

Jean-Louis Cech
Systems Architecture/Integration/Maintenance

Cell : +33659 714 837
Office : +33169 015 849
jean-louis.cech@laposte.net

Serveur Mesnil Administration

Rédacteur : Jean-Louis Cech

Date création : 5 Novembre 2009

Mise à jour : 30 Octobre 2010

SERVEUR MESNIL DEBIAN 5

DELL PRECISION WS 420 MT

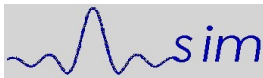
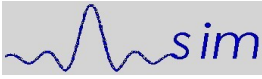


Table des matières

Introduction.....	4
Inventaire matériel du serveur.....	4
Installation du logiciel d'inventaire.....	4
Disques durs.....	4
Inventaire des disques installés.....	4
Disque dur HDA.....	4
Disque dur HDB.....	4
Disque SCSI n°1.....	5
Disque SCSI n°2.....	5
Affectation des partitions.....	5
Installation DEBIAN 5.....	6
Réseau.....	6
Installation des Applications et Services.....	6
Recherche d'un paquet à installer.....	7
Installation du paquet.....	8
Erreur de sélection d'un paquet.....	8
Inventaire logiciel serveur.....	8
Sauvegardes - Récupérations.....	9
Sauvegardes.....	9
Sauvegardes quotidiennes - Particularités.....	9
Sauvegardes hebdomadaires - Particularités.....	9
Récupération des données.....	10
Serveur de Domaine Windows-Samba.....	10
Gestion des comptes utilisateurs / machines.....	11
Gestion des utilisateurs.....	11
Gestion des machines du domaine.....	11
Serveur FTP.....	12
FTP Paramétrage.....	12
FTP restrictions MS Internet Explorer.....	12
FTP Administration.....	12
Serveurs WEB.....	12
Serveur WEB classique.....	13
Serveur courriel entrant (POP).....	13
Serveur de courriel sortant (SMTP).....	13
Sécurisation des serveurs.....	13
Fail2ban - Installation.....	13
Fail2ban - paramétrage.....	13
/etc/fail2ban/fail2ban.conf.....	13
/etc/fail2ban/jail.conf.....	13
/etc/fail2ban/filter.d/[filtre du log du service].....	13
Mise en oeuvre de fail2ban.....	14
Exemple de service actif [SSH].....	14
Activation de la supervision de vsftpd.....	14
Activation de la supervision WEB [apache2].....	14
Relancer fail2ban.....	15
Test de validité des paramètres de « Bannissement ».....	15
Log des bannissements.....	16
Annexes.....	17
Annexe 1 Fournisseur accès Internet.....	17
Annexe 2 Enregistrement domaine.....	17
Annexe 3 Configuration matérielle.....	17
Annexe 4 Gestion des postes de travail côté serveur.....	18
Annexe 5 Samba - Fichier de configuration.....	19



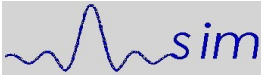
Jean-Louis Cech

Systems Architecture/Integration/Maintenance

Cell : +33659 714 837

Office : +33169 015 849

jean-louis.cech@laposte.net



Introduction

Le présent document a pour objet l'assistance à la maintenance et à l'administration du serveur Mesnil, il ne constitue pas un document de formation, celle-ci est pré requise tant pour LINUX que pour Windows.

Inventaire matériel du serveur

Le serveur est un ancien poste de travail Dell. Sa composition matérielle est fournie en annexe, cet inventaire est fourni par un logiciel qui sera installé une fois la machine fonctionnelle.

Installation du logiciel d'inventaire

En annexe 3 est décrite la procédure d'installation et d'exécution du logiciel.

Disques durs

La machine embarque deux disques durs IDE repérés par :

```
/dev/hda  
/dev/hdb
```

de taille respective de 40 et 500 giga octets.

Ces disques sont connectés à la carte mère par l'interface IDE0, l'interface IDE1 est réservée aux deux lecteurs graveurs de CD/DVD.

Afin de garantir un niveau de performances élevé, il a été installé deux disques SCSI 3 de 73 Go. Ces deux disques, au moins dans un premier temps, n'assurent aucune redondance, en RAID 0, ils sont repérés par :

```
/dev/sda  
/dev/sdb
```

Leurs adresses physiques sur le bus sont respectivement 1 et 2, ces adresses sont fixées par des cavaliers placés sur la carte interface placée sur les connecteurs des disques.

Inventaire des disques installés

Les disques installés dans le système sont initialisées par la commande « fdisk », toutefois cette initialisation est prise en charge lors de l'installation en ce qui concerne les disques actifs du système installé. La description des disques est donné à titre indicatif.

