

Sme-server : s'héberger sois même

Table des matières

1. Introduction.....	3
2. Choix du mode opératoire du serveur.....	4
3. Informations à lire avant de démarrer l'installation.....	6
4. Installation.....	7
5. Post-Installation.....	11
6. Premiers pas après l'installation.....	19
7. Premières manipulations impératives.....	22
8. Installation de programmes supplémentaires jugés indispensables.....	23
9. Description du server-manager.....	25
Collaboration.....	25
<i>Utilisateurs.....</i>	<i>25</i>
<i>Groupes.....</i>	<i>26</i>
<i>Quotas.....</i>	<i>27</i>
<i>Pseudonymes.....</i>	<i>27</i>
<i>i-bays.....</i>	<i>28</i>
Administration.....	29
<i>Sauvegarder ou restaurer.....</i>	<i>29</i>
<i>Créer une disquette de réinstallation.....</i>	<i>30</i>
<i>Visualiser les fichiers journaux.....</i>	<i>30</i>
<i>Analyse des fichiers du journal courrier.....</i>	<i>31</i>
<i>Redémarrer ou arrêter.....</i>	<i>31</i>
Sécurité.....	31
<i>Accès à distance.....</i>	<i>31</i>
<i>Réseaux locaux.....</i>	<i>32</i>
<i>Renvoi de port.....</i>	<i>32</i>
Divers.....	33
<i>Soutien technique et licences.....</i>	<i>33</i>
<i>Créer votre tout premier site Web.....</i>	<i>33</i>
Configuration.....	34
<i>Date et heure.....</i>	<i>34</i>
<i>Groupe de travail.....</i>	<i>35</i>
<i>Répertoire.....</i>	<i>35</i>
<i>Imprimantes.....</i>	<i>36</i>
<i>Noms d'hôte et adresses.....</i>	<i>36</i>
<i>Domaines.....</i>	<i>37</i>
<i>Courrier électronique.....</i>	<i>38</i>
<i>Vérifier la configuration.....</i>	<i>39</i>
10.Génération d'un certificat SSL CACERT (ancienne méthode).....	39
11.OPNvpn Bridge et PHPki.....	44
Installation.....	44
12.Exemple de création d'Ibay NPDS.....	44
13.Généralité quant à l'hébergement pour plusieurs personnes.....	48
14.Le mode passerelle et le réseau idéal.....	50

Création d'une machine de backup.....	50
<i>Machine sous Linux (backup de vos serveurs SME ou postes de travail Ubuntu)</i>	51
<i>Backup de machines sous windows</i>	52
Contrôle d'un onduleur MGE.....	54
Installer un serveur IRC.....	55
15. Quelques astuces utiles.....	56
Masquer le listing des fichiers dans les i-bays.....	56
Résoudre les noms d'hôte dans les logs.....	56
Personnaliser les messages d'erreur standards d'Apache.....	56
PHP Register Globals On ou OFF	59
Autoriser les scripts PHP à accéder à certains répertoires (important pour l'upload sous NPDS).....	59
Autoriser l'accès aux fichiers distants.....	60
Modifier la taille des fichiers pouvant être envoyés sur le serveur.....	60
Limiter la taille des courriels pouvant être envoyés.....	61
Ajouter un disque dur pour stocker une ou plusieurs i-bay(s).....	61
Réutiliser un disque dur contenant une ou plusieurs i-bay(s).....	64
Supprimer les alertes de rkhunter concernant l'accès SSH par root.....	65
Imagemagick.....	65
GANDI.....	66
<i>Allowoverride sur une ibay</i>	66
Allowoverride sur une ibay.....	66
Rewriting et .htaccess.....	67
InnoDB et Mysql (pour Dotclear).....	68
Configuration avancée du serveur FTP.....	68
16. Netographie.....	71

1. Introduction

Ce petit tutorial va tenter de vous expliquer en quoi consiste sme-server (7.4 actuellement) et en quoi il pourrait vous servir. J'ai tenté de faire un compendium de plusieurs sites et de plusieurs forums ainsi que des astuces qui me semblent importantes pour la bonne compréhension de tous.

Sme-server est un Os linux vous permettant de déployer rapidement un serveur d'hébergement sur une ancienne machine. Il est pourvu d'une interface web visible dans le réseau qui s'appelle le **server-manager** qui vous permet de configurer votre serveur (gestion de nom de domaine, ouverture de ports, création de dossiers hébergeant vos sites web, etc).

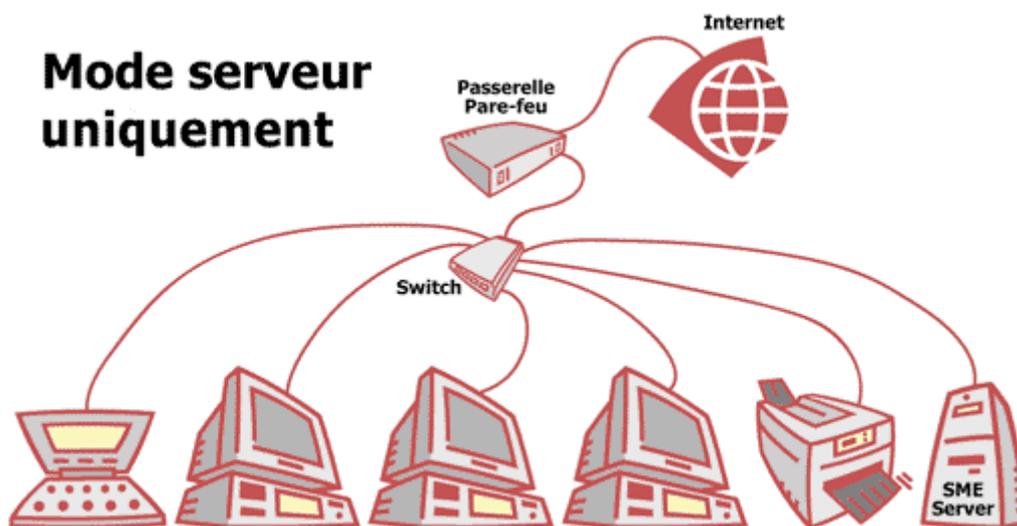
Pour télécharger sme-server => <http://sme-mirror.voxteno.com/releases/7/iso/i386/>

2. Choix du mode opératoire du serveur

La première question que vous devez vous poser est : ais-je besoin d'un serveur de développement ou d'un serveur qui peut gérer mon réseau et le protéger?

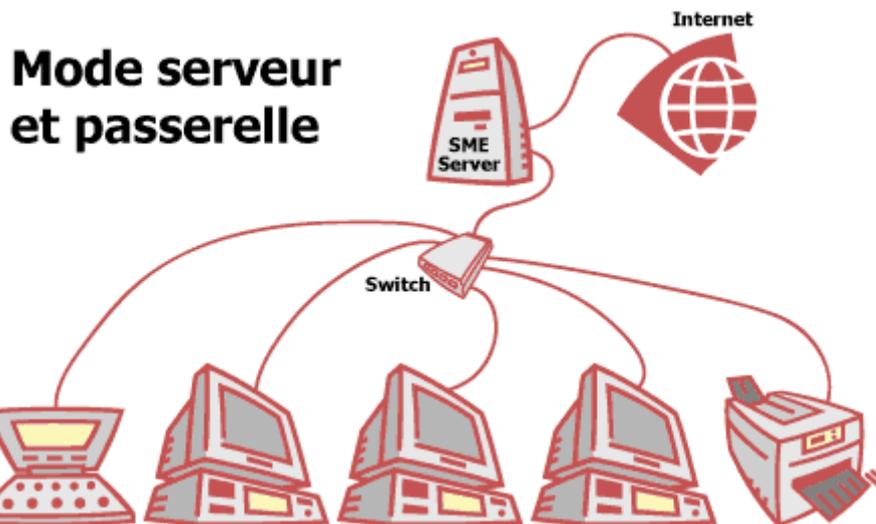
- Si vous souhaitez juste un serveur pour tester vos sites web et les héberger : mode **serveur only** = 1 seule carte réseau dans la machine.

Serveur uniquement : SME ne gère pas la connexion à Internet ; c'est généralement un autre système (passerelle et pare-feu) déjà en place qui en a la charge. Au niveau des fonctionnalités, SME ne gère donc pas la sécurité du réseau et n'offre alors que ses fonctions de serveur, à savoir serveur Web, serveur de courrier, partage de fichiers (par FTP, Samba ou via les [i-bays](#)), etc.



- Si vous souhaitez un serveur gérant votre réseau : **serveur et passerelle** = 2 cartes réseaux dans la machine.

Serveur et passerelle : SME gère la connexion globale à Internet ; c'est par lui que vont transiter toutes les données entre les ordinateurs de votre réseau local et Internet. Ainsi, en plus de partager une connexion unique à Internet pour toutes vos machines, SME va s'intercaler de façon transparente dans les transferts de données afin de protéger les accès à votre réseau local et de minimiser les risques d'intrusion. Les fonctionnalités offertes par SME sont alors les mêmes qu'en mode **serveur uniquement** et sont, pour la plupart, directement accessible depuis Internet.



- **Serveur privé et passerelle** : SME se comporte de la même façon que dans le mode **serveur et passerelle** sauf que l'ensemble des services Web et messagerie sont totalement invisibles depuis l'extérieur du réseau et que les règles de pare-feu sont plus restrictives pour assurer une sécurité accrue à votre réseau local.

En fonctionnement normal, SME peut être entièrement administré à distance à l'aide d'une interface Web appelée [gestionnaire du serveur](#) ou par SSH (accès sécurisé à la ligne de commande). Ainsi, l'accès physique au serveur devient quasi inutile et vous pourrez même débrancher le clavier et le moniteur (pensez à configurer le BIOS pour qu'il accepte de fonctionner sans ces composants).

N'oubliez pas que l'ordinateur sur lequel vous allez installer SME lui sera totalement dédié : tous les disques dur seront formatés et SME sera installé dessus. Cela signifie que tant que cet ordinateur est utilisé comme serveur, vous ne pouvez pas lancer d'autres systèmes d'exploitation ni l'utiliser pour autre chose.

Personnellement, je conseille le mode serveur et passerelle car votre réseau sera protégé par le firewall de votre serveur et vous pourrez y adjoindre des machines dédiées à certaines tâches (ou d'autres sme).

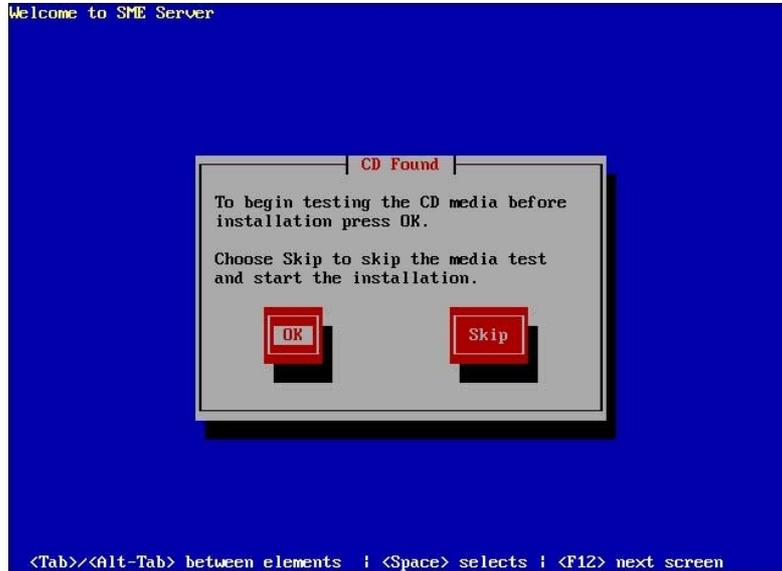
3. Informations à lire avant de démarrer l'installation

Afin de ne pas vous énervez avec sme-server lors de son installation, voici quelques trucs :

1. Sélectionnez bien le nombre de cartes réseaux qu'il vous faut en fonction du mode opératoire de votre serveur : sachez qu'il y'a toujours moyen de reconfigurer le serveur après son installation en utilisant le login « **admin** » à l'invitation de la console.
2. La première carte réseau qui se configure est l'interface pointant vers le réseau interne. Pour faire simple, votre sme est reliée à votre routeur, donc son adresse IP doit être dans le range IP de votre routeur et posséder le même subnetmask. Si vous décidez de publier vos site sur internet n'oubliez pas de faire pointer la **demilitared zone** de votre routeur vers l'adresse IP de la sme.
3. Pour le choix de l'IP de votre serveur choisissez un IP fixe!!!
4. Si vous choisissez le mode **serveur et passerelle**, la première à configurer sera l'interface interne (càd celle pointant vers votre réseau) et la seconde carte sera l'interface externe, càd celle que vous connecterez au routeur . Personnellement, je met l'interface interne à 10.0.0.1 avec un subnetmask de 255.0.0.0 alors que l'interface allant vers le routeur prend l'adressage IP et le subnetmask du routeur.
5. A la fin de l'installation on vous demande une adresse IP en cas de firewall => mettez y **l'adresse IP de votre routeur** (le routeur doit fournir le DHCP pour fournir les dns primaire et secondaire).
6. En ce qui concerne le choix du nom de domaine de votre serveur vous avez deux choix :
 1. Vous ne possédez pas de nom de domaine officiel et vous ne décidez pas d'en acheter un pour le moment => créez un compte gratuit sur dyndns.org. Assurez vous que votre routeur possède une méthode de rafraichissement de votre IP pour cet opérateur si vous ne possédez pas une IP fixe. Il existe néanmoins une contribution pour sme permettant de gérer cette opération.
 2. Vous désirez acquérir une dns payante car vous n'en avez pas => inscription chez dyndns.org avec achat d'une dns de votre choix et le pack de gestion de dns pour pouvoir créer des alias. La procédure de rafraichissement sera identique que pour une dns gratuite.
 3. Vous possédez une dns payante chez un registrar autre que dyndns.org => assurez-vous de posséder une IP fixe chez votre FAI et de faire pointer votre domaine vers votre IP fixe.

4. Installation

1. Gravez l'ISO sur un cd et démarrer la machine en sélectionnant le boot sur le cdrom.
2. On skip le test du media (cette opération peut être effectuée si l'on a un doute sur la gravure).



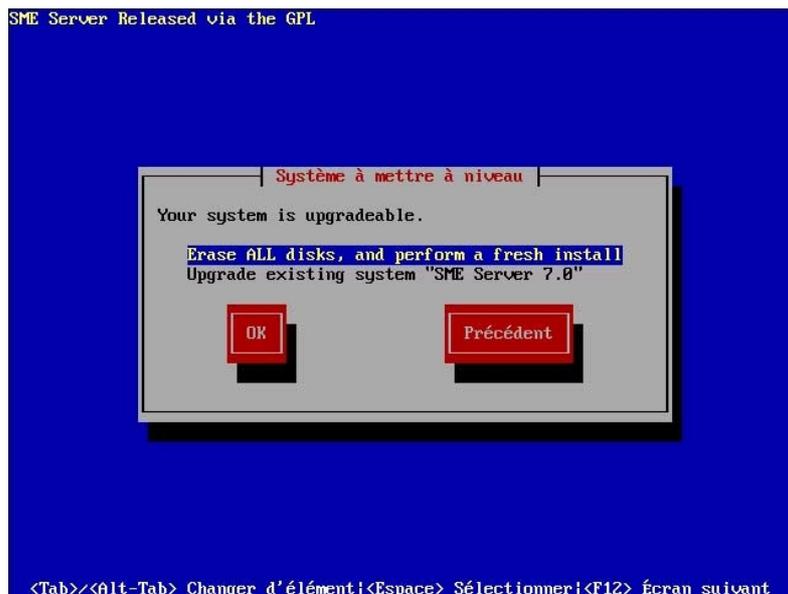
3. On sélectionne la langue d'installation : ici le Français.



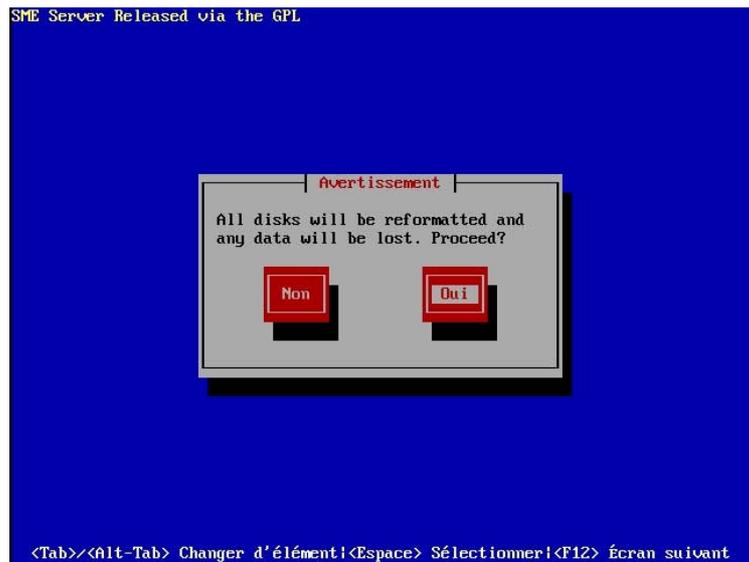
4. On sélectionne de la langue du clavier : ici clavier Français.



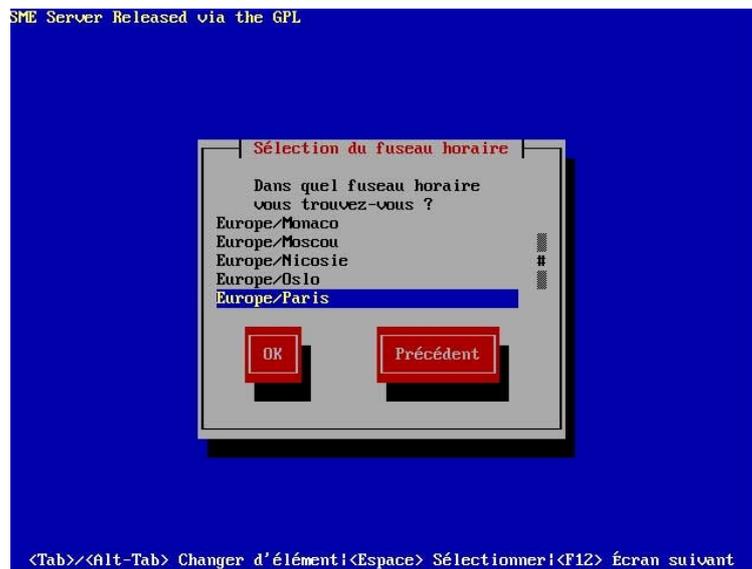
5. Dans le cas présent une installation de SME a été détectée, l'installateur propose l'upgrade. Nous choisissons de ne pas upgrader le système.



