

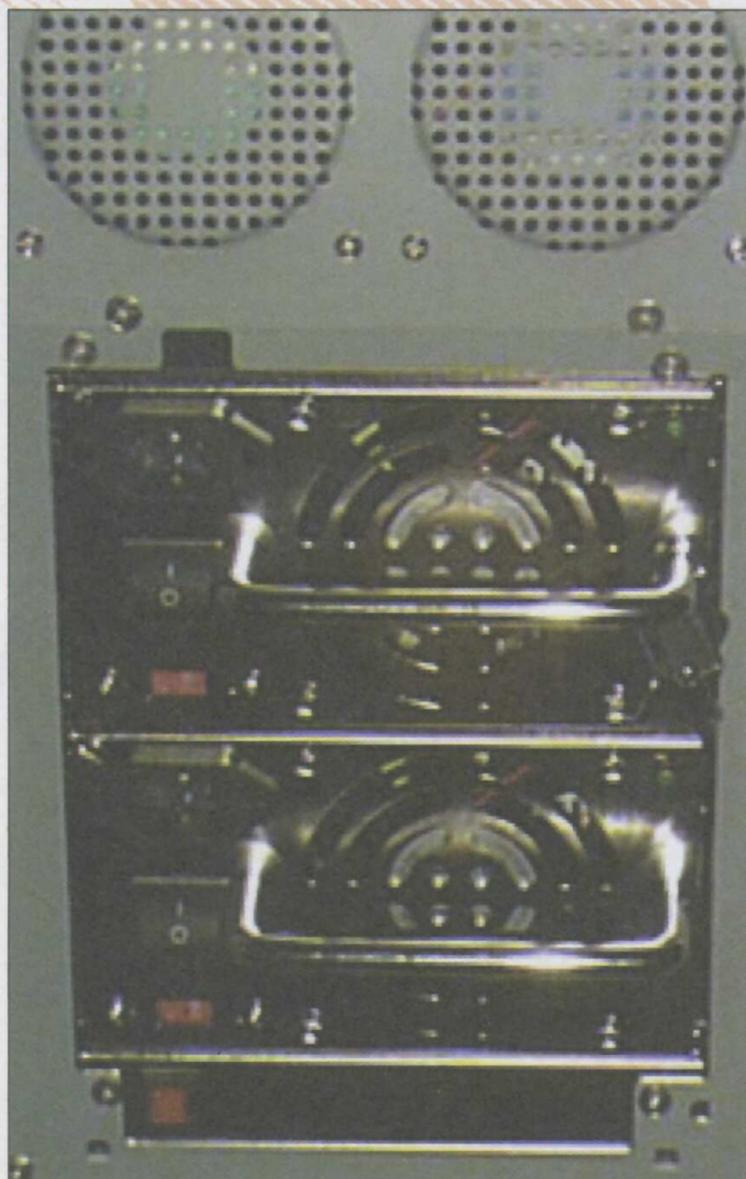
Devenir fournisseur d'accès à Internet

Découvrez le matériel et les logiciels nécessaires afin de proposer, pourquoi pas, les services des "grands" avec un budget "mini".

Le but de cet article n'est pas tant de vous asséner un cours magistral que de vous communiquer quelques notions issues d'une expérience pratique.

Le problème posé est le suivant : comment disposer

ou proposer des services Internet au-delà du simple hébergement de documents statiques ? Autrement dit, comment, avec un investissement réduit, fournir toute la panoplie de services qu'offrent les prestataires Internet, à savoir la gestion de serveurs Web "dynamiques" (utilisant divers automates non-envisageables en Java, JavaScript, ou tout autre langage dont les programmes sont exécutés du côté du navigateur), la gestion de serveurs Web sécurisés, notamment pour le commerce électronique et la gestion de serveurs DNS, FTP, SMTP, POP et IMAP, conçus spécifiquement pour le traitement du courrier électronique ?



Face arrière du serveur (le bouton-poussoir rouge permet de couper l'alarme sonore déclenchée en cas de panne d'une des alimentations).

Choisir sa connexion

Plusieurs solutions se présentent, dont les principales sont : la ligne louée, le "câble", le call-back RNIS et l'hébergement de machine.

La ligne louée équivaut à l'Eldorado pour tous ceux qui souhaitent s'assurer une présence durable sur Internet ; toutefois, sous nos latitudes, son accès reste réservé aux plus fortunés. Contrairement aux Etats-Unis, il faut compter en moyenne un coût mensuel de 5 000 francs H.T. pour une ligne 64 Kbits. Il faudra aussi ajouter un forfait presque toujours obligatoire pour l'installation et la configuration d'environ 15 000 francs. RMistes, s'abstenir.

Même si ces sommes peuvent encore vous sembler raisonnables, il faut garder à l'esprit que le débit est relativement faible et que, pour le démarrage d'une activité dont on ne peut que difficilement établir les revenus à court terme, un tel privilège occasionne des charges fixes importantes. En outre, il faut ne pas oublier que, si cette pratique se développe et exige de nouveaux locaux ou tout simplement un débit plus élevé, on vous demandera à nouveau des frais d'installation et de configuration comparables aux dépenses initiales, car elle nécessite le remplacement des équipements fournis (bien que depuis peu, la tendance est à la livraison d'équipements et de lignes légèrement surévalués par rapport à votre demande, pour justement ne pas vous contraindre à tout changer à la première demande d'augmentation de débit). Vient ensuite le câble. Disponible dans quelques villes de France et annoncé depuis longtemps à Paris, c'est l'exemple le plus flagrant de mauvaise "bonne affaire". Par expérience, il n'y a moyen de se prononcer que sur le prestataire qui prétend offrir un service digne de ce nom dans les villes de Strasbourg, Annecy et Le Mans. Non seulement, les techniciens ont une compétence "limitée", mais en plus, l'offre à 660 francs H.T. par mois avec le modem permettant de jouer le rôle de ser-

serveur net ?

veur se révèle désastreuse, en raison du nombre horriblement élevé de problèmes techniques de tous ordres (bug dans le modem câble, provoquant une perte régulière de connexion, bande passante en "sortie" ridicule, manque total de communication et de respect vis-à-vis des clients, mensonges et langue de bois pour masquer les défaillances sont le lot hebdomadaire, pour ne pas dire quotidien). Conclusion de ce calvaire de dix-huit mois : si parader deux minutes en téléchargement un fichier à la vitesse de 250 Ko/s en réception peut offrir un intérêt, il en va tout autrement quant il s'agit d'assurer un service fiable pendant plus de trois jours consécutifs.

Le call-back RNIS se trouve très rarement proposé par les FAI (Fournisseurs d'Accès Internet), car il est trop facilement l'objet de contestations au moment du règlement des factures, tant le fossé entre les estimations du client en coût de communication et la réalité peuvent se révéler importantes. En effet, dans le principe, votre serveur réside dans vos locaux et à chaque fois qu'il se voit sollicité, c'est le FAI faisant office de relais qui reçoit la requête et se connecte sur votre adaptateur RNIS (selon les modalités, il se trouve éventuellement en mesure de raccrocher pour être rappelé aussitôt depuis votre serveur). Enfin, la communication peut s'effectuer. On comprendra facilement que toute cette démarche est rapidement coûteuse et que les temps de connexion, souvent jugés trop importants par les internautes, s'allongent de manière rédhibitoire. Mais même si le temps de connexion avec un bon routeur RNIS dure 3 ou 4 secondes, plus d'un aura déjà été voir un autre site. Il s'agit donc d'une solution très spécialisée, que l'on réservera plutôt à des organismes voulant disposer d'une sorte d'Intranet étendu et qui peuvent trouver un intérêt à bénéficier du maillage qu'offrent les FAI, plutôt que d'établir régulièrement des communications longue distance.

Dernière idée évoquée et qui sera la seule développée ici : l'hébergement de machine.

Il correspond à un principe peu répandu, très certainement en raison d'une diminution de la liberté

d'action par rapport au serveur, que ce procédé occasionne. Il est pour beaucoup inconcevable de ne plus avoir, physiquement, de machine sous la main. La peur de se retrouver avec un serveur planté, que l'on ne peut bien évidemment pas rebooter à distance, constitue l'une des appréhensions les plus récurrentes. Toutefois, cette situation n'est pas dramatique, à condition d'utiliser un système fiable, tel qu'Unix.

Malgré tout, pour les paranoïaques chroniques, certains prestataires qui développent leur activité d'hébergement de machines proposent depuis peu à leurs clients un système, destiné à télécommander via le téléphone la prise électrique sur laquelle est branché l'ordinateur hébergé. Le principe se montre simple : vous composez le numéro de téléphone communiqué par le prestataire, suivi d'une combinaison, et l'alimentation est coupée puis établie.

