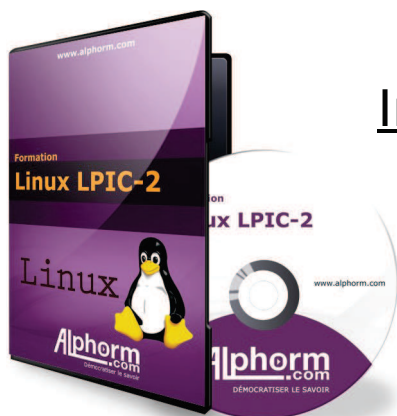




Introduction

Présentation de la formation

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

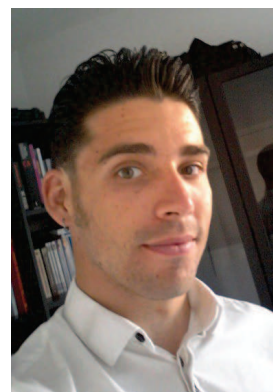
Plan

- Présentation du formateur
- Qu'est ce que Linux
- Le plan de formation
- Présentation de la formation
- Outils nécessaires
- Comment travailler
- Les références des ressources logicielles
- Les liens utiles



Présentation du formateur

- Noël Macé
- alphorm@noelmace.com
- Formateur consultant expert Unix et FOSS
- Mes références :
 - Mon profil Viadeo : <http://fr.viadeo.com/fr/profile/noel.mace>
 - Mon parcours : <http://vizualize.me/noelmace>
 - Mon site : <http://noelmace.com>
 - Contacts
 - Blogs
 - Base de connaissance
 - CV
 - Etc ...



Qu'est ce que Linux ?

- Un kernel
 - Développé par Linux Torvalds à partir de Minix
 - En 1991
- Un système d'exploitation
 - Libre et open source
 - Issu du projet GNU (1983)
 - Leader sur :
 - les serveurs web (65%)
 - Les systèmes embarqués
 - Les super-calculateurs

Le plan de formation

LPIC 201

- Topic 201: Noyau Linux
- Topic 202: Démarrage du système
- Topic 203: Système de fichiers et périphériques
- Topic 204: Administration avancée des périphériques de stockage
- Topic 205: Configuration réseau
- Topic 206: Maintenance système
- Topic 207: Domain Name Server

LPIC 202

- Topic 208: Services web
- Topic 209: Partage de fichiers
- Topic 210: Gestion des clients du réseau
- Topic 211: Services de Messagerie
- Topic 212: Sécurité système
- Topic 213: Dépannage

Certification

- LPIC2 : <http://www.lpi.org/linux-certifications/programs/lpic-2>



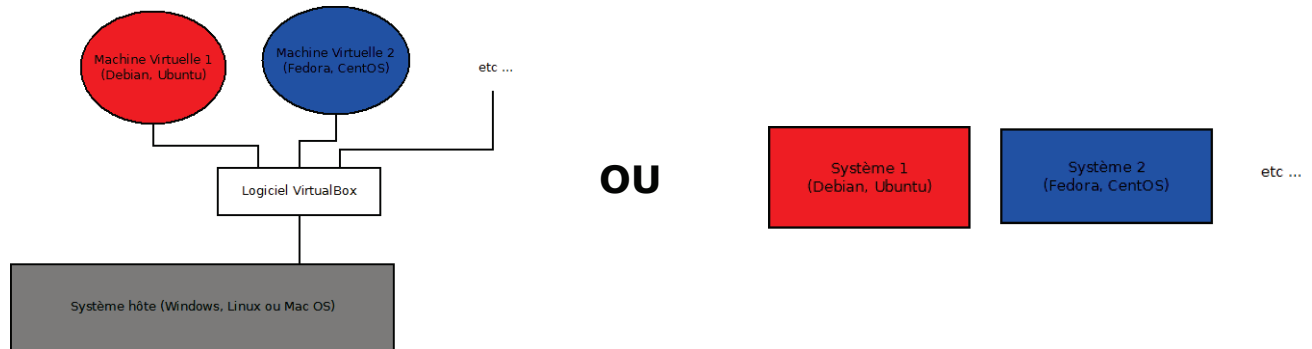
Présentation de la formation

- Orientée certification
 - Basée sur le parcours officiel
- Acquisition d'un grand nombre de connaissances
 - Pratiques
 - théoriques

Outils nécessaires

- Deux grandes familles de distribution Linux :
 - Debian (Ubuntu, Damn Small Linux, etc ...)
 - Red Hat (RHEL, Fedora, Centos, Mandriva, etc ...)
- Peu de ressources matérielles exigées :
 - Dual-boot Debian / Fedora
 - Ou Machines virtuels (virtualbox)

🔒 Outils nécessaires (2)



🔒 Comment travailler

- La pratique, toujours la pratique :
 - Utiliser Linux au quotidien
 - Être curieux !
 - Reproduire les opérations effectuées dans chaque vidéo
- Se documenter
 - Un très grand nombre de ressources sont disponibles
 - Ce cours ne peut pas tout traiter
 - Lire le man !
 - Effectuer des recherches sur internet

Les références des ressources logicielles

- Linux Debian :

<http://www.debian.org>

- Fedora :

<http://fedoraproject.org/>

- Virtualbox :

<https://www.virtualbox.org/>

- Virtualboxes :

<http://virtualboxes.org/>

Les liens utiles

- Supports officiels et communautaires des distributions :

- [Ubuntu \(en\)](#)
- [Ubuntu-fr](#)
- [Debian](#)
- [Gentoo \(en\)](#)
- [Fedora \(en\)](#)
- [RedHat \(en\)](#)
- [OpenSuse \(en\)](#)
- [Archlinux \(en\)](#)

- Supports recommandés par LPI :

- [LPIC-1 & LPIC-2 free educational manuals](#)
- [Free online exam preparation guide for LPIC-2](#)

- Examens d'entraînement :

- [Linux Praxis](#)
- [PenguinTutor](#)
- [MC MCSE](#)

- Forums et irc :

- [forum ubuntu-fr](#)
- [le forum des débutant de DLFP](#)
- [linuxforums.org \(en\)](#)
- [forum Linux de développez.com](#)

- Autres ressources utiles :

- [The Linux Documentation Project](#)
- [Linux Documentation by die.net](#)
- [Linux Kernel Documentation](#)
- [Comment ça marche](#)
- [Yet Another « Guide d'installation de Linux »](#)
- [Linux pas-à-pas](#)
- [section Linux de developpez.com](#)
- [Flashcard exchange](#)

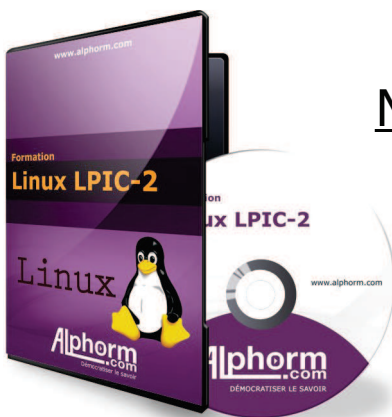


Go !

Linux LPIC-2

tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

Alphorm.com



Noyau Linux

Composants du noyau

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2

tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

Plan

- Rappel : le noyau Linux
- Récupérer les sources
- Structure
- Dossiers principaux
- Les différents "types" de monobloc
- Documentation



Rappel : le noyau Linux

- offre une abstraction matérielle pour les logiciels
- gestion des processus
- partie la plus critique de l'OS
- rôle central

🔗 Récupérer les sources

- <http://www.kernel.org>
- `Linux-version.tar.gz` ou `bz2` ou `xz`
 - Décompresser (commande `tar`) dans `/usr/src/`
 - Ou dans un autre répertoire, puis établir un lien symbolique
- Par paquet
 - Debian etc ...

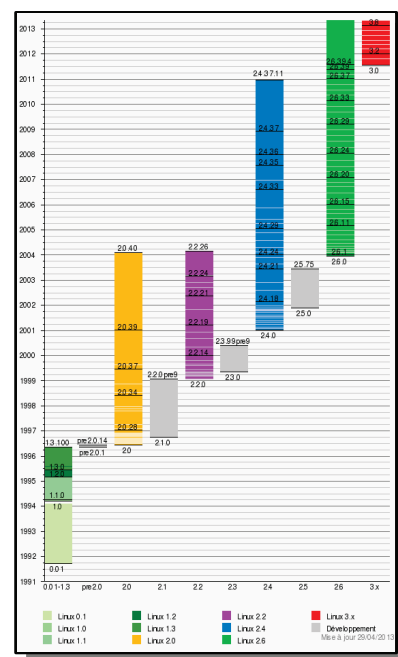
```
# apt-get install linux-source
```

- CentOS (plus de paquet `kernel-source`)

```
$ rpm -i http://vault.centos.org/6.4/updates/Source/SPackages/kernel-2.6.32-358.6.2.el6.src.rpm
```

🔗 Versioning

- Trois (voir quatre) nombres :
 - exemples :
 - `2.6.24(.x)` = majeure 2 - mineure 6 - révision 24
 - `3.9(.x)` = version 3 - révision 9



Structure

- Un fichier principal
 - "monobloc"
 - Fonctionnalités critiques
 - Directement chargé au démarrage
- Des modules
 - Optionnellement
 - Chargés et déchargés dynamiquement

Dossiers principaux

- ./drivers
- ./fs
- ./net

Les différents "types" de monobloc

- vmlinux
- vmlinuz
- zImage
- BzImage
- kernel

Documentation

- /usr/src/linux-*/README
- /usr/src/linux-source-2.6.x/Documentation/
 - 00-INDEX

Ce qu'on a couvert

- Comment récupérer les sources d'un noyau Linux.
- Quelle est la structure du noyau Linux.
- Comment mieux comprendre son arborescence.