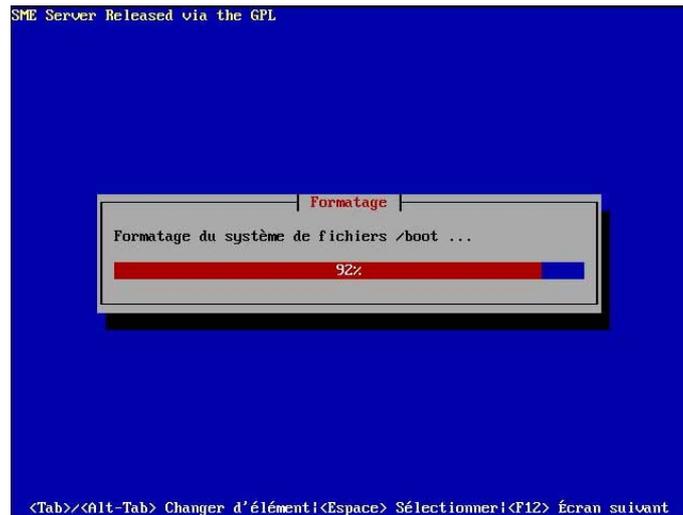
6. L'installateur prévient de la perte définitive des données situées sur le disque.



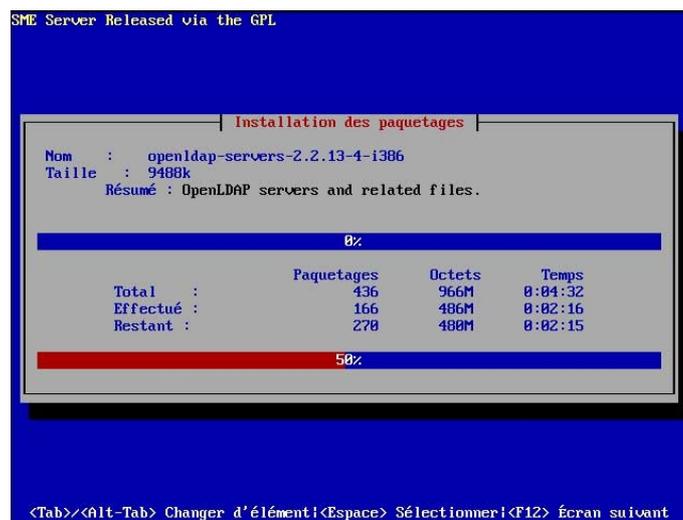
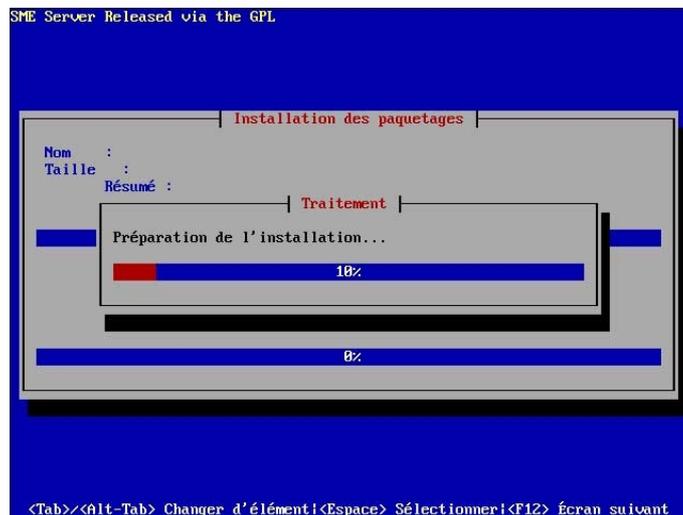
7. On sélectionne le fuseau horaire.



8. L'installateur lance le formatage des disques.



9. L'installation en elle même débute.

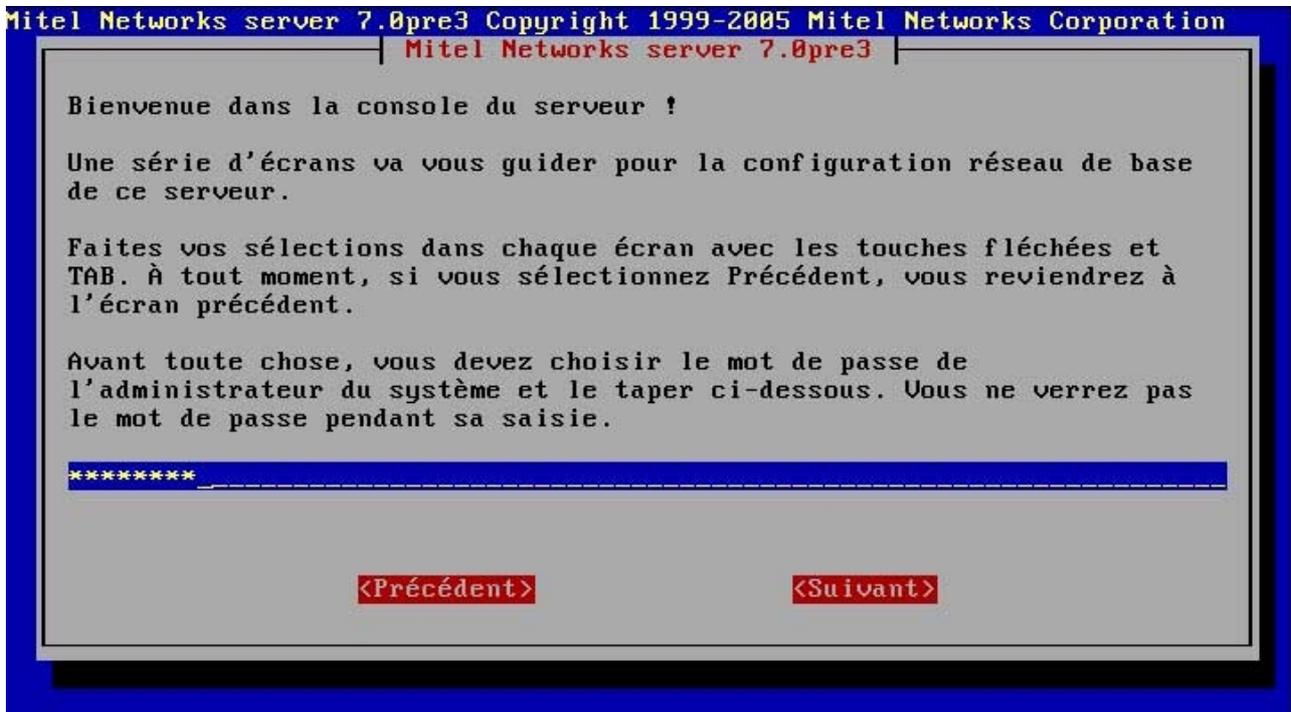


Fin de l'installation.

5. Post-Installation

ETAPE 1 :

Nous configurons le mot de passe du compte admin et nous le revalidons pour vérification.



Si le mot de passe était trop simple un écran apparaît.



ETAPE 2 :

On renseigne le nom de domaine de la machine (ici expertlinux.fr mais vous placez votre domaine gratuit ou payant ici).



ETAPE 3 :

On renseigne le nom de la machine.

Mitel Networks server 7.0pre3 Copyright 1999-2005 Mitel Networks Corporation

Nom du système

Veillez taper le nom du système de ce serveur.

Vous devriez sélectionner un nom de système unique pour chaque serveur.

Le nom du système doit commencer par une lettre et peut comprendre des lettres, chiffres et traits d'union.

tux

<Précédent> <Suivant>

ETAPE 4 :

On renseigne les paramètres de la carte réseau locale (vers votre réseau si en serveur et passerelle, je conseille l'adressage 10.0.0.1 / ou vers votre routeur si c'est en serveur only => attention, en serveur only, placer une adresse IP qui est dans le range de votre routeur) :

Mitel Networks server 7.0pre3 Copyright 1999-2005 Mitel Networks Corporation

Paramètres du réseau local

Veillez taper l'adresse IP locale de ce serveur.

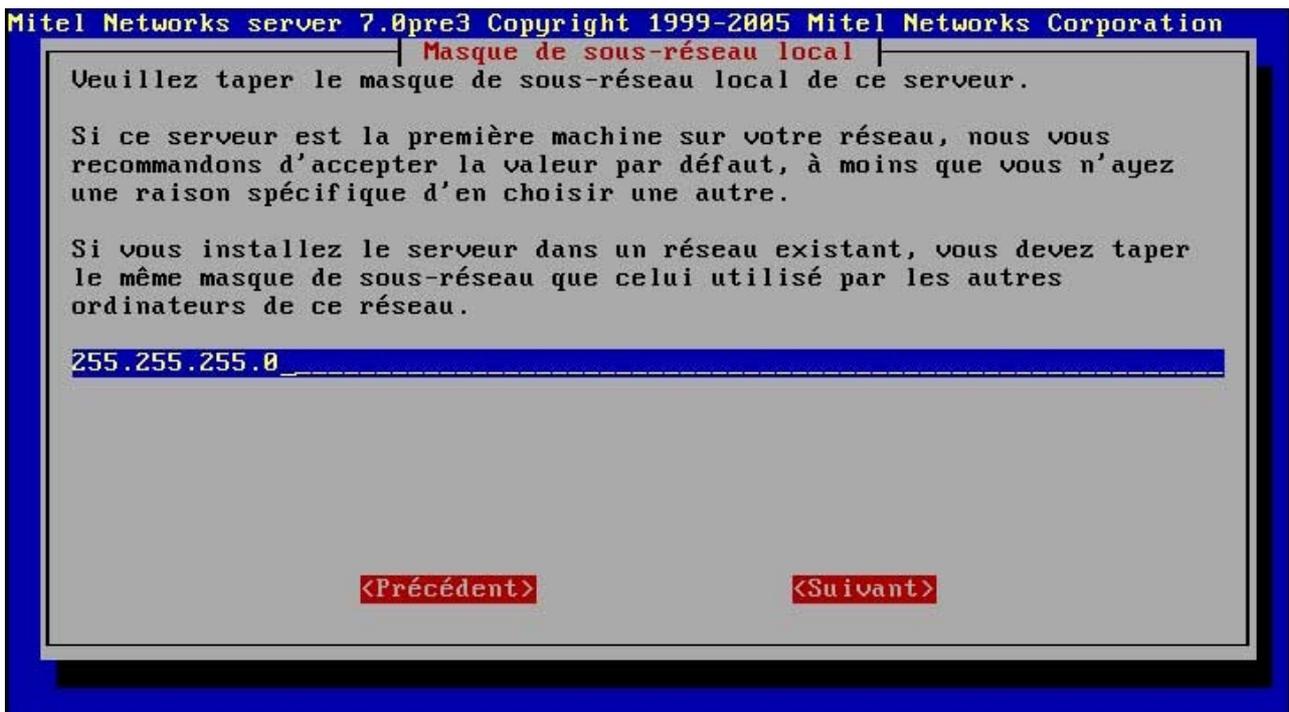
Si ce serveur est la première machine sur votre réseau, nous vous recommandons d'accepter la valeur par défaut, à moins que vous n'ayez une raison spécifique d'en choisir une autre.

Si vous installez ce serveur dans un réseau existant, vous devez choisir une adresse qui ne soit pas utilisée par un autre ordinateur de ce réseau.

10.45.25.75

<Précédent> <Suivant>

Et un subnetmask adapté à votre mode opératoire : en serveur only, celui de votre routeur et en serveur et passerelle je conseille 255.0.0.0



ETAPE 5 :

La machine n'étant pas destinée à effectuer les fonctions de routage nous sélectionnons serveur uniquement, vous pouvez toutefois sélectionner serveur et passerelle si vous voulez que votre serveur gère et protège votre réseau => vous tomberez alors sur la configuration de la seconde carte réseau.



ETAPE 6 :

On spécifie l'adresse IP du routeur (si le réseau dispose d'une connexion internet).

Mitel Networks server 7.0pre3 Copyright 1999-2005 Mitel Networks Corporation

Adresse IP de la passerelle

En mode serveur uniquement, ce serveur n'utilisera qu'une seule interface réseau connectée au réseau local. Si vous avez un pare-feu et que vous souhaitez utiliser ce serveur comme serveur de messagerie électronique/Web, consultez la documentation de ce pare-feu pour avoir les détails de sa configuration.

Veillez taper l'adresse IP de la passerelle que ce serveur doit utiliser pour accéder à Internet. Laissez le champ vide si vous n'avez pas d'accès à Internet.

10.45.25.254

<Précédent> **<Suivant>**

ETAPE 7 :

Si l'on souhaite laisser le serveur assurer les fonctions DHCP on laisse les paramètres par défaut.

Mitel Networks server 7.0pre3 Copyright 1999-2005 Mitel Networks Corporation

Configuration du serveur DHCP

Veillez indiquer si vous souhaitez que ce serveur fournisse un service DHCP à votre réseau local. Vous pourrez ainsi assigner automatiquement des adresses IP aux autres ordinateurs du réseau configurés en clients DHCP.

Nous vous recommandons de configurer tous vos postes clients avec DHCP.

Garder Paramètre actuel : Allumé

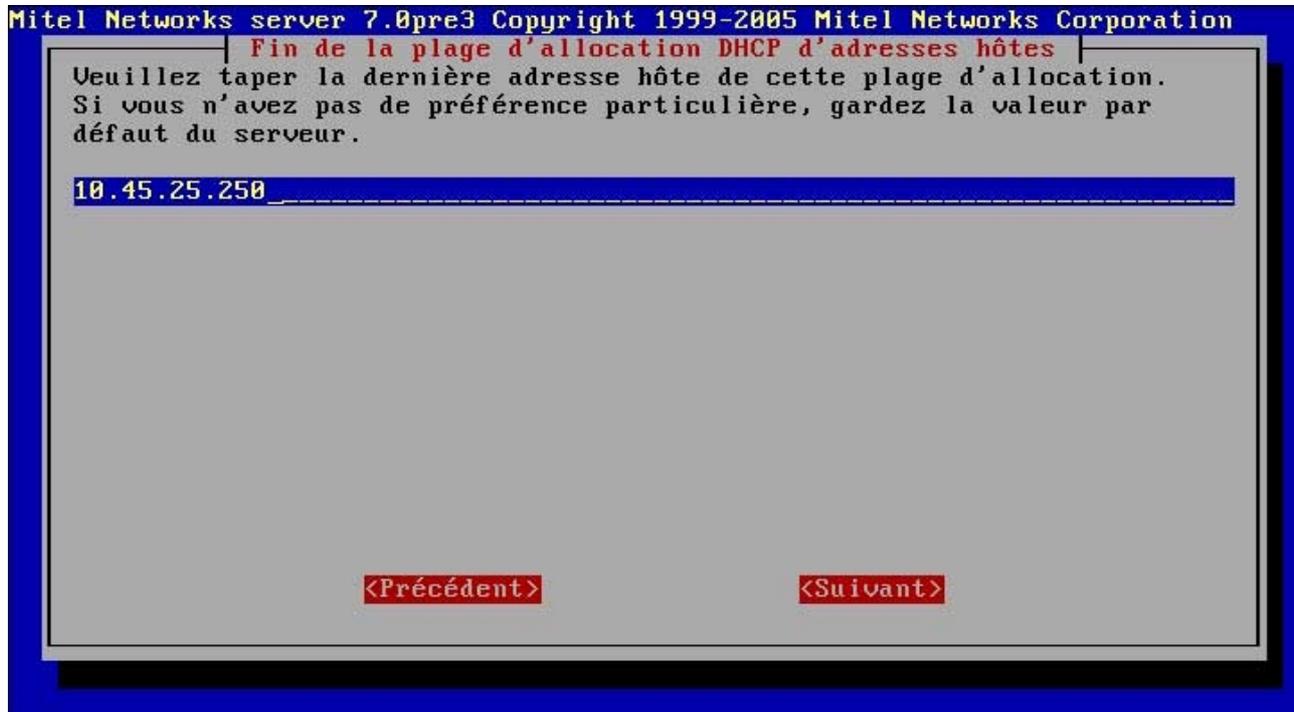
Allumé Fournit le service DHCP au réseau local
éteint Ne fournit pas de service DHCP au réseau local

<Précédent> **<Suivant>**

Ci dessous on configure le début de l'étendue DHCP, si vous avez choisis l'adressage 10.0.0.1 commencez à 10.0.0.2 :



Ci dessous on configure la fin de l'étendue DHCP (10.0.0.25 par exemple) :



ETAPE 8 :

Lors de la configuration du DNS on laisse la configuration libre, personnellement je met ici l'adresse IP de mon routeur sinon il n'ya pas d accès à internet de la part de la sme :



ETAPE 9 :

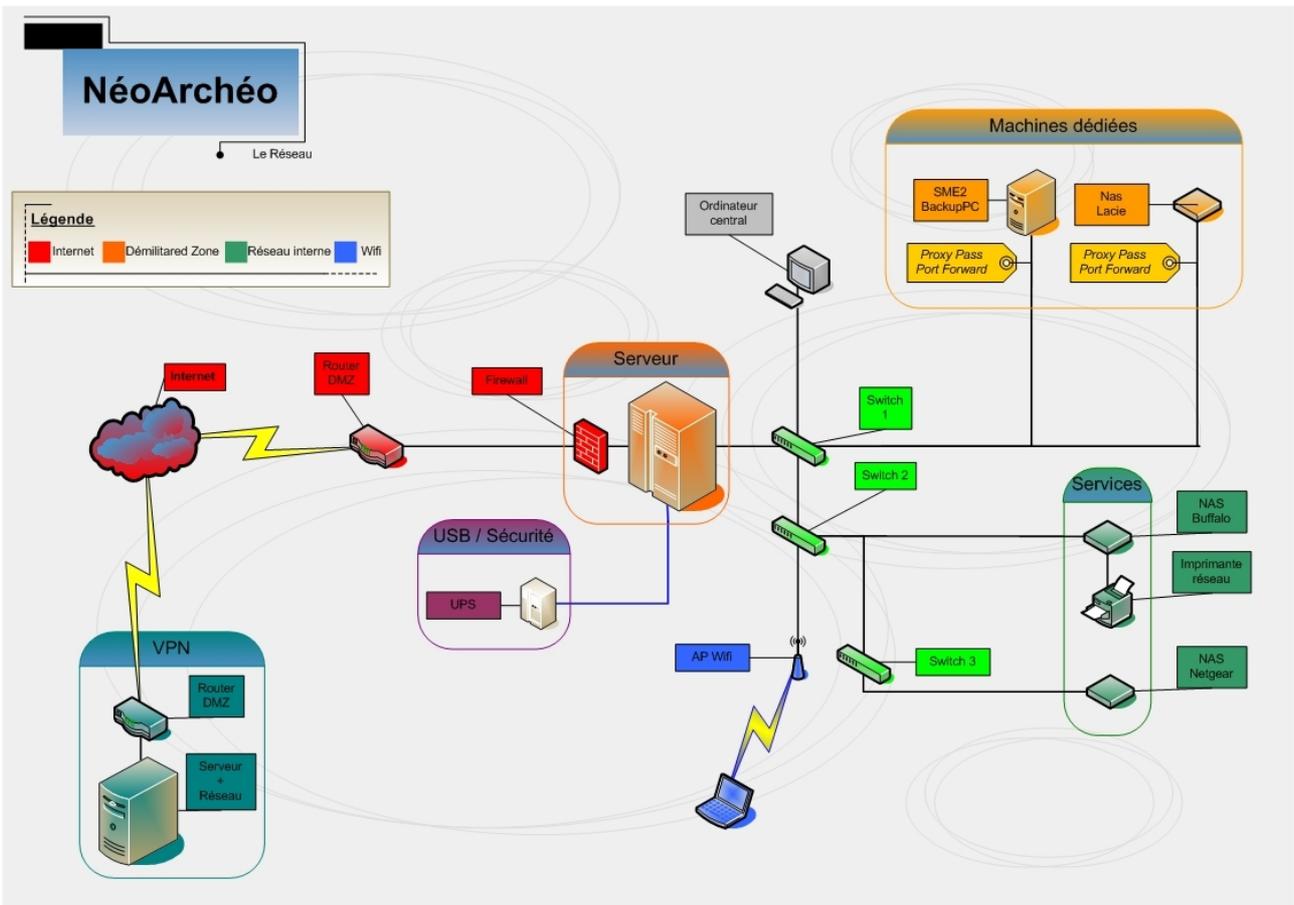
Fin de la post-installation.



