identifiant '**admin**' et password '**php**' et les développeurs avec l'identifiant '**prod**' et password '**php**'.
- 192.168.1.83 : Front office de la plate-forme de production
- 192.168.1.84 : Back office de la plate-forme de production
- 192.168.1.85 : Front office PGR
- 192.168.1.86 : Bacsshd écoute l'ip 192.168.1.80:22

l'export X11 est autorisé

- la connexion au compte root est autorisée office PGR
- 192.168.1.87 : Administration des PGR de production
- 192.168.1..88 : Site AFIDE
- 192.168.1..89 : Back-office du site AFIDE
- 192.168.1.110 : Sites clients (dont un site spécial qui s'appelle bac_a_sable qui contient des scripts de test et des essais d'interface)

4.7.1.3.3 PostgreSQL

le serveur postgres écoute sur l'ip 192.168.1.80:5432

Il est configuré pour utiliser les champs système oids (ce qui ne correspond pas à la configuration par défaut depuis la version 8.1 je crois), car ce champ système est encore utilisé dans certains scripts de production pour tester le dernier enregistrement.

4.7.1.3.4 MySQL

MySQL est utilisé pour le wiki, egrouppware, les synchros et les numéros de licences des logiciels d'AFIDE. Sa configuration est une configuration de base.

4.7.1.3.5 Samba

Samba est utilisé pour les partages Windows. Chaque utilisateur (que cela soit en production ou l'administration a un home directory ('/home/<nom_utilisateur>') et tous les utilisateurs ont un répertoire commun de partage ('/home/share/<nom_utilisateur>').

Attention, pour qu'un utilisateur utilise un partage samba, il est nécessaire de créer un compte unix (avec ou sans shell), mais il faut également créer un compte samba à l'aide de la commande :
smbpasswd -a nom_de_l_utilisateur

4.7.1.4 Outils

Sur la page d'accueil de la production (192.168.1.80, htaccess:admin/php) sont accessibles :

- La page de gestion des synchros
- La page de gestion des backups (attention, quand on fait une modification sur les backup, il ne faut pas oublier de générer la crontab grâce au lien prévu à cet effet).
- Une page pour faire un whois
- L'outil de gestion de la carte Raid (attention, depuis un problème avec un disque défaillant, cet outil est devenu instable, je n'ai pas réussi à résoudre le problème. Ne pas utiliser cet outils quand la prod travail car il y a un risque de blocage du serveur)
- eGroupWare : outils de gestion de projet
- Accès aux logs du serveur (uniquement les logs apache et postgresql pour aider les développeurs)
- Les statistiques du serveur de production
- Une page phpinfo()
- phppgadmin et phpmyadmin
- bugzilla (non utilisé encore)
- Le wiki de documentation de la production sur lequel se trouve quelques documentation utiles pour l'administration.
- Les documentations générées par PHPDoc et PHPDocumentor
- Les documentations php et postgresql

En ligne de commande :

- pgadmin3

4.7.2 Le serveur en ligne

4.7.2.1 Détail du matériel

nom : hannibal

domaine : afide.fr

processeur : bi-xéon dualcore 3.0Ghz

mémoire Ram : 4096MB

cartes réseau : 3 cartes ethernet (une 3com 3c905C et deux intel Gigabit)

Contrôleur Raid : 3ware Inc 9xxx-series SATA-RAID

Disque dur : 3 disque Hitachi de 160GB en raid 5

4.7.2.2 Interfaces réseau

Le serveur possède 3 interfaces :

- em0 (interface de secours)
- em1
 - ip réelle : 217.113.207.1/27
 - ip virtuelle : 217.113.207.2-29/32
 - dns utilisées (dns publiques) : 194.206.126.253, 62.210.64.50, 193.55.10.101
 - adresse de passerelle : 217.113.207.30
- xl0 (interface de secoure)

4.7.2.3 Services en place

Une description détaillée des domaines et des services associés est disponible dans le fichier de mot de passe.

4.7.2.3.1 SSH

sshd écoute l'ip 217.113.207.1:22

l'export X11 n'est pas autorisé

la connexion au compte root n'est pas autorisé

Pour se connecter au serveur en ligne, il y a deux comptes utilisateur importants :

- **webafide** : compte qui regroupe tout ce qui tourne autour du serveur web (synchro à partir du serveur de prod notamment)
- **admin** : est le compte de l'administrateur. ce compte a les droits sudoers du root, donc pour se connecter en root sur le serveur en ligne, il faut se logger en tant qu'admin, puis faire un **sudo bash** ou **sudo su**.