La description des disques est donnée par la commande suivante qui est disponible sur les distributions « Live » ou les systèmes installés :

```
/sbin/fdisk /dev/ « identifiant disque »
```

Disque dur HDA

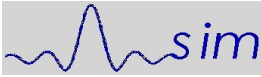
Ce disque contient Windows XP, il porte aussi le secteur MBR qui contient les informations nécessaires en particulier au « Multi-Boot ».

```
Disk /dev/hda: 40.0 GB, 40020664320 bytes  
255 heads, 63 sectors/track, 4865 cylinders  
Units = cylinders of 16065 * 512 = 8225280 bytes  
Disk identifier: 0x10ba10b9
```

Device	Boot	Start	End	Blocks	Id	System
/dev/hda1	*	1	4864	39070048+	7	HPFS/NTFS

Disque dur HDB

Ce disque sert aux sauvegardes, son usage est explicité plus bas.



Disk /dev/hdb: 500.1 GB, 500107862016 bytes
255 heads, 63 sectors/track, 60801 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x4b3a74a3

Device	Boot	Start	End	Blocks	Id	System
/dev/hdb1	*	1	60801	488384001	83	Linux

Disque SCSI n°1

Ce disque porte le système d'exploitation.

Disk /dev/sda: 72.8 GB, 72839168000 bytes
255 heads, 63 sectors/track, 8855 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x0001ecf1

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1	486	3903763+	83	Linux
/dev/sda2		487	3404	23438835	83	Linux
/dev/sda3		3405	3890	3903795	82	Linux swap / Solaris
/dev/sda4		3891	8855	39881362+	83	Linux

Disque SCSI n°2

Disque pour usages divers, sa partition n'est pas figée, elle sera modifiée en fonction des besoins. Ce disque porte le système d'exploitation.

Disk /dev/sdb: 72.8 GB, 72839168000 bytes
255 heads, 63 sectors/track, 8855 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xc7e1a79f

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1	*	1	512	4112608+	83	Linux
/dev/sdb2		513	3430	23438835	83	Linux
/dev/sdb3		3431	3916	3903795	82	Linux swap / Solaris
/dev/sdb4		3917	8855	39672517+	83	Linux

Affectation des partitions

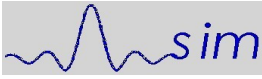
Les partitions sont affectées afin de pouvoir exécuter une réinstallation du serveur sans perdre les données de travail. De plus un protocole de sauvegarde utilise une partition dédiée située sur un disque dur autonome.

En fonctionnement normal les partitions sont affectées comme suit :

```
cat /etc/mtab
/dev/sdb2 / ext3 rw,errors=remount-ro 0 0
tmpfs /lib/init/rw tmpfs rw,nosuid,mode=0755 0 0
proc /proc proc rw,noexec,nosuid,nodev 0 0
sysfs /sys sysfs rw,noexec,nosuid,nodev 0 0
procbususb /proc/bus/usb usbfs rw 0 0
udev /dev tmpfs rw,mode=0755 0 0
tmpfs /dev/shm tmpfs rw,nosuid,nodev 0 0
devpts /dev/pts devpts rw,noexec,nosuid,gid=5,mode=620 0 0
/dev/sdb1 /boot ext3 rw 0 0
/dev/sdb4 /home ext3 rw 0 0
rpc_pipefs /var/lib/nfs/rpc_pipefs rpc_pipefs rw 0 0
nfsd /proc/fs/nfsd nfsd rw 0 0
```

Partition - Taille	Point de Montage	Affectation
/dev/sda/		
Sda1 - 4 Go	/boot	Fichiers pour amorcer
sda2 - 24 Go	/	Partition système
sda3 - 4 Go	SWAP	
hda4 - 40 G	/home	Données utilisateurs

IMPORTANT :



Lors d'une **réinstallation** il ne faut pas formater la partition /home

Installation DEBIAN 5

DEBIAN fournit l'ensemble des fichiers utiles pour son installation. Plusieurs solutions sont possibles, la plus simple consiste à réaliser une installation réseau à partir d'une image ISO récupérée sur le site.

Pour cet ordinateur l'installation en fenêtre graphique est simple, directe, les paramètres de GRUB sont automatiques et ne nécessitent aucune adaptation.

Réseau

Le serveur est équipé de deux interfaces réseau, il n'assure pas l'interface avec le WAN, à savoir le routage, cette fonction relève du Modem-Routeur livré par le FAI.

Les deux interfaces sont identifiées par eth0 et eth1, la première est celle implantée sur la carte mère, la seconde a été ajoutée dans un connecteur PCI. Cette dernière n'est pas utilisée pour les fonctions standard de connexion au réseau local, elle sera affectée ultérieurement.