Activation des paramètres de configuration

Veillez patienter pendant que vos paramètres de configuration sont activés...

Voilà par exemple d'un réseau en serveur et passerelle



6. Premiers pas après l'installation

L'installation terminée, nous allons configurer la SME Server 7.4

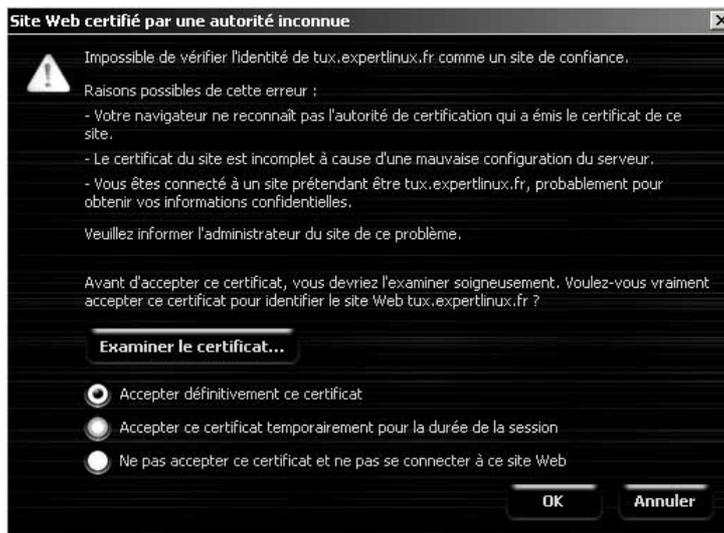
Lors du boot du serveur, ce dernier affiche les services actifs et ceux désactivés

```
Démarrage de nut : [ OFF ]
Démarrage de raidmonitor : [ OK ]
Démarrage de apmd : [ OK ]
Démarrage de oidentd : [ OK ]
Démarrage de masq : [ OK ]
Démarrage de network : [ OK ]
Démarrage de irqbalance : [ OK ]
Démarrage de crond : [ OK ]
Démarrage de acpid : [ OK ]
Démarrage de dhcpd : [ OFF ]
Démarrage de mysqld : [ OK ]
Démarrage de dnscache : [ OK ]
Démarrage de imap : [ OK ]
Démarrage de imaps : [ OK ]
Démarrage de ippm : [ OFF ]
Démarrage de pop3 : [ OK ]
Démarrage de pop3s : [ OK ]
Démarrage de tinydns : [ OK ]
Démarrage de diald : [ OFF ]
Démarrage de pppoe : [ OFF ]
Démarrage de lpd : [ OK ]
Démarrage de dhcpd : [ OK ]
Démarrage de smtp-auth-proxy : [ OFF ]
Démarrage de clamd : [ OK ]
Démarrage de freshclam : _
```

Pour pouvoir administrer le serveur a distance, il faut s'assurer que la configuration DNS du poste client pointe bien sur l'adresse IP du serveur.

L'accès à l'interface d'administration se fait par une connexion https et l'url d'administration serait : <https://10.0.0.1/server-manager/>

Lors de la première connexion un message d'alerte du au certificat de sécurité apparait (il suffit d'accepter)



Une demande d'authentification apparaît, il faut spécifier le login admin et le mot de passe associé.



A ce stade nous arrivons sur l'interface de configuration du serveur.



L'interface est divisée en 5 Sections.

- Collaboration
- Administration
- Sécurité
- Configuration
- Divers

Chacune de ces sections permet de définir certains paramètres du serveur.

7. Premières manipulations impératives

A ce stade votre sme devrait être bien configurée et vous devriez savoir atteindre le server-manager à l'aide de l'adresse <http://10.0.0.1/server-manager> (si 10.0.0.1 est l'adresse IP de votre sme). Installez le certificat de sécurité et vous tomberez sur la page de login.

Nous allons maintenant procéder par étape : ce qu'il faut faire en premier lieu et installer.

1. Mettez à jour votre sme à partir du server-manager (n'oubliez pas à la fin du téléchargement et de l'installation des paquets, qui peut durer un certain temps, de cliquer sur le bouton « *reconfigurer* »). Votre machine redémarre et se reconfigure d'elle même.
2. Téléchargez le programme putty (windows ou ubuntu) et allez ouvrir le port ssh dans le serveur manager dans la rubrique « *accès à distance* » définissez le degré d'accès. Vous pouvez aussi définir la politique d'accès au ftp.

The screenshot shows a configuration page with three main sections: PPTP, SSH, and FTP. Each section has a title, a brief description, and several configuration options with dropdown menus or input fields.

- Paramètres PPTP**: Includes a text box for "Nombre de connexions simultanées" set to 0.
- Gestion à distance**: Includes a text box for "Réseau" and "Masque de sous-réseau".
- Paramètres SSH**: Includes a dropdown for "Accès par terminal sécurisé (SSH)" set to "N'autoriser l'accès que depuis les réseaux locaux", and two "Oui" buttons for "Autoriser l'administrateur à se connecter au serveur par SSH" and "Autoriser l'authentification par SSH à l'aide de mots de passe standards".
- Paramètres FTP**: Includes a dropdown for "Accès FTP" set to "Aucun accès", and a dropdown for "Accès FTP par mot de passe" set to "N'autoriser l'authentification que depuis les réseaux locaux".

At the bottom right, there is an "Enregistrer" button.

3. Désormais vous pouvez accéder à la console de votre serveur via le programme putty (adresse de votre serveur sur le port 22 appelé ssh). => Pour reconfigurer votre serveur loggez vous avec le compte admin, pour installer des programme utilisez le compte root.
4. Pour joindre les répertoires de votre serveur utilisez winscp (Windows) ou gftp (Ubuntu) en connexion SFTP.

8. Installation de programmes supplémentaires jugés indispensables

Pour trouver des plugins (appelées contributions) vous devrez vous rendre sur <http://wiki.contribs.org>

Il existe beaucoup de contributions, vous pouvez en avoir la liste en tapant cette commande dans la console sous le compte root :

```
yum --disablerepo=* --enablerepo=smecontribs list available
```

Pour installer une contribution, exécuter cette commande :

```
yum --enablerepo=smecontribs install packagename
```

C'est à partir de ce site que nous allons trouver les lignes de code à insérer dans la console de votre serveur sous putty pour installer des programmes supplémentaires via la console avec le compte **root (attention pour ne pas être frustré si vous commencé avec linux => 1 ligne = 1 commande.)**:

1. **Phpmyadminmulti** => <http://wiki.contribs.org/Phpmyadminmulti/fr>

Vous aurez besoin de phpmyadmin pour gérer votre base de données mysql. Cette version est multi-utilisateur et vous offrira la possibilité de créer des comptes séparés pour les personnes dont vous hébergerez les sites.

2. **Service control** => http://wiki.contribs.org/Service_Control/fr

Vous permettra de désactiver des services de votre sme ou de changer leur port d'accès.

3. **Denyhost** => <http://wiki.contribs.org/Denyhosts/fr>

Cette contribution vous protégera contre les tentatives de piratage sur le port ssh (3 essais loupé et l'IP est bloquée deux semaines).

4. **System-monitor** => <http://wiki.contribs.org/SystemMonitor/fr>

System-monitor vous créera un panel générant des courbes statistiques de votre matériel (charge cpu / ram / mise en réseau / t°, ...).

5. **Disk usage** => <http://wiki.contribs.org/Diskusage>

Statistiques liées à vos disques durs (important pour connaître la place qu'il vous reste, l'état des disques durs, etc...)

6. **Remote user access** => http://wiki.contribs.org/FTP_Access_to_Ibays

Vous permet de définir le chemin d'accès (path d'arrivée) sur le ftp en fonction du nom des users et leur accès au bash en ssh.

7. **Awstats** => <http://wiki.contribs.org/AWStats>

Générateur de statistiques des domaines créés sur la machine : un must pour les statistiques de vos site.

8. **MYSQL5 et PHP5** => http://smeserver.pialasse.com/index.php/Php_5_mysql_5

Cette méthode vous permettra de faire passer votre sme à MYSQL5 et PHP5, je l'ai déjà fait plusieurs fois et ça fonctionne sans aucun problème. En revanche, notez que les mise à jour ne supportent pas nécessairement ce passage et que la rétroaction en V4 pour ces deux programmes expliquée en fin de tutorial ne fonctionne pas !!!! Afin de ne pas perdre d'informations, comme la méthode est plus ou moins périlleuse, nous vous enjoignons de vérifier à chaque mise à jour de sme-server, si la procédure n'a pas changé.

MYSQL5

Cette méthode vous permettra d'installer Mysql5 sans installer PHP5. Toutes les autres méthodes vous installent des paquets appartenant à php5 et risquant de vous obliger à faire la mise à jour vers php5 en même temps.

N'oubliez pas de faire un backup si vous utilisez déjà votre Sme pour des projets.

```
mysqldump -aec >mondump.sql
```

La commande de récupération des paquets nécessaires (**une seule ligne**):

```
yum update --enablerepo=centosplus mysql-server --exclude=php-pdo  
--exclude=php-common --exclude=php-mysql --exclude=perl-DBD-MYSQL  
--exclude=perl
```

Veillez à ce que les paquets suivants ne soient pas installés ou mis a jours:

1. php-pdo
2. php-common
3. php_mysql
4. perl-Filter
5. perl-Tim-Hires
6. perl
7. perl-DBD

Les fichiers Perl vous empêcheraient d'accéder au server-manager, et les fichiers php engendreraient un changement dans php.ini, vous empêchant de vous connecter à mysql via php tel qu'il est installé sur SME.

Exécutez ensuite les commandes suivantes (**lignes séparées sont des lignes uniques**):

```
cat /usr/share/mysql/mysql_fix_privilege_tables.sql | /usr/bin/mysql --force
--user=root --host=localhost -database=mysql

mysql -e "GRANT SELECT,INSERT,UPDATE,DELETE ON horde.* TO
'horde'@'localhost';FLUSH PRIVILEGES"

service mysqld stop;
service mysqld start;
/etc/rc.d/init.d/mysql.init restart;
```

La commande `cat /usr/share/mysql/mysql_fix_privilege_tables.sql...` peut donner quelques erreurs, ne vous en inquiétez pas.

PHP5

En fonction de votre version et de vos besoins, il vous faudra choisir une des méthodes suivantes mais avant tout, vous devez installer mysql5. Autant mysql 5 peut fonctionner avec php4, autant les paquets mysql 4 pour php5 ne sont pas disponibles.:

1. PHP 5 sur une SME 7.3

Activation du repository CentOs et téléchargement des paquets et validez à l'invitation par « Y » (**ligne unique**):

```
yum --enablerepo=centosplus install php.i386 php-pear-Net-Socket php-pear-Auth-
SASL php-pear-DB php-pear-HTTP php-pear-Mail php-pear-XML-Parser php-gd
```

Certaines erreurs peuvent apparaître pendant l'installation des paquets comme :

- *PHP Warning*
- *PHP Startup*
- *Unable to load dynamic library '/usr/lib/php/modules/mbstring.so' -*
/usr/lib/php/modules/mbstring.so
- *cannot open shared object file*
- *No such file or directory in Unknown on line 0*

Ces erreurs sont causées par le redémarrage de httpd sans la mise à jour des fichiers templatés par SME. On va corriger cela à la prochaine commande. Ne vous inquiétez pas, tout va

bien !

Redémarrez le service :

```
expand-template /etc/php.ini
expand-template /etc/httpd/conf/httpd.conf
service httpd-e-smith restart
```

Et vérifiez le bon fonctionnement de votre serveur. Php-domxml n'est logiquement plus nécessaire, le paquet php-xml installé en version 5 doit prendre le relais. Vérifiez tout de même le bon fonctionnement du webmail `https://SERVER/webmail`.

2. Update août 2009 pour la version 7.4

Lors de la mise à jour vers sme 7.4, si vous avez php5 d'installé, celle-ci refusera de se faire à cause d'un conflit php-domxml. Vous serez obligé de désinstaller php5 le temps de la mise à jour vers 7.4 (**lignes séparées sont des lignes uniques**) :

```
service httpd-e-smith stop

rpm -e --nodeps php-mysql php-imap php-pdo php-gd php-mbstring php-pear php-
ldap php-xml php php-cli

yum install php php-mysql php-imap php-domxml php-gd php-pear php-ldap php-
mbstring e-smith-horde

expand-template /etc/php.ini
expand-template /etc/httpd/conf/httpd.conf
service httpd-e-smith start
```

Mettez à jour votre Sme à l'aide de la commande « **yum update** » et rebootez avec « **signal-event post-upgrade; signal-event reboot** ». Réinstaller php5 avec les commandes suivantes (**attention, la première ligne est unique**) :

```
yum --enablerepo=centosplus install php.i386 php-pear-Net-Socket php-pear-Auth-
SASL php-pear-DB php-pear-HTTP php-pear-Mail php-pear-XML-Parser php-gd

expand-template /etc/php.ini
expand-template /etc/httpd/conf/httpd.conf
service httpd-e-smith restart
```

3. Mettre a jour php5 par la suite

Commande assez simple :

```
yum update php --enablerepo=centosplus
```

En cas d'un refus d'accès au server-manager, pas de panique, vous devrez utiliser les lignes suivantes (cela résulte d'un problème de transition de l'encodage ISO à UTF8 du serveur manager)

=> 1 ligne = 1 commande.

```
=> cd  
=> wget http://smeserver.pialasse.com/fichiers/convert_utf-8.sh  
=> chmod +x convert_utf-8.sh  
=> sh convert_utf-8.sh
```

Normalement, à partir de ce moment, vous possédez tout ce qu'il faut pour héberger des sites web. La suite de ce tutorial va vous donner quelques astuces pour bien configurer les ibays et certaines de leurs fonctions.

9. Description du server-manager

Collaboration

Utilisateurs

Cette page permet de créer, modifier ou supprimer des comptes utilisateur. A l'installation de SME, seul le compte **admin** est créé et seulement deux options sont accessibles pour gérer cet utilisateur :

- **Modifier** : permet d'indiquer les prénom et nom de l'administrateur ainsi que l'autorisation à se connecter au serveur depuis un client VPN (ce qui comprend également les accès en SFTP)
- **Réinitialiser le mot de passe** : permet, de la même façon qu'avec le [gestionnaire de mots de passe](#), de changer le mot de passe de l'utilisateur en question

Pour créer de nouveaux comptes utilisateur, il suffit de cliquer sur le bouton **Ajouter un utilisateur**. On arrive alors sur une page permettant d'indiquer les différentes informations concernant cet utilisateur :

- **Nom du compte** : c'est généralement le nom, le prénom, une contraction des deux. Ce nom servira à l'authentification de l'utilisateur sur le système et composera sa première adresse e-mail (par exemple *titi@votre_domaine.xxx*). Choisissez de préférence un nom court
- **Prénom** et **Nom** : servent principalement à définir les adresses e-mail secondaires (*prenom.nom@votre_domaine.xxx* et *prenom.nom@votre_domaine.xxx*, voir la section sur les [pseudonymes](#)). Un courriel envoyé à l'une de ces trois adresses ira donc toujours dans la même boîte aux lettres
- **Service, Société, Adresse, Ville et Téléphone** : ces informations ne sont utiles qu'à ceux qui exploiteront le serveur LDAP (serveur d'adresses) de SME. A noter que ces valeurs peuvent être modifiées de façon globale pour tous les utilisateurs dans la page sur l'[annuaire LDAP](#)
- **Délivrance des courriels** et **Adresse de renvoi** : vous permet de choisir le mode de réception des courriels : soit ils sont délivrés uniquement sur le serveur SME, soit il sont renvoyés automatiquement à une adresse que vous pouvez spécifier, ou bien encore envoyé sur les deux
- **Accès par client VPN** : permet de spécifier si l'utilisateur peut se connecter au serveur SME par l'intermédiaire d'un client VPN (si c'est en PPTP, voir la page sur les [accès à distance](#)). Si l'utilisateur doit pouvoir se connecter en SFTP au serveur, vous devez autoriser cette option
- **Membre des groupes** : si vous avez créé des [groupes](#), vous pouvez indiquer à quel(s) groupe(s) cet utilisateur appartient (très utile pour l'exploitation des [i-bays](#))

Une fois qu'un utilisateur standard est créé, son nom apparaît sur la page principale et son compte est verrouillé : vous devez impérativement lui indiquer un mot de passe pour qu'il soit utilisable. Ensuite, comme pour le compte admin, vous pouvez modifier les informations du compte et réinitialiser son mot de passe, mais vous avez alors deux options supplémentaires :

- **Verrouiller le compte** : permet de bloquer l'accès au compte. Les e-mail sont toujours stockés, mais tout accès aux données du serveur est interdit à l'utilisateur. Pour déverrouiller le compte, il suffira de réinitialiser son mot de passe

- **Supprimer** : supprime le compte ainsi que toutes les données de l'utilisateur en question

Groupes

A l'instar de la gestion des [utilisateurs](#), cette page permet de gérer les groupes d'utilisateurs. A l'installation, aucun groupe n'existe et vous devrez cliquer sur le bouton **Ajouter un groupe** pour en créer un. Apparaît alors une page où vous pourrez indiquer :

- **Nom du groupe** : comme pour les noms d'utilisateurs, je vous recommande d'utiliser ici un nom court mais explicite
- **Brève description / Alias de groupe Windows** : vous pouvez indiquer une description qui vous permettra d'identifier parfaitement le groupe. Dans le cas d'une utilisation de votre serveur dans un environnement type Windows, ce nom de groupe peut être utilisé comme un groupe standard Windows
- **Membres du groupe** : cochez tous les utilisateurs qui devront faire partie de ce groupe

Une fois le groupe créé, il apparaît sur la page principale et vous avez alors deux actions possibles pour le gérer :

- **Modifier** : permet de redéfinir la description et les membres faisant partie du groupe
- **Supprimer** : supprime tout simplement le groupe

Notez que si vous souhaitez envoyer un courriel à l'ensemble des membres d'un groupe, il vous suffit d'indiquer le nom du groupe comme destinataire du message (*nom_du_groupe@votre_domaine.xxx*) : le serveur SME se chargera de transmettre le message à chacun des utilisateurs.