Le serveur de prod et le serveur en ligne dispose de clé privés/clé public appropriées afin qu'il n'y ait pas de demande de mot de passe. C'est indispensable pour effectuer les tâches planifiées comme les backups.

4.7.2.3.2 Apache

Apache est configuré avec des hôtes virtuelles le détail est dans le fichier de mots de passe.

4.7.2.3.3 PostgreSQL

Pour des raisons de sécurité, le serveur Postgresql n'écoute que le loopback.

ps : Cependant, temporairement et avec l'accord du chef de projet, le serveur écoute l'ip du site Afide. Cette modification est changeable dans le fichier : /usr/local/pgsql/data/pg_hba.conf a été faite pour utiliser pgadmin3 pour faire des modifications sur les bases en ligne.

Comme le serveur de production, il est configuré pour utiliser les champs système oids.

4.7.2.4 Outils

Sur la page d'administration (<https://admin.afide.fr>, htaccess:admin/wrackyooob) sont accessibles :

- les statistiques par site web et les statistiques d'utilisation du réseau
- L'outil de gestion de la carte Raid (celui en ligne fonctionne très bien)
- Nagios (que je n'ai pas encore configuré)
- une page phpinfo()
- phppgadmin et phpmyadmin

4.8 Les outils utilisés (par moi, et juste pour info)

4.8.1 Logiciels

Listing des outils que j'utilise :

- sous linux/unix (os principal sur mon poste) :
 - une console shell
 - un client ssh
 - un navigateur
 - un logiciel de messagerie
 - Open office
 - client VNC
 - pgadmin3
- sous Windows (indispensable de temps en temps pour les applications qui ne fonctionnent pas sous linux) :
 - Norton Ghost (pour déployer les images par le réseau)
 - Putty (pour avoir une console shell)
 - Cygwin (afin de pouvoir exploiter l'export display à partir d'un poste windows)
 - WinSCP (idéal pour le transfert de fichier via ssh)

4.8.2 Matériel

Les outils que j'utilise sont les grands classiques... Tourne-vis, marteau (pour les pc récalcitrants), testeur de câble, pince à dénuder, ...

A l'heure actuelle, ils sont à la cave, juste à côté du serveur de production.

5 Les tâches courantes

5.1 Déploiement des salles

Pour le déploiement des salles, j'utilise une ancienne version de Norton Ghost corporate. Il serait intéressant de mettre en place une méthode de déploiement plus récente et plus efficace.

Ce qui est nécessaire pour le déploiement des salles se trouve sur le serveur de production :

- **/home/share/ressource/ghost** : les images ghost des postes
- **/home/share/ressource/drivers** : les drivers des imprimantes
- **/home/share/ressource/software**s : tous les logiciels utilisés pour les formations (les numéros de série sont sur **<http://192.168.1.80/gestion/licences/>**)

Tous les cd d'installation sont en théorie dans le bureau de M. Stern et l'admin en a une copie.

5.2 Veille et conseils

La veille technologique est une part non négligeable du poste d'administrateur. D'une part pour pouvoir proposer des perspectives d'avenir pour les projets en cours, mais également pour mettre en place des outils qui facilitent et/ou optimisent le travail des utilisateurs (prod, administration, stagiaires, formateurs, ...).

Certaines veilles découlent d'un besoin explicitement exprimé (ex : besoin de pouvoir compiler et/ou crypter le code php de la plate-forme pour pouvoir la vendre, que doit-on utiliser et à quel prix ?), alors que d'autre découlent d'initiative de la part de l'administrateur (ex : qui sont les principaux acteurs du marché en matière de télécommunication ? lesquelles sont les plus avantageux ?).

5.3 La documentation

Ce document est la mise en pratique du titre de cette partie. La documentation est le seul vecteur de communication sur lequel les autres peuvent se baser en cas d'absence (ou comme le cas présent, de départ). J'ai réalisé un bon nombre de documentations (sans doute pas assez), qui devraient être utiles à mon successeur.

Une documentation doit être un support vivant et évolutif. C'est dans cette optique d'évolution que j'ai mis en place un wiki comme support de documentation. Cet outil permet effectivement de modifier perpétuellement tout son contenu (chose beaucoup plus pénible à réaliser sur un document texte, ou pire, sur un papier).