201.1 Kernel Components

Weight : 2

Description : Candidates should be able to utilise kernel components that are necessary to specific hardware, hardware drivers, system resources and requirements. This objective includes implementing different types of kernel images, identifying stable and development kernels and patches, as well as using kernel modules.

Key Knowledge Areas:

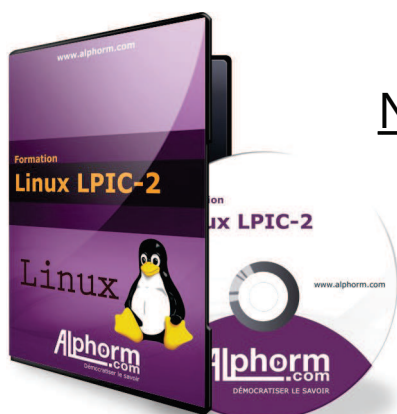
- Kernel 2.6.x documentation
- Kernel 3.x documentation

The following is a partial list of the used files, terms and utilities:

- /usr/src/linux
- /usr/src/linux/Documentation
- zImage
- bzImage



Alphorm.com



Noyau Linux

Application de correctifs (patches) à un noyau

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Méthode simple
- Tester
- Permettre une récupération
- Restauration à partir de fichiers .orig



Introduction

- Permet de mettre à jour l'image d'un noyau
 - à partir de sources pré-existantes
- Plus léger donc plus rapide à récupérer qu'un noyau complet.
- Permet d'ajouter ou modifier un ou plusieurs éléments
 - ajout de fonctionnalités
 - drivers tiers ou expérimentaux
 - correction de bugs
 - etc ...

Méthode simple

- se déplacer dans le dossier source

```
# cd /usr/src/
```

- décompresser et appliquer le patch

```
# gzip -cd patch-version.gz | patch -p0
```

```
# bzip2 -dc patch-version.bz2 | patch -p0
```

```
# patch -p0 < patch-version
```

- L'option -p permet de situer le patch par rapport aux sources
 - -p0 si dans /usr/src
 - -p1 si dans /usr/src/linux

Tester

```
# patch -p1 -dry-run < fichier_du_patch
```

🔒 Permettre une récupération

- Plusieurs méthodes, suivant l'application du patch
 - Méthode de patching simple : appliquer un patch à l'envers

```
# zcat patch-2.4.22.gz | patch -p0 -R
```

- Effectuer une sauvegarde avant le patch

```
# patch -B oldfiles/ -p0 < patch-file
```

- récupération

```
# diff -ur linux-2.4.21 oldfiles/linux-2.4.21 > recover-2.4.21-patch
```

- Conserver les fichiers d'origine

```
# patch -b -P0 < fichier_patch
```

🔒 .orig

```
for file in $(find linux-2.4.29 | grep orig)
do
FILENAME=$(echo $file | sed 's/\.orig//')
mv -f $file $FILENAME
done
```

Ce qu'on a couvert

- Qu'est qu'un patch.
- Comment appliquer un patch.
- Comment récupérer une image avant patching.

201.3 Patching a kernel

Weight : 1

Description : Candidates should be able to properly patch a kernel to add support for new hardware. This objective also includes being able to properly remove kernel patches from already patched kernels.

Key Knowledge Areas:

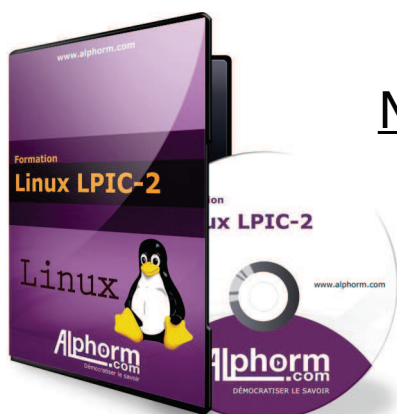
- Kernel Makefiles

The following is a partial list of the used files, terms and utilities:

- patch
- gzip
- bzip2



Alphorm.com



Noyau Linux

Personnalisation et configuration du noyau

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Étudier son matériel
- La commande make
- Nettoyage
- Configuration
- Démonstration



Introduction

- Une personnalisation du noyau est indispensable avant sa compilation.
 - choix des fonctionnalités à intégrer
 - modularité

La commande make

```
$ make [ -f makefile ] [ options ] ... [ targets ] ...
```

- Permet
 - la configuration
 - la compilation
 - l'installation
- Plusieurs "cibles" (make targets)

Etudier son matériel

- Rappels LPIC1
 - lspci
 - lsmod
 - etc ...
- Méthodes "génériques"
 - manuel du matériel
 - inspection visuelle

Nettoyage

- "Cibles" de make
 - clean
 - mrproper
 - distclean

Configuration

- Plusieurs types d'interfaces utilisateur
- création d'un fichier `/usr/src/linux/.config`
- "Cibles" de make
 - par CLI : `config`
 - via ncurses : `menuconfig`
 - via X : `xconfig`
 - via GTK+ : `gconfig`
 - à partir d'une ancienne configuration : `oldconfig`

Ce qu'on a couvert

- Comment préparer la compilation du noyau Linux.

201.4 Customise, build and install a custom kernel and kernel modules (*Partiellement*)

Weight : 2

Description : Candidates should be able to customise, build and install a 2.6 or 3.x kernel for specific system requirements, by patching, compiling and editing configuration files as required. This objective includes being able to assess requirements for a kernel compile as well as build and configure kernel modules.

Key Knowledge Areas:

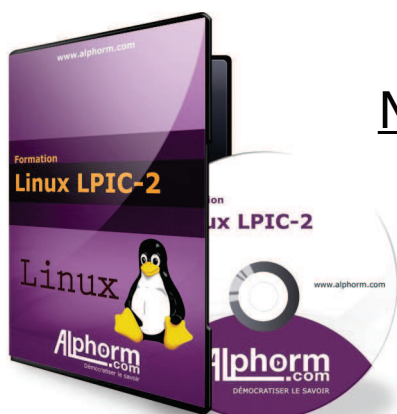
- Customize the current kernel configuration.
- /usr/src/linux/

The following is a partial list of the used files, terms and utilities:

- /usr/src/linux/*
- /usr/src/linux/.config
- make targets: config, menuconfig, xconfig, gconfig oldconfig



Alphorm.com



Noyau Linux

Compilation du noyau

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Résumé des opérations
- Vérifier les dépendances
- Méthode simple et complète
- Compiler le monobloc
- Compiler les modules dynamiques
- INITlal Ram Disk
- Création d'un initrd
- mkinitrd
- mkinitramfs



Résumé des opérations

```
# make dep && make clean && make bzImage && make modules \  
> && make modules_install
```

- Vérifier les dépendances
- Nettoyer
- Compilation de monobloc
- Compilation des modules
- Installation des modules

Ⓛ Vérifier les dépendances

```
$ make dep
```

- S'assurer que toutes les dépendances sont en place
 - exemples : fichiers include

Ⓛ Méthode simple et complète

```
$ make [all]
```

- Dans le répertoire des sources
- Construit le monobloc et les modules
- Suffisant
 - si aucune erreur
 - et tout les utilitaires nécessaires présent
- Astuce

```
$ make [all] | grep -iw "error"
```

Compiler le monobloc

```
$ make [zImage | bzImage]
```

- Permet de choisir le type de monobloc à compiler

Compiler les modules dynamiques

```
$ make modules
```

Créer un package

- Pour CentOS

```
$ make rpm
```

- Pour Debian

```
$ make-kpkg kernel_image
```

INITial Ram Disk

- Rappel : cf LPIC1
- Chargé au démarrage
- Système de fichier
 - initramfs (cramfs, squashfs)
 - chargé en mémoire vive
- Contient certains modules nécessaires au démarrage
 - permet d'utiliser un kernel minimal
 - plus grande souplesse

Création d'un initrd

- Nombreux outils
- Varient suivant les distributions
- Deux plus courants :
 - mkinitrd
 - mkinitramfs

mkinitrd

```
# mkinitrd image KernelVersion
```

- Options
 - --version
 - -v : verbose
 - --preload=MonModule
 - --with=MonModule
 - --builtin=MonModule
 - -f: permettre d'écraser une image existante
 - --fstab=filename
 - --image-version
 - --nocompress
 - --nopivot
 - --omit-lvm-modules
 - --omit-raid-modules

- Exemple

```
# mkinitrd /boot/initrd-2.6.35.4.img 2.6.35.4
```

mkinitramfs

```
# mkinitramfs -o /boot/initramfs-2.6.35.4.img 2.6.35.4
```

- Options :
 - -d confdir
 - -k
 - -o outfile
 - -r root
 - -v
 - --supported-host-version=version
 - --supported-target-version=version

Ce qu'on a couvert

- Comment compiler le kernel.
- Comment créer un initrd.