Quotas

Un système de gestion des quotas permet de limiter l'espace disque utilisable par un utilisateur (cela comprend ses courriels, ses documents personnels ainsi que ceux qu'il place dans les [i-bays](#)).

Sur cette page, vous pouvez voir la liste des utilisateurs avec les limites que vous leur imposez (par défaut, il n'y en a pas), ainsi que l'espace qu'ils utilisent.

Pour modifier les quotas d'un utilisateur, vous devez cliquer sur le lien **Modifier** et vous arrivez sur une page où vous devez spécifier :

- **Limite avec période de grâce** : c'est la limite à partir de laquelle l'utilisateur est averti par courriel (chaque nuit) qu'il doit restreindre la quantité de données qu'il possède. Si ce quota est dépassé pendant sept jours consécutifs, il se retrouvera dans le cas ci-dessous
- **Limite absolue** : c'est la limite à partir de laquelle l'utilisateur ne peut plus rien stocker sur le serveur (un message d'erreur est renvoyé indiquant qu'il n'y a plus d'espace disponible sur le serveur) ni recevoir ses nouveaux courriels (ils ne seront disponibles que lorsque l'espace utilisé sera retombé sous cette limite absolue)

Si vous le souhaitez, vous pouvez ne définir qu'une seule limite et si vous voulez supprimer le quota, il suffit d'indiquer la valeur zéro pour les deux limites.

Pseudonymes

Comme nous l'avons aperçu dans la section [utilisateurs](#), SME gère des alias (ou pseudonymes) de compte pour la messagerie. A l'installation du serveur, cinq pseudonymes sont créés, pointant chacun vers un ou plusieurs utilisateurs :

- **everyone** : un message envoyé en interne à *everyone@votre_domaine.xxx* sera retransmis automatiquement à tous les utilisateurs définis sur le serveur
- **mailer-daemon** : un message envoyé à *mailer-daemon@votre_domaine.xxx* sera retransmis automatiquement à l'administrateur
- **postmaster** : un message envoyé à *postmaster@votre_domaine.xxx* sera retransmis automatiquement à l'administrateur
- **abuse** : un message envoyé à *abuse@votre_domaine.xxx* sera retransmis automatiquement à l'administrateur

Un autre pseudonyme peut être présent : il s'agit de **anonymous** qui pointe par défaut sur le compte de l'administrateur.

Pour chaque utilisateur, comme nous l'avons vu, deux pseudonymes sont automatiquement créés, de la forme *prenom.nom* et *prenom_nom*. Pour gérer ces pseudonymes, vous avez deux options :

- **Modifier** : permet de modifier l'utilisateur ou le groupe vers lequel va pointer le pseudonyme
- **Supprimer** : supprime tout simplement le pseudonyme

Enfin, pour créer un nouveau pseudonyme, vous avez juste à cliquer sur le bouton **Ajouter un pseudonyme**, indiquer le nouveau pseudo et le nom de l'utilisateur ou du groupe associé.

Il est également possible de faire un pseudonyme de pseudonyme, ce qui peut s'avérer utile dans le cas où une personne occupe un poste particulier comprenant plusieurs fonctions : chaque pseudonyme de fonction pointant sur le pseudonyme de poste. Ainsi, si une autre personne occupe le poste, il n'y a que le pseudonyme de poste à modifier.

i-bays

Les i-bays (terme malheureusement intraduisible) constituent des espaces de stockage particuliers extrêmement utiles et puissants, notamment pour le travail collaboratif.

Pour être un petit peu technique, sachez que chaque i-bay contient trois répertoires :

- **cgi-bin** : peut contenir des scripts CGI pour un éventuel site Web
- **files** : c'est un espace de stockage de fichiers. Si l'i-bay est utilisée pour stocker un site Web, ce répertoire pourra être accessible directement par FTP à l'adresse du site ; et en cas d'accès via le partage de fichiers, c'est ici que seront stockées les données du groupe de travail
- **html** : pour créer un site Web, c'est dans ce répertoire que vous devrez mettre vos fichiers constituant le site : si vous naviguez sur l'i-bay avec un navigateur Internet, vous accéderez directement aux données de ce répertoire

Pour information, sur le serveur, toutes les i-bays sont stockées dans le répertoire **/home/e-smith/files/ibays/**. Dès l'installation, il existe une i-bay particulière que l'on appelle **Primary** (ou Primaire) qui contient le site primaire du serveur (situé donc dans le répertoire **/home/e-**

smith/files/ibays/Primary/).

Pour étudier un peu mieux ces i-bays, imaginons que nous souhaitions développer un nouveau site Web. Nous allons donc créer une nouvelle i-bay en cliquant sur le bouton **Ajouter une i-bay**. Apparaît alors une page où nous devons indiquer :

- **Nom de l'i-bay** : comme pour les noms d'utilisateurs ou de groupes, il vaut mieux utiliser ici un nom court mais explicite
- **Description** : vous pouvez indiquer une description qui vous permettra d'identifier parfaitement l'i-bay
- **Groupe** : désigne le groupe propriétaire de l'i-bay. Les membres de ce groupe (ou tout le monde, si vous choisissez **everyone**) pourront avoir certains droits (définis dans l'option suivante) sur les fichiers contenus dans cet espace de travail
- **Accès de l'utilisateur par le partage de fichiers ou le protocole FTP** : vous indiquez ici qui peut écrire et lire des fichiers via le partage de fichiers (type Windows ou AppleShare) ou FTP (accès utilisateur authentifié)
- **Accès public par le Web ou le protocole FTP anonyme** : vous pouvez définir ici les restrictions d'accès à l'i-bay en cas d'accès via HTTP ou FTP (accès utilisateur anonyme). Si vous sélectionnez un choix où un mot de passe est exigé pour accéder aux données, vous devrez le définir à l'issue de la création de l'i-bay (voir plus bas)
- **Exécution du contenu dynamique (CGI, PHP, SSI)** : autorise ou interdit l'exécution de scripts dans le site Web (dans le cas, bien sûr, où l'i-bay contiendrait un site Web)

Notez que les accès FTP sont conditionnés par les paramètres globaux indiqués dans la page [accès à distance](#).

Avec cet ensemble d'options vous pourrez, par exemple, autoriser un groupe particulier à créer et modifier les fichiers composant le site ; les autres utilisateurs déclarés sur le serveur pouvant avoir accès à ces mêmes fichiers en lecture uniquement (toujours par exemple). S'agissant d'un projet privé pour votre entreprise, vous pourrez imposer l'accès par mot de passe aux personnes se connectant au site depuis Internet (si le serveur est configuré en serveur et passerelle, bien sûr), les personnes se connectant depuis le réseau local n'ayant pas besoin de s'authentifier pour visualiser le site.

Vous voyez alors sûrement mieux la puissance, la facilité de configuration et les nombreuses possibilités qu'offre un tel mécanisme.

Une fois l'i-bay créée, elle apparaît sur la page principale et vous disposez alors des options suivantes pour la gérer :

- **Modifier** : permet de modifier les options que nous venons d'étudier
- **Réinitialiser le mot de passe** : permet d'affecter ou de modifier le mot de passe de l'i-bay, dans le cas où vous auriez défini un accès avec mot de passe
- **Supprimer** : supprime tout simplement l'i-bay ainsi que tous les fichiers qui peuvent s'y trouver

Comme nous le verrons plus loin, vous pourrez très facilement associer un nom de domaine Internet à une i-bay dans la page [domaines](#).

Administration

Sauvegarder ou restaurer

SME permet de gérer les sauvegardes/restaurations des données contenues sur le serveur de deux façons différentes :

- Sauvegarde partielle sur un ordinateur distant du serveur
- Sauvegarde complète et automatique sur un lecteur/enregistreur de bande situé sur le serveur

Dans le premier cas, il vous suffit de sélectionner l'option **Sauvegarder dans l'ordinateur de bureau**. Votre navigateur vous demandera alors un emplacement où stocker la sauvegarde ; choisissez un endroit sûr car toutes vos données contenues dans ce fichier de sauvegarde ne sont alors plus protégées par le serveur.

En cas de besoin, vous sélectionnerez l'option **Restaurer depuis l'ordinateur de bureau** et indiquerez l'emplacement de votre fichier de sauvegarde pour restaurer toutes vos données.

Une troisième option vous permet de **Vérifier le fichier de sauvegarde de l'ordinateur distant** pour vous assurer que votre sauvegarde s'est déroulée correctement ; comme pour la restauration, vous devrez juste indiquer l'emplacement de votre fichier de sauvegarde et attendre l'affichage du contenu de la sauvegarde.

Dans le deuxième cas, vous devrez avant toute chose **Configurer la sauvegarde sur bande**. Vous pourrez alors indiquer l'heure de la sauvegarde quotidienne ainsi que l'heure d'envoi d'un mail à l'administrateur pour lui rappeler de mettre une bande dans le lecteur.

Pour la restauration, vous aurez juste à insérer la bande à restaurer dans le lecteur et à sélectionner l'option **Restaurer à partir de la bande**.

Pour information, la sauvegarde partielle contient l'ensemble des répertoires **/root/**, **/home/e-smith/** (comprenant notamment les paramètres de configuration du serveur, les répertoires personnels des utilisateurs et les i-bays) et une partie de **/etc/** comprenant les comptes d'utilisateur et de groupe, les mots de passe, les paramètres Samba et SSH et, enfin, les templates personnalisés.

Créer une disquette de réinstallation

Cette page permet de créer une disquette bootable contenant l'ensemble des paramètres de configuration de votre serveur afin de pouvoir le réinstaller dans les plus brefs délais (en cas de crash disque, par exemple). Associé à une [sauvegarde](#) régulière, c'est une option importante pour retrouver rapidement une situation opérationnelle en cas de perte de données.

La procédure de création consiste juste à introduire une disquette vierge dans le serveur et à cliquer sur le bouton **Créer**.

Visualiser les fichiers journaux

Cette page vous permet de visualiser le contenu des fichiers de logs (situés dans **/var/log/**) qui s'avèrent fort utiles pour déceler d'éventuels problèmes. Je vous recommande de vous documenter

sur ces différents fichiers (ils sont standards sous Linux) avant d'essayer de les exploiter. Pour les visualiser vous avez plusieurs options possibles :

- **Choisir le fichier journal à afficher** : vous permet de sélectionner le fichier à visualiser
- **Modèle de filtre (facultatif)** : permet de n'afficher que les lignes contenant le terme que vous spécifiez ici
- **Modèle surbrillance (facultatif)** : permet d'afficher en gras les lignes contenant le terme que vous spécifiez ici
- **Fonctionnement** : permet de visualiser le fichier directement dans votre navigateur ou bien de le télécharger sur votre machine. Notez que dans le deuxième cas le fichier est téléchargé intégralement, sans prendre en compte les deux options précédentes

Analyse des fichiers du journal courrier

Cette page permet d'afficher de nombreux rapports et statistiques concernant le serveur de messagerie. Il vous suffit de **Choisir un type de rapport** dans le menu déroulant et de cliquer sur le bouton **Générer un rapport** pour obtenir le résultat.

Redémarrer ou arrêter

Comme le nom de cette page l'indique, vous pourrez ici arrêter ou redémarrer votre serveur. Personnellement, j'ai plutôt tendance à préconiser l'exécution de ces commandes directement en local sur le serveur (voir la commande **shutdown**) afin de vérifier si les séquences d'arrêt et de démarrage se déroulent correctement.

Sécurité

Accès à distance

Cette page (à mon avis l'une des plus importantes) permet de gérer les autorisations d'accès à distance sur le serveur. Vous pourrez notamment définir :

- **Paramètres PPTP** : si certains de vos utilisateurs doivent se connecter à votre VPN via PPTP, vous devez indiquer ici le nombre maximum de connexions simultanées. Pensez bien à indiquer cette option dans la page [usagers](#)
- **Gestion à distance** : permet de définir une ou plusieurs classe(s) d'adresse(s) IP à partir desquelles vous pouvez accéder au gestionnaire de serveur via HTTPS. Ainsi, si vous souhaitez pouvoir administrer le serveur de votre entreprise depuis l'une de vos succursales, il vous suffira d'indiquer la plage d'adresses publiques de votre succursale (du type 123.123.123.96/255.255.255.240, par exemple). Si vous souhaitez supprimer une classe d'adresses, il vous suffit de cocher la case **Supprimer** correspondante et de cliquer sur le bouton **Enregistrer**
- **Paramètres Secure shell** : permet de configurer l'accès à votre serveur via SSH afin d'accéder à la ligne de commande du serveur à distance et de façon sécurisée. Vous disposez pour cela de trois options :
 - **Accès Secure shell** : je recommande ici de sélectionner au moins l'accès à partir de réseaux locaux
 - **Permettre l'accès à la ligne de commande administrative avec Secure shell** : si vous souhaitez pouvoir vous connecter avec le compte **root** (administrateur système), vous devez sélectionner **Oui**
 - **Permettre l'accès par Secure shell à l'aide des mots de passe standard** : si vous sélectionnez **Oui** ici, vous aurez la possibilité de vous connecter en indiquant le nom d'utilisateur et son mot de passe. Dans le cas contraire, vous devrez vous connecter en utilisant une clé RSA

Notez que, par défaut, seuls les utilisateurs **root** et **admin** peuvent ouvrir une session en ligne de commande sous SME

- **Paramètres FTP** : vous spécifiez ici les paramètres globaux d'accès au serveur via FTP. Si l'on reprend l'exemple que j'ai donné plus haut pour les [baies d'information](#) et que l'on souhaite que les utilisateurs puissent, en outre, stocker et récupérer des fichiers via FTP, vous devrez ici **Permettre l'accès tout public (tout Internet)** et **Accepter les mots de passe de partout**. Notez tout de même que le protocole FTP n'est pas sécurisé et que faire transiter un mot de passe de cette façon via Internet peut présenter un risque

Réseaux locaux

Si votre réseau local est composé de plusieurs classes d'adresses IP et que toutes vos machines doivent pouvoir exploiter les ressources du serveur SME (comme le serveur SMTP, par exemple), vous devrez indiquer les paramètres du réseau à ajouter. Si l'on reprend l'exemple de la succursale étudié pour la gestion à distance dans [accès à distance](#), on devrait alors indiquer :

- **Adresse réseau** : 123.123.123.96
- **Masque de sous-réseau** : 255.255.255.240

- **Routeur** : laisser vide puisqu'il n'y a pas de routeur entre le serveur SME (directement relié à Internet) et les machines de la succursale possédant des adresses IP publiques. Dans le cas contraire, il suffirait d'indiquer ici l'adresse IP du routeur (sur la même plage d'adresses que le serveur SME, bien sûr)

Si vous souhaitez supprimer une classe d'adresses, il vous suffit de cliquer sur le lien **Supprimer** correspondant.

Renvoi de port

Cette page permet de gérer le renvoi de certains ports sur d'autres machines du réseau local. Par défaut, aucun renvoi de port n'est configuré.

Imaginons que vous ayez un serveur IRC sur une machine de votre réseau local et que vous souhaitiez que des internautes puissent y accéder. Vous devrez donc cliquer sur le bouton **Création de règle de renvoi de port** et indiquer les paramètres

- **Protocole** : vous utiliserez généralement le protocole TCP, sauf cas particulier dépendant de l'application serveur cible
- **Port(s) source** : indiquez ici le ou les port(s) qui sera (seront) utilisé(s) par les clients sur Internet. C'est généralement le port utilisé par l'application serveur cible
- **Adresse IP de l'hôte de destination** : indiquez l'adresse IP de la machine sur laquelle va fonctionner le serveur
- **Port(s) de destination** : indiquez ici le ou les port(s) sur le(s)quel(s) fonctionne l'application serveur cible, au cas où il(s) serai(en)t différent(s) du ou des port(s) source(s)

Dans l'exemple du serveur IRC, il pourrait être utile de renvoyer les ports de 6667 à 6670 vers la machine dédiée. Dans ce cas, il suffirait d'indiquer **6667-6670** dans le champ ports source et juste 6667 comme port destination (par exemple).

Si vous souhaitez supprimer un renvoi de port, il suffit de cliquer sur le lien **Supprimer** correspondant.

Divers

Soutien technique et licences

Cette page affiche juste la licence d'utilisation de SME ainsi que la GNU General Public License en version anglaise.

Créer votre tout premier site Web

Cette page permet de créer une page Web (que je trouve franchement bien laide) dans le site primaire. Il vous suffit de remplir les différents champs, comme indiqué, et de cliquer sur le bouton **Créer**. Attention, la création de cette page remplacera tout fichier index.htm présent à la racine du site primaire.

Configuration

Date et heure

Cette page permet de régler les paramètres de date et heure du serveur. SME propose deux méthodes de mise à jour de l'heure :

- **Régler la date et l'heure** : vous devez indiquer à la main tous les paramètres (mois, jour, an, heure, min, sec, AM/PM et fuseau horaire). Pour le fuseau horaire, si le serveur se trouve en France métropolitaine, vous devrez sélectionner **Europe/Paris**
- **Activer le serveur temporel de réseau** : indiquez ici le nom ou l'adresse IP d'un serveur de temps NTP si vous souhaitez utiliser cette option

Dès la fin de l'installation de SME, c'est l'une des toutes premières choses que vous devriez faire. Au cas où le fuseau horaire ne correspondrait pas au votre, je vous recommande de configurer l'heure manuellement la première fois. Ensuite, vous pourrez indiquer un serveur NTP sur lequel SME viendra se recalculer régulièrement.