Adresse LAN de eth0 : 192.168.22

```
dell:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:b0:d0:3e:93:3f
          inet addr:192.168.1.22  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::2b0:d0ff:fe3e:933f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:91613 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88972 errors:0 dropped:0 overruns:0 carrier:0
          collisions:4420 txqueuelen:1000
          RX bytes:15918355 (15.1 MiB)  TX bytes:68059450 (64.9 MiB)
          Interrupt:16 Base address:0xc00

eth1      Link encap:Ethernet  HWaddr 00:50:fc:46:a6:42
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:17 Base address:0xdc00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:593 errors:0 dropped:0 overruns:0 frame:0
          TX packets:593 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:758950 (741.1 KiB)  TX bytes:758950 (741.1 KiB)
```

Remarque Octobre 2010 :

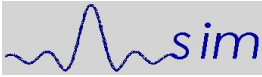
- L'affectation des adresses réseau par Bouygues est particulièrement peu conviviale, il convient de se reporter à paragraphe spécifique sur ce sujet.

Installation des Applications et Services

Debian offre deux modes d'installation des applications et services :

- le mode graphique via un applicatif semblable à tous ceux trouvés dans les autres distributions. Ce procédé reste intuitif mais il est peu souple.
- Le mode commande en s'appuyant sur le site :
<http://packages.debian.org/stable/>

L'installation se déroule en deux phases :



1. Recherche sur le site Debian du paquet à installer
2. Installation du paquet proprement dit.

Recherche d'un paquet à installer

On souhaite installer un compilateur Fortran. Via un moteur de recherche poser la requête suivante : lenny fortran

✕
Rechercher
Recherche

Environ 31 100 résultats (0,13 secondes)
Recherche avancée

▶ [Debian User Forums • View topic - fortran compiler on debian lenny](#) ☆ - [Traduire cette page]
6 messages - 4 auteurs - Dernier message : 29 juin 2008
i have a lenny desktop system, but i cant find anywhere the gnu fortran compiler.. does anyone know anything? ...
[forums.debian.net/viewtopic.php?t=27597](#) - En cache - Pages similaires

[Debian -- Details of package fortran-compiler in lenny](#) ☆ - [Traduire cette page]
Debian >> Packages >> lenny (stable) >> virtual >> fortran-compiler ... Virtual Package: fortran-compiler. This is a virtual package. ...
[packages.debian.org/lenny/fortran-compiler](#) - En cache

[Debian -- Détails du paquet source gcc-4.3 dans lenny](#) ☆
[lenny] [lenny-backports] [squeeze] [sid] ... gfortran-4.3: The GNU ...
[packages.debian.org/fr/source/lenny/gcc-4.3](#) - En cache

[Debian -- Détails du paquet source gcc-4.2 dans lenny](#) ☆
Debian >> Paquets >> lenny (stable) >> Source >> devel >> gcc-4.2 ...
[packages.debian.org/.../lenny/gcc-4.2](#) - En cache - Pages similaires

[Debian -- Détails du paquet gfortran-4.3 dans lenny](#) ☆
This is the GNU Fortran compiler, which compiles Fortran 95 on platforms ...
[packages.debian.org/fr/lenny/gfortran-4.3](#) - En cache

[+ Plus de résultats de debian.org](#)

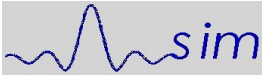
Parmi les réponses suivantes sélectionner :

packages.debian.org/lenny/fortran-compiler

The screenshot shows the Debian website page for the virtual package `fortran-compiler` in the `lenny` distribution. The page title is "Paquet virtuel : fortran-compiler". It includes a search bar, navigation links for other distributions (squeeze, sid, experimental), and a list of packages providing the compiler, with `gfortran` being the primary one. The page also contains a footer with contact information and a copyright notice.

Le paquet à installer se nomme **gfortran**

L'invocation de ce paquet dans le paragraphe suivant résout les dépendances requises.



Installation du paquet

Dans une fenêtre « Terminal », en disposant des droits d'administration, lancer la commande suivante et observer le déroulé :

```
dell:~# apt-get install gfortran
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  gfortran-multilib gfortran-doc
The following NEW packages will be installed:
  gfortran
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1124B of archives.
After this operation, 41.0kB of additional disk space will be used.
Get:1 http://ftp.u-strasbg.fr lenny/main gfortran 4:4.3.2-2 [1124B]
Fetched 1124B in 0s (4543B/s)
Selecting previously deselected package gfortran.
(Reading database ... 156609 files and directories currently installed.)
Unpacking gfortran (from ../gfortran_4%3a4.3.2-2_i386.deb) ...
Processing triggers for man-db ...
Setting up gfortran (4:4.3.2-2) ...
```

Le compilateur Fortran est disponible, il reste à le tester.