201.4 Customise, build and install a custom kernel and kernel modules (*Partiellement*)

Key Knowledge Areas:

- /usr/src/linux/
- Build a new kernel and appropriate kernel modules.

The following is a partial list of the used files, terms and utilities:

- make
- /usr/src/linux/*

201.2 Compiling a kernel (*Partiellement*)

Weight : 2

Description : Candidates should be able to properly configure a kernel to include or disable specific features of the Linux kernel as necessary. This objective includes compiling and recompiling the Linux kernel as needed, updating and noting changes in a new kernel, creating an initrd image and installing new kernels.

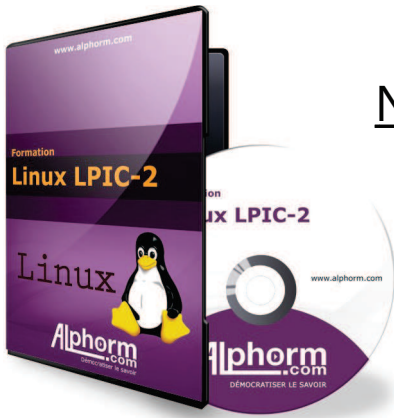
Key Knowledge Areas:

- /usr/src/linux/
- Kernel 2.6.x make targets
- Kernel 3.x make targets

The following is a partial list of the used files, terms and utilities:

- mkinitrd
- mkinitramfs
- make
- make targets (config, xconfig, menuconfig, oldconfig, mrproper, zImage, bzImage, modules, modules_install)





Noyau Linux

Installation d'un noyau et de modules noyau

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Méthode simple et complète
- system.map
- Modules
- Configuration de GRUB



Ⓛ Méthode simple et complète

```
# make install
```

- Installe tout les composants
 - copie du monobloc dans /boot
 - system.map (voir plus loin)
 - création et mise en place d'un initrd
 - modification éventuelle de GRUB

Ⓛ system.map

- pointeurs vers certaines fonctions du kernel
 - utiles pour débbugger certains problèmes
 - pas indispensable

```
# cp System.map /boot/System.map-2.6.35.4  
# rm /boot/System.map  
# ln -s /boot/System.map-2.6.35.4 /boot/System.map
```

Modules

- Dans `/lib/modules/kernel-version/`

```
# make modules_install
```

Configuration de GRUB

- Legacy (rappel LPIC1)

```
title GNU/Linux, kernel 2.6.8
root (hd0,0)
kernel /boot/vmlinuz-2.6.8
root=/dev/hda1 ro
initrd /boot/initrd.img-2.6.8
savedefault
boot
```

- GRUB2 : cf LPIC1

Ce qu'on a couvert

- Comment installer un noyau Linux.

201.2 Compiling a kernel (suite)

Key Knowledge Areas:

- GRUB configuration files

The following is a partial list of the used files, terms and utilities:

- make targets (modules_install)

201.4 Customise, build and install a custom kernel and kernel modules (Partiellement)

Weight : 2

Description : Candidates should be able to customise, build and install a 2.6 or 3.x kernel for specific system requirements, by patching, compiling and editing configuration files as required. This objective includes being able to assess requirements for a kernel compile as well as build and configure kernel modules.

Key Knowledge Areas:

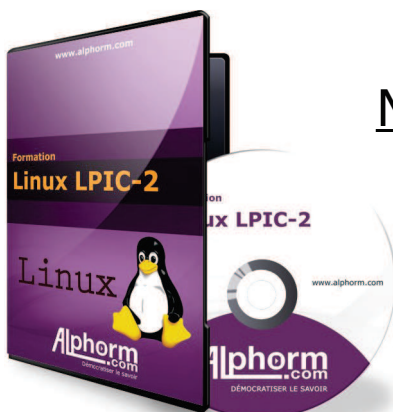
- Install a new kernel and any modules.
- Ensure that the boot manager can locate the new kernel and associated files.

The following is a partial list of the used files, terms and utilities:

- make
- /boot/*
- make targets: install, modules_install



Alphorm.com



Noyau Linux

Gestion et interrogation du noyau et des modules en exécution

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Afficher les modules actuellement chargés
- Charger un module
- Décharger un module
- Informations
- Configuration
- Dépendances



Introduction

- Rappels : cf LPIC1 – Chapitre 5.8 (matériel)
 - gestion dynamique des modules
 - afficher, charger et décharger
- Pour aller plus loin :
 - informations
 - configuration
 - dépendances

Ⓛ Afficher les modules actuellement chargés

```
$ lsmod
```

Module	Size	Used by
isofs	35820	0
zlib_inflate	21888	1 isofs
floppy	65200	0
nls_iso8859_1	5568	1
nls_cp437	7296	1
vfat	15680	1
fat	49536	1 vfat
sr_mod	19236	0
ide_cd	42848	0
cdrom	39080	2 sr_mod,ide_cd

nom

taille

nombre et noms des modules l'utilisant

Ⓛ Charger un module

```
# insmode chemin_vers_le_module
```

- charge un seul et unique module
- nécessite d'avoir chargé les modules dont il dépend
- Exemple :

```
# insmod /lib/modules/2.6.26/kernel/drivers/block/floppy.ko
```

Charger un module (2)

```
# modprobe nom_du_module
```

- Options :
 - -v : verbose
 - -C fichier : changer de fichier de configuration
 - /etc/modprobe.conf par défaut
 - -n : test
 - -r : décharger un module
 - -- show-depends
 - -l : lister les modules disponibles

Décharger un module

```
# rmmod nom_du_module
```

- Permet de libérer de la mémoire
- Options :
 - -v : verbose
 - -f : force
 - -w : wait

Informations

```
$ modinfo [-0] [-F field] [modulename|filename ...]
```

```
$ uname [-snrvmapio]
```

Configuration

- /etc/modules.conf ou /etc/modprobe.conf ou /etc/modprobe.d/*
- Directives :
 - alias aliasname result
 - depfile=full_path
 - path=path
 - keep
 - options modulename module-specific-options
 - cf modprobe
 - pre-install module command
 - etc ...

Dépendances

- `/lib/modules/kernel-version/modules.dep` : liste des dépendances
 - générée par la commande **depmod -a**
 - à partir des chemins indiqués dans `/etc/modules.conf`
 - utilisé par **modprobe**
 - pour déterminer l'ordre de (dé)chargement des modules
 - déchargement : de gauche à droite
 - chargement : de droit à gauche

Ce qu'on a couvert

- Gestion des modules et du kernel.

201.4 Customise, build and install a custom kernel and kernel modules (*Partiellement*)

Key Knowledge Areas:

- Module configuration files

The following is a partial list of the used files, terms and utilities:

- module tools
- depmod

201.5 Manage/Query kernel and kernel modules at runtime

Weight : 3

Description : Candidates should be able to manage and/or query a 2.6.x or 3.x kernel and its loadable modules.

Key Knowledge Areas:

- Use command-line utilities to get information about the currently running kernel and kernel modules.
- Manually load and unload kernel modules.
- Determine when modules can be unloaded.
- Determine what parameters a module accepts.
- Configure the system to load modules by names other than their file name.

The following is a partial list of the used files, terms and utilities:

- `/lib/modules/kernel-version/modules.dep`
- module configuration files in `/etc`
- `/proc/sys/kernel/`
- depmod
- insmod
- lsmod
- rmmod
- modinfo
- modprobe
- uname





Démarrage du système

Personnalisation du démarrage système

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS
Contact : alphorm@noelmace.com

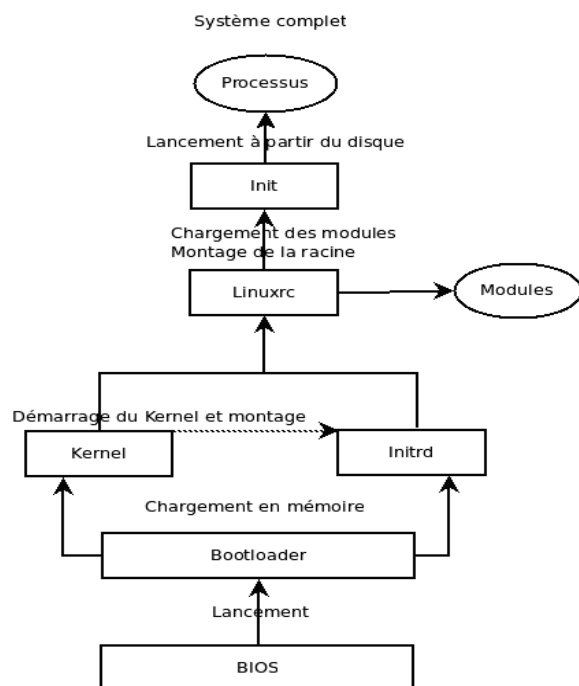
Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Rappels LPIC1
 - procédure de démarrage
 - runlevels
 - chkconfig
 - update-rc.d
 - afficher et changer de runlevel
 - inittab
- inittab : actions
 - au démarrage
 - à l'entrée dans un runlevel
 - relatives à l'alimentation
 - diverses