Groupe de travail

Cette page permet de définir les paramètres de groupe de travail Windows et AppleShare de SME. Vous pourrez ainsi définir les paramètres suivants :

- **Groupe de travail Windows** : si le serveur doit être intégré dans un groupe de travail ou un domaine Windows existant, indiquez le nom de ce groupe ou domaine. Si vous créez un nouveau groupe ou domaine, vous pouvez indiquer le nom que vous souhaitez (si possible court mais explicite)
- **Nom de serveur** : indiquez ici le nom que portera votre serveur SME au sein du groupe de travail. Ce nom doit être unique
- **Contrôleur de groupe de travail et de domaine** : si vous souhaitez que votre serveur SME fasse office de serveur de domaine Windows pour votre réseau, sélectionnez **Oui** ici. Il est généralement intéressant de configurer SME en serveur de domaine, sauf s'il en existe un autre sur le même domaine, bien sûr
- **Profils d'abonnés itinérants** : dans le cas où SME serait contrôleur de domaine, vous pouvez sélectionner **Oui** ici si vous souhaitez que les profils utilisateurs soient stockés sur le serveur. Avantage : cela permet de garder le même profil quelque soit l'ordinateur sur lequel on travaille ; inconvénient : les profils ont tendance à devenir de plus en plus volumineux et le temps de téléchargement à chaque ouverture/fermeture de session peut alors devenir problématique

Notez qu'en qualité de serveur de domaine, SME dispose du partage NETLOGON (matérialisé par le répertoire `/home/e-smith/files/samba/netlogon/`) et que l'administrateur pourra donc modifier le script d'ouverture de session par défaut (`netlogon.bat`).

Répertoire

Cette page permet de gérer les paramètres du serveur d'annuaire LDAP. Vous pouvez ainsi définir le type d'**Accès au répertoire LDAP** (uniquement depuis le réseau local ou bien depuis tout Internet) et les paramètres qui seront associés par défaut aux utilisateurs nouvellement créés.

Si vous modifiez les paramètres par défaut, vous pouvez faire en sorte qu'ils soient automatiquement associés aux utilisateurs déjà existant en sélectionnant l'option **Effectuer mise à jour avec les nouvelles valeurs par défaut** dans le menu déroulant **Usagers existants**.

Pour accéder à ce serveur LDAP depuis un logiciel client de messagerie, vous devrez juste indiquer le nom ou l'adresse IP de votre serveur et le port de communication : **389**.

Imprimantes

Cette page vous permet de configurer des imprimantes partagées pour l'ensemble de vos utilisateurs authentifiés sur le serveur. Il vous suffit de cliquer sur le bouton **Ajouter une imprimante** pour accéder à une page où vous pourrez définir les paramètres suivants :

- **Nom de l'imprimante** : comme toujours, je vous recommande d'utiliser ici un nom court mais explicite
- **Brève description** : vous pouvez indiquer une description qui vous permettra d'identifier parfaitement l'imprimante
- **Emplacement** : sélectionnez le type d'imprimante dans le menu déroulant. Si vous sélectionnez **Imprimante réseau...**, vous arrivez à une deuxième page où vous devez indiquer :
 - **Le nom d'hôte ou l'adresse IP de l'imprimante réseau** : indiquez ici l'adresse IP de l'imprimante ou un nom d'hôte auquel vous pourrez associer une adresse IP dans la page [noms d'hôte et adresses](#)
 - **Nom de l'imprimante réseau (entrez « raw » en cas d'incertitude)** : comme indiqué, autant laisser la valeur par défaut (il s'agit du nom généralement utilisé pour les files d'impression)

Si vous souhaitez supprimer une imprimante, il suffit de cliquer sur le lien **Supprimer** correspondant.

Notez que SME ne permet de gérer que le partage des imprimantes. Il vous faudra donc installer les drivers des imprimantes que vous souhaitez exploiter sur chacun de vos ordinateurs clients.

Noms d'hôte et adresses

Cette page permet de gérer les noms d'hôte par domaine déclaré (le domaine principal défini à l'installation dans la [console de serveur](#) et les domaines virtuels définis dans la page [domaines](#)) ainsi que les associations nom/adresse IP et adresse IP/adresse MAC (souvent utile en cas d'utilisation du serveur DHCP).

Par défaut, chaque domaine configuré dispose de six noms d'hôte : **ftp**, **mail**, **proxy**, **wpad**, **www** et le nom du système défini à l'installation dans la console de serveur. Si cela ne suffisait pas et que, par exemple, vous souhaitiez que l'un de vos domaines soit accessible sur votre serveur par le nom *w3.votre_domaine.xxx*, il vous suffirait de cliquer sur le bouton **Ajouter un nom d'hôte** et de remplir les champs suivants :

- **Nom d'hôte** : dans notre cas, il faudrait mettre *w3*
- **Domaine** : sélectionnez le nom de votre domaine dans la liste (*votre_domaine.xxx*, dans notre cas)
- **Emplacement** : comme on considère que l'hôte *w3* est le serveur SME, vous devez sélectionner **Auto**. Les deux autres choix, **Local** et **Distant** désignent respectivement des machines situées sur le réseau local et des machines accessibles via Internet (dans ce cas, l'adresse doit bien sûr être publique)
- Le reste de la page ne nous intéresse pas puisqu'il s'agit d'options concernant la version commerciale de SME : **Publier globalement** étant utilisé pour mettre à jour les services DNS du ServiceLink

Imaginons maintenant que *w3* serve à héberger un site sur une machine dédiée de votre réseau local. Vous devriez donc sélectionner **Local** comme **Emplacement** et indiquer l'adresse **IP locale** de la machine dédiée (à ce niveau, il est inutile de remplir le champ **Adresse Ethernet** que nous étudierons par la suite).

Troisième cas de figure : *w3* est une fois encore sur une autre machine que le serveur SME que vous êtes en train d'administrer, mais cette fois, cette machine est accessible via Internet. Vous l'aurez deviné, il faudra sélectionner un **Emplacement Distant** et l'adresse IP publique de cette machine.

Il va sans dire (même si ça va mieux en le disant...) que votre serveur DNS global (généralement celui de votre registrar) doit bien rediriger tous vos noms d'hôtes vers l'adresse IP publique de votre serveur SME. Par ailleurs, dans les deux derniers cas que nous venons de voir, il faudra bien entendu que la machine dédiée soit configurée pour gérer les requêtes faites à *w3.votre_domaine.xxx*.

Une deuxième utilisation de cette page est celle que nous avons évoquée dans la section [imprimantes](#) : cela revient à ajouter une entrée dans le serveur DNS local de SME. Pour cela, il suffit d'ajouter le nom d'hôte que l'on a donné précédemment à l'imprimante réseau locale, de sélectionner le nom du domaine principal, et d'indiquer son adresse IP.

La dernière utilisation (généralement la plus courante car très utile pour connaître à tout moment l'adresse IP d'une machine du réseau local) est la réservation des adresses IP dans le cas de l'utilisation du serveur DHCP de SME. La procédure est similaire à celle que nous venons de voir pour l'imprimante : vous devrez juste spécifier l'adresse IP et l'adresse Ethernet (MAC) de la carte réseau correspondante. Ainsi, à chaque fois que le poste client se connectera au réseau, en plus des paramètres DHCP classiques, il se verra toujours affecter la même adresse IP.

Pour gérer chaque hôte créé, vous avez deux options :

- **Modifier** : permet juste de modifier l'emplacement de l'hôte et, suivant l'option que vous aurez sélectionnée, ses adresses IP et/ou Ethernet
- **Supprimer** : supprime tout simplement l'hôte

Domaines

Cette page permet de gérer les domaines virtuels dans le cas où votre serveur SME servirait à héberger des sites (et/ou à recevoir des e-mail, par exemple) accessibles par des noms de domaine différents. Ainsi, si en plus de *votre_domaine.xxx*, vous souhaitez héberger un site (situé par exemple dans une [baie d'information](#)) accessible par l'URL *www.domaine_bis.xxx*, vous devrez cliquer sur le bouton **Ajouter un domaine virtuel** et indiquer :

- **Nom de domaine** : dans notre cas, il faudrait taper *domaine_bis.xxx*
- **Brève description** : vous pouvez indiquer une description qui vous permettra d'identifier parfaitement ce domaine
- **Contenu** : vous devez sélectionner ici la [baie d'information](#) vers laquelle le domaine doit pointer (il peut bien entendu s'agir du site principal)

Comme pour les noms d'hôte, assurez-vous que les paramètres DNS de votre registrar soient correctement configurés pour que les requêtes faites au domaine en question soient bien redirigées vers l'adresse IP publique de votre serveur SME.

Courrier électronique

Cette page permet de gérer tous les paramètres de courrier électronique. Elle est scindée en trois sections qui, suivant votre configuration propre, peuvent se recouper :

- **Paramètres généraux** : comme son nom l'indique, c'est ici que vous allez définir le mode de fonctionnement global de votre serveur SME pour le courrier et notamment :
 - **Mode de récupération du courrier électronique** : dans le cas où votre serveur SME devrait récupérer vos mails chez votre fournisseur Internet (FAI, FSI ou ISP), vous devez définir ici la méthode à utiliser. C'est une option très rarement utilisée et le choix dépend de l'offre de votre fournisseur ; vous pouvez donc généralement laisser l'option par défaut **Standard (SMTP)**
 - **Adresse de renvoi pour les avis administratifs** : le serveur envoie de temps en temps des e-mails à l'attention de l'administrateur du système (par défaut, le compte **admin**). Si vous souhaitez que ces messages soient envoyés sur un autre compte de messagerie, vous devez indiquer ce compte ici
 - **Courrier électronique destiné à des usagers inconnus** : sélectionnez ici la méthode que va suivre votre serveur dans le cas où il recevrait des courriers vers l'un des domaines gérés par votre serveur, mais dont l'utilisateur serait inconnu du système. Si vous n'utilisez pas de système anti-spam (type SpamAssassin), l'option **Retourner à l'expéditeur** est souvent la meilleure car il s'agit généralement de courrier indésirable

- **Accès serveurs POP et IMAP** : sélectionnez ici le type d'accès aux serveurs de courrier entrant de SME. Par soucis de sécurité, je vous recommande de choisir **Ne permettre l'accès qu'à partir de réseaux locaux** car à chaque connexion à ce type de serveur, vos nom d'utilisateur et mot de passe ainsi que le contenu de vos messages sont envoyés en clair (i.e. non cryptés) sur le réseau. Si vous avez absolument besoin d'accéder à votre messagerie depuis Internet, il vaudra alors mieux utiliser l'option ci-dessous
- **Activer/désactiver la messagerie Web** : SME dispose d'un accès aux comptes de messagerie grâce à une interface Web dont vous pouvez définir ici la méthode d'accès. Je vous recommande vivement de sélectionner **Activé (accès HTTPS sécurisé seulement - recommandé)** à moins que vous ne soyez certain de ne jamais avoir besoin de ce service
- **Serveurs de courrier électronique délégués** : dans le cas où vous ne souhaiteriez pas que votre serveur SME fasse office de serveur de messagerie (à moins que vous n'ayez une bonne raison de le faire, laissez SME gérer votre courrier), vous pourriez indiquer :
 - **Adresse du serveur de courrier interne** : si vous possédez un serveur de messagerie dédié sur votre réseau local, indiquez ici son nom ou son adresse IP
 - **Adresse du serveur de courrier du fournisseur de services Internet** : si vous préférez utiliser le serveur de messagerie de votre fournisseur Internet (FAI, FSI ou ISP), indiquez ici son nom ou son adresse IP
- **Paramètres ETRN ou multipoint** : si, dans la première section de cette page, vous avez sélectionné un mode de récupération du courrier en ETRN ou en multipoint (ou si vous utilisez la géniale contribution [fetchmail-generator](#) de Vincent Filali), vous devrez indiquer les paramètres suivants :
 - **Serveur de courrier électronique secondaire** : indiquez juste le nom ou l'adresse IP du serveur de messagerie (laissez vide pour la contribution de Vincent)
 - **Pendant les heures de bureau (8 h à 18 h) des jours de la semaine** : indiquez la fréquence de récupération des messages pendant les "heures de bureau"
 - **En dehors des heures de bureau (8 h à 18 h) des jours de semaine** : idem en dehors des "heures de bureau"
 - **Pendant la fin de semaine** : idem pour le week-end
 - **Compte d'utilisateur POP (pour le mode multipoint)** : en cas d'utilisation du mode multipoint, indiquez le nom du compte permettant de récupérer les messages
 - **Mot de passe d'utilisateur POP (pour le mode multipoint)** : indiquez le mot de passe du compte multipoint que vous venez d'indiquer
 - **Sélectionnez la méthode de tri (pour le mode multipoint)** : la méthode par défaut doit fonctionner dans la majorité des cas (exploite les en-têtes **To:** et **Return-To:**)
 - **Sélectionnez l'en-tête de tri (pour le mode multipoint)** : indiquez votre méthode de tri (en-tête spécifique ajoutée par votre fournisseur Internet)

Vérifier la configuration

Cette page ne fait qu'afficher un résumé des paramètres de configuration : paramètres réseau, noms principaux du serveur ainsi que des informations sur les domaines gérés par le serveur.

10. Génération d'un certificat SSL CACERT (ancienne méthode)

Si vous avez besoin d'installer un site marchand sur votre sme ou simplement parce que vous jugez que votre serveur se doit de posséder un certificat SSL reconnu pour qu'il soit parfaitement configuré, je vais vous expliquer la marche à suivre (cette procédure n'est pas expliquée complètement sur le wiki de contribs).

Premièrement vous devriez vous créer un compte sur le site de CACERT

=> <https://www.cacert.org/index.php?id=1>

Une fois ce compte créé, ajoutez votre domaine sur cacert en vous rendant dans les options du site sur => Domaines => Ajouter

Maintenant nous allons pouvoir générer la clef partagée entre le site de CACERT et votre serveur de production. Voici les différentes étapes :

1. connectez vous à l'aide de putty avec le compte root.
2. Entrez ces commandes :

```
mkdir ~/cacert
cd ~/cacert
vi cacert_csr_request
```

3. Remplissez ce nouveau fichier avec ce code :

```

#!/usr/bin/perl

use strict;
use esmith::util;
use esmith::ConfigDB;
use esmith::DomainsDB;

my $config = esmith::ConfigDB->open;
my $domainsdb = esmith::DomainsDB->open_ro;

my $domain = $config->get('DomainName')->value;
my %domain_names = map { $_->{key} => 1 } grep { $_->key ne $domain }
$domainsdb->domains;

my @domains = ($domain, keys %domain_names);

open(CONFIG, ">$domains[0].config") or die "Can't open openssl config file:
$!";
print CONFIG "HOME = .\nRANDFILE = \${ENV::HOME}/.rnd\n\n";
print CONFIG "[ req ]\ndefault_bits = 1024\ndistinguished_name =
req_distinguished_name\n";
print CONFIG "req_extensions = v3_req\nprompt = no\n\n";
print CONFIG "[ req_distinguished_name ]\nCN = $domains[0]\n\n";
print CONFIG "[ v3_req ]\nbasicConstraints = CA:FALSE\nkeyUsage =
nonRepudiation,digitalSignature,keyEncipherment\n";
print CONFIG "subjectAltName = critical,", join ",", map { "DNS:$_,DNS:*.$_" }
@domains;
print CONFIG "\n";
close(CONFIG) or die "Closing openssl config file reported: $!";

unless ( -f "$domains[0].key" )
{
    open(KEY, ">$domains[0].key") or die "Can't open key file: $!";
    unless (open(SSL,"-|"))
    {
        exec("/usr/bin/openssl",
            qw(genrsa -rand),
            join(':',
                qw(
                    /proc/apm
                    /proc/cpuinfo
                    /proc/dma
                    /proc/filesystems
                    /proc/interrupts
                    /proc/ioports
                    /proc/bus/pci/devices
                    /proc/rtc
                    /proc/uptime
                )),
            '1024')
            || die "can't exec program: $!";
    }
    while (<SSL>)
    {
        print KEY $_;
    }
    close(SSL) or die "Closing openssl pipe reported: $!";
    close(KEY) or die "Closing key file reported: $!";
}

open(CSR, ">$domains[0].csr") or die "Can't open csr $!";

```

```
unless (open(SSL, "-|"))
{
    exec("/usr/bin/openssl",
        qw(req -config), "$domains[0].config",
        qw(-new -key), "$domains[0].key",
        qw(-days 730 -set_serial), time())
    || die "can't exec program: $!";
}
while (<SSL>)
{
    print CSR $_;
}
close(SSL) or die "Closing openssl pipe reported: $!";
close(CSR) or die "Closing csr file reported: $!";
```

4. Pour sauvegarder et quitter ce fichier, appuyez d'abord sur la touche ESC (escape), « :w » (pour sauvegarder les modifications sans les « ») puis « :q » (pour quitter l'éditeur de texte sans les « »).

5. Changez les droits d'écriture de ce fichier et exécutez le :

```
chmod u+x cacert_csr_request
./cacert_csr_request
```

6. Générer le certificat (attention vous devez insérer votre domaine) :

```
cat domain.csr
```

7. Copier cette clef dans => Certificats de Serveur => Nouveau sur le site de CACERT.
8. Créez un fichier nommé domain.crt (ou domaine est votre nom de domaine complet) dans le répertoire cacert qui se trouve dans /root/ et copiez y aussi la clef (directement avec winscp).
9. Copiez les fichiers à leur emplacement final (attention, remplacez les noms des fichiers dans vos commandes) :

```
cp {domain}.crt /home/e-smith/ssl.crt/{domain}.crt
cp {domain}.key /home/e-smith/ssl.key/{domain}.key
```

10. Renseignez votre sme pour qu'elle utilise ces fichiers (attention, remplacez les noms des fichiers dans vos commandes) :

```
config setprop modSSL crt /home/e-smith/ssl.crt/{domain}.crt
config setprop modSSL key /home/e-smith/ssl.key/{domain}.key
```

11. Finalisez l'installation du certificat sur votre SME :

```
signal-event console-save
reboot
```

11.OPNvpn Bridge et PHPki

Je tiens tout d'abord à remercier Daniel Berteaud du site firewall-services.com, développeur des deux contributions sus citées, pour son aide indispensable quant à la marche à suivre de la configuration des deux programmes.