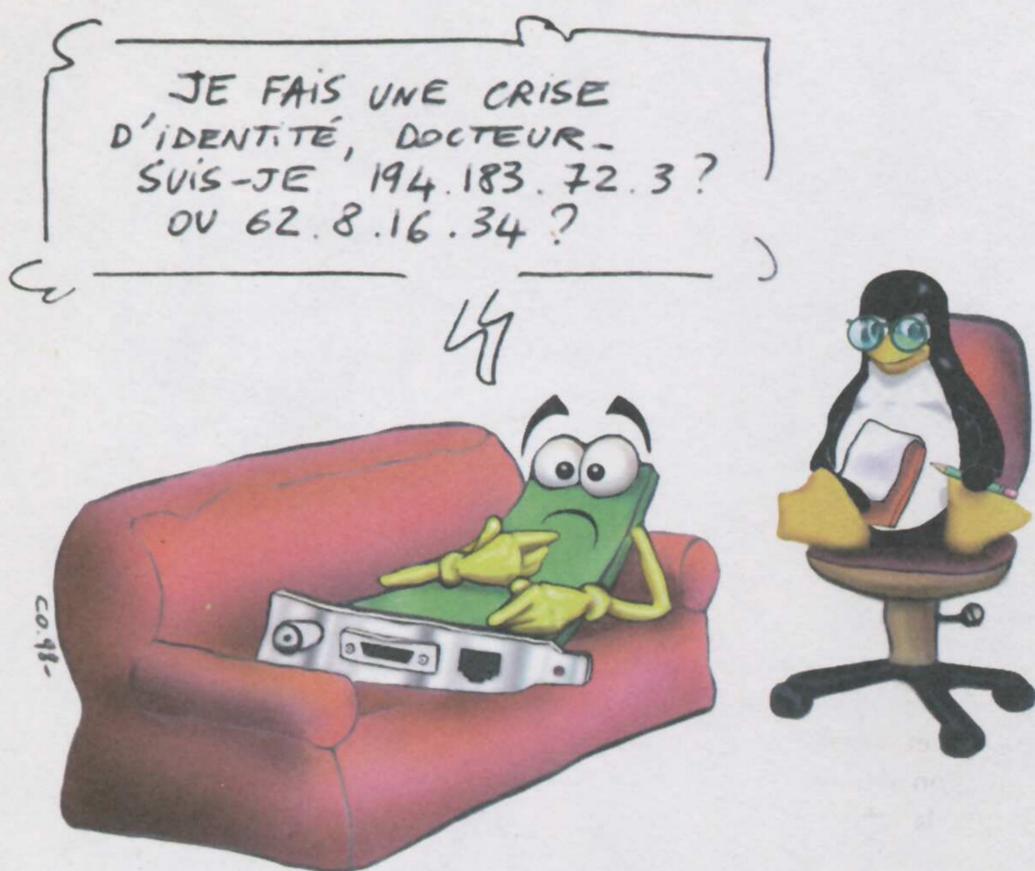
Arguments en faveur de l'hébergement de machine

Si on prend le cas d'un hébergeur correctement équipé, il revêtira l'aspect d'une salle informatique climatisée, dotée d'onduleurs (avec une bande passante importante partagée entre plusieurs opérateurs), ainsi que d'une connexion de secours, qui à elle seule peut être des dizaines de fois plus importante que la ligne 64 Kbits évoquée plus haut. En règle générale, vous êtes libre d'exploiter ce que vous voulez sur les machines que vous hébergez, et de la façon que vous le souhaitez. En cela, vous avez une marge de manœuvre, ni plus, ni moins importante qu'avec une ligne louée et des ordinateurs qui resteraient en vos locaux.

Ce type d'hébergement existe depuis plusieurs mois maintenant chez la plupart des FAI les plus importants, surtout chez ceux qui ne cherchent pas à s'implanter sur le marché le plus pourvu en abonnés, au forfait le moins cher. On peut citer



On espace les racks si possible pour répartir les sources de chaleur.



Les conséquences de l'abus d'adresses IP virtuelles.

entre autres Imaginet, Oléane, Internet Fr ou Magic OnLine.

Les prix évoluent en moyenne entre 2 000 et 5 000 francs H.T. par mois et par machine hébergée. Le forfait d'installation équivaut généralement au coût de location pour un mois, avec souvent des prix qui varient du simple au double, suivant que votre machine est prête pour un branchement immédiat ou qu'elle requiert au contraire une configuration de la part du FAI.

Les offres des FAI

Parmi les points qui différencient les offres de ce type, on trouve la méthode de calcul du volume de données échangées sur votre serveur (cumul des entrées et sorties). Certains simulent sur leur réseau interne une ligne louée dotée d'un certain débit, dont dépendra votre abonnement et sur laquelle est reliée votre ordinateur. D'autres procèdent par sondage pour établir une estimation du volume consommé. En fait, certains reconnaissent qu'ils ne sont pas en mesure d'établir un compte exact du volume de données échangées. Voilà probablement une des raisons qui incite bon nombre de ces fournisseurs d'accès à vous proposer des volumes importants dans le forfait de base en estimant que celui-ci ne sera jamais dépassé. Internet Fr offrait avant l'été un hébergement à 2 000 francs par machine avec un volume disponible de 1 Go par mois, et d'un jour à l'autre, ce volume est passé à 10 Go sans augmentation de prix.

Une autre différence très importante réside dans le coût, extrêmement fluctuant d'un hébergeur à l'autre, des adresses IP "prêtées". Celles-ci constituent une denrée indispensable pour qui veut proposer des sites Web personnalisés avec les noms de domaines de ses clients. En effet, tout site Web

que l'on souhaite rendre accessible avec son propre nom de domaine, par le biais d'une adresse du genre `www.client-final.com` plutôt que sous la bannière du prestataire comme dans `www.prestataire.net/client_final`, devra disposer de sa propre adresse IP, même si à terme cette contrainte se trouve vouée à disparaître, grâce à l'utilisation systématique de serveurs et de clients Web compatibles avec la norme HTTP/1.1. D'ici là, il est important pour ne pas dire indispensable de pouvoir disposer d'autant d'adresses IP que de sites Web associés à des noms de domaines distincts. Il ne s'agit ici que des serveurs Web, car pour les autres services, cette notion n'a pas forcément de sens. Sauf exception, la gestion de plusieurs domaines sur un seul serveur n'est pas prévue en standard dans le protocole FTP, mais des pis-aller existent. Pour SMTP, la situation diffère, car il se révèle parfaitement capable de s'acquitter de la gestion de plusieurs domaines sans nécessiter plus d'une adresse IP (même s'il est tout à fait possible d'employer en dépit du bon sens cette technique). Pour DNS, on se heurte à une absurdité de taille, car non seulement, il n'a nul besoin de plusieurs adresses IP, mais en plus, cette diversité est susceptible d'occasionner des ennuis colossaux, comme nous le verrons plus bas.

Autre aspect de cette question : il s'agit bien de prêt. En effet, il n'est pas inutile de savoir que depuis quelques temps, l'organisme responsable de l'attribution des adresses IP à travers le monde, IANA, ne vend plus d'adresses comme elle a pu le faire jusqu'à une certaine époque : celle, pas si lointaine, où l'évocation de pénurie d'adresses prêtait encore à sourire. Depuis lors, les plus importants FAI demandent humblement qu'on leur prête des adresses au fur et à mesure que leurs besoins, et ceux de leurs clients, augmentent. N'importe qui peut a priori en solliciter, mais il faut justifier d'un besoin minimal de 4096 adresses. Dans le cas contraire, vous vous adressez à votre FAI qui sert de relais, éventuellement remplacé par son propre FAI si lui-même est trop "petit". L'adresse IP fournie ne vous est donc pas vendue ; le prix qu'on vous en demande correspond à un compromis entre des frais administratifs et un coût que l'on qualifiera de "dissuasif". Celui-ci tente de vous faire réfléchir à deux fois avant de réclamer par avance une quantité astronomique d'adresses, ce qui explique que les FAI pratiquent des tarifs très contrastés.

Quelle plate-forme ?

Comme il a été dit précédemment, le coût dépend du nombre de machines.

Désormais, le but du jeu consiste donc, dans un premier temps, à trouver le bon système pour limiter au maximum le nombre d'ordinateurs à héberger. Dans un second temps,

il faudra ramener ledit nombre à un, puisque dès la deuxième machine, on revient dans des tranches de prix suffisamment élevées pour s'interroger sur l'à-propos d'une ligne louée.

Evidemment, si vous possédez déjà un serveur qui correspond parfaitement à vos besoins, vous pouvez sauter le passage suivant et vous rendre directement à la partie traitant des aspects logiciels.

Stations de travail

Si les stations de travail de marque Sun, HP, Digital, IBM ou Silicon offrent des qualités non négligeables, elles possèdent en revanche deux défauts dont le plus visible vient du prix d'achat et le plus pernicieux est le coût OU les contraintes en cas de maintenance. Même si ces constructeurs font régulièrement des opérations promotionnelles destinées à nous faire croire que l'on peut s'offrir une station à 25 000 francs, la vérité se réduit le plus souvent à proposer des machines, dont la configuration de base pour ce prix se révèle inadaptée à nos besoins ou incomplète. Machines diskless (sans disque dur), disque de 500 Mo seulement ou bien encore mémoire tout juste utile au fonctionnement d'un ZX81, constituent autant de facteurs handicapants. Et une fois équipé de cette station avec 500 Mo de disque et 16 Mo de RAM, aurez-vous encore les moyens d'acheter l'indispensable disque de 1 Go à 10 000 francs ou la barrette de 32 Mo à 4 000 francs ? Et ne vous y trompez pas : si la mémoire est bel et bien spécifique, le disque dur SCSI en revanche offre un modèle strictement identique à celui équipant votre compatible PC, à la différence près qu'il a reçu un autocollant magique aux couleurs du fabricant des stations de travail. Il existe bien des composants compatibles, mais les fournisseurs sont relativement peu nombreux et assez discrets, du fait certainement d'un marché plutôt restreint.

Pour enfoncer le clou, il convient de préciser que les coûts de maintenance de ces ordinateurs sont très élevés et que les pièces détachées, réservées à ceux qui veulent régler leurs problèmes tout seuls, n'ont pas un prix plus économique. Il est très important de savoir que si vous optez pour une maintenance personnelle, vous aurez peut-être à fournir une pièce défectueuse, comme une carte mère par exemple, pour pouvoir en acquérir une nouvelle et devrez attendre ensuite deux à trois semaines pour la recevoir. Ce qui, vous l'admettez, peut occasionner quelques gênes dans le cas d'un serveur censé fonctionner 24 h sur 24. Dans

ces conditions, le seul recours pour avoir des pièces détachées disponibles rapidement consiste à acheter un double du premier ordinateur.