Rappel LPIC1 : procédure de démarrage



Rappel LPIC1 : Runlevels

Run Level	Debian	Suse	RedHat
N	amorçage		
0	ARRET		
S	mono-utilisateur au démarrage		
1	mono-utilisateur commuté		mono-utilisateur
2	multi-utilisateur	Multi-utilisateur déconnecté	...
3	...	mode connecté (réseau)	multi-utilisateur en mode console
4	...	...	...
5	...	mode-graphique (X11)	
6	redémarrage		
8	...		
9	...		

chkconfig

- Lister les associations services / runlevel

```
# chkconfig --list [service]
```

- modifier le comportement d'un service pour un ou plusieurs runlevels

```
# chkconfig --level [0123456] service [on/off/reset]
```

- ajouter un service

```
# chkconfig --add service
```

update-rc.d

- désactiver un service

```
# update-rc.d NomService remove
```

- modifier le comportement d'un service pour un ou plusieurs runlevels

```
# update-rc.d NomService start XX 2 3 4 5 . stop XX 0 1 6 .
```

- ajouter un service

```
# update-rc.d NomService defaults
```

Afficher et changer de runlevel

- afficher le runlevel actuel

```
$ runlevel
```

- changer de runlevel

```
# init [0123456Qq]
```

```
# telinit [0123456Qq]
```

- Eteindre ou redémarrer

```
# shutdown [-rhc] time ["Warning Message"]
```

```
# halt / # reboot / # poweroff
```

Rappel : inittab

- /etc/inittab
- configuration de init
- id:runlevels:action:process

inittab : actions au démarrage

- sysinit
- boot
- bootwait
- initdefault

inittab : actions à l'entrée dans un runlevel

- once
- ondemand

inittab : actions relatives à l'alimentation

- powerwait
- powerfail
- powerokwait
- powerfailnow

inittab : actions diverses

- off
- ctrlaltdel
- kdbrequest

Ce qu'on a couvert

- Rappels : procédures de démarrage et runlevels
- Les actions de inittab.

202.1 Customising system startup and boot processes

Weight : 4

Description : Candidates should be able to query and modify the behaviour of system services at various run levels. A thorough understanding of the init structure and boot process is required. This objective includes interacting with run levels.

Key Knowledge Areas:

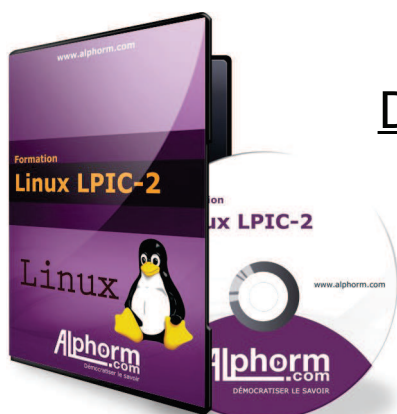
- Linux Standard Base Specification (LSB)

The following is a partial list of the used files, terms and utilities:

- /etc/inittab
- /etc/init.d/
- /etc/rc.d/
- chkconfig
- update-rc.d



Alphorm.com



Démarrage du système

Linux Standard Base

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Une famille de spécifications
- Librairies et commandes
- Système
- Fonctions disponibles pour les bootscripts
- Packaging



Introduction

- crée en juillet 2001
 - dernière version : 4.1 (fev 2011)
 - cf Linux Foundation
 - ISO depuis la version 2.0.1 (nov 2001)
- Standardisation des distributions GNU/Linux
 - étend POSIX, FHS, Single Unix Specification, etc ...
 - pour l'interopérabilité
 - librairies, utilitaires, scripts, etc ...

Une famille de spécifications

- spécification d'une architecture processeur
- deux parties : LSB-generic et LSB-arch

Librairies et commandes

- génériques
 - ex : libdl, libcrypt, libpthread
- spécifiques à une architecture
 - ex : libc, libm
- spécification d'un chemin, d'un nom et d'un format
- Plus de 130 commandes
 - ex : cp, tar, kill, gzip

Système

- cron
- runlevels
- utilisateurs et groupes (uid/gid)
- bootscripts
 - actions : start, stop, restart, force-reload & status
 - reload & try-restart (optionnels)
 - fonctions, chemin

Fonctions disponibles pour les bootscripts

- /lib/lsb/init-functions
- lancer un programme en tant que démon

```
start_daemon [-f] [-n nicelevel] [-p pidfile] pathname [args...]
```

- stopper un programme

```
killproc [-p pidfile] pathname [signal]
```

- renvoyer le ou les pid d'un programme

```
pidofproc [-p pidfile] pathname
```

Packaging

- non indispensable
- RPM
 - compatibilité sous Debian grâce à alien

Ce qu'on a couvert

- Ce qu'est la LSB.
- Son importance au niveau de la procédure de démarrage.

202.1 Customising system startup and boot processes

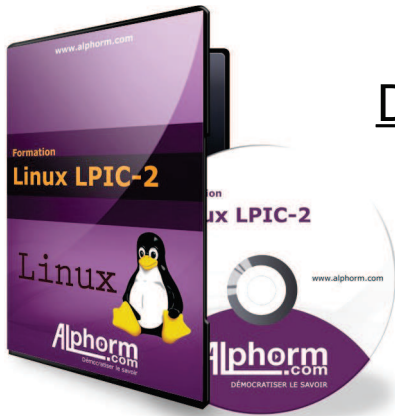
Weight : 4

Description : Candidates should be able to query and modify the behaviour of system services at various run levels. A thorough understanding of the init structure and boot process is required. This objective includes interacting with run levels.

Key Knowledge Areas:

- Linux Standard Base Specification (LSB)





Démarrage du système

Récupération du système

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- GRUB : personnalisation du démarrage
- GRUB legacy Shell
 - Commandes de démarrage
 - Commandes diverses
 - Sauvetage
- GRUB2 Shell
 - Sauvetage
- fsck



GRUB : personnalisation du démarrage

- Choix du système ou du kernel
 - flèches haut et bas sur le menu
- Single user mode
 - éditer une entrée du menu (touche e)
 - ajouter l'option "single" en fin de ligne "kernel"
 - Enter pour valider
 - Touche b pour démarrer
- Changer les paramètres du kernel
 - même démarche que pour le single user mode
 - remplacer "single" par le ou les paramètre(s)

GRUB legacy Shell

- permet d'interagir directement avec GRUB
 - via CLI
- disponible au démarrage (touche "c")
- ou sous GNU/Linux (et autres systèmes Unix)
 - par émulation

```
# grub
```

Commandes de démarrage

- afficher l'aide

```
grub > help
```

- sélectionner un périphérique racine

```
grub > root [DEVICE [HDBIAS]]
```

- chargement d'un kernel à partir du périphérique racine

```
grub > kernel [--no-mem-option] [--type=TYPE]
```

- chargement de modules

```
grub > module FILE [ARG ...]
```

```
grub > modulenounzip FILE [ARG ...]
```

- démarrage

```
grub > boot
```

Commandes diverses

- trouver sur quel bloc un fichier est stocké

```
grub > blocklist FILE
```

- afficher la "géométrie" d'un disque

```
grub > geometry DRIVE [CYLINDER HEAD SECTOR]
```

- création d'une nouvelle partition

```
grub > partnew PART TYPE START LEN
```

- chargement d'un initrd

```
grub > initrd FILE [ARG ...]
```

Sauvetage

- Démarre directement sur le shell
 - erreur la plus courante : GRUB ne trouve pas les fichiers nécessaires
- retrouver les fichiers (commande find)

GRUB2 Shell

- Basé sur le scripting
 - nombreuses commandes internes
 - disponibles aussi bien via la CLI interne que pour les scripts

Sauvetage

1) afficher l'aide

```
grub rescue> help
```

2) afficher les variables

```
grub rescue> set
```

3) lister les partitions reconnues

```
grub rescue> ls
```

4) redéfinir la valeur des variables

```
grub rescue> set prefix=(hd0,msdos3)/boot/grub
```

```
grub rescue> set root=hd0,msdos3
```

5) passer en mode normal si besoin

fsck

• Sortie

- 0 - Aucune erreur
- 1 - Erreurs du fs corrigées
- 2 - Le système doit être redémarré
- 4 - Erreurs du fs non corrigées
- 8 - Erreurs opérationnelles
- 16 - Erreur de syntaxe ou d'usage
- 128 - Erreur de librairie partagée

• Message : "fsck failed. Please repair manually"

- Ctrl-D pour ignorer
- sinon, entrer le mot de passe root pour lancer sulogin
 - accès à fsck et résolution des problèmes éventuels manuellement

Ce qu'on a couvert

- Résoudre les pannes au démarrage du système.

202.2 System recovery

Weight : 4

Description : Candidates should be able to properly manipulate a Linux system during both the boot process and during recovery mode. This objective includes using both the init utility and init-related kernel options.