Créer le programme test.f, le compiler et l'exécuter.

```
jlc@dell:~/agl/fortran$ cat test.f

c      Programme de test du compilateur Fortran
c      integer*2 kl

c      do 100 kl=10, 15, 3
c         print 1, kl
100    continue

c      stop 123
1      format (i4)
c      end
```

Lancer la compilation

```
jlc@dell:~/agl/fortran$ gfortran test.f
```

Lancer l'exécutable

```
jlc@dell:~/agl/fortran$ ./a.out
10
13
STOP 123
```

Cette procédure d'installation se répète pour chaque service à installer.

Erreur de sélection d'un paquet

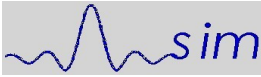
Dans le pire des cas, la tentative d'installation d'un service déjà en place donne l'erreur suivante :

```
dell:~# apt-get install gfortran
Reading package lists... Done
Building dependency tree
Reading state information... Done
gfortran is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Inventaire logiciel serveur

La version du système d'exploitation est la Debian 5.

Le tableau ci-dessous récapitule des fonctions logicielles activées.



Fonction réalisée	Logiciel installé
Serveur WEB sur port 80	Apache
Serveur FTP	VSFTP
Bureautique	Open Office
Serveur de Domaine Windows	SAMBA
Serveur d'impression	CUPS
Serveur de bases de données	MySQL
Serveur de sauvegarde	Script spécifique

Sauvegardes – Récupérations

La fonction est assurée par un script spécifique « /root/admin/backup ». Il est lancé soit automatiquement par le gestionnaire des tâches programmées, crontab, soit à la demande en commande clavier.

Les temps de traitement sont évalués à une heure de traitement par tranche de cinq Giga octets de données traitées depuis le répertoire /home.

Les temps de sauvegarde ou restauration sont sensiblement équivalents.

Sauvegardes

La sauvegarde ne concerne que le répertoire /home car tous les autres répertoires sont par définition issus de l'installation ou de la vie propre du système. Toutefois certains fichiers systèmes spécifiques feront l'objet d'un traitement particulier car ils sont paramétrés de façon spécifique, parmi ceux-ci on trouve les fichiers de configuration des serveurs, les scripts...

La sauvegarde se déroule en cinq étapes :

1. Montage de la partition /dev/hdb1 sur /mnt/bu
2. Copie des différents fichiers spécifiques vers un répertoire sous /home
3. Exécution de la commande « tar -cvvf DEST SOURCE » Cette commande crée en sortie deux fichiers, l'un contient les données, l'autre contient la liste des noms des fichiers sauvegardés.
4. L'ensemble est zippé et archivé dans le répertoire « daily » ou « weekly » pour les sauvegardes quotidiennes et hebdomadaires respectivement.
5. Démontage de la partition de sauvegarde.

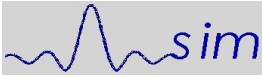
Sauvegardes quotidiennes – Particularités

Les fichiers issus des sauvegardes quotidiennes sont repérés par un préfixe sur un chiffre qui indique le numéro UNIX du jour de la sauvegarde. Dans ce cas le Dimanche vaut « 0 », le Lundi « 1 » jusqu'au Samedi qui vaut « 6 ».

A titre d'exemple, le fichier de données issu de la sauvegarde du Jeudi est nommé : « 4.tar.gz », le fichier index contenant la liste des fichiers sauvegardés est nommé : « 4.file.log.gz ». De ce fait, la sauvegarde du Lundi écrase celle du Lundi précédent.

Sauvegardes hebdomadaires - Particularités

En ce qui concerne les sauvegardes hebdomadaires, la méthode d'attribution



directe de préfixe circulaire est impossible, une autre règle est appliquée en calculant le modulo du numéro de la semaine par le nombre de semaines de recul que l'on souhaite maintenir. Cette valeur est inscrite en dur dans le script dans la variable CYCLE.

Les sauvegardes hebdomadaires sont archivées dans le répertoire « weekly », elles sont issues de la sauvegarde du Lundi.

Récupération des données

La récupération des données est une opération strictement manuelle, elle est décrite ci-dessous, chaque étape doit être respectée, sa durée est proportionnelle à la taille des fichiers archives, il faut savoir être patient.

Attention, ici le préfixe 4 fait référence à la sauvegarde du Jeudi, il est fourni à titre d'exemple.

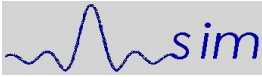
1. Se logger en administrateur/
2. Monter la partition archive
mount /dev/hdb1/ /mnt/bu
3. Vider le répertoire temporaire de tous les fichiers
rm -Rf /mnt/bu/tmp/*
4. Copier les fichiers archives contenant les données à récupérer dans le répertoire temporaire vidé précédemment, par exemple ici on récupère la sauvegarde réalisée le Jeudi précédant
cp /mnt/bu/daily/4* /mnt/bu/tmp/
5. Vérifier la présence dans le répertoire de travail la présence des fichiers archives
ls -l /mnt/bu/tmp
6. Lancer la décompression des fichiers archives, une fois la commande terminée l'extension .gz a disparu,
gunzip /mnt/bu/tmp/*
7. Lancer la décompression du fichier archive par les deux commandes suivantes
**cd /mnt/bu/tmp/
tar -xvzf 4.tar**
8. A ce niveau l'ensemble de l'arborescence du répertoire /home est disponible, il reste à restituer les informations par une commande de copie.
9. Vider le répertoire de travail
rm -Rf /mnt/bu/tmp/*
10. Démontez la partition archive
**cd /root
umount /mnt/bu/**

Serveur de Domaine Windows-Samba

Le serveur agit comme serveur de domaine. Le fichier de configuration est fourni en annexe.

Lors l'initialisation du serveur, il est important de créer un compte d'administration sous SAMBA. Pour faire simple il est recommandé de le créer sous « root » en passant la commande suivante :

