Jean-Louis Cech Cell : +33 659 714 837

Systems Architecture / Integration / Maintenance jl.web.cech@gmail.com

Serveur Administration

Rédacteur : Jean-Louis Cech

Date création : 15 Décembre 2012

Mise à jour :

Serveur EeePC
Ubuntu 12.04 (LTS)

Jean-Louis Cech Cell : +33 659 714 837

Systems Architecture / Integration / Maintenance jl.web.cech@gmail.com

Table des matières

Jean-Louis Cech Cell : +33 659 714 837

Systems Architecture / Integration / Maintenance jl.web.cech@gmail.com

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 notebook ASUS EeePC. 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/sda
/dev/sdb

de taille respective de 240 et 2000 giga octets.

Ces disques sont connectés à la carte mère respectivement par l'interface SATA pour le disque interne, le deuxième disque est externe, il est connecté via une interface USB 2. La connexion de lecteurs/graveurs externe se fera elle aussi via un port USB 2 libre.

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 SDA

Ce disque contient est intégralement alloué à l'OS, Linux UBUNTU 12.04. Aucune provision pour un double boot n'est prévue.

```
Disk /dev/sda: 160.0 GB, 160041885696 bytes
255 heads, 63 sectors/track, 19457 cylinders, total 312581808 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0003ee43

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     7999487     3998720   83  Linux
/dev/sda2         7999488    70500351    31250432   83  Linux
/dev/sda3        70502398   312580095   121038849    5  Extended
/dev/sda5        70502400    78499839     3998720   82  Linux swap / Solaris
/dev/sda6        78501888   312580095   117039104   83  Linux
```

Disque dur SDB

Ce disque contient deux partitions sdb1 et sdb2. Elles sont allouées respectivement pour sdb1 au stockage des données volumineuses, en particulier le multimedia et pour sdb2 aux archive de sauvegarde dont l'usage est explicité plus bas.

```
Disk /dev/sdb: 2000.4 GB, 2000398934016 bytes
255 heads, 63 sectors/track, 243201 cylinders, total 3907029168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x6b5fcb50

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1            2048  2097154047  1048576000   83  Linux
/dev/sdb2      2097154048  3907029167   904937560   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/fstab
/# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
proc            /proc           proc    nodev,noexec,nosuid 0       0
# / was on /dev/sda2 during installation
UUID=07151869-86b0-4f57-82df-7395a71f31fa /               ext4    errors=remount-ro 0       1
# /boot was on /dev/sda1 during installation
UUID=0fb4629b-aa08-41c1-9a20-5b828d20f3eb /boot           ext4    defaults        0       2
# /home was on /dev/sda6 during installation
UUID=94e09634-907b-496a-ad59-fb6182c12671 /home           ext4    defaults        0       2
# swap was on /dev/sda5 during installation
UUID=90821df6-af08-497c-a2b5-5a751785ec2a none            swap    sw              0       0
#
# Montage disque externe
/dev/sdb1      /mnt/nas       auto    rw      0       0
```

Partition - Taille	Point de Montage	Affectation
/dev/sda		
Sda1 – 4 Go	/boot	Fichiers pour amorcer
sda2 - 32 Go	/	Partition système
sda3 - 4 Go	SWAP	
hda6 – 120 G	/home	Données utilisateurs

IMPORTANT :

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

Installation UBUNTU 12.04

UBUNTU 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, l'une WiFi qui ne sera pas mise en œuvre, l'autre filaire en RJ 45. C'est cette dernière qui est utilisée.