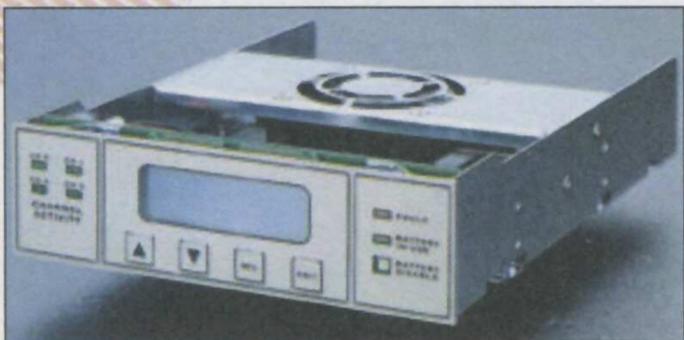
En revanche, il faut rester objectif, ces matériels sont bien souvent plus simples à mettre en œuvre que des PC, le nombre de combinaisons matérielles étant infiniment moins grand ; d'autre part, ils se montrent plus fiables sur le long terme. De plus, un logiciel stratégique comme *Netscape Enterprise Server* tourne essentiellement sur les Unix des stations de travail et beaucoup plus rarement sur les Unix existant dans le monde PC. On en reparlera plus loin au sujet des serveurs sécurisés et du commerce électronique.

La solution du PC

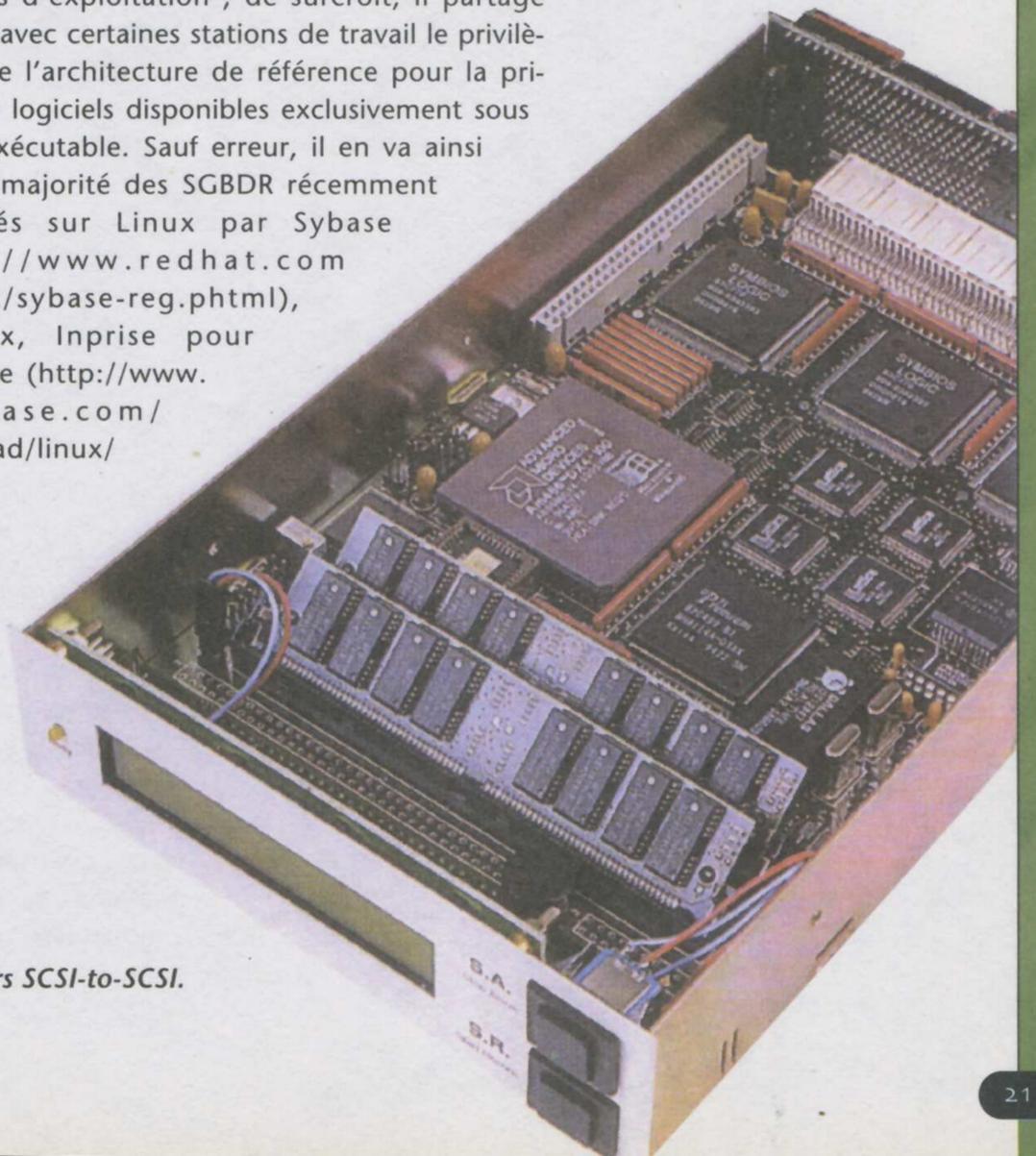
Bien évidemment, et heureusement, les PC sont là. Ici encore, on trouve deux écoles : les pro-constructeurs et les pro-dégriffés.

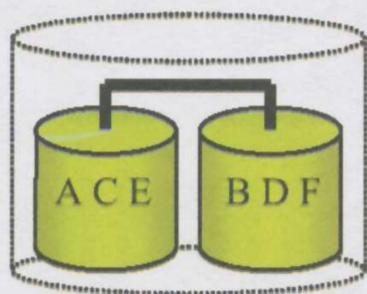
Afin de respecter le plus scrupuleusement possible le thème de cet article, nous nous focaliserons sur les PC que l'on monte soi-même sur le rebord de la table dans la cuisine. Le souci n'est pas exclusivement d'ordre pécuniaire, il est aussi de nature technique, car en assemblant soi-même sa machine, on en connaît a priori mieux les détails de tous les composants (modèle, révision, version du BIOS, fournisseur, etc.). Si vous cherchez, par exemple, à ne pas vous retrouver dans une situation désagréable comme celle évoquée dans le cadre de la maintenance des stations de travail, prenez garde à ne pas doter votre serveur d'une carte exceptionnelle s'il n'en existe qu'un fournisseur et que celui-ci est régulièrement en rupture de stock.

En ce qui concerne le logiciel, le compatible PC offre sans contexte le plus grand choix possible de systèmes d'exploitation ; de surcroît, il partage souvent avec certaines stations de travail le privilège d'être l'architecture de référence pour la primeur de logiciels disponibles exclusivement sous forme exécutable. Sauf erreur, il en va ainsi pour la majorité des SGBDR récemment proposés sur Linux par Sybase (<http://www.redhat.com/redhat/sybase-reg.phtml>), Informix, Inprise pour InterBase (<http://www.interbase.com/download/linux/>)

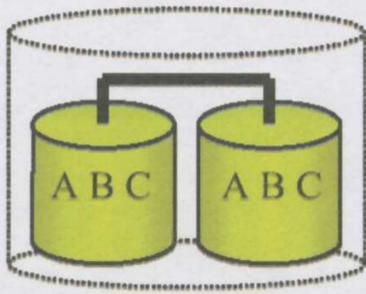


Deux modèles de boîtiers SCSI-to-SCSI.

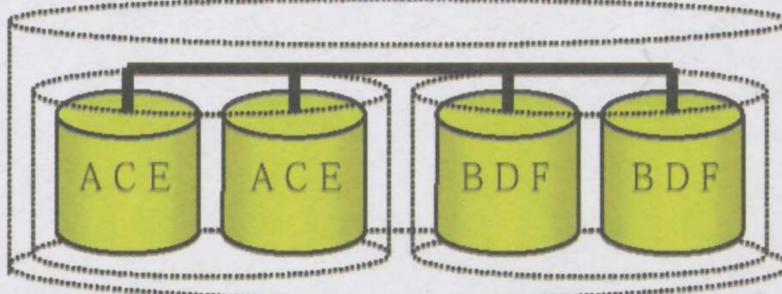




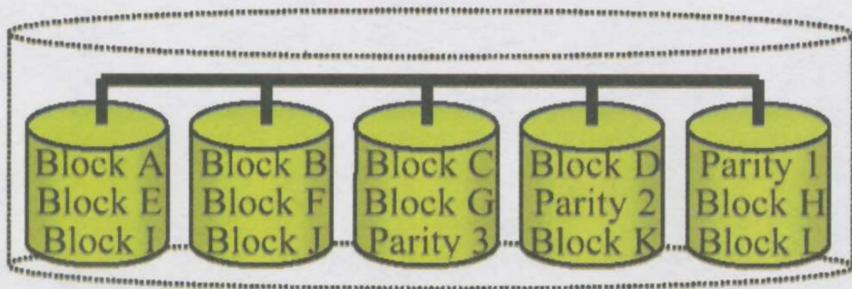
Raid niveau 0



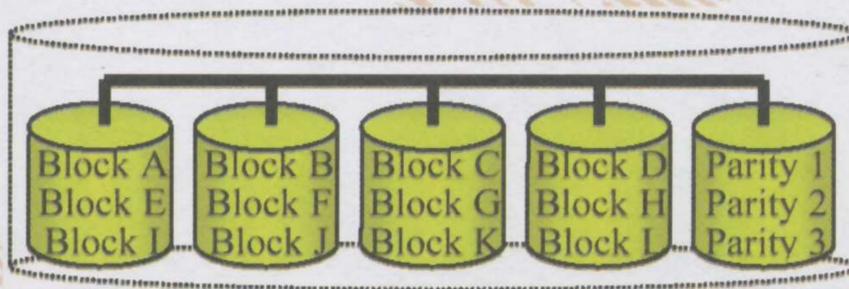
Raid niveau 1



RAID 10



RAID niveau 5



RAID niveau 4

Illustration des différents niveaux de RAID.

linux_info.html) ou encore Oracle (<http://technet.oracle.com/>). C'est un argument à prendre en considération pour le choix final.