```
/usr/bin/passwd -a root
```



Cette commande ajoute « root » aux administrateurs visibles depuis Windows. Toutefois le mot de passe de ce compte « root » pour Linux et Windows pourra différer. Ce compte et mot de passe seront à utiliser lors de l'intégration d'un poste de travail dans le domaine.

ATTENTION : L'utilisation de chiffres dans le nom du domaine, par exemple « WRKSP2 » génère des incompatibilités, il faut impérativement utiliser un nom de domaine en alphabétique seul, par exemple « WRKSPTWO ».

Gestion des comptes utilisateurs / machines

Le serveur gère deux type d'utilisateurs,

1. les utilisateurs des postes de travail Windows connectés au domaine,
2. les postes de travail intégrés dans le domaine.

Gestion des utilisateurs

Les utilisateurs sont gérés par un applicatif GUI (Graphical User Interface) soit plus simplement à la main via la commande **useradd**. Une entrée est créée dans **/etc/passwd** avec les droits issus de cette commande. A cette phase ils sont inconnus de SAMBA et doivent être déclarés. Il faut passer par utilisateur UNIX existant la commande :

```
smbpasswd -a [nom_utilisateur]
```

Cette commande fixe aussi le mot de passe de l'utilisateur dans le domaine, ce mot de passe est libre et n'a à priori aucun lien avec le mot de passe sur le compte UNIX.

Pour l'utilisateur jlc les deux entrées respectives sont :

```
dell:~/admin# cat /etc/passwd | grep jlc  
jlc:x:1000:100:Jean-Louis Cech,,,:/home/jlc:/bin/bash
```

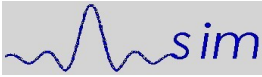
```
dell:~/admin# cat /etc/samba/smbpasswd | grep jlc  
jlc:1000:XXXXXXXXXXXXXXXXXXXXX:18CC6BA7C872C73B957AB084CEF20A88:[U]:LCT-4CCD21AA:
```

ATTENTION : l'affectation automatique de l'ID des utilisateurs débute à 1000 dans la DEBIAN alors que dans d'autres versions, FEDORA par exemple, elle débute à 500. En cas de repiquage de l'arborescence /home il faudra faire attention à la réaffectation des répertoires utilisateurs.

Gestion des machines du domaine

L'insertion d'une machine dans le domaine se déroule en trois étapes :

- Paramétrer le poste de travail Windows pour qu'il puisse intégrer le domaine. Un exemple de séquence est donné en annexe.
- Créer le compte de cette machine dans le serveur au moyen du script **deviceadd** en fournissant en paramètre le nom de la machine dont le compte doit être créé. Ce script automatise cette fonction, son code est fourni en annexe.
- Finaliser l'intégration ddu poste de travail Windows ans le domaine en se connectant une première fois.



Serveur FTP

FTP Paramétrage

Le serveur FTP active vsftpd (Very Safe FTP) qui est réputé fiable, simple à paramétrer. Son fichier de paramétrage **/etc/vsftpd.conf** est fourni ci dessous.