Key Knowledge Areas:

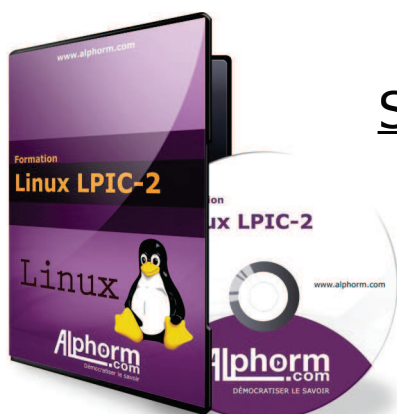
- inittab
- GRUB
- grub shell

The following is a partial list of the used files, terms and utilities:

- init
- mount
- fsck
- telinit



Alphorm.com



Système de fichiers et périphériques

Intervention sur le système de fichier GNU/Linux

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction : Rappels LPIC1
 - Créer un système de fichier
 - FAT
 - SWAP
 - mount
 - paramètres
 - umount
 - Fstab : exemple
 - Périphérique
 - Point de montage
 - fstype et options
 - dump et fsck
- Aller plus loin
 - État actuel des montages
 - UUID
 - Connaître l'UUID d'une partition
 - Générer un UUID
 - Vider le buffer



Introduction : Rappels LPIC1

- créer un système de fichier
 - création (formatage)
 - montage
 - manuel
 - automatique

Créer un système de fichier

```
# mkfs.fstype partition
```

```
# mkfs -t fstype partition
```

- Options :
 - -c : recherche de secteurs défectueux
 - -m *pourcentage* : pourcentage d'espace réservé
 - 5 par défaut

FAT

```
# mkfs.msdos partition
```

```
# mkfs.vfat partition
```

- Options :
 - -F fat-size : type / taille de FAT

SWAP

- Extension de la mémoire

- type code 0x82

- "formatage"

```
# mkswap partition
```

- utilisation

```
# swapon partition
```

- ou cf /etc/fstab

mount

```
$ mount [options] [device] [mountpoint]
```

- Options :

- -a : all (/etc/fstab)
- -r : ro
- -v : verbose
- -w : rw (défaut pour la plupart)
- -t fstype

- Options :

- -L label
- -U uuid
- -o paramètres

Paramètres

- default
- loop
- auto / noauto
- user / nouser
- users
- ro
- rw
- etc ...

mount

```
$ mount [options] [device] [mountpoint]
```

- | | |
|------------------------------------|-----------------|
| • Options : | • Options : |
| ▪ -a : all (/etc/fstab) | ▪ -L label |
| ▪ -r : ro | ▪ -U uuid |
| ▪ -v : verbose | ▪ -o paramètres |
| ▪ -w : rw (défaut pour la plupart) | |
| ▪ -t fstype | |

Paramètres

- default
- loop
- auto / noauto
- user / nouser
- users
- ro
- rw
- etc ...

umount

```
$ umount [options] [device] [mountpoint]
```

- Options :
 - -a : all
 - -f : force
 - -r : si échec, remonter en ro
 - -t fstype

Fstab : exemple

- /etc/fstab

#device	mount point	filesystem	options	dump	fsck
/dev/hda1	/	ext3	defaults	1	1
UUID=3631a288-673e-40f5-9e96-6539fec468e9 \	/usr	reiserfs	defaults	0	0
LABEL=/home	/home	reiserfs	defaults	0	0
/dev/hdb5	/windows vfat		uid=500,umask=0	0	0
/dev/hdc	/media/cdrom	iso9660	users,noauto	0	0
/dev/sda1	/media/pen	auto	users,noauto	0	0
server:/home	/other/home	nfs	users,exec	0	0
//winsrv/shr	/other/win	cifs	users,credentials=/etc/creds	0	0
/dev/hda4	swap	swap	defaults	0	0

Périphérique

#device	mount point	filesystem	options	dump	fsck
/dev/hda1	/	ext3	defaults	1	1
UUID=3631a288-673e-40f5-9e96-6539fec468e9 \	/usr	reiserfs	defaults	0	0
LABEL=/home	/home	reiserfs	defaults	0	0
/dev/hdb5	/windows vfat		uid=500,umask=0	0	0
/dev/hdc	/media/cdrom	iso9660	users,noauto	0	0
/dev/sda1	/media/pen	auto	users,noauto	0	0
server:/home	/other/home	nfs	users,exec	0	0
//winsrv/shr	/other/win	cifs	users,credentials=/etc/creds	0	0
/dev/hda4	swap	swap	defaults	0	0

- udev
- adresse
- UUID=uuid
- LABEL=label

Point de montage

#device	mount point	filesystem	options	dump	fsck
/dev/hda1	/	ext3	defaults	1	1
UUID=3631a288-673e-40f5-9e96-6539fec468e9 \	/usr	reiserfs	defaults	0	0
LABEL=/home	/home	reiserfs	defaults	0	0
/dev/hdb5	/windows	vfat	uid=500,umask=0	0	0
/dev/hdc	/media/cdrom	iso9660	users,noauto	0	0
/dev/sda1	/media/pen	auto	users,noauto	0	0
server:/home	/other/home	nfs	users,exec	0	0
//winsrv/shr	/other/win	cifs	users,credentials=/etc/creds	0	0
/dev/hda4	swap	swap	defaults	0	0

- dossier vide dans un autre fs
 - /
 - /home
 - swap

fstype et options

#device	mount point	filesystem	options	dump	fsck
/dev/hda1	/	ext3	defaults	1	1
UUID=3631a288-673e-40f5-9e96-6539fec468e9 \	/usr	reiserfs	defaults	0	0
LABEL=/home	/home	reiserfs	defaults	0	0
/dev/hdb5	/windows	vfat	uid=500,umask=0	0	0
/dev/hdc	/media/cdrom	iso9660	users,noauto	0	0
/dev/sda1	/media/pen	auto	users,noauto	0	0
server:/home	/other/home	nfs	users,exec	0	0
//winsrv/shr	/other/win	cifs	users,credentials=/etc/creds	0	0
/dev/hda4	swap	swap	defaults	0	0

- cf mount

dump et fsck

#device	mount point	filesystem	options	dump	fsck
/dev/hda1	/	ext3	defaults	1	1
UUID=3631a288-673e-40f5-9e96-6539fec468e9 \	/usr	reiserfs	defaults	0	0
LABEL=/home	/home	reiserfs	defaults	0	0
/dev/hdb5	/windows	vfat	uid=500,umask=0	0	0
/dev/hdc	/media/cdrom	iso9660	users,noauto	0	0
/dev/sda1	/media/pen	auto	users,noauto	0	0
server:/home	/other/home	nfs	users,exec	0	0
//winsrv/shr	/other/win	cifs	users,credentials=/etc/creds	0	0
/dev/hda4	swap	swap	defaults	0	0

- dump : sauvegarde de la partition
 - 1 = oui
 - 0 = non (quasi toujours à notre époque)
 - usage de dump déconseillé aujourd'hui
- fsck : vérification de l'intégrité du fs au démarrage
 - 0 = non (reiserfs)
 - 1 = premier (racine)
 - 2 ou plus = les autres, dans l'ordre

Aller plus loin

- état actuel des montages
- UUID
- sync

État actuel des montages

- via la commande mount

```
$ mount
```

- à partir du fichier /etc/mtab
 - configuration maintenue en espace utilisateur par mount
- fichier /proc/mounts
 - maintenu par le kernel
 - toujours à jour (contrairement à /etc/mtab)

UUID

- Universal Unique Disk Identifier
- nombre hexadécimal de 32 chiffres
 - 128bits
- permet d'identifier à peu près n'importe quoi
- ne change pas tant que le fs n'est pas modifié
 - évite toute reconfiguration en cas de changement d'identifiant de la partition
 - modification du branchement
 - OS multiples
 - etc ...

Connaître l'UUID d'une partition

```
# blkid /chemin/vers/la/partition
```

- Exemple

```
# blkid /dev/sda1
```

- sous Debian : paquet e2fsprogs

Générer un UUID

- Manuellement :
 - grâce au packet Debian : uuid-runtime

```
# uuidgen [-t|-r]
```

- deux méthodes des génération
 - -r : random (pseudo-aléatoire)
 - grâce à /dev/random
 - par défaut
 - -t : time-based
 - horloge système + adresse ethernet du système (si présent)
- Pour la génération automatique : uuidd (uuid daemon)

Vider le buffer

- stocké dans la RAM
- pour y supprimer les données stockées :

```
# sync
```

- appelé automatiquement
 - au reboot
 - à l'extinction

Ce qu'on a couvert

- La gestion et configuration des systèmes de fichier
 - formatage, montage et interrogation

203.1 Operating the Linux filesystem

Weight : 4

Description : Candidates should be able to properly configure and navigate the standard Linux filesystem. This objective includes configuring and mounting various filesystem types.