Tolérance de pannes

Le but ne consiste pas ici à vous apprendre comment monter un PC ; par conséquent, nous nous attacherons uniquement aux moyens d'améliorer sa tolérance aux pannes.

Bien qu'aucune pièce ne se trouve à l'abri d'une panne dans un ordinateur, il en est trois qui se distinguent particulièrement, tout simplement à cause de leur composante mécanique : les disques durs, l'alimentation et enfin le ventilateur qui surmonte le radiateur, placé sur le processeur.

Pour ce dernier, la meilleure parade serait justement de ne pas avoir besoin de ventilateur. Cela s'avère envisageable en employant un radiateur de taille suffisante ; la disposition des composants variant sensiblement d'une configuration à l'autre, les fabricants de radiateurs en limitent l'encombrement aux dimensions du processeur. En outre, ils le complètent par un ventilateur qui, comme exprimé ci-dessus, fait partie des premières pièces à tomber en panne, provoquant ainsi le blocage dudit processeur. Dans ce cas, la plupart des constructeurs ont un avantage en équipant majoritairement leurs ordinateurs avec des radiateurs surdimensionnés, évitant ainsi les ventilateurs.

En ce qui concerne l'alimentation, la parade est du même ordre et porte le nom d'"alimentation redondante" ("Redundant Power Supply") ; pour bien faire, il demeure préférable que l'on puisse l'extraire à chaud ("hot-swap").

En raison de problèmes très compréhensibles d'encombrement, ce genre d'alimentation ne peut être montée que sur un nombre très restreint de boîtiers, bien souvent usinés dans cette optique. Et

même intégré dans son boîtier, ce type de matériel n'est que très rarement proposé à la vente en tant que pièce détachée aux clients finaux.

Remarque importante : ce ne sont pas deux alimentations indépendantes qui nécessiteraient des connecteurs et une électronique supplémentaires sur la carte mère, ainsi que sur tous les périphériques à alimenter. Il s'agit bien de deux alimentations qui ne délivrent l'énergie que sur un unique jeu de fils comme pour une alimentation simple, et dont la seule vocation est de fournir constamment du courant même si l'une d'elles tombe en panne. Faites attention à l'existence éventuelle de boîtiers n'acceptant pas le format ATX, car prévus pour des cartes mères spécifiques.

En dernier recours, vous pouvez aussi vous procurer une machine montée dans un tel boîtier chez quelques intégrateurs, qui présentent ces produits dans leurs publicités.

Les disques durs

Le cas du disque dur est plus compliqué, car les solutions sont très nombreuses et la fourchette de prix est fort large.

Cela peut aller de 150 francs H.T. du giga pour un simple disque IDE de 6,4 Go à plus de 4 000 francs H.T. le giga pour des solutions de haute fiabilité. Le choix dépend donc du budget, mais avant toute chose d'une bonne connaissance des multiples produits existants.

Le système RAID

Le RAID ("Redundant Arrays of Inexpensive Disks") étant la plus répandue des solutions proposées de nos jours, nous évoquerons trois des principales

façons de le mettre en œuvre. Mais avant cela, un bref rappel des différents niveaux de RAID couramment employés s'impose. Le niveau 0, qualifié de "striping", n'a rien à voir avec la sécurité. Il ne sert qu'à signaler au système d'exploitation que l'ensemble de disques durs (des volumes physiques) se résume désormais à une seule entité (notion de volume logique), de sorte que la capacité d'un filesystem peut dépasser celle du disque le plus grand et se retrouver ainsi à cheval sur deux disques ou plus. Le niveau 1, qualifié de "mirroring", permet, comme son nom le laisse deviner, d'avoir pour chaque disque employé un frère jumeau qui constamment le reflète de manière fidèle. Le RAID 1 est utilisable à partir de deux disques.

Il existe un niveau "composite", le RAID 0+1, parfois appelé RAID 10, qui ne s'envisage qu'à partir de quatre disques, puisque deux d'entre eux vont assurer le striping et les deux autres, servir de miroirs aux premiers. On saute les niveaux 2 et 3 pour arriver directement aux 4 et 5. Similaires dans leur principe, ils se distinguent principalement par la façon dont ils répartissent les données sur les disques et les tâches dans lesquelles il se révèlent les plus adaptés. Disons pour simplifier les choses que le RAID 4 se montre sans doute plus approprié pour l'acquisition de grandes quantités de données comme c'est le cas avec la télévision numérique par exemple, surtout qu'il est moins répandu que le RAID 5, ce qui nous épargne de fait un surcroît de réflexion. L'idée de base consiste à réserver l'équivalent de la capacité d'un des disques du groupe pour y entreposer le résultat de l'opération booléenne XOR (OU exclusif), appliquée aux données inscrites sur les autres disques du groupe. Pour cette raison, un groupe RAID de niveau 4 ou 5 se définit par un minimum de trois disques. L'avantage par rapport au niveau 1 est d'autant plus flagrant que le nombre de disques compris dans le groupe s'avère conséquent, car si en RAID 1, la moitié des disques se trouve consacrée à la sécurité, en RAID 4 ou 5, il n'y aura toujours qu'un unique disque dévolu à cette tâche (miracle de la table de vérité de l'opérateur logique XOR). Il existe plusieurs autres niveaux de RAID, mais nous ne nous y intéresserons pas ici. Le RAID 0, sous diverses appellations, étant disponible en standard ou en option sous forme logicielle pour plusieurs Unix (*Logical Volume Manager* sur HP-UX et AIX, *Driver Md* sur Linux, *Driver Ccd* sur FreeBSD, composant de *Solstice DiskSuite* sur Solaris) et ce niveau de RAID n'intervenant pas dans les considérations de sécurité, le sujet ne connaîtra pas plus ample développement.

Solution logicielle

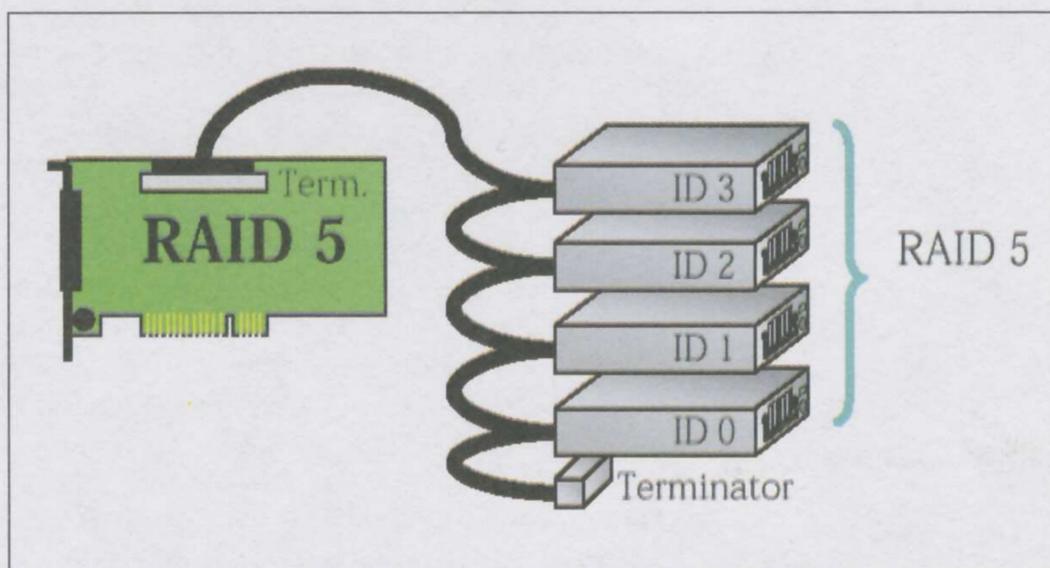
La parenthèse étant close, nous pouvons parler maintenant de nos trois méthodes pour disposer d'un système RAID. La première est purement logicielle. Linux, en particulier, bénéficie d'un "patch" pour ajouter les fonctions RAID niveaux 1, 4 et 5 au noyau (que vous retrouverez si vous le désirez dans <ftp://ftp.kernel.org/pub/linux/daemons/>

[raid/beta](ftp://ftp.kernel.org/pub/linux/daemons/raid/)), ainsi qu'une panoplie d'outils (ftp://ftp.kernel.org/pub/linux/daemons/raid). Mais, cette solution, aussi séduisante et économique soit-elle, pose deux problèmes. Le plus négligeable est l'absence de solution totalement satisfaisante pour arrêter une configuration employant ce patch, donnant ainsi lieu à un fsck à chaque démarrage. Plus embarrassant, le disque principal est parfois victime d'une faille, ce qui empêche le démarrage car, dans ce cas, il ne faut pas compter sur les autres disques, puisqu'un contrôleur IDE ou SCSI de base n'est pas prévu pour surmonter ce problème. On abandonne donc cette idée puisqu'elle ne se trouve guère adaptée dans le cas d'une machine hébergée.