Adresse LAN de eth0 : 192.168.22

```
eth0      Link encap:Ethernet  HWaddr 90:e6:ba:96:e5:45
          inet addr:192.168.1.22  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::92e6:baff:fe96:e545/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48653107 errors:532503 dropped:0 overruns:0 frame:174315
          TX packets:62899587 errors:4357 dropped:0 overruns:0 carrier:4358
          collisions:18121969 txqueuelen:1000
          RX bytes:4141691836 (4.1 GB)  TX bytes:3687423185 (3.6 GB)
          Interrupt:45

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:110084 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110084 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9401310 (9.4 MB)  TX bytes:9401310 (9.4 MB)

wlan0     Link encap:Ethernet  HWaddr 00:25:d3:8f:a7:7a
          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)
```

Installation des Applications et Services

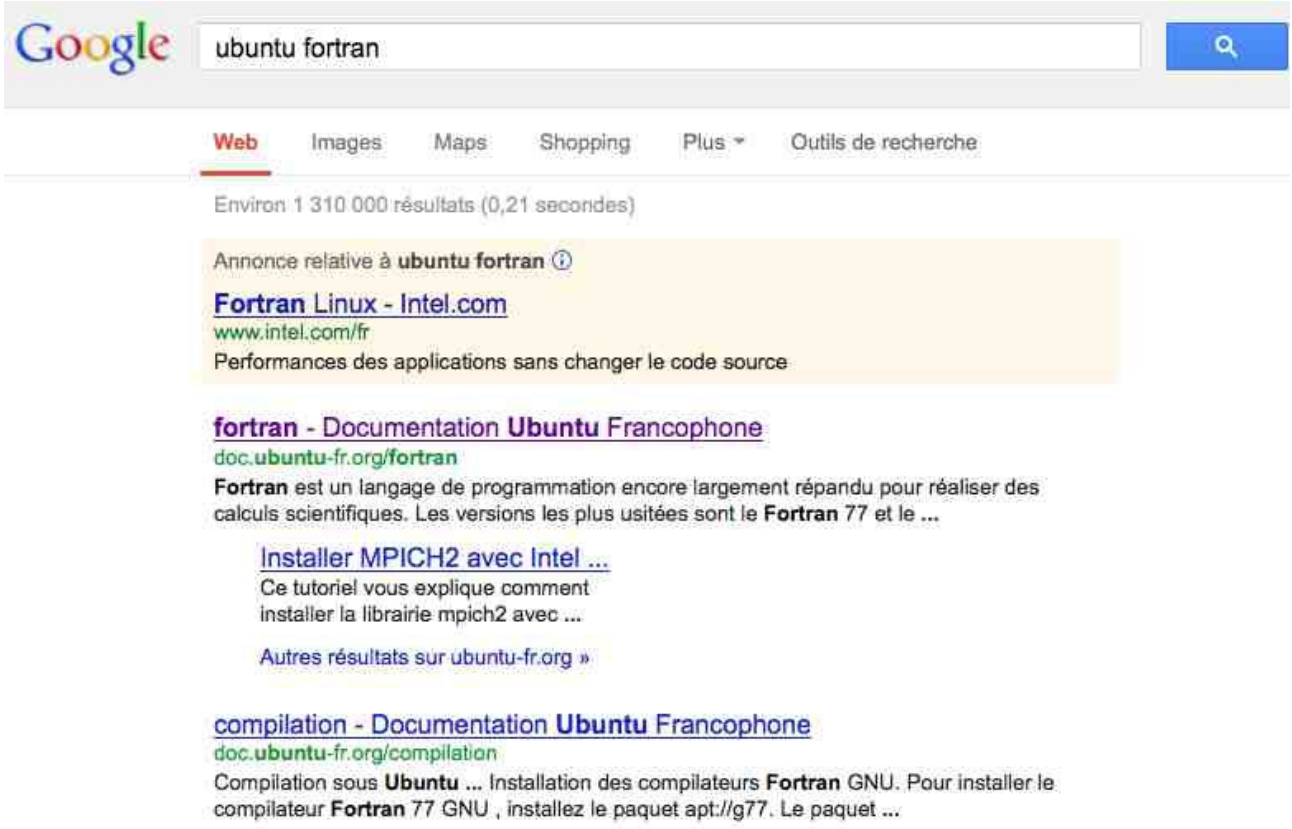
UBUNTU s'appuie sur un noyau Debian, sa bonne réputation de stabilité présente à priori de nombreux avantages. La différence entre les deux distributions relève essentiellement de l'ouverture de UBUNTU vers des applications plus ouvertes et donc moins « Secure ». Toutefois, l'expérience actuelle prouve que ce léger retrait en ce qui concerne la sécurité n'est pas, au jour de la rédaction de ce document, une menace réelle pour ce type de serveur.