OPNvpn Bridge est une contribution qui va vous permettre d'installer un serveur VPN (Virtual Private Network) sur votre sme. Cela vous permettra de vous connecter au réseau de votre sme pour la monitorer et avoir accès à votre server-manager depuis internet. Il va sans dire que vous pourrez aussi travailler en réseau décentralisé (c'est à dire au travers d'Internet) avec vos collaborateurs (fichiers partagés etc).

PHPki est, quant à lui, le gestionnaire des certificats de votre SME. Il va gérer les clés et les certificats de votre VPN, autant serveur que client. Cette partie du tutorial sera complétée au fur et à mesure de notre apprentissage de l'outil, car celui-ci peut gérer d'autres types de certificats.

Installation

Rien de bien compliqué, installez en premier OpnVPN Bridge :

```
yum --enablerepo=smecontribs install smeserver-openvpn-bridge
```

Ensuite, installez PhpKi :

```
yum --enablerepo=smecontribs install smeserver-phpki
expand-template /etc/httpd/conf/httpd.conf
expand-template /etc/httpd/pki-conf/httpd.conf
sv t /service/httpd-e-smith
sv u /service/httpd-pki
```

Reconfigurez le serveur afin de n'avoir aucun problème et aller forwarder le port **UDP 1194** sur votre router vers l'adresse IP votre serveur (même si le serveur est en DMZ).

Configuration

Nous allons en premier lieu configurer PHPki dans le server-manager (manage certificates) et remplir tous les champs requis à la génération du certificat root.

- *Organisation*
- *Department*
- *Common Name of the Master CA*
- *E-mail (technical contact)*
- *City*
- *State*
- *Country Code*
- *Password (to protect the private key of the Master CA)*

- *Validity of the CA*
- *Keys size*
- *URL of your PKI*

Dès que ces champs seront configurés, vous pourrez voir la véritable interface d'administration de PHPki.

1. Dans PHPki, créez un nouveau certificat pour le serveur de type "VPN Server Only", sans mot de passe (un nom commun simple, sans espace et autres caractères).
2. téléchargez le certificat (que l'on vient de créer) et la clé au format PEM. Vous pouvez ouvrir ces deux fichiers avec un éditeur de texte.
3. Téléchargez le certificat root au format PEM (vous pouvez aussi l'ouvrir avec un éditeur de texte).
4. Rendez vous dans le menu OpenVPN-Bridge du server-manager, puis, dans « *configuration des certificats* » où vous allez remplir les champs suivants :
 - **URL de mise à jour de la CRL** : ce champ devrait déjà être rempli si PHPki est installé sur le même serveur, la valeur par défaut convient au bon fonctionnement du service.
 - **Certificat Racine (ou CA)** : coller le contenu du certificat root téléchargé plus tôt.
 - **Certificat serveur** : coller le contenu du certificat serveur téléchargé juste avant. **Attention à ne pas inverser le certificat serveur et le certificat racine.**
 - **Clé privée du serveur** : idem, mais avec le contenu de la clé.

Le dernier champ est optionnel. Vous pouvez soit coller la clé secrète disponible dans PHPki (**display static pre-shared key**), soit mettre une « *passphrase* » libre ou le laisser vide. Il faudra copier la même clé sur tous les clients.

Désormais, dans l'administration d'opnVPN vous devriez voir en vert :

État des certificats : **Les certificats sont en place, le service est prêt à fonctionner**

Configuration d'un client VPN

Pour pouvoir joindre le serveur en VPN, il vous faudra le programme Windows **OpnVPN GUI** (il existe des alternatives pour Linux. A savoir que l'important réside dans le fichier de configuration, la clef et le certificat que vous allez générer. La marche à suivre pour le client est identique sous toutes les plateformes.

1. Créez un nouveau certificat dans PHPki, sans mot de passe, de type "**VPN Client only**".
2. téléchargez le certificat créé au format **pkcs12**.
3. Placez ce fichier dans le répertoire « *config* » d'openvpn GUI sur la machine cliente.
4. Téléchargez la clé statique depuis PHPki "**download the static pre-shared key**".
5. Placez la dans le répertoire de « *config* » d'openvpn GUI sur la machine cliente.
6. Allez dans le panel "**OpenVPN-Bridge**" et cliquez sur "**Afficher un exemple de configuration cliente**".
7. Copiez le contenu dans un fichier « **client.ovpn** » dans le répertoire « *config* » d'openvpn GUI sur la machine cliente. Modifiez juste la ligne « user.p12 » par le nom de votre fichier .p12 pour l'adapter au nom du certificat créé. Faites de même pour la ta-key.

Vous pouvez éventuellement fixer une IP pour ce client en créant une règle de configuration. Dans le cas contraire, l'IP sera allouée de façon dynamique à partir de la plage configurée sans les options d'OPNvpn Bridge.

Le client peut désormais lancer la requête de connexion via le programme OPNvpn GUI. Dès sa connexion, il se retrouvera insérer dans le réseau du serveur et pourra accéder au server-manager via son adresse IP réseau. Il sera aussi possible au client de visualiser les répertoire partagés du serveur via samba.

Génération des certificats SSL

En fait, PHPki est complètement indépendant. Rien ne vous empêche de mettre un certificat CACERT pour apache, et de garder uniquement PHPki pour la gestion des certificats VPN. Mais, tant qu'à faire, vous pouvez utiliser votre PKI pour apache.

Pour ça, il faut aller dans PHPki et générer un nouveau certificat de type "**SSL Server**". Pour le nom commun, je conseille de mettre :

*.domain.tld (à remplacer par votre nom de domaine)

Comme ça, le nom du certificat sera valide pour tout les sous-domaines (www.domain.tld, extranet.domain.tld, blah.doman.tld etc...).

Ensuite, vous téléchargez le certificat et la clé privée au format PEM et vous les placez sur votre SME dans les répertoires :

/home/e-smith/ssl.crt/ (pour le certificat)
/home/e-smith/ssl.key/ (pour la clef)

Puis, vous configurez apache pour utiliser ce nouveau certificat :

```
db configuration setprop modSSL crt /home/e-smith/ssl.crt/votrecertif.pem  
key /home/e-smith/ssl.key/votrekey.pem (attention c'est une seule ligne)  
signal-event domain-modify
```

Voilà, apache utilise maintenant le certificat personnel. Il n'y a plus qu'à aller dans PHPki, cliquer sur "*Download the root certificate*" (pas en PEM), et votre navigateur devrait vous demander si vous voulez l'importer.

Une fois accepté, tout les certificats signés par ce certificat racine (comme celui que vous venez de signer pour apache) seront considérés comme valides par votre navigateur.

12.Exemple de création d'Ibay NPDS

Les ibays sont des répertoires permettant le stockage de données ou de programmes
une ibay peut être d'accès public ou privé.
par défaut sme met les ibays dans
/home/e-smith/files/ibays/nom de l'ibay

la structure pour une ibay nommée test sera
/home/e-smith/files/ibays/test/cgi-bin (lieu de stockage de vos scripts CGI) ,
home/e-smith/files/ibays/test/html (pour stocker un site)
/home/e-smith/files/ibay/test/files pour stocker des fichiers.

Il existe plusieurs moyen d'accéder à une ibay, en mode terminal (putty) par son lien internet
(<http://ipduserver/ibay>) ou en ftp (<ftp://ipduserver/ibay>), pour accéder à une ibay qui nécessite un
mot de passe avec un butineur, il suffit de donner comme adresse
<ftp://nomdel'ibay:motdepasse@ipduserver> ou [@nomdudomaine](ftp://nomdudomaine)

Je vais tenter ici de vous expliquer comment installer NPDS de manière à ce que tout fonctionne
parfaitement (upload y compris).

1. Création de l'ibay qui va contenir NPDS => rendez vous dans votre server-manager
Collaboration => Ibay et cliquez sur le bouton « ajouter une ibay ».
2. Dans le formulaire de création, rentrez un nom, une description, choisissez « Everyone »,
Ecriture=groupe, lecture=tous, tout internet sans mot de passe et activez cgi/php et mysql.
3. Vous pouvez déjà voir que votre ibay est créée en vous rendant sur
<http://10.0.0.1/nomdel'ibay>
4. Transférez NPDS dans le répertoire de l'ibay à l'aide de winscp (windows) ou gftp (ubuntu)
[faites attention que vous vous connecter avec votre login et pass root en SFTP] dans le
répertoire /home/e-smith/files/ibays/nomedelibay/html/
5. Faites appartenir tous les fichiers à l'utilisateur www (apache) en vous rendant en root avec
putty et en tapant la commande suivante (à refaire à chaque ajout de fichier), n'oubliez pas
de modifier cette commande en fonction du nom de votre ibay :

```
chown -R www /home/e-smith/files/ibays/nomedelibay/html/
```

6. Appliquez le fichier chmod de hotfirenet pour chmoder l'intégralité de vos fichiers =>
<http://www.hotfirenet.com/download.php?op=geninfo&did=2>
7. Rendez vous dans phpmyadmin (que vous avez installé sur votre sme) pour y créer votre
base de donnée. Donnez lui le nom de votre ibay (pour des raison de facilité).
8. Permettez l'écriture des fichiers dans un répertoire (pour l'upload et aussi pour le rewriting)
en tapant les commandes suivantes sous putty (modifier nomdelibay par le nom de votre

ibay) :

```
db accounts setprop nomdelibay PHPBaseDir /home/e-smith/files/ibays/nomdelibay/  
signal-event ibay-modify nomdelibay
```

9. Modifier la taille d'envoi maximum des fichiers (s'applique pour tout le serveur) en utilisant les commandes ci-jointe (ici maximum 50Mo):

```
config setprop php UploadMaxFileSize 50M  
config setprop php PostMaxSize 60M  
signal-event console-save
```

10. Configurer votre upload.conf comme suit :

```

<?PHP
/*****
/* DUNE by NPDS
/* =====
/*
/* NPDS Copyright (c) 2002-2007 by Philippe Brunier
/*
/* This module don't use anyone of the config.php variable for security */
/* reasons
/*
/* This program is free software. You can redistribute it and/or modify */
/* it under the terms of the GNU General Public License as published by */
/* the Free Software Foundation; either version 2 of the License.
*****/

// Taille maxi des fichiers en octets
$max_size = 500000;

// Si votre variable $DOCUMENT_ROOT n'est pas bonne (notamment en cas de redirection)
// vous pouvez en spécifier une ici (c'est le chemin physique d'accès à la racine de
votre site en partant de / ou C:\)
// par exemple /data/web/mon_site OU c:\web\mon_site SINON LAISSER cette variable VIDE
$DOCUMENTROOT = "/home/e-smith/files/ibays/nomdelibay/html";

// Autorise l'upload DANS le répertoire personnel du membre (true ou false)
$autorise_upload_p = "true";

// Sous répertoire : n'utiliser que si votre NPDS n'est pas directement dans la racine
de votre site
// par exemple si : www.mon_site/npds/... alors $racine="/npds" (avec le / DEVANT)
sinon $racine="";
$racine = "";

// Répertoire de téléchargement (avec le / terminal)
$rep_upload = $racine."/modules/upload/upload/";

// Répertoire de stockage des fichiers temporaires (avec le / terminal)
$rep_cache = $racine."/modules/upload/tmp/";

// Répertoire/fichier de stockage de la log de téléchargement (par défaut
/logs/security.log)
$rep_log = $racine."/logs/security.log";

// URL HTTP de votre site (equivalent à $nuke_url) mais sans le contenu de $rep_upload !
$url_upload = "http://www.monsite.org";

// URL de la feuille de style à utiliser pour la présentation de la fenetre d'upload (ou
"")
global $cookie, $user, $Default_Theme, $theme;
if (isset($user)) {
    if ($cookie[9]=="") $cookie[9]=$Default_Theme;
    if (isset($theme)) $cookie[9]=$theme;
    $tmp_theme=$cookie[9];
    if (!$file=@opendir("themes/$cookie[9]")) $tmp_theme=$Default_Theme;
} else {
    $tmp_theme=$Default_Theme;
}
$url_upload_css = $racine."/themes/".$tmp_theme."/style/style.css";

/* ----- DIVERS ----- */
// Gère l'affichage de la Banque Images et Documents : "0000" => rien / "1111" => tous
// 1 (true) ou 0 (False)
// - 1er position : afficher les images de !divers
// - 2ième position : afficher les images de !mime
// - 3ième position : afficher les images de la racine du répertoire (celles qui seront
téléchargées)
// - 4ième position : afficher les documents

```

```
$ed_profil="1111";

// Nombre d'image par ligne dans l'afficheur d'image de l'editeur HTML
$ed_nb_images=10;

// suffix des fichiers autorisés (séparé par un espace)
$extension_autorise="doc xls pps ppt sxw xls sxi sxd sxg stw rtf txt pdf zip rar tar tgz
gif jpg jpeg png swf";

// Taille maxi en affichage des images dans les banques de l'Editeur HTML
$width_max=100;
$height_max=100;

// Limite de l'espace disque alloué pour l'upload (en octets)
$quota=5000000;
?>
```

11. Configurez votre config.php en y entrant les informations suivantes (localhost, admin, mot de passe admin, nom de la db).

A ce stade votre NPDS est prêt à l'emploi :p

13. Généralité quant à l'hébergement pour plusieurs personnes

Pour héberger plusieurs personnes, vous devrez faire la même chose que pour l'installation de NPDS. En revanche vous devrez créer un compte pour ce nouvel utilisateur et dévier son nom de domaine vers son répertoire.

1. Création d'un groupe qui s'appellera « *clients* » (en lettre minuscule) dans Collaboration => Groupes
2. Création d'un nouvel utilisateur en vous rendant dans le serveur-manager Collaboration => Utilisateurs (il faudra que vous donniez à celui ci un mot de passe comme demandé lors de la création de l'utilisateur, notez le quelque part vous en aurez besoin et en plus, ce client peut le perdre ...). N'oubliez pas ensuite de cliquer sur « *réinitialiser le mot de passe* » et de créer un mot de passe à ce nouvel utilisateur sinon le compte restera verrouillé.
3. Une fois ce client créé, retournez dans Collaboration => Groupes pour qu'il fasse partie de ce groupe d'utilisateur.
4. Créer une ibay destinée à ce client.
5. Nous allons maintenant lui attribuer son quota disque dur en se rendant dans Collaboration => Quotas. Choisissez le nom du client dans la liste et « *modifier* ». Tapez le quota sous la forme d'un entier auquel vous pouvez ajouter le suffixe unitaire "K" pour kilooctet, "M" pour mégaoctet, ou "G" pour gigaoctet. Si aucun suffixe n'est entré, l'unité par défaut sera le mégaoctet. Si l'une des limites est définie à "0", cette limite sera désactivée pour l'utilisateur correspondant.
6. Comme nous avons installé phpmyadminmulti, nous allons pouvoir créer la base de donnée personnelle de ce membre en se rendant dans phpmyadmin (<http://10.0.0.1/myadmin>) avec le compte administrateur (admin). Allez dans « *privilèges => Ajouter un utilisateur* ».
7. Entrez les données demandées (nom de l'utilisateur, localhost, son mot de passe) et choisissez « *Créer une base portant son nom et donner à cet utilisateur tous les privilèges sur cette base* ». Allez recharger les privilèges dans la page d'accueil de phpmyadmin.
8. Occupons nous maintenant de son ftp => suivez le tutorial en anglais se trouvant à cette adresse => http://wiki.contribs.org/FTP_Access_to_Ibays . Certaines des étapes sont déjà expliquées dans le début de ce chapitre.
9. N'oubliez pas de permettre l'écriture des fichiers dans un répertoire (pour l'upload et aussi pour le rewriting) comme expliqué dans l'installation de npds.
10. Pour la gestion du domaine, deux possibilités s'offre à vous : soit l'ibay créée sera un alias de votre domaine principal (celui entré lors de la post-installation du serveur) soit ce sera un domaine indépendant. Dans les deux cas, l'opération est presque identique et se gère dans le panel des domaines.

- Dans le cas d'un alias, rendez vous sur la configuration de votre nom de domaine chez votre registrar et créez cet alias (faite le pointer vers votre domaine principal du point de vue du refresh à l'aide de la balise CNAME). Allez ensuite ajouter votre alias comme un nouveau nom de domaine (alias.domaine.com) dans le serveur manager et faite le pointer sur la bonne ibay. Pour ne pas avoir de problème avec des « *www* » comme il s'agit d'un alias, rendez vous dans la « *Gestion des noms d'hôte et des adresses* » et effacez tous les sous alias en présence pour ce nouveau domaine (ils utiliseront le ftp, le mail, etc de votre domaine principal vu que cet alias est lié à votre domaine principal : ce n'est pas un compte client !!!). Ajouter maintenant un hôte à votre domaine principal, toujours dans la « *Gestion des noms d'hôte et des adresses* », à l'aide du bouton qui se trouve en haut de page. Indiquez juste l'alias en choisissant le domaine auquel il se rapporte.
- Dans le cas d'un nouveau domaine, créer le dans « *domaines* » et choisissez l'ibay auquel il se rapporte. N'oubliez pas de créer les alias chez votre registrar (www/ftp/mail/...).

14. Le mode passerelle et le réseau idéal

Création d'une machine de backup

Nous allons ici mettre en place une seconde machine qui va servir de machine de backup, autant pour votre serveur de production, votre serveur de développement et vos postes de travail.

Afin de mettre en place cette machine de backup, il vous faudra disposer d'une machine pourvue d'un assez gros disque dur pour supporter le backup total de départ des machines et leurs backups incrémentiels. Il existe plusieurs manières et plusieurs programmes permettant de faire des sauvegardes à partir de SME mais nous choisirons celui qui nous semble le plus adapté à un environnement réseau hétéroclite (linux, windows, mac). Nous utiliserons donc Backuppc, une solution souvent utilisées en entreprise.

1. Installer une SME sur votre matériel pourvu d'un gros disque dur.
2. Configurer cette SME en **server-only** pour faire partie de votre réseau et de votre groupe de travail windows.
3. Configurer l'accès SSH **visible seulement de l'intérieur du réseau**.
4. Mettez à jour la nouvelle SME
5. Installer **SME7Admin** => <http://sme.firewall-services.com/spip.php?article9> et configurez le correctement afin qu'il vous envoie des mails de maintenance.
6. Installez **DiskUsage** afin de monitorer la place qu'il vous reste sur votre disque dur => <http://wiki.contribs.org/Diskusage>
7. Installez enfin **BackuPPC** => <http://sme.firewall-services.com/spip.php?article44> et effectuer une reconfiguration et restart de la machine pour que tout soit parfaitement en ordre avant de commencer. Pour voir différents screenshots de l'interface de backuPPC => <http://sme.firewall-services.com/spip.php?article17> .