5.4 Le maintien des serveurs

Le bon fonctionnement des serveurs est un élément vital pour l'entreprise (sans serveur de production, pas de production et sans serveur en ligne, pas d'outil de communication public).

Pour éviter les bons trop importants entre les versions des logiciels comme j'en ai déjà subi les conséquences, je conseil à mon successeur de suivre régulièrement les mise à jour des versions tout en restant prudent et en veillant à ce que cela ne perturbe pas l'existant.

Pour ce faire, j'ai écrit un petit script qui fait automatiquement la construction de la base de données des logiciels portés par rapport aux versions des dépôts et qui averti l'administrateur par mail toutes les semaines en cas de nécessité de mise à jour. Ce script se trouve sur le serveur de prod (/root/script_admin/maj_ports.sh) ainsi que sur le serveur en ligne (/usr/home/admin/script_admin/maj_ports.sh)

Les procédures de mises à jour sont décrites dans le wiki ainsi que l'historique de ces dernières.

6 Les tâches à venir

A partir de ce point du document, il ne s'agit plus de l'existant, mais juste de réflexions ou d'ébauches de réflexion que je n'ai pas envie de mettre aux oubliettes. Cependant, chacun possédant ses méthodes, et ne détenant pas les meilleures (loin de là), donc ce que je vais exposer par la suite n'est que mon opinion et **n'est pas** une suite de chose à faire "à ma manière".

6.1 Restructuration du réseau local

Le réseau tel qu'il existe ne correspond plus au besoin d'Afide. Pour donner des pistes de travail, voici ce que je préconise pour restructurer le réseau.

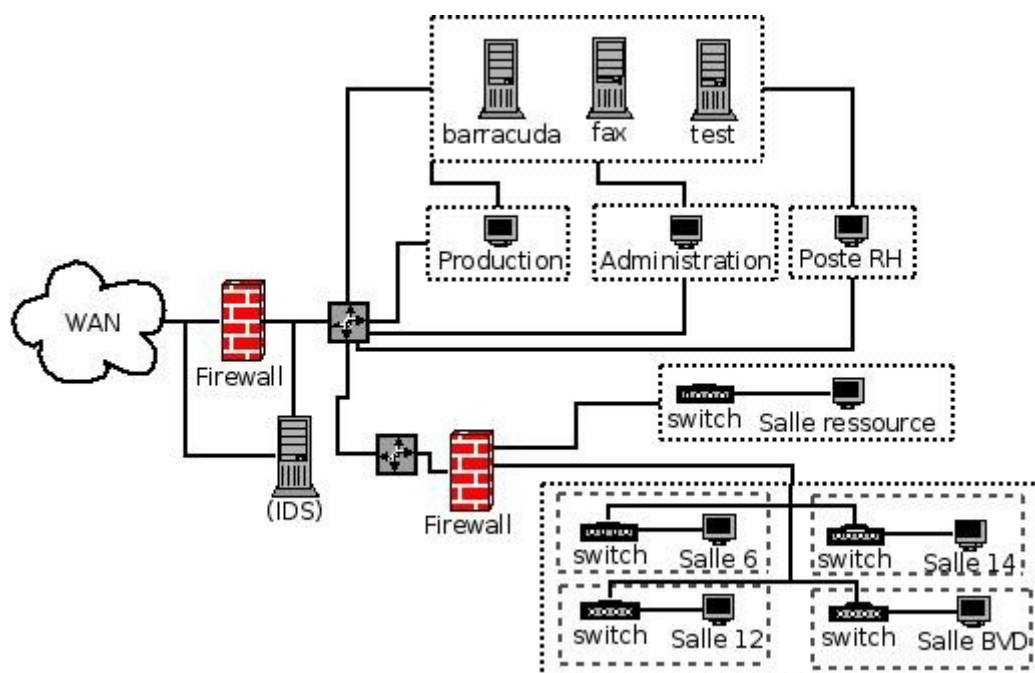
6.1.1 Les aménagements physiques

- En premier lieu, il serait intéressant de déplacer la freebox, car elle est actuellement dans un bureau et sa place idéale serait dans la baie de brassage (il faudrait faire passer les fils dans le faux plafond).
- Ensuite, un gros chantier serait de refaire la baie de brassage qui a une organisation un peu chaotique. Je n'ai pas encore eu le temps de m'y plonger, mais c'est assez difficile de s'y retrouver dans ce plat de spaghetti. Il serait intéressant de dissocier le réseau informatique du réseau téléphonique.