L'installation ne pose aucun problème particulier à un utilisateur moyennement familier avec Linux. L'installation des « paquets » complémentaires se fera soit via l'interface graphique livrée en standard, soit via les commandes passées dans une fenêtre Terminal.

Les modalités de l'installation des paquets n'est pas couverte par ce document, les sites dédiés, UBUNTU, Debian, couvrent parfaitement ce topic. Toutefois un exemple est donné ci-dessous.

Recherche d'un paquet à installer

On souhaite installer un compilateur Fortran. Pour cela il faut disposer du nom exact du paquet. Le nom est obtenu sur le site UBUNTU comme suit.



Parmi les réponses suivantes sélectionner :

fortran – Documentation Ubuntu Francophone

On se retrouve dirigé vers la page suivante :

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 :

```
machine:~# 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
        integer*2 kl

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

        stop 123
1       format (i4)
        end
```

Lancer la compilation

```
user@machine:~/agl/fortran$ gfortran test.f
```

Lancer l'exécutable

```
user@machine:~/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 :

```
machine:~# 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	Libre Office
Serveur de Domaine Windows	SAMBA
Serveur d'impression	CUPS
Serveur de bases de données	MySQL
Serveur de sauvegarde	Script spécifique

Applicatifs et verbes complémentaires

Verbes natifs UBUNTU

Certains scripts ou applicatifs complémentaires ont été installés. La liste non exhautive ci-dessous en liste quelques uns, ils sont installés en tant que de besoin à la volée :

- rsync : synchronisation de répertoires sur deux machines
- curl : récupération d'une URL en chaîne texte
- lshw : inventaire matériel de la machine

Autres verbes

Certains scripts non natifs UBUNTU sont ajoutés. Ils sont issus majoritairement soit de « Source Forge » soit écrits pour résoudre des problématiques ponctuelles et locales. Afin de rendre les scripts personnels accessibles à tous les utilisateurs du serveur, bien que centralisés dans un seul répertoire, « /root/admin/nom_du_script », un lien symbolique est créé dans « /usr/local/bin ». Parmi les scripts utiles il y a :

- dirsize : fournit l'occupation disque d'un répertoire,
- stringinfile : fournit le numéro de ligne d'une chaîne de caractères dans un fichier,
- deviceadd : ajoute une machine Windows dans un domaine SAMBA,

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/sdb2 sur /mnt/bu
2. Copie ce différents fichiers spécifiques vers un répertoire sous /home/root qui a été créé à cet effet. Une fois la sauvegarde faite, les contenus de ce répertoire seront effacés.
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 précédant.

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 recule 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 archive
   ls -l /mnt/bu/tmp
6. Lancer la décompression des fichiers archive, une fois la commande terminée l'extention .gz a disparu,
   gunzip /mnt/bu/tmp/*
7. Lancer la décompression du fichier archive par les deux commandes suivantes
   cd /mnt/bu/tmp/
   tar -xvvf 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. Démonter 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 pas Windows avec un mot de passe qui pourra différer du mot de passe « root » Linux. 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:XXXXXXXXXXXXXXXXXXXX: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 (VSFTP)

FTP Paramétrage

Le serveur FTP active vsftp (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_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 » dans le même fichier que tous les accès, on spécifie la destination par la ligne :

```
xferlog_file=/var/log/auth.log
```

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 et les protocoles TCP et UDP

VSFTP accepte indifféremment les protocoles TCP et UDP. L'expérience montre que certains clients FTP utilisent soit l'un soit l'autre. Par exemple FILEZILLA utilise UDP alors que CYBERDUCK utilise TCP.