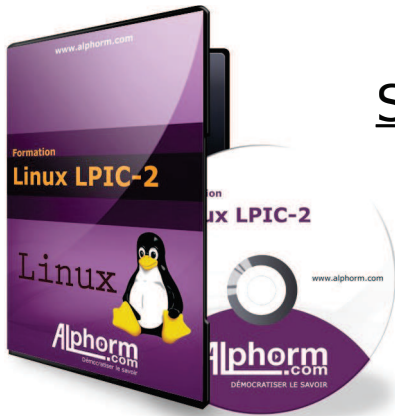
Key Knowledge Areas:

- The concept of the fstab configuration
- Tools and utilities for handling SWAP partitions and files
- **Use of UUIDs**

The following is a partial list of the used files, terms and utilities:

- /etc/fstab
- /etc/mtab
- /proc/mounts
- mount and umount
- sync
- swapon
- swapoff





Système de fichiers et périphériques

Maintenance d'un système de fichiers Linux

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- introduction
- Vérifier et réparer un système de fichiers
 - fsck
 - rappel démarrage
 - commande
 - e2fsck
 - xfs_check et xfs_repair
 - badblocks
- Afficher des informations sur le système de fichiers
 - dumpe2fs
 - xfs_info et xfs_metadump
- ajuster les paramètres des systèmes de fichiers
 - tune2fs
 - reiserfstune
 - xfs_admin
- Débugueurs pour systèmes de fichiers
 - debugfs et debugreiserfs
 - commandes de debugfs
- Sauvegarde d'un système de fichiers XFS
 - xfsdump
 - xfsrestore



Introduction

- des outils différents suivant les fs
 - ext (2,3,4)
 - ReiserFS
 - XFS
- cf LPIC1
 - Chapitre 5 – 13) Introduction aux fs

Vérifier et réparer un système de fichiers

- fsck
 - rappel démarrage
 - commande
- e2fsck
- badblocks
- xfs_check et xfs_repair
- badblocks



fsck

- une commande centrale
- vérifier l'intégrité d'un système de fichiers
 - et le réparer
- uniquement sur les fs non montés ou en ro

Rappel démarrage

- Sortie
 - 0 - Aucune erreur
 - 1 - Erreurs du fs corrigées
 - 2 - Le système doit être redémarré
 - 4 - Erreurs du fs non corrigées
 - 8 - Erreurs opérationnelles
 - 16 - Erreur de syntaxe ou d'usage
 - 128 - Erreur de librairie partagée
- Message : "fsck failed. Please repair manually"
 - Ctrl-D pour ignorer
 - sinon, entrer le mot de passe root pour lancer sulogin
 - accès à fsck et résolution des problèmes éventuels manuellement

Commande

```
# fsck [-sACVRTNP] [-t fstype] [--] [fsck-options] filesystems
```

- Options :

- -A : vérifier tout les fs marqués "à vérifier" dans /etc/fstab
- -C : indiquer une barre de progression (pour e2fsck)
- -V : verbose
- -N : test
- -t *fstype* : indiquer (forcer) le type de fs

e2fsck (fsck.e2fs)

```
$ e2fsck [ -pacnyrdfvstFSV ] device
```

- Options

- -s : sérialise les opérations de fsck
 - à favoriser dans le cas d'une vérification de plusieurs systèmes de fichiers en mode interactif
- -R : ignorer le système de fichier racine
 - dans le cas d'une analyse de tout les fs grâce à -A
- -a : réparer automatiquement le système de fichiers
 - sans poser de question
- -f : force la vérification même si le système de fichiers semble propre.
- -n : utilisation non interactive (par "non")
 - Ouvre en lecture-seule le système de fichiers
 - répond «non» à toutes les questions
- -y : Répond «yes» à toutes les questions
 - permet ainsi l'utilisation non interactive d'e2fsck.
- -P : Répare automatiquement (sans poser la moindre question)
 - en anglais «preen» signifie lisser

xfs_check et xfs_repair

- vérifier la cohérence d'un système de fichier XFS

```
$ xfs_check [options] device
```

- le plus souvent appelé via fsck.xfs
- réparer un système de fichier XFS corrompu ou endommagé
 - accède directement au périphérique grâce au raw device associé
 - permet de contourner le kernel (caches, buffers)

```
$ xfs_repair [options] device
```

- Le fs DOIT être démonté auparavant !

badblocks

- rechercher des blocs défectueux sur un périphérique

```
$ badblocks [options] [-o fichier_sortie] périphérique [dernier-bloc] [bloc-départ]
```

- recommandation : ne pas lancer directement
 - appeler via l'option -c de e2fsck ou mke2fs
- Option :
 - -o fichier_sortie
 - écrire la liste des blocs défectueux dans le fichier

Ⓛ Afficher des informations sur le système de fichiers

- dumpe2fs
- xfs_info et xfs_metadump



Ⓛ dumpe2fs

```
# dumpe2fs [options] device
```

- Options :
 - -b : affiche les blocs qui sont marqués défectueux.
 - -h : n'affiche que les informations de super-bloc

🕒 xfs_info et xfs_metadump

- informations techniques

```
# xfs_info device
```

- copier les métadonnées du fs

```
$ xfs_metadump
```

🕒 Ajuster les paramètres des systèmes de fichiers

- tune2fs
- reiserfstune
- xfs_admin



tune2fs

```
# tune2fs [options] device
```

- Options :
 - -c *max-mount-counts*
 - -C *mount-count*
 - -i *intervalle*
 - -j : journalisation
 - -m *pourcentage*
 - -r *blocs*

reiserfstune

- similaire à tune2fs
 - mais pour reiserfs

```
# reiserfstune [ -f ] [ -j | --journal-device FILE ]  
[ --no-journal-available ] [ --journal-new-device FILE ]  
[ --make-journal-standard ] [ -s | --journal-new-size N ]  
[ -o | --journal-new-offset N ] [ -t | --max-transaction-  
size N ] [ -b | --add-badbblocks file ] [ -B | --badblocks  
file ] [ -u | --uuid UUID ] [ -l | --label LABEL ] device
```

xfs_admin

```
# xfs_admin [options] device
```

- Options :
 - -j
 - -l
 - -u
 - -L *label*
 - -U *uuid*
 - -U generate

Débogueurs pour systèmes de fichiers

- debugfs
- debugreiserfs
- commandes debugfs



Debugfs et debugreiserfs

```
$ debugfs device
```

```
$ debugreiserfs device
```

- dumpe2fs + tune2fs + autres outils
- débogage

Commandes debugfs

- show_super_stats / stats
- stat nom_fichier
- undelete inode nom / undel inode nom
- lsdel / list_deleted_inodes
- write fichier-interne fichier-externe
- cd, ln, rm, etc ...
- list_requests / lr / help / ?
- quit

🕒 Sauvegarde d'un système de fichier XFS

- xfsdump
- xfsrestore



🕒 xfsdump

- créer un "dump" (image de sauvegarde incrémentielle)

```
# xfsdump [ options ] -f dest [ -f dest ... ] filesystem
```

- Exemples

- vers un périphérique de sauvegarde (bande magnétique)

```
# xfsdump -l 0 -p 30 -f /dev/st0 /home
```

- vers un fichier

```
# xfsdump -l 0 -p 30 -f /backups/home-backup /home
```

xfsrestore

- restaurer un fs à partir d'une sauvegarde

```
# xfsrestore [ options ] -f source [ -f source ... ] dest
```

- Exemple
 - mode itératif

```
# xfsrestore -i -f /backups/home-backup /newhome
```

Ce qu'on a couvert

- Vérifier et réparer un système de fichiers
- Optimiser un système de fichiers

203.2 Maintaining a Linux filesystem

Weight : 3

Description : Candidates should be able to properly maintain a Linux filesystem using system utilities. This objective includes manipulating standard filesystems.

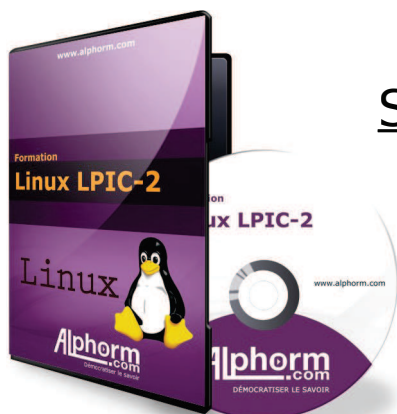
Key Knowledge Areas:

- Tools and utilities to manipulate and ext2, ext3 and ext4
- Tools and utilities to manipulate reiserfs V3
- Tools and utilities to manipulate xfs

The following is a partial list of the used files, terms and utilities:

- fsck (fsck.*)
- badblocks
- mkfs (mkfs.*)
- dumpe2fs, xfsdump, xfsrestore
- debugfs, debugreiserfs
- tune2fs, reiserfstune
- mkswap
- xfs_info, xfs_check and xfs_repair





Système de fichiers et périphériques montage automatique

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
- Autofs
- Configuration
- Fichier principal de configuration
- Fichiers de configuration additionnels



Introduction

- (re)montage automatique
 - grâce à un démon
 - à chaque fois d'un utilisateur tente d'accéder à un fs non monté
- Particulièrement utile pour :
 - les systèmes de fichiers accessibles via le réseau
 - les périphériques amovibles (CD-ROMS, clés usb, etc ...)