6.1.2 Reconfiguration du réseau

Les besoins d'Afide ayant changés, et la configuration du réseau ne correspondant plus aux besoins actuels, voici la solution de l'architecture réseau que je propose au nouvel admin.

6.1.2.1 Schéma



6.1.2.2 Explications

L'idée de base est de scinder le réseau actuel en plusieurs réseaux et sous-réseaux. D'abord pour une question de sécurité, puis pour une question de qualité du réseau (moins d'encombrement dans les tubes). J'ai distingué 6 réseaux, et dont un réseau défini par quatre sous-réseaux :

- un réseau dans lequel serait les serveurs
- un réseau pour la production
- un réseau pour l'administration (secrétariat, direction, responsable des formations, ...)
- un réseau pour les postes des consultants en ressources humaines
- un réseau pour la salle ressources
- un réseau pour les salles de formations séparé en quatre sous réseau (un sous-réseau par salle)

Les réseaux de la production, de l'administration et des postes RH doivent avoir accès au réseau des serveurs, ne serait-ce que pour avoir accès aux données du serveur de production (qui sert de serveur de fichier également).

Pour les routeurs et les firewall, je conseil (ce n'est qu'un conseil) d'utiliser openBSD (connu pour sa politique de sécurité paranoïaque). Quelques vieilles machine de la cave feront l'affaire.

Une des idées qui m'a traversé l'esprit était de mettre en place une petite DMZ avec un serveur web auquel aurait accès les stagiaires en local, mais aussi de l'extérieur. En effet, une question redondante qui m'a souvent été posé par les stagiaires était : "*Est ce que je peux avoir accès à mon poste à partir de chez moi ?*", ce à quoi je répondais toujours *non*, bien sur. Mais il s'avère que cela serait vraiment très appréciable pour les stagiaires (et ce surtout en période de projet, surtout quand ils sont orientés web) de pouvoir avoir accès à leur travail, aux supports de cours, et de pouvoir le partager avec leur groupe, et le tout à partir de chez eux.

L'adressage pourrait se faire en ipv6, mais n'étant pas à l'aise avec cette techno, je me passerai de donner mon avis...

6.1.2.3 Un adressage dynamique

Actuellement, et parce que je ne l'ai pas changé depuis que je suis arrivé, tout l'adressage du parc est en ip fixe, il pourrait être appréciable et cela pourrait présenter un réel gain de temps lors du déploiement des salles si l'adressage était dynamique.

6.1.2.4 Politique antivirale

L'antivirus utilisé quand je suis arrivé était norton antivirus corporate. Il est vieux, out of date, gourmand et peu efficace. Je l'ai remplacé temporairement par AVG Free, qui est un bon antivirus, mais il faudrait soit le faire passer en version pro ou autre, soit utiliser un autre antivirus (mais par pitié, pas Norton... ;).

6.2 La téléphonie

Le réseau téléphonique a également besoin d'un petit coup de neuf. Pour cela, il y a dans la cave, en bas à gauche dès qu'on descend l'escalier, du matériel neuf ou presque (postes, pabx, ...). D'autre part, les besoins en terme de téléphonie ont changés et l'existant est assez chaotique (mélange du réseau téléphonique avec le réseau informatique dans la baie de brassage). J'avais commencé à prendre contact et faire faire des devis auprès de la société SCT telecom (courtier) qui peuvent refaire l'installation et prendre en charge nos communications (avantages financiers par rapport à l'opérateur historique).

6.3 Modification de l'architecture du serveur en ligne

En mai 2006, le serveur en ligne (un vieux pentium2) était hébergé dans un datacenter Verizon (anciennement MCI et encore plus anciennement UUNET). Nous avions donc un vieux serveur et une bande passante de 512MB/s. J'ai donc proposé un changement d'hébergeur (moins cher et avec une plus grande bande passante) et un changement de serveur. J'avais planifié une installation et une migration des données sur un moi et demi. Malheureusement, la livraison du serveur a eu deux mois de retard, si bien que j'ai dû faire l'installation et la migration des données sur 10 jours (journée de 22h... difficile). Cette migration s'est bien passé, mais je n'ai par conséquent pas eu le temps de mettre en place tout ce que j'avais prévu.