```
dell:~# cat /etc/vsftpd.conf
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=027
anon_upload_enable=YES
anon_mkdir_write_enable=YES
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
#chown_username=jlc
xferlog_file=/var/log/auth.log
syslog_enable=yes
#xferlog_file=/var/log/vsftpd.log
xferlog_std_format=YES
idle_session_timeout=600
async_abor_enable=YES
ftpd_banner=Welcome to JLC FTP service administred by Yavesh.
ls_recurse_enable=YES
local_root=/home/
anon_root=/home/commun/ftp/
pam_service_name=vsftpd
userlist_enable=NO
listen=YES
```

Il faut noter que pour des raisons de tranquillité, l'accès anonymous n'est pas autorisé.

Afin de centraliser la gestion des accès le fichier de « log » spécifié par la ligne « xferlog_file » centralise aussi les accès liés à SSH.

FTP restrictions MS Internet Explorer

Comme indiqué, il ne permet pas les connexions anonymes, de ce fait il est important de noter que la configuration par défaut du navigateur Internet Explorer ne permet pas les échanges, il faut impérativement **décocher** la ligne suivante :

Utiliser le mode FTP passif (compatibilité avec les pare-feu...)

On accède à cette ligne par

Outils -> Options Internet puis Onglet Avancé et descendre l'ascenseur jusqu'à la ligne FTP passif.

FTP Administration

Si vsftpd n'est pas actif il est possible de le lancer à la main par :

```
dell:~# /etc/init.d/vsftpd start
Starting FTP server: vsftpd.
```

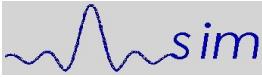
Le fichier de log spécifique est localisé dans :

```
/var/log/auth.log
```

il contient les transactions réalisées ainsi que les login incorrects.

Serveurs WEB

Une réservation de nom de domaine a été faite pour une durée de deux années auprès de Rapidomaine à compter du 9 Avril 2008. Les échanges de courriels se



font via
jl.cech@free.fr

Rapidomaine a été choisi pour des raisons de coût et de flexibilité du paramétrage.

En annexe on retrouve l'état de l'enregistrement du domaine et des redirections.

Serveur WEB classique

DEBIAN fournit un serveur Apache préconfiguré. Cette configuration diffère significativement de la configuration standard. On retrouve les fichiers de configuration dans `/etc/apache2/` à priori, ils sont laissés dans l'état de leur installation.

Les fichiers du serveur WEB sont installés dans `/var/www` .

Serveur courriel entrant (POP)

Non installé

Serveur de courriel sortant (SMTP)

Non installé

Sécurisation des serveurs

Cette machine est ouverte sur le WEB, elle est donc sujette à des attaques diverses. Au delà de la sécurité intrinsèque offerte par DEBIAN, il convient de se prémunir contre les attaques « Force Brute » qui tentent de trouver par des tentatives répétées un couple ID->PW. Afin de limiter les tentatives d'intrusion il a été installé l'appli « Fail2ban »

Fail2ban – Installation

Fail2ban fait partie des applicatifs validés par Debian, il s'installe simplement par la commande :

```
apt-get install fail2ban
```

Fail2ban – paramétrage

En standard, lors de son installation, fail2ban protège le serveur SSH contre les attaques. En revanche les tentatives d'intrusion FTP ou WEB ne sont pas activées.

/etc/fail2ban/fail2ban.conf

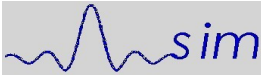
Ce fichier contient essentiellement la destination des actions de « bannissement ». Il n'est pas utile de le modifier.

/etc/fail2ban/jail.conf

Le fichier `/etc/fail2ban/jail.conf` contient les paramètres de fonctionnement du service. C'est dans ce fichier que sont paramétrées les actions à réaliser par service et en particulier où trouver les logs des services à surveiller.

/etc/fail2ban/filter.d/[filtre du log du service]

Les logs sont des chaînes de texte, leur identification relève de la gestion



d'expressions régulières. Ces expressions de filtrage se trouvent dans le répertoire `/etc/fail2ban/filter.d/[filtre du log du service]` .

Des filtres prédéfinis par service sont pré-installés, il convient de les vérifier et éventuellement les adapter.

Mise en oeuvre de fail2ban

Exemple de service actif [SSH]

Le paragraphe consacré à ssh est le suivant :

```
[ssh]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 6
```

- **enabled** prend deux valeurs possibles : `[true|false]`
- **port** fait référence au service que l'on retrouve dans `/etc/services`
- **filter** pointe le filtre à utiliser pour extraire du fichier de log les éléments pertinents
- **logpath** pointe le fichier qui contient les éléments de log à filtrer
- **maxretry** fixe le nombre de tentatives infructueuses avant bannissement.

Activation de la supervision de vsftpd

Modifier la section `[vsftpd]` de `jail.conf` comme suit :