Cette différence peut générer quelques soucis en particulier dans les réglages des tables de routages afin de rendre le serveur visible depuis le WEB. A titre d'exemple la BBOX imposera de créer deux règles FTP, l'une pour TCP et l'autre pour UDP.

FTP Administration

Si vsftpd n'est pas actif il est possible de le lancer par « start » ou le relancer par « restart »à la main par :

```
root@picolo:~# service vsftpd restart
vsftpd stop/waiting
vsftpd start/running, process 3259
```

Le fichier de log spécifique est localisé dans :

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

il contient les transactions réalisées ainsi que les login incorrects.

Serveur WEB (Apache)

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 des trouver par des tentatives répétées un couple ID<->PW. Afin de limiter les tentatives d'intrusion il a été installé l'applicatif « Fail2ban ».

La sécurisation passe par la génération de fichiers de log, ces fichiers sont localisés dans /var/log/. Afin d'éviter l'accumulation inutile de vieux logs il convient de paramétrer la fonction logrotate. Son paramétrage est décrit plus bas.

Logrotate

Logrotate permet la gestion des fichiers de log et en particulier l'élimination des anciens fichiers.

Logrotate est activé par la fonction crontab, il n'est pas utile de modifier le fonctionnement de crontab standard.

Paramétrage de logrotate

Deux fichiers définissent les paramètres de fonctionnement, on les trouve respectivement dans :

```
/etc/logrotate.conf          Fichier de configuration générale.
/etc/logrotate.d             Répertoire des paramètres individuels.
```

Le mode de fonctionnement de logrotate n'est pas décrit ici, se reporter aux manuels disponibles, en revanche la configuration telle qu'utilisée dans ce serveur est donnée en Annexe.

Test de logrotate

Après modification du fichier /etc/logrotate.conf ou d'une entrée dans /etc/logrotate.d il est possible de tester les nouveaux paramètres sans rien modifier dans les fichiers de log en passant la commande suivante sous root :

```
logrotate -d /etc/logrotate.conf
```

L'affichage écran du résultat est explicite.

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 vsftp

Modifier la section **[vsftp]** 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 vsftp 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 même 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 l'enregistrement du domaine « depancech.com » est assuré par « Rapidomain.com ».

Ce fournisseur a été choisi pour son coût et la simplicité de la mise en oeuvre de la réservation.

Toutefois il semble que les modalités de mise en oeuvre de la gestion des paramètres du DNS, en particulier pour la gestion locale des comptes de courriels ne soit pas possible.

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.
```

En copiant ce fichier dans un répertoire pointable par le serveur WEB, il est possible de rendre cet inventaire accessible, rendre ce fichier accessible ne pose, à priori, pas de problème de sécurité.

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:XXXXXXXXXXXXXXXXX: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
```

Annexe 6 Logrotate - Fichier de configuration

Les ajustements sont insérés en fin de fichier.

Attention : si les fichiers de log doivent être utilisés par un autre utilisateur que « root », il est important de donner des droits d'accès ouverts en lecture, par exemple 644.

```
jlc@dell:~$ cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

# system-specific logs may be configured here
# Specifier le nom complet du fichier extension .log comprise
# Attention de laisser des droits de lecture ouverts 644
#

# Fichier issu du traitement de fail2ban
/var/log/activity.log {
    missingok
    weekly
    notifempty
    rotate 52
    delaycompress
    create 0644 root utmp
}

# Fichier de log des data du Fluke 97
/var/log/edf.log {
   missingok
   monthly
   notifempty
   rotate 12
   delaycompress
   create 0644 root utmp
}
```