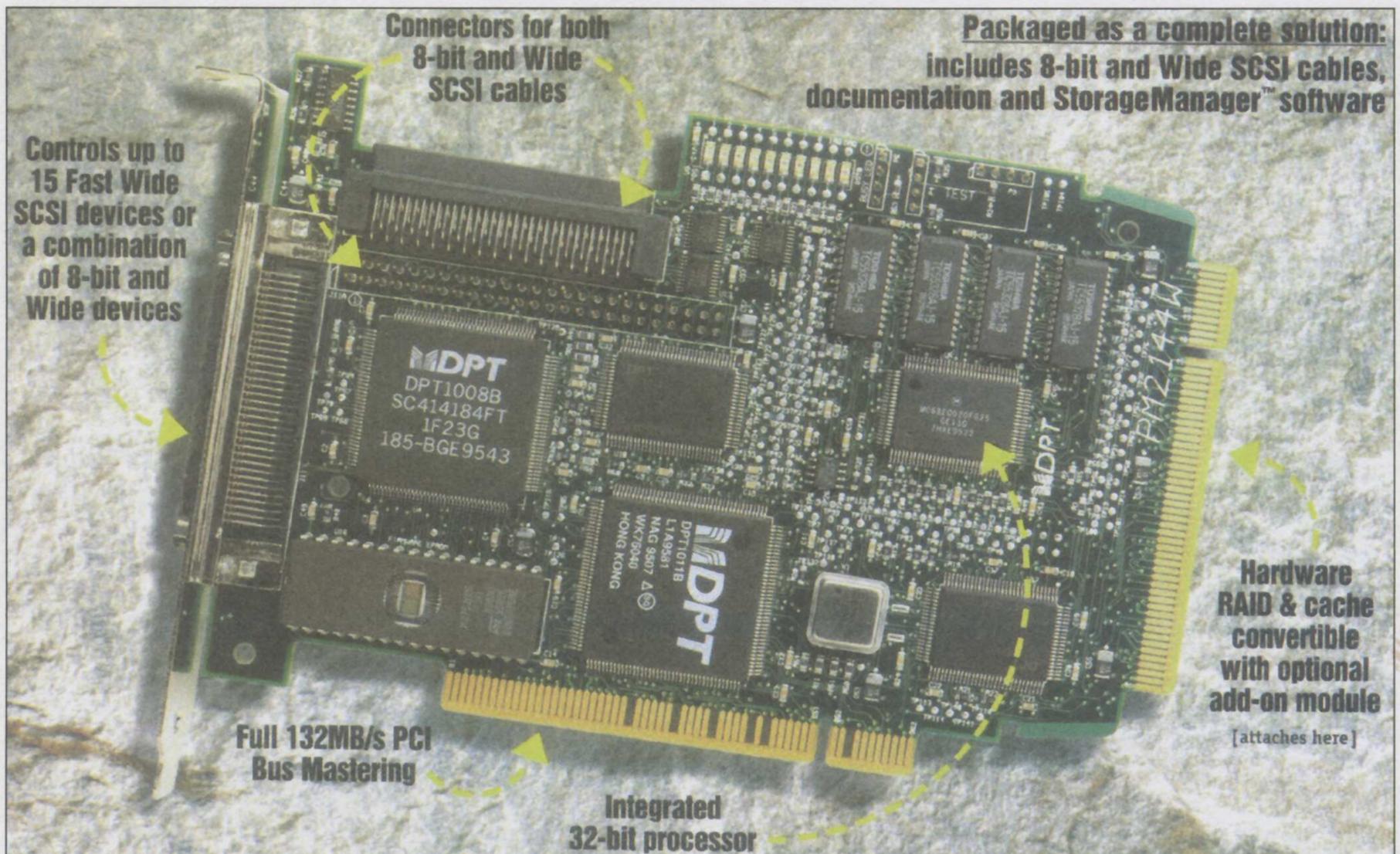
Solutions matérielles

Les deux autres méthodes sont donc matérielles. On distingue des contrôleurs SCSI qui autorisent, en standard ou en option, la gestion de certains modes RAID et des boîtiers spécialisés installés entre le contrôleur SCSI "classique" et les disques durs. Ce dernier procédé est connu sous le nom de SCSI-to-SCSI.

La carte SCSI avec RAID reste la solution la plus économique mais requiert un driver adapté. Le SCSI-to-SCSI en revanche, bien que plus cher, est a priori totalement indépendant du système d'exploitation. Les deux systèmes se révèlent donc parfaitement appropriés pour nos besoins, d'autant que les contrôleurs SCSI-to-SCSI sont le plus souvent disponibles sous forme de boîtiers au format 5"1/4, demi ou pleine hauteur, occupant donc l'espace traditionnellement réservé à un ou deux disques dans l'unité centrale ; ils comprennent généralement un afficheur LCD et quelques touches sur la façade. Pour la carte SCSI avec RAID, le choix qui s'impose comme une évidence est le contrôleur DPT modèle *PM2144W*, pour la simple raison qu'il bénéficie d'un driver développé sous l'œil attentif de DPT. De plus, un HOWTO lui est destiné et se consacre à ses capacités RAID, parce qu'il s'agit d'un matériel "relativement" peu onéreux et enfin parce qu'on peut le trouver assez facilement. En fait, la carte seule n'assume pas les fonctions RAID ; pour cela, il faut lui adjoindre un module *RC4040* qui devra obligatoirement être



Principe de connexion d'un RAID niveau 5.



Contrôleur SCSI. On remarque le large connecteur situé à droite et destiné à recevoir le module RAID matériel, doté de quatre supports pour la mémoire cache.

doté de mémoire cache non fournie, ECC ou simple EDO. Compte tenu des tarifs de la mémoire ECC, autant se contenter de quatre barrettes EDO SIMM 72 broches tout à fait standard de 16 Mo chacune, pour un total de 64 Mo de cache à un coût ridiculement bas, inférieur à 500 francs T.T.C. chez n'importe quel discounteur.

À noter qu'un conditionnement comprenant la carte PM2144W ET l'option RC4040 existe sous la référence PM2144WR (<http://www.dpt.com/pm2144wr.htm>). Les modèles 2044W et 2144UW fonctionnent tout aussi bien. Et très certainement aussi les autres cartes des familles 2X44 et 3334.

Une seconde marque, ICP Vortex (http://www.icp-vortex.com/prod/prod_e.html) citée dans l'HOWTO consacré à la DPT, revendique une compatibilité avec Linux, mais ces cartes, aussi bonnes soient-elles, ont un prix exorbitant.

Pour le SCSI-to-SCSI, il y a pléthore de produits. On trouve notamment les matériels CMD (<http://www.cmd.com/storage/products/info.cfm>) et Infortrend (<http://www.infortrend.com/products.htm> ou <http://www.infortrend.co.uk/>) ou la célèbre marque Mylex (<http://www.mylex.com/products/dac960erc/dac960sui.html>). En outre, il existe sur ce marché une "exception culturelle", Syred (<http://www.syred.com/>), constructeur français qui non seulement développe de très bons produits mais, une fois n'est pas coutume, les propose à des tarifs raisonnables, tout en offrant de surcroît un support digne de ce nom.

Un avantage indéniable, au moins dans l'état actuel des choses, d'un contrôleur SCSI-to-SCSI (cf les familles Prestige et Regency de chez Syred) est la présence d'un port série qu'il suffit de relier à l'un des connecteurs de l'unité centrale, afin de pouvoir communiquer à tout moment avec ce matériel. Cette manipulation donne également le privilège de scruter en permanence tout message d'erreur pour être rapidement averti de la défaillance d'un disque, en relayant l'information via le courrier électronique. Cette fonction devrait incomber au driver dans le cas de la carte DPT mais malheureusement, celui-ci ne la prend pas en charge.

Un autre atout offert par certains contrôleurs SCSI-to-SCSI comme sur le modèle DAC960 SXI de chez Mylex est la possibilité de lui adjoindre une carte fille qui améliore les performances en temps normal, mais surtout assure une redondance en cas de panne de la carte principale.

Un dernier avantage du SCSI-to-SCSI sur le driver de la carte DPT consiste à pouvoir à tout moment se renseigner sur l'état des disques, grâce à la liaison série, sans avoir l'obligation de relancer le système pour employer sous DOS le programme de gestion de la carte. Une telle particularité offre, à distance, un intérêt non négligeable. Avec une DPT, en cas de problème, ce sont les personnes hébergeant votre machine qui vont subir l'alarme sonore sans se trouver en mesure de l'interrompre avant votre intervention. Les boîtiers SCSI-to-SCSI

ont pour leur part un bouton facilement accessible.

La génération de contrôleurs SCSI-to-SCSI qui arrive en ce moment se met à l'heure Internet, en se voyant doté d'une Interface Ethernet, ce qui offre des perspectives très intéressantes.

Combien de disques au minimum et dans quelle configuration ?

Sans considérer l'espace jugé nécessaire, optez pour quatre disques dès le départ, de capacités identiques et, si possible, du même modèle. Avec quatre disques, vous pouvez vous offrir deux niveaux de sécurité. L'idée est de grouper trois disques en RAID 5 et de déclarer le dernier en "hot-spare". Dans cette situation, le contrôleur (carte SCSI ou boîtier SCSI-to-SCSI) utilisera le disque "hot-spare" pour remplacer tout élément défaillant du groupe RAID, ce qui constitue le premier niveau de sécurité. En outre, le RAID 5 lui-même vous assure un fonctionnement, même en cas de panne de l'un des disques du groupe, ce qui représente une deuxième sécurité. La capacité utile dans ce cas de figure est équivalente (si les disques ont la même taille) à deux disques. Il convient de noter que l'emploi d'un niveau RAID de type 0+1, même si la capacité utile est comparable, ne vous assure pas un tel degré de sécurité.

Autre matériel

En ce qui concerne le bureau ou le domicile, il vous faudra une configuration, si possible équivalente à celle hébergée, à l'exception du nombre de disques, de l'alimentation, de la quantité de mémoire ou de la fréquence du processeur, qui peuvent être moindres que sur le serveur.

L'idée se résume ainsi : avoir le privilège d'emprunter à cette machine des pièces non redondantes sur le serveur dans une situation d'urgence (processeur, carte réseau, barrette mémoire, etc.). Le principal reste que le serveur fonctionne, même avec des performances dégradées. Vous avez ensuite tout le temps voulu pour remplacer la pièce manquante. Sa fonction ne se limite pas à être un stock de pièces de rechange. Elle se révèle aussi et surtout essentielle pour la validation de vos expérimentations et de vos développements, ainsi que pour la compilation des sources que vous ne manquerez pas de récupérer régulièrement. La coupure franche imposée entre le serveur hébergé et le poste de développement facilite une plus grande rigueur dans les deux étapes "validation" puis "exploitation".