```
[vsftpd]
enabled = true
port = ftp,ftp-data,ftps,ftps-data
filter = vsftpd
logpath = /var/log/auth.log
maxretry = 6
```

Vérifier que le service vsftpd dépose bien ses logs dans `/var/log/auth.log`

Activation de la supervision WEB [apache2]

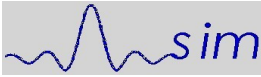
Un serveur WEB est souvent attaqué par des robots qui tentent de trouver des répertoires non publiés. Fail2ban permet de se protéger contre ces agressions. Le filtre est `/etc/fail2ban/filter/apache-noscript.conf`. Ce filtre est un peu trop étroit, il convient de l'élargir en créant un script semblable mais moins restrictif. Ce filtre est nommé ici **apache-depancech.conf**

Modifier la section `[apache]` de `jail.conf` comme suit :

```
[apache]
enabled = true
port = http,https
filter = apache-depancech
logpath = /var/log/apache2/error.log
maxretry = 6
```

Copier **apache-noscript.conf** dans **apache-depancech.conf** et le modifier comme suit :

```
dell:~# cat /etc/fail2ban/filter.d/apache-depancech.conf
# Fail2Ban configuration file
#
```



```
# Author: Cyril Jaquier
# Modif JL Cech pour coller à error.log 28 Oct 2010
#
# $Revision: 658 $
#

[Definition]

# Option: failregex
# Notes.: regex to match the password failure messages in the logfile. The
#         host must be matched by a group named "host". The tag "<HOST>" can
#         be used for standard IP/hostname matching and is only an alias for
#         (?:::f{4,6}:)?(?P<host>\S+)
# Values: TEXT
#
failregex = [[\client <HOST>[]] (File does not exist|not found or unable to stat)
            [[\client <HOST>[]] script '/\S*(\.\php|\.\asp|\.\exe|\.\pl)\S*' not found or unable
to stat *$

# Option: ignoreregex
# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
#
ignoreregex =
```

Relancer fail2ban

Relancer le service fail2ban par :

```
dell:~# /etc/init.d/fail2ban restart
Restarting authentication failure monitor: fail2ban.
```

Test de validité des paramètres de « Bannissement »

Fail2ban met à disposition une commande pour valider la qualité des paramètres pour un service donné, par exemple ici la supervision de SSH. Le premier paramètre correspond à la désignation du fichier de log, le second au filtre à utiliser.

```
dell:~# fail2ban-regex /var/log/apache2/error.log /etc/fail2ban/filter.d/apache-noscript.conf
```

```
Running tests
=====
```

```
Use regex file : /etc/fail2ban/filter.d/apache-noscript.conf
Use log file    : /var/log/apache2/error.log
```

```
Results
=====
```

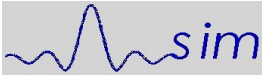
```
Failregex
|- Regular expressions:
  [1] [[\client <HOST>[]] (File does not exist|script not found or unable to stat):
  /\S*(\.\php|\.\asp|\.\exe|\.\pl)
  [2] [[\client <HOST>[]] script '/\S*(\.\php|\.\asp|\.\exe|\.\pl)\S*' not found or unable to
stat *$
|- Number of matches:
  [1] 1 match(es)
  [2] 1 match(es)
```

```
Ignoreregex
|- Regular expressions:
|- Number of matches:
```

```
Summary
=====
```

```
Addresses found:
[1]
  201.116.227.194 (Tue Oct 26 00:57:41 2010)
[2]
  61.12.3.162 (Tue Oct 26 08:08:16 2010)
```

```
Date template hits:
0 hit(s): Month Day Hour:Minute:Second
410 hit(s): Weekday Month Day Hour:Minute:Second Year
```



```
0 hit(s): Weekday Month Day Hour:Minute:Second
0 hit(s): Year/Month/Day Hour:Minute:Second
0 hit(s): Day/Month/Year Hour:Minute:Second
0 hit(s): Day/Month/Year:Hour:Minute:Second
0 hit(s): Year-Month-Day Hour:Minute:Second
0 hit(s): Day-Month-Year Hour:Minute:Second[.Millisecond]
0 hit(s): TAI64N
0 hit(s): Epoch
0 hit(s): ISO 8601
```

Success, the total number of match is 2

However, look at the above section 'Running tests' which could contain important information.

L'exemple ci-dessus montre que le filtre apache-noscript.conf trouve peu d'accès non désirés :

Success, the total number of match is 2

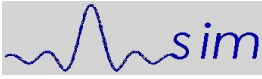
Dans les mêmes conditions le filtre apache-depancech.com repère lui

Success, the total number of match is 199

Log des bannissements

Les bannissements se trouvent dans le fichier /var/log/fail2ban.log. Ce fichier sera exploité pour pointer les adresses IP des perturbateurs.