Nous allons maintenant configurer backuPPC pour que l'interface soit en français. Pour ce faire, rendez vous dans le server-manager, menu backupPC, entrez le **login admin et son mot de passe**, cliquez sur « **Edit Config** », choisissez « **CGI** » dans le menu supérieur et mettez la variable « **Language** » en « **fr** » => Cliquez sur le gros bouton « **Save** » en haut à droite de l'interface de BackupPC.

N'ayant pas de Mac sous la main, nous allons voir ensemble comment configurer les processus de backup pour une machine sous linux et une sous windows.

Machine sous Linux (backup de vos serveurs SME ou postes de travail Ubuntu)

1. Ajoutez une nouvelle machine dans l'interface de BackupPc => « **Modifier les machines** », pour les machines linux, je préfère personnellement mettre son adresse IP dans le champ « **host** », mettez « **root** », dans le champ « **user** » .
2. Sauvegarder cette configuration en cliquant sur le bouton « **Sauvegarder** » en haut à gauche.
3. Nous allons maintenant devoir générer une clef RSA qui permettra à la machine de backup de se connecter aux ordinateurs distant sans avoir besoin de mot de passe. Voici les commandes que vous allez devoir effectuer en mode console sous le compte root :

```
su -s /bin/bash backuppc
ssh-keygen -t rsa -b 2048           # utilisez un passphrase vide
exit
```

4. Une fois la clef générée, il va falloir l'exporter sur la machine distante. Utilisez ces commandes, toujours en root sur la machine de backup. Entrez juste l'IP de la machine distante à la place de « **host_or_IP_to_be_backed_up** ». Attention, les deux dernières lignes de commande n'en forment qu'une mais pour Ubuntu, vous devez d'abord attribuer un mot de passe au compte root sur votre Ubuntu à l'aide de la commande : **sudo passwd root** qui vous demandera 3 fois de rentrer un mot de passe. N'oubliez pas de créer le répertoire /root/.ssh si il s'agit d'une Ubuntu à configurer pour un backup.

```
remote_host=<host_or_IP_to_be_backed_up>
ssh-keyscan -t rsa $remote_host >> ~backuppc/.ssh/known_hosts
scp ~backuppc/.ssh/id_rsa.pub
root@$remote_host:/root/.ssh/authorized_keys
```

5. Vous pouvez tester si l'accès à la machine distante s'effectue bien sans avoir besoin de mot de passe en effectuant les commandes suivantes. Entrez juste l'IP de la machine distante à la place de « **name_or_IP_of_the_remote_host** » :

```
su -s /bin/bash backuppc           #become backuppc user
ssh -l root <name_or_IP_of_remote_host>
exit                                 #from the remote_host
exit                                 #from the backuppc user back
to root
```

6. Choisissez maintenant dans la liste déroulante la machine que vous avez ajoutée dans le panel d'ajout de machine et choisissez dans la nouvelle interface « **Modifier la configuration** ».
7. Rentrer l'adresse IP de la machine dans le champ « **ClientNameAlias** » et sauvegarder.
8. Cliquez sur le lien « **Xfer** » dans le menu supérieur. Choisissez « **rsync** » comme méthode « **XferMethod** » et peuplez la liste des répertoire que vous voulez sauvegarder.

Personnellement, je sauvegarde les dossiers suivant de mon serveur de production et de développement :

```
/root
/etc/e-smith/templates-custom
/opt/webshare
/home/e-smith
```

9. Sauvegarder la configuration de ce client à l'aide du bouton « **Sauvegarder** » en haut à gauche.
10. Cliquez sur le lien d'accueil de la machine que vous venez de configurer et cliquez sur le bouton « **Démarrer la sauvegarde complète** » pour effectuer la première sauvegarde. Les sauvegarde incrémentielle s'effectueront toutes les 24h (sauf si vous décidez d'en lancer une manuellement à partir de cette interface).

Vous pouvez dès à présent rajouter des machines linux supplémentaires à sauvegarder.

Backup de machines sous windows

Nous allons maintenant voir comment configurer la sauvegarde de machines tournant sous windows.

1. Comme pour la première étape de la méthode pour les machines Linux, ajoutez une machine supplémentaire. Entrez le nom réseau de votre machine windows et « *Administrateur* » comme utilisateur.
2. Idem.
3. Pour permettre à la machine de backup d'accéder à votre machine et de faire la sauvegarde des dossiers souhaités, il vous faudra partager sur le réseau les dossiers incriminés. Personnellement, je ne sauvegarde que « **C:\Documents and Settings** » dans lequel se trouve aussi bien mes documents et le contenu de mon bureau. Chose importante, le compte administrateur de la machine windows doit être protégée impérativement par un mot de passe de connexion de session.
4. Étape 6 pour les machines linux.
5. Idem que l'étape 7 pour les machines linux.
6. Cliquez sur le lien « **Xfer** » dans le menu supérieur. Choisissez « **Smb** » comme méthode « **XferMethod** » et peuplez la liste des répertoire que vous voulez sauvegarder. Ajoutez le login et le mot de passe de votre compte Administrateur de la machine windows que vous allez sauvegarder, soit :

Administrateur	#SmbShareUserName
le mot de passe	#SmbSharePasswd

Je sauvegarde mon dossier partagé qui est le suivant :

Administrateur #(nom du dossier partagé)
--

7. Sauvegarder la configuration de ce client à l'aide du bouton « *Sauvegarder* » en haut à gauche.
8. Cliquez sur le lien d'accueil de la machine que vous venez de configurer et cliquez sur le bouton « *Démarrer la sauvegarde complète* » pour effectuer la première sauvegarde. Les sauvegarde incrémentielle s'effectueront toutes les 24h (sauf si vous décidez d'en lancer une manuellement à partir de cette interface).

BackupPpc possède une foultitude d'autres réglages comme la mise en place des horaires de backups, le temps de conservation des sauvegardes etc ... vous pourrez trouver ces informations, si vous souhaitez aller plus loin avec ce mode de sauvegarde, soit dans la documentation présente dans le menu du logiciel, soit sur le site officiel du programme => <http://backuppc.sourceforge.net/>

Contrôle d'un onduleur MGE

Si vous décidez de vous héberger vous-même, il vous faudra évidemment installer un onduleur au moins pour votre serveur de production qui ne devra subir aucune déconnexion et dont la sauvegarde du matériel électrique est d'une importance capitale. Pour éviter toute panne due à une défaillance de votre réseau électrique nous vous conseillons d'acheter un onduleur adapté à votre configuration (rapport puissance onduleur et puissance de votre alimentation). Les onduleurs MGE sont les plus courants dans le commerce, ils possèdent un port USB de monitoring et sont compatibles Linux. A cet effet, voici comment relier votre onduleur sur votre serveur SME, vous devrez ensuite le configurer à bon escient pour que, lors d'une coupure électrique, l'onduleur lance les commandes d'arrêt de la machine lorsque le seuil de batterie dépasse une certaine limite, évitant un arrêt brutal.

Le tuto officiel de cette manipulation est consultable à l'adresse suivante :

http://wiki.contribs.org/Uninterruptable_Power_Supply

L'installation présente est réalisée avec un onduleur MGE Protection Center 600 possédant une prise USB.



1. Arrêtez votre serveur, mettez en place l'onduleur et reliez votre serveur à une des prises de l'onduleur. Reliez l'onduleur à votre serveur SME via le câble USB fourni avec le matériel (préférez un port USB2 si votre machine est ancienne mais possède les deux types de connexions).
2. Allumez votre serveur lorsque tous les branchements sont effectués.
3. Pour activer la prise en charge de votre onduleur par SME, vous devez taper les commandes suivantes dans la console en tant qu'administrateur :

```
config setprop nut status enabled
signal-event post-upgrade
signal-event reboot
```

4. Lorsque le serveur est de nouveau en service, retournez en root dans la console et configurez la connexion de l'onduleur sur le port USV de votre serveur à l'aide des commandes suivantes (les informations suivantes sont propres aux onduleurs MGE) :

```
config setprop nut Model usbhid-ups
config setprop nut Device /dev/ttyS0
config setprop nut status enabled

config show nut #vous affiche votre configuration

signal-event post-upgrade
signal-event reboot
```

5. Lorsque le serveur est de nouveau accessible, en root, rentrez la commande suivante pour vérifier si votre onduleur communique avec votre serveur (vous devriez voir toutes les informations) :

```
upsc UPS@localhost
```

6. Les UPS MGE étant préconfigurés de manière correcte, nous n'avons pas modifier la configuration d'arrêt du serveur, mais si vous le souhaitez, le tutorial original traite de cette partie dans son chapitre « **Modifying UPS Parameters** »

Installer un serveur IRC

1. Télécharger le paquet suivant et installez-le :

```
wget ftp://ftp.pbone.net/mirror/yum.trixbox.org/centos/4/RPMS/ircd-hybrid-7.2.1-2.i386.rpm
```

```
rpm -i ircd-hybrid-7.2.1-2.src.rpm
```

2. Configurer le fichier /etc/ircd/ircd.conf

Dans serverinfo => name=«domaine» (ex : domaine.org)

Dans auth, commenter la ligne => # password= «password»

15. Quelques astuces utiles

Masquer le listing des fichiers dans les i-bays

Par défaut, si un répertoire dans une i-bay ne contient pas de fichier index.html ou index.php, il est possible de visualiser la liste des fichiers présents dans le répertoire. Si vous souhaitez supprimer cette fonctionnalité pour une i-bay toto, il suffit de taper :

```
db accounts setprop toto Indexes disabled
signal-event ibay-modify toto
```

Résoudre les noms d'hôte dans les logs

Si vous utilisez des générateurs de statistiques d'utilisation de votre serveur Apache, Vous devez préférer connaître le nom d'hôte (reverse-DNS) de vos visiteurs plutôt que leur adresse IP. Or, par défaut, le serveur n'enregistre que l'adresse IP.

Pour enregistrer les noms d'hôtes, il vous suffit de taper :

```
config set httpd-e-smith configuration HostnameLookups on
signal-event console-save
```

Pour revenir à la configuration standard, remplacez **on** par **off**

Personnaliser les messages d'erreur standards d'Apache

Par défaut, lorsqu'une requête HTTP échoue, le service Apache renvoie une page d'erreur standard bien moche... Il est toutefois possible de personnaliser ces pages d'erreur pour chaque i-bay.

Pour cela, il va falloir créer un fragment de template personnalisé avec votre éditeur de texte préféré (mcedit, vi, pico, nano, etc.) :

```
mkdir -p /etc/e-smith/templates-custom/etc/httpd/conf/httpd.conf/
vi /etc/e-smith/templates-custom/etc/httpd/conf/httpd.conf/95AddErrDoc2ibays
```

Dans ce fichier, tapez le code PERL suivant :

```

{
  use esmith::AccountsDB;
  my $adb = esmith::AccountsDB->open_ro();

  local @page =
('206','301','302','400','401','402','403','404','405','500','502');
  local $texte;

  foreach my $ibay ($adb->ibays)
  {
    $texte = "";
    foreach my $err_num (@page)
    {
      local $errorMessage = $ibay->prop($err_num);
      if ($errorMessage)
      {
        $texte .= "    ErrorDocument $err_num $errorMessage\n";
      }
    }
    if ($texte)
    {
      $OUT .= "\n<Directory /home/e-smith/files/ibays/" . $ibay->key .
"/html>\n";
      $OUT .= $texte;
      $OUT .= "</Directory>\n";
    }
  }
}

```

Comme vous pouvez le voir, je n'ai pris en compte "que" certains codes d'erreur. S'il vous en manque, il vous suffit de les rajouter dans le tableau **@page**. D'un autre côté, vous n'êtes pas obligé de personnaliser tous les codes proposés.

Pour mémoire, les codes les plus fréquemment retournés sont le **404** (page introuvable), le **403** (accès interdit) et le **401** (accès non autorisé). Vous pourrez trouver une liste complète de ces codes sur le site www.indexa.fr.

La personnalisation de la page peut se présenter sous trois formes distinctes (cf. la [documentation de Apache](#)) :

- une URL locale vers laquelle la redirection sera effectuée
- une URL vers un serveur externe, vers lequel la redirection sera effectuée
- un message à afficher. Le message doit être précédé par des guillemets ("). Tout ce qui suit ces guillemets est affiché. Notez que le préfixe (") n'est pas affiché

Ainsi, pour rediriger l'erreur **404** de l'i-bay **toto** vers la page locale **/erreurs/404.html**, vous devrez taper :

```
db accounts setprop toto 404 /erreurs/404.html
signal-event ibay-modify toto
```

De la même façon, pour rediriger l'erreur **403** de l'i-bay **toto** vers l'URL **http://un_site.truc/403.php**, vous devrez taper :

```
db accounts setprop toto 403 http://un_site.truc/403.php
signal-event ibay-modify toto
```

Enfin, pour n'afficher qu'un simple texte (attention à bien respecter l'enchaînement guillemet simple, guillemet double, texte à afficher, guillemet double, guillemet simple) :

```
db accounts setprop toto 401 '"La requête nécessite une identification de
l'utilisateur."'
signal-event ibay-modify toto
```

Pour supprimer la personnalisation d'un message, il vous suffit de taper, par exemple :

```
db accounts delprop toto 401
signal-event ibay-modify toto
```

Il est possible d'utiliser la fonction 'd'url rewriting' d'apache a l'aide du module " mod_rewrite " et donc de bénéficier des fichiers .htaccess sou SME 7.x

Pour le module, il est chargé de base sur SME-SERVER 7.x, par contre les fichiers .htaccess ne sont pas pris en compte par défaut.

L'installation d'un rpm va permettre de débloquent la situation. Téléchargez le rpm [e-smith-htaccess](#) et placer le dans le répertoire root via winscp afin de l'installer sur votre serveur.

Installez le rpm :

```
rpm -Uvh e-smith-htaccess-1.1-2.noarch.rpm
```

A la fin de l'installation, une erreur vous sera signalée :

```
" Warning: template processing succeed for //etc/httpd/conf/httpd.conf : 1
frame at /sbin/e-smith/expand-template line 45 "
```

Votre serveur refusera de faire fonctionner apache, et votre site sera injoignable.

Nous allons corriger cette erreur due au fait que le RPM est conçu pour SME V6.5 et non V7.x.

Visualisez le fichier : vi /etc/e-smith/templates-custom/etc/httpd/conf/httpd.conf/90e-smithAccess40ibays

à la ligne n° 7 vous trouverez :

```
' tie %accounts, 'esmith::config', '/home/e-smith/accounts';'
```

qu'il faut remplacer par :

```
' tie %accounts, 'esmith::config', '/home/e-smith/db/accounts';'
```

Ensuite il faut faire prendre en compte les modifications effectuées :

```
/sbin/e-smith/expand-template /etc/httpd/conf/httpd.conf
```

Puis:

```
/etc/init.d/httpd reload
```

Voilà les fichiers .htaccess sont pris en compte

PHP Register Globals On ou OFF

Certains programme en php utilisent la variable Register Globals On ou OFF.

Au lieu de modifier PHP.ini, un simple :

```
db accounts setprop <VotreIbay> PHPRegisterGlobals enabled
```

```
signal-event ibay-modify <VotreIbay>
```

Vous pouvez déterminer l'utilisation de cette variable pour chaque Ibay.

Autoriser les scripts PHP à accéder à certains répertoires (important pour l'upload sous NPDS)

Par défaut, pour des raisons de sécurité, les scripts PHP situés dans les i-bays, y compris le Primary, ne peuvent accéder qu'à des fichiers contenus dans cette i-bay (en cas de tentative d'accès à une partie non autorisée de l'arborescence, Apache renverrait l'erreur "**Warning: open_basedir restriction in effect.**"). Or, pour certains scripts, il est nécessaire de pouvoir récupérer des infos ailleurs ; c'est le cas par exemple de [phpSysInfo](#) qui va chercher plusieurs éléments dans le répertoire /proc/.

Pour ce faire, il faut modifier la restriction **PHPBaseDir** de l'i-bay dans la configuration du serveur.

Si l'on reprend notre exemple de phpSysInfo, en imaginant qu'il soit situé dans l'i-bay toto (c'est original, hein...), il faudrait taper les lignes suivantes dans un terminal, en tant que root :

```
db accounts setprop toto PHPBaseDir /home/e-smith/files/ibays/toto/./proc/  
signal-event ibay-modify toto
```

On voit sur la première ligne les différents chemins, séparés par le signe deux-points ":", accessibles par les scripts PHP de l'i-bay (l'i-bay elle-même et **/proc/**).

Autre exemple : si une i-bay avait juste besoin d'accéder aux autres i-bays, il suffirait alors d'indiquer **/home/e-smith/files/ibays/** comme **PHPBaseDir**.

Attention, si vous autorisez l'accès au chemin **/rep**, cela donnera accès aux répertoires **/rep1/** et **/rep2/** (en supposant qu'ils existent, bien entendu).

De ce fait, si vous souhaitez restreindre l'accès à un répertoire spécifique, ajoutez le slash final (par exemple : **/rep1/**).

On pourrait également envisager de donner l'accès à l'ensemble de l'arborescence mais, comme je l'ai indiqué plus haut, cela constituerait un risque au niveau de la sécurité du serveur : imaginez un script mal conçu qui modifierait ou effacerait des fichiers essentiels au bon fonctionnement du système ! Certains pirates pourraient notamment exploiter des scripts mal sécurisés et modifier le système de fichier à leur guise...

Autoriser l'accès aux fichiers distants

Par défaut, pour des raisons de sécurité, le serveur n'autorise pas l'accès (fonctions **fopen** et apparentés, **include**, **require**, fonctions de manipulation d'images, etc.) aux fichiers distants via les protocoles HTTP et FTP, notamment.

Cependant, si vous avez besoin de cette fonctionnalité, vous pouvez l'activer de cette façon :

```
config setprop php AllowUrlFopen On  
signal-event console-save
```

Et, bien entendu, pour revenir à la configuration de départ, remplacez **On** par **Off**.

Modifier la taille des fichiers pouvant être envoyés sur le serveur

Par défaut, le serveur n'autorise les utilisateurs à lui envoyer que des fichiers d'au maximum 10 Mo et des formulaires de 20 Mo. Selon vos besoins, vous pouvez augmenter ou diminuer ces valeurs. Ceci est particulièrement intéressant si vous avez besoin d'envoyer des fichiers très volumineux via le webmail. Par exemple, pour pouvoir envoyer des fichiers d'au plus 50 Mo via des formulaires d'au plus 60 Mo, vous devrez taper :

```
config setprop php UploadMaxFileSize 50M
config setprop php PostMaxSize 60M
signal-event console-save
```

Cependant, l'envoi de fichiers très volumineux risque de créer un nouveau problème : par défaut, le serveur n'autorise l'exécution d'un script que pendant une durée de 30 secondes. De plus, la mémoire utilisable pour une opération est limitée à 32 Mo.