Pour ce qui a trait à la télémaintenance, comprenant entre autres l'envoi sur le serveur des nouveaux programmes, on préférera très nettement une connexion RNIS à une connexion RTC et puisqu'il existe désormais des routeurs Ethernet/RNIS à des prix très abordables, il n'y a pas de raison de

se priver. Certains modèles, dont le ZyXEL Prestige 100 (<http://www.zyxel.fr/>), sont dotés du protocole NAT, permettant à plusieurs machines (jusqu'à vingt) de partager un abonnement unique souscrit auprès de votre FAI. Un routeur a de plus l'énorme avantage de demeurer totalement indépendant des systèmes d'exploitation ; il se connecte généralement plus vite qu'un simple adaptateur RNIS, cette opération ne nécessitant que trois à quatre secondes en moyenne.

Si après cela, il vous reste encore quelques deniers, vous pourrez envisager de les investir dans des racks amovibles pour disques durs, mais pas ceux en plastique que l'on trouve à moins de 100 francs chez les discounters. Non ! Il s'agit de boîtiers tout en métal avec ventilateur, affichage de l'ID en clair par segments lumineux, modification de cet ID par le biais d'un commutateur facilement accessible et surtout, qui autorisent le "hot-swap" (l'échange du disque sans arrêt du système, grâce au contrôleur RAID). Vous les découvrirez chez Elan Systems et Additional DESIGN. Ils ne sont pas indispensables, mais vous faciliteront énormément tout travail de maintenance.

Pour conclure sur la configuration matérielle, un lecteur de CD-Rom IDE nous semble largement suffisant et permettra souvent plus facilement qu'avec un contrôleur SCSI de procéder à l'installation sans recourir à une disquette de démarrage.

Le logiciel

A propos de notre solution de serveur "économique", le choix du système d'exploitation se révèle assez simple ; nous adopterons donc, ce qui ne surprendra personne, Linux ou FreeBSD, qui offrent de nombreux avantages. Le premier offre la possibilité de compiler. En effet, la plupart des Unix "commerciaux" ne fournissent de base qu'un compilateur rudimentaire, si bien qu'il faut se contenter des logiciels du domaine public que des âmes charitables auront pris soin de compiler et de rendre disponibles sur le Net. Cela devient vite rébarbatif, lorsque l'exécutable ainsi compilé n'est compatible qu'avec une version du système légèrement plus récente que celle que vous possédez (typique avec HP-UX, par exemple). Autrement, il vous faudra encore sortir votre chéquier ; prenez garde, l'acquisition d'un environnement de développement peut atteindre un prix démesuré. De surcroît, alors que SunOS et dans une moindre mesure Solaris, jusqu'à une époque pas si lointaine, faisaient autorité en matière de nouveaux programmes, à l'heure actuelle, il est devenu rare que les Unix libres ne profitent pas très rapidement de la primeur de nouveaux développements. Tout du moins en ce qui concerne le domaine Internet, seul cas qui nous intéresse ici.

IP virtuelles

Le point suivant est capital et va conditionner considérablement le choix du système. Il s'agit de la capacité à gérer des adresses IP virtuelles, aussi appelées "aliases IP". Cette notion s'avère cruciale si l'on souhaite pouvoir héberger des sites Web

possédant leur propre nom de domaines. Dans ce dernier cas, cette propriété est baptisée *Multi-homing* par certains (Netscape par exemple), ou *Virtual Host* (apache) par d'autres.

Le principe ayant connu une démocratisation relativement tardive, il ne se trouve par conséquent disponible que dans les versions suffisamment récentes des divers systèmes. Cela explique aussi que sa mise en œuvre et la terminologie employée diffèrent autant d'un système à l'autre.

Un point particulier à vérifier concerne la capacité pour ces systèmes à accepter non seulement des adresses IP virtuelles mais de plus, des adresses aptes à se trouver dans des classes différentes, avec ce que cela implique dans la configuration des netmasks, du routage et de divers autres aspects. Cela ne signifie pas pour autant que le prestataire vous hébergeant cherchera à vous causer du tracas en vous fournissant des adresses de classes différentes quand vos besoins augmenteront ; simplement, il disposera des adresses que l'organisme d'attribution voudra bien lui confier.

Le routage justement. Il y a peu à dire, si ce n'est que les démons assurant un routage dynamique, tels que *gated*, *routed* ou autres, ne se voient guère appréciés. Il convient de les désactiver et de spécifier à la place l'adresse IP de la passerelle que vous communiquera la société assurant votre hébergement.

DNS

Si vous décidez de gérer vous-même votre ou vos DNS, il est un autre point particulier à prendre en considération par rapport à ces fameuses adresses IP virtuelles. Il s'agit d'une limitation, dont le symptôme traduit une erreur, concernant le nombre de fichiers ouverts par le démon serveur de noms (*named*). Le problème est que, par défaut, *named* va "écouter" chacune des adresses IP, réelles ET virtuelles, pour la réception des requêtes qui lui seront formulées. Ce faisant, il réclame un grand nombre de "handles", ce qui se révèle inexploitable, dès que le nombre d'adresses IP virtuelles devient trop important. La parade passe soit par l'ajout d'un patch "officieux" (<http://www.ultra.net/~jzp/andrews.patch.txt>) pour les versions de *named* inférieures à la 5, soit, et c'est de loin la solution la plus propre, par l'emploi du "nouveau" serveur de nom, *BIND* version 8.1.2 (sources à l'adresse <http://www.isc.org/bind.html>). Cette mouture récente offre en standard une directive (*listen-on*) permettant de spécifier explicitement l'adresse ou les adresses que le démon devra scruter. Le seul point noir actuel réside dans le manque substantiel de documentation (papier en particulier) au sujet de la nouvelle syntaxe adoptée, mais cet inconvénient se trouve contrebalancé par le fait que les fichiers de description des zones écrits à l'intention des versions 4.X de *named* ne requièrent pas de modification, pour être exploités par les versions 8.X. En fait, seul le fichier *named.boot*, renommé *named.conf*, nécessite une conversion ; en outre,

on se voit aidé dans cette tâche par un utilitaire écrit en Perl et inclus en standard (ceci est par ailleurs expliqué dans le fichier *DNS-HOWTO-7*).

Concernant la maintenance, le texte *DNS-HOWTO-6*, tout petit et fort intéressant, livre un script bien pratique pour l'actualisation du fichier de cache (celui qui donne les adresses des serveurs DNS de référence) et que l'on invoquera à l'aide d'une ligne dans le fichier */etc/crontab* ou */etc/crontab.local*, suivant le système utilisé. Bien que trouvé dans la documentation Linux, ce script profitera à tout le monde, moyennant une éventuelle et minime adaptation.

S'il vous appartient de choisir la séquence de lancement du serveur de noms et du serveur HTTP, veuillez scrupuleusement à conserver cet ordre : *named* PUIS, n'importe quand MAIS "plus tard", *httpd*. Il est clairement indiqué pour apache que les directives *ServerName*, bientôt disséminées par vos soins dans chaque description d'hôte virtuel (*Virtual Host*), requièrent au moment où elles sont lues l'accessibilité du nom auquel elles font référence, sous peine de dysfonctionnement.

Prenez garde aussi à ce que l'emploi d'un serveur de noms n'empêche pas obligatoirement celui du fichier */etc/hosts* ou même d'un serveur NIS. Pour l'essentiel des Unix récents, une notion de priorité se voit généralement mise en œuvre, par le biais de fichiers de configuration dont le plus courant est désormais */etc/nsswitch.conf*. Dans une moindre mesure, il peut exister un fichier */etc/host.conf*. Il faut aussi prêter particulièrement attention au contenu de */etc/resolv.conf*, en particulier sur HP-UX, où un paramétrage incorrect par rapport à la réalité de votre configuration est susceptible de rendre très délicat l'accès à votre environnement de travail sous sa forme graphique. Comme le mode texte ne pose pas de problème, une connexion via telnet peut aider à se tirer de cet éventuel écueil (problème évoqué dans le document <http://www.am.qub.ac.uk/users/j.pelan/DNSandVUE.html>).

En passant, prenez quelques minutes pour éditer le fichier */etc/inetd.conf* et y mettre en commentaire tous les programmes qui n'auront aucune raison d'être sollicités sur votre serveur.

SMTP

Pour le protocole SMTP, on n'hésitera pas à télécharger la toute dernière version sur le site <http://www.sendmail.org/>, ne serait-ce que pour faire bénéficier vos clients de ses options contre le spamming. Mais le point de *sendmail* qui nous intéresse plus particulièrement dans le cadre de cet article (faire beaucoup avec peu) concerne sa capacité à gérer plusieurs domaines. Cela devient possible essentiellement grâce à deux "features", *use_cw_file* et *virtusertable*. La première permet de notifier à *sendmail* l'ensemble des domaines qu'il aura en charge. La seconde joue un petit peu le rôle d'une table d'alias, en indiquant les destinataires finaux associés à chaque adresse de courrier électronique des différents domaines traités.