```
2010-10-27 16:41:38,079 fail2ban.actions: WARNING [ssh] Ban 178.34.144.80
2010-10-27 16:51:38,136 fail2ban.actions: WARNING [ssh] Unban 178.34.144.80
2010-10-27 18:24:32,739 fail2ban.actions: WARNING [vsftpd] Ban 86.69.156.198
2010-10-27 18:34:32,792 fail2ban.actions: WARNING [vsftpd] Unban 86.69.156.198
2010-10-28 11:03:47,016 fail2ban.actions: WARNING [apache] Ban 86.69.156.198
2010-10-28 11:13:47,075 fail2ban.actions: WARNING [apache] Unban 86.69.156.198
2010-10-28 17:23:26,319 fail2ban.actions: WARNING [apache] Ban 69.64.79.164
2010-10-28 17:33:26,387 fail2ban.actions: WARNING [apache] Unban 69.64.79.164
```

Annexes

Annexe 1 Fournisseur accès Internet

Fournisseur : Bouygues

Adresse WAN :

Adresse GATEWAY et DNS : 192.168.1.254

Gestion des tables de routage : Affectation de la DMZ au serveur.

Annexe 2 Enregistrement domaine

Depuis 2008 le domaine « depancech.com » est assuré par « Rapidomain.com ».

Annexe 3 Configuration matérielle

La configuration matérielle est fournie par un logiciel spécifique « lshw », son exécution fournit un fichier très complet, il ne peut être inclus dans cette annexe.

Installation du logiciel :

```
sudo apt-get install lshw
```

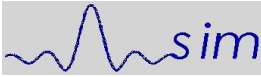
Génération du fichier d'inventaire :

```
/usr/bin/lshw > /root/hwconfig
```

On obtient un fichier texte

```
/usr/bin/lshw -html > /root/hwconfig.html
```

On obtient un fichier lisible par un navigateur.



Annexe 4 Gestion des postes de travail côté serveur

Le script propose une interface texte pour faciliter la création des comptes « Machine » LINUX et Windows-Samba. Le script est lancé sous root par la commande :

```
/root/admin/deviceadd nom_de_la_machine_a_integrer
```

Exemple de création du compte machine dont le nom Windows est « legros ».

```
dell:~/admin# ./root/admin/deviceadd legros
Creation UNIX device = OK pour legros
Added user legros$.
Creation SAMBA device = OK pour legros
```

Entrée dans le fichier **/etc/passwd** pour cette machine. Un compte machine se repère par le caractère \$ en fin du nom :

```
legros$:x:1001:1001::/dev/null:/bin/false
```

Entrée dans le fichier **/etc/samba/smbpasswd** pour cette même machine :

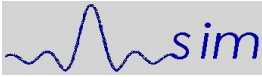
```
legros$:1001:XXXXXXXXXXXXXXXXXX:31DCA453EFF15EDAC3AD6276CB4AC511:[W          ]:LCT-4CCDD332:
```

```
#####
# Ajout de Client de Domaine SAMBA
#
# appel : /root/admin/deviceadd NOM_NETBIOS
#
#####

pc=$1

/usr/sbin/useradd -s /bin/false -d /dev/null $pc\$
if [ $? -eq 0 ] ; then
    echo "Creation UNIX device = OK pour "$pc
else
    echo "Erreur creation UNIX de "$pc" corriger probleme"
    echo "reprendre a la console !!!"
    echo ""
    exit
fi

smbpasswd -a -m $pc
if [ $? -eq 0 ] ; then
    echo "Creation SAMBA device = OK pour "$pc
else
    echo "Erreur creation SAMBA de "$pc" corriger probleme"
    echo "reprendre a la console !!!"
    echo ""
fi
```



Annexe 5 Samba - Fichier de configuration

```
cat /etc/samba/smb.conf

[global]
    workgroup = mesnil
    netbios name = DELLDEBIAN
    server string = Samba
    encrypt passwords = yes
    security = user
    os level = 255
    preferred master = yes
    domain logons = yes
    local master = yes

    wins support = yes
    username map = /etc/samba/smbusers

[homes]
    comment = Repertoire utilisateur
    browseable = yes
    read only = no
    create mask = 600
    directory mask = 700
    path = /home/%U

[public]
    comment = Repertoires communs
    path = /home/commun
    guest ok = yes
    read only = no
    create mask = 664

;[netlogon]
;    comment = NetLogDir
;    path = /home/netlogon
;    guest ok = yes
;    writeable = no
;    share modes = no
;    browseable = no

[genaccess]
    comment = Tout le monde
    path = /home
    writable = no
    browseable = yes

[printers]
    comment = All Printers
    path = /var/spool/samba
    printable = yes
    printer name = smbprinter
    guest ok = yes
    force group = users
```