Pour augmenter ces valeurs (par exemple 10 minutes et 100 Mo), voici la marche à suivre :

```
config setprop php MaxExecutionTime 600
config setprop php MemoryLimit 100M
signal-event console-save
```

Attention tout de même à ne pas autoriser de valeurs trop importantes car votre serveur pourrait ne pas avoir les ressources suffisantes pour traiter vos requêtes. Vous risqueriez donc de nuire à sa stabilité.

A l'inverse, vous pouvez choisir de baisser les valeurs par défaut si votre configuration matérielle est limitée.

Limiter la taille des courriels pouvant être envoyés

Par défaut, vous pouvez envoyer des courriels sans aucune restriction de taille. Cependant, pour des raisons de restriction de bande passante, vous pouvez imposer une limite à la taille des messages envoyés via le serveur.

Ainsi, pour limiter la taille des courriels envoyés à 4 Mo, il vous suffit de taper :

```
config setprop qmail MaxMessageSize 4000000
signal-event email-update
```

Ajouter un disque dur pour stocker une ou plusieurs i-bay(s)

Au fil du temps, il arrive que la capacité de stockage du disque dur sur lequel vous avez installé SME devienne insuffisante. Nous allons donc voir une procédure permettant d'ajouter un nouveau disque dur pour stocker une ou plusieurs i-bays, voire même la totalité de **/home/** si vous le souhaitez.

Pour simplifier les choses, nous allons imaginer que sur le nouveau disque dur il n'y aura, au final, qu'une i-bay contenant par exemple des images ISO (nous l'appellerons **ibay_iso**) :

1. Avant tout, éteignez le serveur et montez le nouveau disque dur. On va dire qu'il est branché en esclave sur la nappe IDE primaire (donc, en **/dev/hdb**). Si vous branchez votre disque ailleurs (sur un autre connecteur ou bien même en SCSI), modifiez le device en fonction de

votre configuration

2. Démarrez votre serveur et ouvrez un shell avec le compte root
3. Il va maintenant falloir créer la partition nécessaire au stockage de notre i-bay. Nous allons pour cela utiliser l'utilitaire **fdisk** et ensuite taper **p** pour voir la table de partitions du disque (vous n'obtiendrez bien sûr pas les mêmes valeurs que celles indiquées ici) :

```
fdisk /dev/hdb

Le nombre de cylindres pour ce disque est initialisé à 1305.
Il n'y a rien d'incorrect avec cela, mais c'est plus grand que 1024,
et cela pourrait causer des problèmes en fonction pour certaines
configurations:
1) logiciels qui sont exécutés à l'amorçage (i.e., vieilles versions de
LILO)
2) logiciels d'amorçage et de partitionnement pour d'autres SE
   (i.e., DOS FDISK, OS/2 FDISK)

Commande (m pour l'aide): p

Disque /dev/hdb: 10.7 Go, 10737418240 octets
255 têtes, 63 secteurs/piste, 1305 cylindres
Unités = cylindres de 16065 * 512 = 8225280 octets

Périphérique Boot   Start      End      Blocks   Id  System
/dev/hdb1           *          1       1200     9638968+ 83  Linux
/dev/hdb3             1201     1305     843412+ 82  Linux swap
```

Dans le cas que j'expose ici, nous voyons que le disque dur a déjà été utilisé et qu'il possède deux partitions (**hdb1** et **hdb3**) que nous allons supprimer avant de créer les nouvelles :

```
Commande (m pour l'aide): d
Numéro de partition (1-4): 1

Commande (m pour l'aide): d
Partition sélectionnée 3
```

Vous pouvez vérifier avec la commande **p** qu'il n'existe plus la moindre partition sur le disque. Nous pouvons maintenant créer notre nouvelle partition (nous allons utiliser la totalité de l'espace, mais ce n'est pas obligatoire). Pour l'exemple, je vais créer une partition principale, mais rien n'empêche de créer une partition étendue avec un lecteur logique.

```
Commande (m pour l'aide): n
Action de commande
  e  étendue
  p  partition primaire (1-4)
p
Numéro de partition (1-4): 1
Premier cylindre (1-1305, default 1): 1
Dernier cylindre ou +taille or +tailleM ou +tailleK (1-1305, default
1305): 1305
```

Là encore, vous pouvez vérifier avec la commande **p** que vos changements ont été correctement pris en compte. Pour les valider, il ne vous reste plus qu'à taper la commande **w** :

```
Commande (m pour l'aide): w
La table de partitions a été altérée!

Appel de ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

4. La partition étant créée, il nous faut maintenant la formater pour pouvoir copier ensuite des données dedans:

```
/sbin/mkfs.ext3 /dev/hdb1
mke2fs 1.35 (28-Feb-2004)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
368000 inodes, 734965 blocks
36748 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=754974720
23 block groups
32768 blocks per group, 32768 fragments per group
16000 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 36 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

5. Pour faciliter et automatiser le montage de cette partition au démarrage, nous allons devoir ajouter une entrée au fichier **/etc/fstab**. Vous devrez donc éditer ce fichier (avec votre éditeur favori : mcedit, vi, pico, nano, etc.) et y ajouter la ligne suivante :

```
/dev/hdb1 /home/e-smith/files/ibays/ibay_iso ext3 usrquota,grpquota
1 1
```

6. Si l'i-bay n'existe pas encore, créez-la dans le [gestionnaire du serveur](#)
7. Il faut maintenant monter la partition (dans un répertoire temporaire préalablement créé), recopier les données de l'i-bay existante dedans, la démonter, supprimer le répertoire utilisé pour le montage, supprimer le contenu de l'i-bay et monter la nouvelle partition dedans :

```
mkdir /mnt/tmp/
mount /dev/hdb1 /mnt/tmp/
rsync -arPv /home/e-smith/files/ibays/ibay_iso/ /mnt/tmp/
umount /dev/hdb1
rmdir /mnt/tmp/
rm -rf /home/e-smith/files/ibays/ibay_iso/*
mount /dev/hdb1
```

8. Enfin, il faut recréer les quotas sur le point de montage et mettre à jour l'i-bay :

```
quotacheck -cguv /home/e-smith/files/ibays/ibay_iso/
signal-event ibay-modify ibay_iso
```

Réutiliser un disque dur contenant une ou plusieurs i-bay(s)

Si vous avez suivi la première partie de cette page et que vous êtes un jour amené à refaire une installation totale de votre serveur, je vous propose cette méthode pour remettre votre disque en place :

Avant tout, n'oubliez surtout pas de **débrancher ce disque** avant de commencer la nouvelle installation ! Et dans tous les cas, **sauvegardez vos données** avant de vous lancer dans ce genre d'opération !

Pour automatiser le montage de cette partition au démarrage, il faut ajouter une entrée au fichier **/etc/fstab**. Vous devez donc éditer ce fichier (avec votre éditeur favori : mcedit, vi, pico, nano, etc.) et y ajouter la ligne suivante (adaptez-la en fonction de votre device et du point de montage) :

```
/dev/hdb1 /home/e-smith/files/ibays/ibay_iso ext3 usrquota,grpquota
1 1
```

- Si votre partition ne contient qu'une seule i-bay, vous devez créer cette i-bay avec le [gestionnaire du serveur](#) **avant** de monter la partition dans le répertoire de l'i-bay
- Si votre partition contient l'ensemble des i-bays (répertoire **/home/e-smith/files/ibays/**), vous pouvez la monter avant de recréer chaque i-bay dans le [gestionnaire du serveur](#)

Rappel : pour monter la partition il vous suffit de taper :

```
mount /dev/hdb1
```

Supprimer les alertes de rkhunter concernant l'accès SSH par root

Comme vous pouvez vous en douter, autoriser l'accès au serveur via SSH par root constitue un risque. C'est pourquoi [rkhunter](#), chargé toutes les nuits de vérifier sommairement la sécurité du serveur, vous informe de ce risque par un mail au titre peu évocateur : **Cron run-parts /etc/cron.daily**.

On peut donc y lire **Warning: root login possible. Change for your safety the 'PermitRootLogin'**. Vous avez alors deux possibilités pour supprimer ce message :

- la solution la plus sécurisante, consistant à désactiver l'option **Autoriser l'administrateur à se connecter au serveur par SSH** dans la page [Accès à distance](#) du gestionnaire du serveur. Mais ceci impose bien entendu de pouvoir se loguer avec un autre compte pour administrer le serveur via SSH
- la solution la plus simple consiste, elle, à supprimer cette alerte depuis le fichier de configuration de rkhunter. Pour cela, vous devez éditer ce fichier **/etc/rkhunter.conf** avec votre éditeur préféré (mcedit, vi, pico, nano, etc.), décommenter et modifier la ligne suivante :

```
vi /etc/rkhunter.conf  
ALLOW_SSH_ROOT_USER=yes
```

Comme ce fichier n'est pas "templatisé", cette seule modification suffit.

Imagemagick

Installer une version plus récente de imagemagick sur SME version 3.4 nécessaire pour gallery 2

```
yum install --enablerepo=* libjpeg libjpeg-devel libpng-devel libpng libpng10  
lib-bzlib libtiff libtiff-devel libwmf libwmf-devel libj2c libj2c-devel
```

Téléchargez le .tgz et envoyez décompresser le sur le serveur.

- configure
- make
- make install

GANDI

Domaine principal du SME

Prerequis:

1. un serveur SME
2. un nom de domaine chez Gandi
3. une connection internet avec IP fixe

How-to:

1- laissez gérer les DNS par les serveurs gandi.net

2- dans "Gérer les zones" définir une zone de champs personnalisée : "mode expert"

3- y insérer ceci (a personnaliser en fonction de votre nom de domaine (ici exemple : domaine.tld, et IP fixe IP.IP.IP.IP)

```
* 3600 IN CNAME domaine.tld
@ 3600 IN A IP.IP.IP.IP
@ 3600 IN MX 20 www.domaine.tld
www 3600 IN A IP.IP.IP.IP
mail 3600 IN A IP.IP.IP.IP
ftp 3600 IN A IP.IP.IP.IP
```

4- une fois validé, attendre que les informations soient propagées vers les serveurs dns de la planète (entre 1 heure et 48 heures)...

Domaine virtuel

même chose si ce n'est que vous devez en plus passer par la case server-manager:

1. créer une ibay pour recevoir le nom de domaine
2. dans domaines, ajouter un domaine virtuel en précisant l'ibay utilisée et DNS de l'internet pour la résolution .

Allowoverride sur une ibay

Obligatoire pour le rewriting, voici les commande pour l'activer pour une ibay :

```
db accounts setprop monibay AllowOverride all
signal-event ibay-modify monibay
```

Rewriting et .htaccess

Nous allons tout d'abord installer un rpm nommé e-smith-htaccess-1.1-2.noarch.rpm

```
wget http://www.lyc-estaque.ac-aix-marseille.fr/web/IMG/rpm/e-smith-htaccess-1.1-2.noarch.rpm
yum localinstall e-smith-htaccess
```

Ne vous inquiétez pas si votre serveur refuse de faire fonctionner Apache, et que votre site est injoignable. Pas de panique, nous allons corriger cette erreur due au fait que ce rpm est à la base conçu pour fonctionner avec sme-server v6.5 et non 7.x.

```
'WARNING: Template processing succeeded for //etc/httpd/conf/httpd.conf: 1
fragme
at /sbin/e-smith/expand-template line 45'
```

Allez modifier le fichier suivant à l'aide de la commande :

```
vi /etc/e-smith/templates-custom/etc/httpd/conf/httpd.conf/90e-
smithAccess40ibays
```

A la ligne n°7, vous devez trouver ceci :

```
' tie %accounts, 'esmith::config', '/home/e-smith/accounts'; '
```

qu'il faut remplacer par cela :

```
' tie %accounts, 'esmith::config', '/home/e-smith/db/accounts'; '
```

Ensuite, relancez apache avec les commandes suivantes :

```
/sbin/e-smith/expand-template /etc/httpd/conf/httpd.conf
/etc/init.d/httpd reload
```

Pour finir, si votre .htaccess ne vous laisse pas accéder à vos page, insérer **Options +FollowSymlinks** avant l'option **RewriteEngine on**.

```
db accounts setprop ibayname FollowSymLinks enabled
db accounts setprop ibayname AllowOverride ALL
signal-event ibay-modify ibayname
/etc/init.d/httpd reload
```

Normalement ça suffit pour la plupart des scripts, mais Wordpress réécrit constamment son fichier .htaccess quand on utilise les permalinks. Il faut alors créer un template pour l'ibay contenant

Wordpress.

Donc, vous allez, à l'aide de Winscp, créer un template dans le répertoire /etc/e-smith/templates-custom/etc/httpd/conf/httpd.conf nommé 92Rewrite, contenant le code suivant (**attention, adaptez le au path de votre ibay**). N'oubliez pas de laissez une ligne d'espace à la fin sinon vous allez bugger votre httpd.conf !!!!

```
<Directory /home/e-smith/files/ibays/hlg/html>
  Options +FollowSymLinks
  AllowOverride All
  order deny,allow
  deny from all
  allow from all
</Directory>
```

Sauvegardez le fichier et quitter l'éditeur. Rendez-vous dans putty en root et entrez les deux lignes de commandes suivantes :

```
/sbin/e-smith/expand-template /etc/httpd/conf/httpd.conf
/etc/init.d/httpd-e-smith restart
```

Retournez chmoder vos répertoires et vos fichiers dans votre ibay.

InnoDB et Mysql (pour Dotclear)

Si vous décidez d'installer Dotclear sur votre SME vous risquez de vous retrouver avec une erreur à l'installation vous affichant que InnoDB n'est pas actif. Pour ce faire, il vous suffit de l'activer à l'aide des commandes suivantes (merci Nicolas2).

```
config setprop mysqld InnoDB enabled
expand-template /etc/my.cnf
service mysqld restart
```

Vous pouvez désormais installer Dotclear avec cette option activée.

Configuration avancée du serveur FTP

Pour l'instant il n'existe qu'un tutorial en anglais qui est recollé ici (car il n'existe plus qu'un site en cache pour cette contribution de sme6 qui fonctionne parfaitement sous sme7.4).

```
wget http://www.eelriver.com/sme/sme-7.0/e-smith-ftp-manager-0.4-3.noarch.rpm
yum localinstall e-smith-ftp-manager-0.4-3.noarch.rpm
```

STEP 1:

e-smith-ftp-manager Panel :

This pannel shows you the ftp configuration of your SME Box :

Name : iBay's name.

Brief description : iBay's descriptions.

Upload Bandwidth (Kb/s) : Upload speed limit.

Download Bandwidth (Kb/s) : Download speed limit.

Upload Resume : Resuming in upload.

Download Resume : Resuming in download.

Guest : Link to modify guest user or group (usefull with a limited bandwidth)

FTP : Link to modify FTP configuration.

STEP 2:

e-smith-ftp-manager Modify proFTPD configuration in iBays Panel :

On this pannel you can change configurations of:

Information bay name: Ibay's name, you can't change this.

Group: Ownership of the i-bay content is assigned to an existing group. The group ownership plays a role in the next setting for user access.

User access via file sharing or user ftp: You need to decide who will be able to add and modify content in the i-bay and who will be able to read the content.

Public access via web or anonymous ftp: Here you set what type of public access you wish to have for the i-bay. If the i-bay is just to be used by a small group of users, you can leave public access set to the default of None. If you want others to be able to access the i-bay via web or anonymous ftp, you can choose to allow access to just the local network or the wider Internet. You also can choose whether or not you wish to require a password.

Maximum FTP connections: Set how many anonymous users can be connected at a same time on your FTP (default SME value: 10).

FTP Upload Limit (Kb/s): Set upload bandwidth limitation (in Kb/s). To have an unlimited bandwidth, enter "no".

FTP Download Limit (Kb/s): Set download bandwidth limitation (in Kb/s). To have an unlimited bandwidth, enter "no".

Allow Resume Upload: This checkbox enable/disable resume on upload (default SME value: disable).

Allow Resume Download: This checkbox enable/disable resume on download. (default SME value: enable).

STEP 3:

e-smith-ftp-manager Guest Panel :

This panel allows you to choose which users or group will have an unlimited FTP bandwidth.

It's usefull when you, administrator, want to up/download a file in this iBay. And if this iBay has a limited bandwidth of 15Kb/s, it will be a long job.

So you can choose, who can have an unlimited bandwidth for accessing this iBay. You must choose between a user OR a group, not twice (because all users are in this group).

STEP 4:

e-smith-ftp-manager General Panel :

(since 0.4-1)

By default, i disable this panel. Because, according to my mind, this kind of

configuration is for advanced users. Peoples who know what they do.

To see this pannel execute following command line :

```
[ root@e-smith root ] # /sbin/e-smith/db ftp set proftpd global_conf  
AdvancedPanel 1
```

Now in first panel you may see a new link :

Click here to modify general proftpd configurations.

In this new Panel you can modify following configurations:

change port : Here you can change proftpd listening port. WARNING:You change this at your own risk!

change server name : Here you can change server name.

change admin mail : Here you can change admin mail

If you change port, don't forget to modify Xinetd (thanks to MasterSleepy).

Modify /etc/services file:

```
# mkdir -p /etc/e-smith/templates-custom/etc/services/
```

```
# cp /etc/e-smith/templates/etc/services/10standard /etc/e-smith/templates-  
custom/etc/services/10standard
```

```
# vi /etc/e-smith/templates-custom/etc/services/10standard
```

Modify "21" value by new port value in line:

```
ftp 21/tcp
```

Save and expand templates :

```
# /sbin/e-smith/expand-template /etc/services
```

STEP 5:

When saving configurations, changes will be applied after all users logoff.

Files in this contrib :

Panels :

```
/root/etc/e-smith/web/functions/proftpd
```

Templates :

```
/root/etc/e-smith/templates-custom/etc/proftpd.conf/05port
```

```
/root/etc/e-smith/templates-custom/etc/proftpd.conf/05ServerAdmin
```

```
/root/etc/e-smith/templates-custom/etc/proftpd.conf/05ServerName
```

```
/root/etc/e-smith/templates-custom/etc/proftpd.conf/40IBayAccess
```

```
/root/etc/e-smith/templates-custom/etc/proftpd.conf/60AnonymousIBay
```

Events :

```
/root/etc/e-smith/events/proftpdconf-modify/S00proftpd-conf
```

PERL Functions :

```
/root/usr/lib/perl5/site_perl/esmith/FtpDB.pm
```

```
/root/usr/lib/perl5/site_perl/esmith/FormMagick/Panel/proftpd.pm
```

Created db file :

```
/home/e-smith/ftp
```

Netographie