Autofs

- implémentation Linux du montage automatique
- composant noyau + démon **automount**
- montage automatique (NFS, CD-ROMs, etc ...)
- démontage après un certain temps sans utilisation

Configuration

- Un fichier principal
 - /etc/auto.master
- Des fichiers "additionnels"
 - généralement un par périphérique (ou type de périphérique)
 - exemple : /etc/auto.cdrom
- Relus à chaque rechargement du démon

```
# /etc/init.d/autofs reload
```

Fichier principal de configuration

- /etc/auto.master

```
# sample /etc/auto.master file
/var/autofs/floppy /etc/auto.floppy --timeout=2
/var/autofs/cdrom /etc/auto.cdrom - timeout=6, sync, nodev, nosuid
```

**dossier de montage fichier de configuration
(additionnel)**

options

- "point d'entrée" de la configuration de automount
- un démon par entrée

🔔 Fichiers de configuration additionnels

- Peuvent être nommés à votre convenance

```
# sample /etc/auto.floppy file  
floppy -user,fstype=auto :/dev/fd0
```

pseudo
répertoire

options de
montage

périphérique

- il est recommandé de se limiter à un périphérique par fichier additionnel
 - et donc par démon

⚠ les "pseudo répertoires" ne sont pas de réels dossiers

🔔 Ce qu'on a couvert

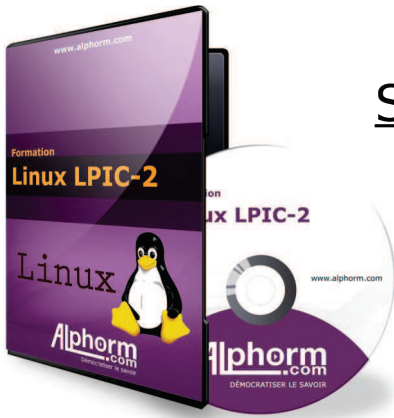
- Qu'est ce que autofs et automount
- les fichiers de configuration d'autofs
 - /etc/auto.master
 - /etc/auto.[dir]

Creating And Configuring Filesystem Options (203.3) - part 1

Weight : 2

Description : Candidates should be able to configure automount filesystems using AutoFS. This objective includes configuring automount for network and device filesystems. Also included is creating filesystems for devices such as CD-ROMs and a basic feature knowledge of encrypted filesystems.





Système de fichiers et périphériques

Systèmes de fichiers pour périphériques optiques

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
- HFS
- Comparatif
- Extensions à l'ISO9660
- Image
- Créer un système de fichier ISO
- Monter une image ISO
- Gravure d'une image ISO
- Faire une copie d'un disque optique



Introduction

- ISO 9660
 - système de fichier des CD-ROMs et DVD-ROMs
 - 3 niveaux :
 - 1 – compatibilité MS-DOS
 - 2 – noms de fichiers pouvant aller jusqu'à 32 caractères
 - 3 – fragmentation possible des fichiers
- remplacé progressivement par l'UDF
 - Universal Disk Format
 - ISO 13346
 - quasi indispensable pour les blu-rays
 - rétro-compatible
 - on peu "fermer" un UDF en ISO, mais ceci est irréversible

HFS

- Hierarchical File System (HFS)
 - inventé par Apple
 - à l'origine pour les disquettes et disques durs
 - pour Mac OS et z/OS

Comparatif

Système de fichiers	ISO 9660	UDF	HFS
Taille max de fichier	2/4Go (8To en level 3)	16Eo soit 16×10^{18} octets	2Go
Taille max d'image	théoriquement illimité	quasi illimité	2To
Nombre max de fichiers / répertoires	65535 répertoires	quasi illimité	65535 fichiers
Noms de fichiers	8.3 en level 1 32 en level 2	255 octets	31 caractères

ISO 9660 est également limité à une profondeur maximale de 8 dossiers incluant la racine

Extensions à l'ISO9660

- Joliet
 - définie et soutenue par Microsoft
 - limite des noms de fichiers passant à 64 caractères unicode
 - largement répandu et intégré aujourd'hui
- Rock Ridge
 - ajout de la sémantique des systèmes de fichiers POSIX
 - limite des noms de fichiers passant à 255 octets
 - UID, GID, timestamps, liens symboliques, devfiles
 - profondeur plus grande (que les 8 dossiers de l'ISO9660)
 - par défaut sous les systèmes Unix

Extensions à l'ISO9660

- El Torito
 - lancé par IMB et Phoenix Technologies (BIOS) en 1995
 - permet de booter à partir d'un support optique (LiveCDs)

Image

- Un cd n'est pas aussi simple à gérer que les autres types de périphériques de stockage
 - réécriture directe impossible
 - même pour les RW (suppression de toute l'image)
- Solution : créer une image avant gravure
 - sur disque dur ou autre
 - directement modifiable

🔗 Créer un système de fichier ISO

```
$ mkisofs [ options ] [ -o filename ] pathspec [pathspec ...]
```

- Exemple :

```
$ mkisofs -r -o cd_image private_collection/
```

- Depuis Debian Squeeze, est remplacé par genisoimage
 - fork avec options identiques
- Options
 - -r : tout fichier publiquement lisible et activation des extensions Rock Ridge
 - -J : MS Joliet extension

🔗 Monter une image ISO

```
$ mount -t iso9660 -o ro,loop=/dev/loop0 cd_image /cdrom
```

Gravure d'une image ISO

- Récupération des informations

```
$ cdrecord -scanbus
```

- Mise en place des variables (optionnel)

```
$ SCSI_BUS=0  
$ SCSI_ID=6  
$ SCSI_LUN=0
```

- Ecriture

```
$ cdrecord -v speed=2 dev=$SCSI_BUS,$SCSI_ID,$SCSI_LUN -data cd_image
```

- ou

```
$ cdrecord -v speed=2 dev=0,6,0 -data cd_image
```

Faire une copie d'un disque optique

- Vers un autre disque optique (par gravure directe)

```
$ cdrecord -v dev=0,6,0 speed=2 -isozsize /dev/scd0
```

- Vers un fichier

```
$ dd if=/dev/scd0 of=cdimage
```

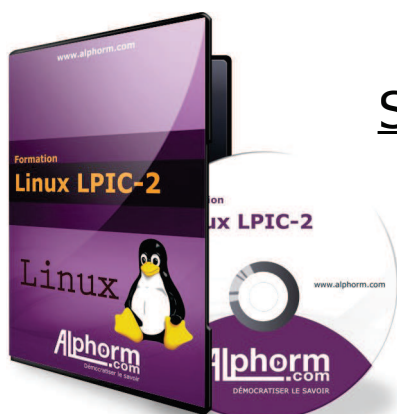
Ce qu'on a couvert

- Les différents systèmes de fichiers pour disques optiques
 - UDF, ISO9660, HFS
- Les extensions : Joliet, Rock Ridge, El Torito
- Comment créer une image ISO (mkisofs)
- Comment graver une image ISO.
- Comment faire une sauvegarde d'un disque optique (dd)

Creating And Configuring Filesystem Options (203.3) - part 2

Weight : 2

Description : Candidates should be able to configure automount filesystems using AutoFS. This objective includes configuring automount for network and device filesystems. **Also included is creating filesystems for devices such as CD-ROMs** and a basic feature knowledge of encrypted filesystems.



Système de fichiers et périphériques Introduction au chiffrement des systèmes de fichiers

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

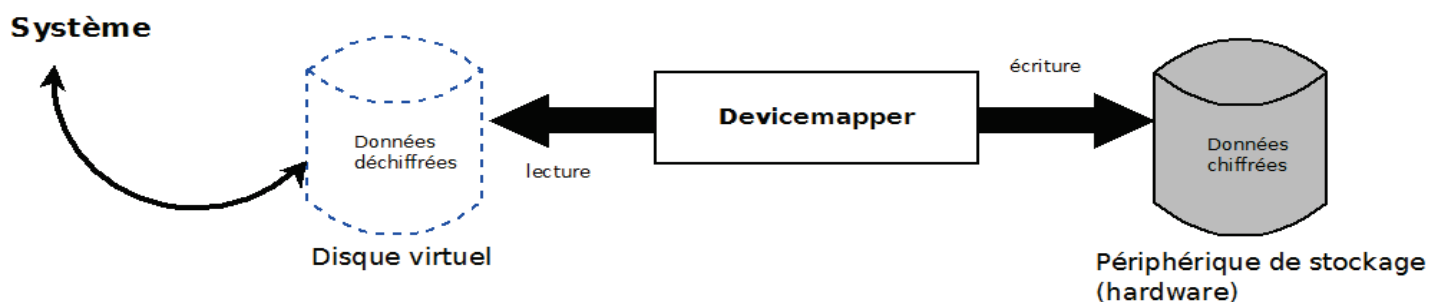
Plan

- Introduction
- Pré-requis
- Test



Introduction

- devicemapper
 - permet de mapper un périphérique bloc à un autre
 - utilisé par RAID et LVM (nous y reviendrons)



Pré-requis

- Pour les modules

```
# echo aes >> /etc/modules
# echo dm_mod >> /etc/modules
# echo dm_crypt >> /etc/modules
# modprobe -a aes dm_mod dm_crypt
```

- Mapper le périphérique avec devicemapper

```
# cryptsetup -y create crypt /dev/sda2
```

- créera un périphérique virtuel /dev/mapper/crypt

Pré-requis

- Ajout d'une entrée dans /etc/crypttab

```
# echo "crypt /dev/hda3 none none" >> /etc/crypttab
```

- Ajout d'une entrée dans /etc/fstab

```
# echo "/dev/mapper/crypt /crypt ext2 defaults 0 1" >> /etc/fstab
```

- Formatage

```
# mke2fs /dev/mapper/crypt
```

Test

- Montage manuel

```
# mkdir /crypt
```

```
# mount /crypt
```

- Le mot de passe entré lors du mappage vous sera demandé
 - il vous sera ensuite demandé à chaque montage
 - donc également à chaque démarrage

Ce qu'on a couvert

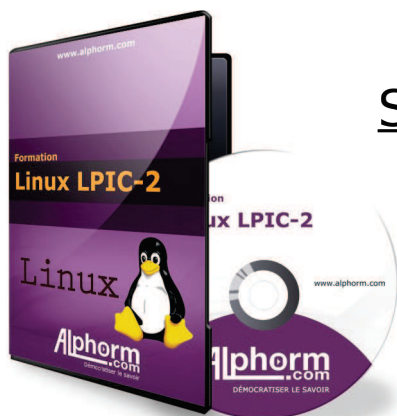
- Comment mettre en place rapidement un système de fichier chiffré.
 - ainsi qu'un petit rappel de mke2fs

Creating And Configuring Filesystem Options (203.3) - part 3

Weight : 2

Description : Candidates should be able to configure automount filesystems using AutoFS. This objective includes configuring automount for network and device filesystems. Also included is creating filesystems for devices such as CD-ROMs and a **basic feature knowledge of encrypted filesystems**.