Software PARADISE

Matériel

Tower Infnitiv II.....	1250 F
Tower Infnitiv II, alim 230W.....	1490 F
Adaptateur écran VGA.....	85 F
Scandoubler interne A1200.....	659 F
Scandoubler A1200T/A4000.....	599 F
Scandoubler externe.....	825 F
— Lecteur de disks HD interne.....	559 F
Nappe IDE 2.5 > 2x3.5.....	125 F
Quadrupleur IDE.....	165 F
Disque dur IDE 3.5, 2.1 GO.....	989 F
Disque dur SCSI 3.5, 2 GO.....	1750 F
Lecteur cd-rom ATAPI x 32.....	420 F
Blizzard PPC 603e 160 Mhz, 68040/25 Mhz.....	2590 F
Cyberstorm PPC 604 180 Mhz, 68040/25Mhz et UW SCSI.....	5190 F
Carte ethernet Amiganet.....	1550 F
Carte son 16 bits Prelude.....	1890 F
16 mo simms 32 bits 60ns.....	190 F
32 mo simms 32 bits 60ns.....	315 F
Rom 3.1 A1200/A3000/A4000.....	349 F
— Souris et tapis Frog design.....	145 F
Joypad Honeybee.....	175 F
Digitaliseur audio + soft.....	350 F
Cable parnet 3 m + soft.....	99 F
CDR SCSI Teac x4 x12.....	2690 F

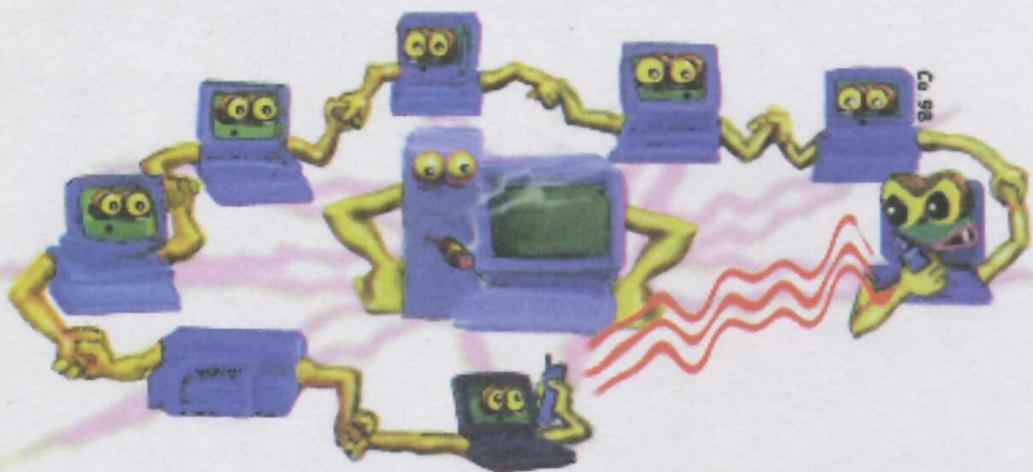
Logiciels

Art studio pro cd.....	260 F
Asimcdfs 3.9a VF.....	355 F
Burn It 2.12 DAO.....	690 F
Deluxe paint 5 cd.....	219 F
Elastic dreams cd.....	520 F
Fusion Mac emulator.....	690 F
Ibrowse 1.2.....	339 F
Miami 3.....	339 F
Network PC + cable //.....	229 F
Oxyron patcher.....	139 F
Pfs 2 cd.....	345 F
Scala MM400 cd.....	565 F
Turbocalc 5.1 cd VF.....	599 F
Turboprint 6.2.....	439 F
Ultimate blitz basic cd.....	219 F
Wordworth 7cd VF.....	490 F
Flying hight cd.....	199 F
Flying hight datas disk 2.....	85 F
Foundation cd.....	279 F
Genetic species cd.....	279 F
Mobile Warfare.....	125 F
Myst cd.....	375 F
On escapee cd.....	279 F
Quake cd.....	379 F
Samba world cup cd.....	273 F
Ultimate Sskidmarks cd.....	159 F
Virtual karting 2.....	179 F
Vulcan cd Bonanza.....	239 F
(Final Odyssey, Uropa 2, Strangers)	
Aminet 24, 25, 26 ou 27.....	85 F
— Aminet set 5 ou set 6.....	209 F
Amimes babes SE.....	179 F
Amiga format cd.....	49 F
Cartoon clipart.....	175 F
Gateway 3 (2cd).....	75 F
Golden demos.....	95 F
Magic publisher.....	179 F
Mods anthology.....	206 F
Scene Xplorer2.....	145 F
System booster.....	115 F
Workbench designer 2.....	120 F

frais de port VPC :
logiciels 35 F, matériel 80 F
tour, écran 100F

Micronik
Computer Service
Revendeur Officiel

Software Paradise - Le Capitole - 3, av. Armand Toulet - 64600 ANGLET - Tel 05 59 57 20 88 - Fax 05 59 57 20 87 - www.Sparadise.com



Interprétation "libre" de l'idée de réseau.

Plutôt qu'un long discours, voyons sur pièce.

Détail du fichier cf/MON_DOMAINE.mc :

```
OSTYPE (linux) dnl
DOMAIN (MON_DOMAINE) dnl
FEATURE (local_lmtp) dnl
FEATURE (smrsh) dnl
MAILER (local) dnl
MAILER (smtp) dnl
```

Les features local_lmtp et smrsh sont destinées à renforcer la sécurité.

Détail du fichier domain/MON_DOMAINE.m4 :

```
define(`confPRIVACY_FLAGS', `goaway,restrictmailq,restrictgrun') dnl
define(`confSMTP_LOGIN_MSG', `$j Sendmail;$b') dnl
FEATURE (access_db) dnl
FEATURE (rbl) dnl
define(`confAUTO_REBUILD', `True') dnl
FEATURE (nouucp) dnl
define(`confDOMAIN_NAME', `mon-domaine.fr') dnl
define(`SMTP_MAILER_MAX', 5000000) dnl
define(`confMAX_MESSAGE_SIZE', 5000000) dnl
FEATURE (use_cw_file) dnl
FEATURE (virtusertable) dnl
```

La première ligne limite l'accès aux données gérées par *sendmail* en interdisant par exemple l'emploi des commandes VRFY et EXPN, pour vérifier les adresses de courrier électronique maintenues sur votre serveur depuis l'extérieur. La seconde change le message d'accueil de *sendmail*, afin de faire disparaître les numéros de version ; ces informations peuvent devenir de redoutables armes dans les mains de ceux qui se tiennent au courant des failles spécifiques à chaque version de ce programme (du moins, c'est ce que l'on nous explique). Les deux suivantes préviennent en partie l'emploi de votre serveur comme relais pour les spammers, ainsi que la réception de courriers émis par des spammers recensés à votre intention ou à celle de vos clients.

Les lignes contenant une valeur numérique limitent la taille des courriers reçus ou relayés.

La directive *use_cw_file* demande à *sendmail* de

lire à chaque démarrage le fichier *sendmail.cw*, pour y trouver la liste des domaines qu'il doit gérer, les vôtres et ceux de vos clients, à raison d'un nom de domaine par ligne.

Enfin, la directive *virtusertable* permet de définir le routage du courrier pour chaque domaine ou pour chaque adresse. En voici un extrait :

```
@domaine-de-client.fr
%1@domaine-de-client.com
initiales@domaine-de-client.com      nom-
de-compte-pop-local
initiale-et-nom@domaine-de-client.com nom-
de-compte-pop-local
prenom-et-nom@domaine-de-client.com
nom-de-compte-pop-local
service@domaine-de-client.com
nom-de-compte-pop-local
groupe@domaine-de-client.com
alias-pointant-sur-plusieurs adresses
inconnu@domaine-de-client.com
error:ce quidam ne travaille pas chez nous
@domaine-de-client.com              nom-
de-compte-pop-local
@autre-domaine-de-client.com
nom-client@son-fai-local.fr
```

Ces différents exemples montrent la majorité des cas pris en compte par cette fonction de routage. Sur la première ligne, on indique de renvoyer sur le même utilisateur, mais sur le domaine "domaine-de-client.com", tous les courriers destinés au domaine "domaine-de-client.fr" : idéal pour les sociétés ayant enregistré leur identité sous plusieurs TLD (Top Level Domains). Les quatre lignes suivantes prouvent combien il est facile d'associer à une destination plusieurs variantes typographiques d'une même adresse ou de désigner une personne comme responsable d'un service (marketing@societe.fr, sav@societe.fr). L'avant-dernière définition, et sa position dans la liste ne doit pas précéder une autre ligne contenant dans sa partie gauche le même nom de domaine, permet de diriger sur un unique destinataire tous les courriers envoyés à des noms non-prévus, en cas d'erreur de frappe par exemple, ou adressés à des termes génériques (support, réclamation, plainte ne constituent que quelques exemples représentatifs de cette dernière catégorie). Cette définition n'est pas obligatoire mais tellement pratique. Imaginez parmi vos clients un travailleur indépendant ; il suffit de saisir cette seule ligne pour qu'il reçoive tous les courriers sans exception (info@client.fr, nom@client.fr, webmaster@client.fr, comptabilite@client.fr, etc.)

La distinction nom-de-compte-pop-local/nom-client@son-fai-local.fr met en évidence les deux cas de figure envisageables par rapport aux clients. Dans le premier, vous collectez leurs courriers et faites office de poste. Cela vous donne le moyen de leur offrir des boîtes personnalisées, alors que l'abonnement qu'ils auront souscrit avec leur FAI local ne leur permet le plus souvent que de posséder

une seule boîte, et en plus aux couleurs de celui-ci (pour ce qui est du nom de domaine). Avantage supplémentaire : la possibilité de leur proposer un accès *IMAP*, alors qu'un nombre infime de FAI supporte ce protocole pour l'instant. Le second cas est typiquement celui du travailleur indépendant qui souhaite recevoir sur la boîte fournie dans l'abonnement de son FAI l'ensemble de ses courriers, sans avoir l'obligation de configurer deux comptes *POP* dans son logiciel ; en outre, ce privilège a fait son apparition assez tardivement.

La directive *virtusertable* n'a pas pour vocation de remplacer le traditionnel fichier d'aliases ; elle possède ses propres prérogatives et les deux outils se complètent.

À titre d'exemple, voici simplement cinq lignes tirées d'un fichier "access" :

```
mon-domaine.fr      RELAY
un-client.com       RELAY

moneyhelp@mymail.com REJECT
mysexshow.com       REJECT
206.156.198.173    REJECT
```

Il permet juste de montrer que l'on a le droit de rejeter non seulement des courriers provenant d'une adresse particulière, mais aussi tous ceux émis à partir d'un site entier, que son nom soit connu ou non.