6.3.1 Le Firewall

Le firewall que j'ai mis en place sur le serveur en ligne est trop permissif. J'ai écrit les règles que je voulais mettre en place, mais je ne les ai pas encore mise en place (faute de temps). Je conseil de faire l'activation du firewall directement dans le datacenter pour éviter ce qui m'est déjà arrivé avec le serveur en ligne, c'est à dire de me coupé tout accès au serveur (gros coup de stress, surtout quand il s'agit du serveur en ligne)...

J'ai écrit un fichier de règles dynamiques en fonction des services lancés. Pour mettre en place le firewall en ligne, il faut aller dans le fichier **/etc/rc.conf** (dans lequel se trouve les directives). Les fichiers de règles se trouvent déjà en ligne, il n'y a que 4 lignes à décommenter et deux à commenter.

Les serveurs en ligne sont souvent les proies des "script kiddies" qui font de multiples tentatives de connexion sur le port ssh avec des logins différents et des dictionnaires de mots de passe. Le serveur d'AFIDE n'échappant pas à cette règle, il y a un script en perl (sshit) qui permet d'ajouter une règle au firewall, bloquant pendant 10min l'ip d'une machine qui a essayé, sans succès, de se connecter en ssh 3 fois en moins de 60s. Pour activer ce script, et ce après la mise en place des nouvelles règles, il suffit d'aller dans le fichier **/etc/syslog.conf** et de décommenter la ligne que j'ai placé à cet effet (c'est indiqué dans le fichier).

6.3.2 La restructuration des espaces client

6.3.2.1 L'existant

Actuellement, la configuration d'apache adopte le fonctionnement suivant :

un client est défini par

- un domaine
- + un virtual host apache pointant vers /usr/local/www/data/sites_externes/<nom_du_client>

Tous les clients sont sur la même ip.

6.3.2.2 Un nouveau mode de fonctionnement

6.3.2.2.1 Pourquoi changer le fonctionnement en place ?

Pour faciliter le déploiement des sites, des plate-formes et pouvoir offrir plus de services aux clients (accès ftp, ssh, ...), nous avons décidé (suite à une longue réflexion personnelle, puis d'équipe et quelques réunions) de mettre en place l'architecture suivante :

un client est défini par un utilisateur unix.

Simple à dire mais pas simple à mettre en place, car cela implique une restructuration complète du système.

Le fait de considérer un client comme un utilisateur système permet de lui offrir de façon sécurisée des services supplémentaires sans modification majeure du système. A titre d'exemple, Apache permet de définir des hôtes virtuels dans /home/*/www, ce qui implique que chaque utilisateur peut posséder son propre espace web dans un dossier ~/www et ce sans modification du fichier de configuration d'apache à chaque ajout de client.

6.3.2.2.2 Mise en place

Voici les points à effectuer pour cette mise en place :

- création d'un home directory spécifique pour les utilisateurs de type client
- mise en jail de ce home directory
- mise en place d'un système de gestion des quotas par utilisateur
- création d'un squelette typique pour la création d'utilisateur de type client
- modification des configurations des services associés (ssh, apache, ...)

6.3.2.2.3 Arborescence

Voici l'arborescence de base que je propose pour chaque utilisateur :

~/cgi-bin/	=> répertoire pouvant contenir des script cgi
~/log/	=> répertoire contenant tous les fichiers de log
auth.log	=> fichier de log des connexions
httpd-access.log	=> fichier de log apache
httpd-error.log	=> fichier de log apache
postgres.log	=> fichier de log de la base de données
~/stats/	=> répertoire contenant les stats du site de ce client
~/www/	=> racine de l'arborescence Web
~/ssh/	=> mandatory
.bash_history	=> mandatory
.bashrc	=> mandatory
.profile	=> mandatory

Bien sur cette arborescence est à étoffer.

7 Le mot de la fin

Voilà, j'espère avoir fait le tour de ce que je pouvais dire à mon successeur. Néanmoins, en cas de gros problème, pour une demande de conseils, ou tout simplement pour me donner des nouvelles de l'avancement des choses à Afide, voici le *HOWTO* pour me joindre :

tel : 06 13 44 72 23

e-mail : remi.fussien@uliniux.org

site : <http://www.uliniux.org> (c'est un petit wiki qui me sert de recueil de connaissance)

msn : jadorelesoleil@hotmail.com (je sais, c'est ridicule...)

/\ Mais attention, je ne suis pas un service hotline /

Il ne me reste plus qu'à souhaiter bon courage à l'équipe et bienvenu au nouvel admin.