Bizarrement, les démons *POP3* et *IMAP* ne se trouvent pas fournis en standard, avec une quelconque distribution d'Unix. Si l'usage encore restreint d'*IMAP* peut l'expliquer, c'est nettement moins compréhensible pour *POP3* qui a depuis longtemps détrôné l'antique (mais pourtant très intéressant) *UUCP* chez les FAI. Pas de souci, vous les trouverez sur les sites <http://www.eudora.com/freeware/servers.html> (QPOPPER) et <http://www.imap.org/>, qui détaille les ressources disponibles dans ce domaine. Pour ce dernier, on vous orientera entre autres sur une version développée à l'Université de Washington (<http://www.washington.edu/imap/>) et qui devrait faire votre bonheur. À noter que les archives *IMAP* contiennent généralement les démons *POP2* et *POP3*. Il existe aussi un projet un peu plus spécifique, baptisé *Cyrus* (<http://andrew2.andrew.cmu.edu/cyrus/imapd/index.html>).

HTTP et SSL

En ce qui concerne HTTP, apache s'impose et ne mérite même pas que l'on s'y attarde... Sauf peut-être, pour ce qui a trait aux transactions sécurisées (<http://www.apache-ssl.org/>). Si tout le monde sait que le protocole SSL est le plus utilisé de nos jours pour sécuriser les sites, et en particulier, ceux qui font du commerce électronique, il s'avère en revanche plus délicat de connaître le moyen d'obtenir le certificat d'authentification, qui rassurera vos clients potentiels. Ce n'est en réalité pas très compliqué, mais malheureusement totalement illégal. En premier lieu, il convient de recenser les organismes qui délivrent les certificats. Pour cela,

se présente une idée très simple : vous prenez les deux navigateurs les plus répandus et dotés en standard d'une partie cliente SSL, *Netscape Communicator* et *Microsoft Explorer*. Normalement, on trouve Verisign/RSA et Thawte. Le premier est de loin le plus connu, certainement à cause de son origine américaine et de son travail en étroite collaboration avec Netscape et Network Solutions, la société qui gère le service InterNIC (<http://rs.inter-nic.net/>), lequel assure l'enregistrement des domaines pour les TLD "net", "edu", "org" et bien entendu "com".

Petite ombre au tableau, Verisign se refusait il y a encore quelques mois à vendre des certificats pour une utilisation avec apache. Cela peut sembler singulier, mais l'obtention d'un certificat dépend en partie du serveur HTTPS employé. Thawte, pour sa part, ne fait pas de discrimination. Cette compagnie sud-africaine a pour elle deux avantages complémentaires : ses certificats, nettement plus abordables que ceux délivrés par Verisign et surtout, sa politique de proximité, qui repose sur un réseau de revendeurs. Son représentant français est la société TBS-Internet (<http://www.fr.thawte.com/>). Un soin tout particulier a été apporté pour expliquer de façon claire avec des documents en français les démarches à mener, tant du point de vue technique qu'administratif, pour acquérir puis installer le certificat.

En ce qui concerne l'illégalité, elle touche apache et constitue l'une de nos fameuses "exceptions culturelles". Vous n'êtes pas sans savoir qu'un débat oppose depuis maintenant quelques années les défenseurs de l'utilisation libre du codage des données, essentiellement à des fins de commerce électronique, au Ministère de l'Intérieur, qui considère ces procédés comme de véritables armes de guerre. Sans rentrer dans la polémique, rappelons que seuls quelques rares pays se montrent aussi regardants quant à l'emploi de ces techniques. Malgré tout, trois ou quatre programmes de type serveur HTTPS sont depuis cette époque officiellement autorisés à exploiter sur le sol français le protocole SSL, avec toutefois des clefs limitées à 40 bits (on parle de 56 dans un avenir proche). Il y a en tout premier le serveur de Netscape, puis celui de Microsoft et enfin un serveur d'IBM pour OS/2 (sans qu'il existe de véritable certitude pour ce dernier). Ce qui reste malheureusement certain, c'est qu'apache ne se trouve pas sur la liste des heureux élus et qu'il y a fort à parier qu'il n'en fera pas partie de sitôt. Voilà pourquoi il pourrait s'avérer utile d'envisager d'autres Unix que Linux ou FreeBSD pour pouvoir exploiter un serveur Netscape, même si des rumeurs circulent depuis fort longtemps quant à la disponibilité future de leurs serveurs Web sur ces environnements. En attendant, vous avez le droit de feindre l'innocence et d'employer apache-ssl sur votre machine ; mais souvenez-vous, nul n'est censé ignorer la loi.

Paiement électronique

L'étape suivante consiste à traiter les commandes enregistrées sur votre site et payées par carte bancaire.

Vous pouvez recourir à la méthode manuelle en achetant ou en louant à votre banque un TPE/VAD (Terminal de Paiement Electronique/Vente A Distance) et en saisissant chaque règlement avec les informations communiquées par votre client. Cependant, un tel matériel coûte cher et vous oblige à tout valider à la main.

Un petit rappel utile en ce qui concerne les commissions prélevées sur chaque règlement s'impose : celles-ci ne sont pas fixées par un quelconque organisme central et se trouvent établies arbitrairement par chaque groupe bancaire. En clair, cela peut aller de 2,50 % au Crédit Agricole par exemple à 0,35 % à la Banque Populaire. Il convient de savoir que les taux sont négociables auprès de certaines banques et que ça l'est d'autant plus facilement que vous conditionnez l'ouverture d'un compte par rapport au contrat que l'on vous proposera. De même, les perceptions sur les règlements faits avec des cartes étrangères ne se trouvent pas soumises aux mêmes taux et cela a aussi des chances de jouer considérablement lors de la discussion. Par exemple, la commission de base de 2,50 % sur les paiements effectués avec des cartes étrangères a pu être ramenée à seulement 1 % sur un contrat signé au Crédit Mutuel.

Il faut souligner au sujet de ce dernier organisme qu'il apparaît probablement comme l'une des banques françaises les plus impliquées dans le développement Internet. Elle a été l'une des premières à proposer bon nombre de services en ligne et s'est lancée depuis peu dans une offre sérieuse, abordable et bien pensée, afin de permettre aux sociétés d'aborder sereinement le commerce électronique (http://www.creditmutuel.fr/centre_commercial/vendez_sur_internet.html). L'idée principale consiste à ne vous décharger QUE de la partie règlement avec un abonnement mensuel raisonnable et sans commission venant s'ajouter à la perception de base, au contraire d'autres offres qui vous prennent littéralement à la gorge. Une économie supplémentaire favorisée par ce service vient de ce qu'il vous épargne l'acquisition et la gestion d'un certificat SSL, puisque la responsabilité de ce type de problème lui incombe désormais.

Quelques sites utiles

● **Pour NEXTSTEP/OPENSTEP :**

<http://www.peanuts.org/>

<ftp://ftp.next.peak.org/pub/next/>

● **Pour Solaris x86 :**

http://ynp.dialup.access.net/scripts/ynpPageGen?sol25_attic

<http://sunsite.unc.edu/pub/packages/solaris/freeware/intel/2.6/>

http://sunsite.unc.edu/solaris/smc/solaris_2.5_list.html

● **Pour Irix :**

http://reality.sgi.com/billh_hampton/anonftp/index.html

<http://www.daveltd.com/bind-irix-port/>

● **Pour HP-UX :**

<http://gatekeep.cs.utah.edu/hppd/hpux/>

<http://hybrid.irfu.se/HP-UX/>

<http://hpwww.epfl.ch/HPUX/patch/catalog.html>

Apportons une information supplémentaire pour les particuliers entreprenants : contrairement à ce qui se pratique dans certains autres pays, les banques françaises ne semblent pas accepter l'idée qu'un particulier puisse percevoir des règlements à l'aide de cartes bancaires.

Pour finir

Certes, il existe un nombre croissant de programmes assurant une interface graphique pour la configuration de la plupart des fichiers décrits dans cet article, mais n'oubliez pas le postulat de base.

En effet, nous parlons d'un serveur hébergé et sur lequel il sera très rassurant de pouvoir intervenir à l'aide de, qui sait, votre Pilot ou votre Psion, doté de son modem et de son mini-programme d'émulation de terminal VT-100, alors que vous assistez au mariage de votre soeur, au fin fond du Périgord. De plus, certains de ces "jolies" programmes ont une fâcheuse tendance à modifier des fichiers automatiquement et à notre insu. Même si cela peut s'avérer judicieux, il demeure toujours désagréable de ne pas être informé des conséquences liées au simple lancement d'un programme de configuration.

Glissons tout de même un petit mot sur les documentations. A coup sûr, certains ouvrages sur les divers logiciels évoqués, en particulier sur *sendmail*, peuvent s'avérer utiles. Pour apache, il y a trop peu de valeur ajoutée par rapport aux documentations électroniques disponibles sur le site et surtout, les directives évoluent pour l'instant un peu trop rapidement, pour s'attacher à une documentation papier. En ce qui concerne les livres traitant de DNS et BIND, il faut sans aucun doute en posséder mais avant tout, la journée de formation qu'offre l'association AFNIC (anciennement NIC France) quand vous signez une convention avec eux pour pouvoir enregistrer les noms de domaines dans le TLD "fr", constitue une expérience nettement plus enrichissante. Bien que l'investissement fasse réfléchir et que la société vous hébergeant vous propose des conditions alléchantes pour l'enregistrement des domaines en "fr", il convient cependant de prendre en considération la réactivité que vous procure une convention avec l'AFNIC vis-à-vis de vos clients.

Revenons aux documentations, l'une des richesses de Linux, afin de préciser qu'une quantité impressionnante de textes rédigés et, pour un nombre croissant d'entre eux, traduits, est accessible dans bien des formats informatiques ou même sur papier (Linux Undercover, par exemple). Même les plus blasés d'entre nous peuvent y puiser régulièrement de nouvelles informations. Leur lecture représente une source constante d'enrichissement et de découvertes.

Si le survol de certaines des notions évoquées dans cet article vous semble trop sommaire, n'hésitez pas à nous en réclamer un développement.

Yannick Cadin -Yannick@kommando.com