Système de fichiers et périphériques

Gestion de périphérique udev

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

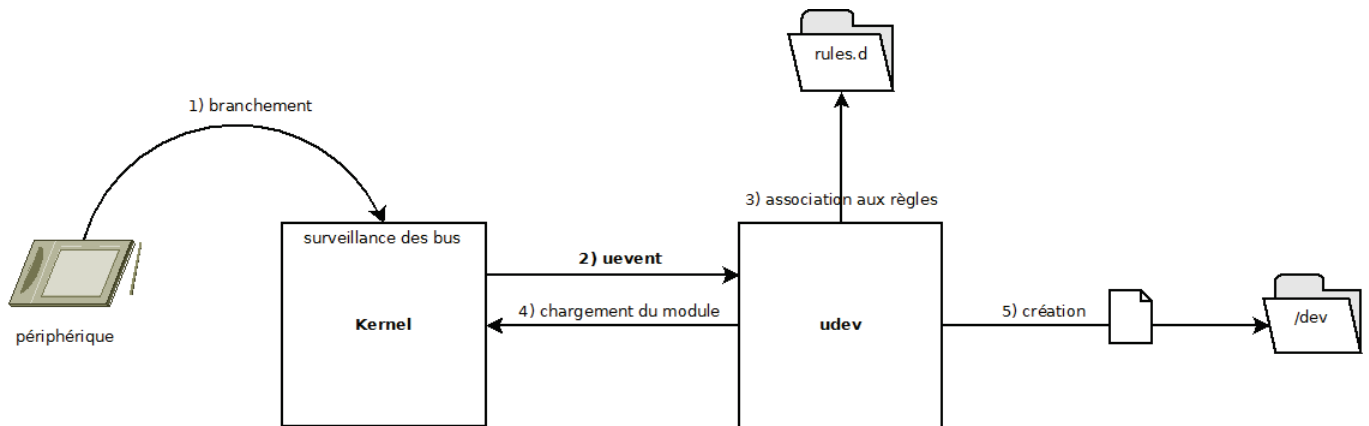
Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

Plan

- Introduction
- uevent
- Configuration
- Règles udev
- Opérateurs
- Quelques clés communes
- udevmonitor



Introduction



uevent

- envoyé par le kernel
 - à chaque (dé)branchement d'un périphérique
- contient les informations sur le périphérique
 - subsystem (net, usb, ...)
 - action (add, remove)
 - attributes (MAC address, vendor, ...)
- est analysé par udev grâce à des règles associées à ces informations

Configuration

- Dans /etc/udev/
 - udev.conf : fichier de configuration principal
 - modifier la priorité de logging (udev_log)
 - rules.d/ : règles personnalisées
 - sinon, lues à partir de /lib/udev/rules.d/

Règles udev

- dans /etc/udev/rules.d/
 - celles par défaut dans /lib/udev/rules.d/
- rassemblées par fichier (catégorie)
- une ligne par règle
 - constituée d'éléments clé/opérateur/valeur séparés par des virgules
- exemple :

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",  
ATTR{address}=="00:21:86:9e:c2:c4", ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"
```



ne jamais créer de règles pouvant entrer en conflit

Opérateurs

Catégorie	Op	Description
Comparaisons	==	égalité
	!=	inégalité
Affectation	=	fixe la valeur à ⚠️ remplace l'intégralité des éléments d'une liste
	+=	ajouter (à la fin d'une liste)
	:=	affectation définitive ⚠️ empêche toute modification ultérieure par une autre règle

Quelques clés communes

Clé	Description
KERNEL	nom de périphérique
SUBSYSTEM	sous-système contenant le périphérique
DRIVER	pilote du périphérique
NAME	nom du nœud associé au périphérique
SYMLINK	liste des liens symboliques noms alternatifs pour le périphérique
ATTR{xxx}	attribut sysfs (model, size, product, etc ...)
PROGRAM	appel d'un programme lors de "l'exécution" de cette règle
ENV{xxx}	valeur d'une variable d'environnement

udevmonitor

- affiche en temps réel
 - les uvents envoyés par le kernel
 - évènements envoyés par udev

```
$ udevmonitor
```

- lien symbolique vers

```
$ udevadm monitor
```

Ce qu'on a couvert

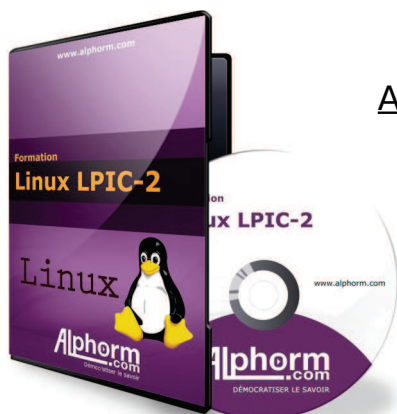
- les règles udev
- udevmonitor

203.4 udev Device Management

Weight : 1

Description : Candidates should understand device detection and management using udev. This objective includes troubleshooting udev rules.





Administration avancée des périphériques de stockage

Configuration RAID

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

Plan

- Introduction
- NRAID – RAID Linéaire
- RAID 0
- RAID 1
- RAID 4
- RAID 5
- RAID combiné
- Exemple : RAID 01
- Disque de rechange
- Pas à pas
- Multiple Devices Admin
- Modes : création et activation
- Modes : modification et surveillance
- Création d'un ensemble RAID
- `/etc/mdadm.conf`
- Résolution de panne
- `/proc/mdstat`



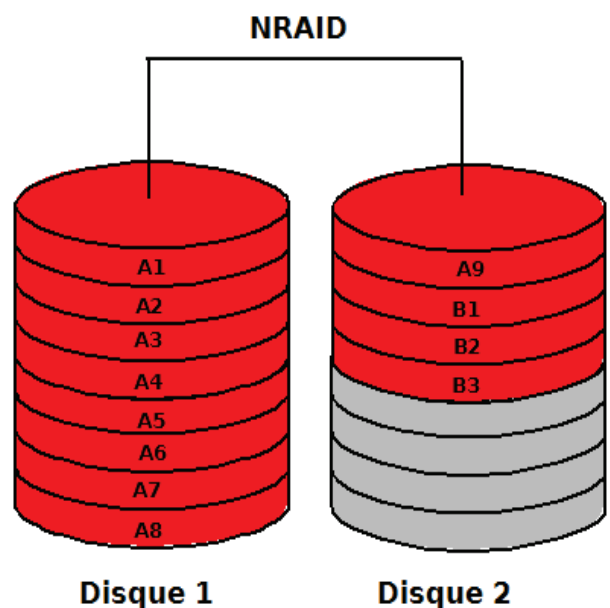
Introduction

- Redundant Array of Independent (or inexpensive) Disks
 - regroupement redondant de disques indépendants
 - groupement de périphériques blocs en un ensemble (ou matrice) RAID
- répartir les données sur plusieurs disques durs
 - tolérance aux pannes (récupération simplifiée)
 - performance
 - transactions par secondes
 - vitesse de transfert
 - sécurité
- logiciel ou matériel

NRAID – RAID Linéaire

- JBOD – Just a Bunch of Disks
- concaténation
 - écriture séquentielle
 - les données sont écrites sur le second disque quand le premier est plein
- aucune redondance
- aucune tolérance aux panne supplémentaire

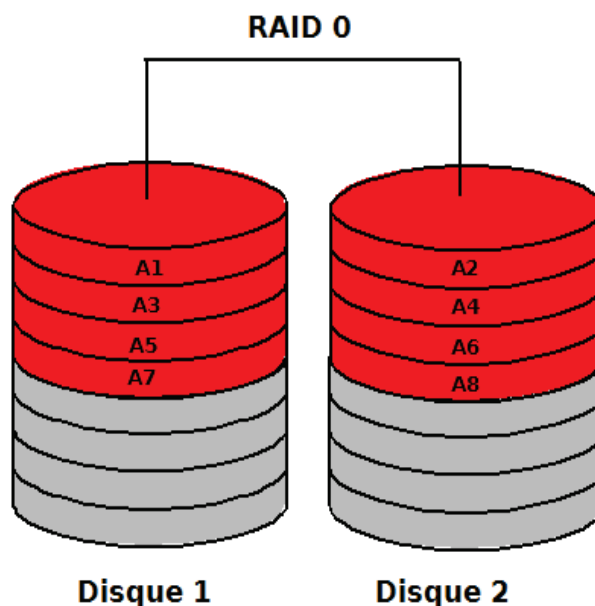
Capacité	somme de tout les disques
Fiabilité	aucune
Cout	minimal



RAID 0

- volume agrégé par bandes
 - "striping"
- répartition des blocs des fichiers
- parallélisation
 - augmentation des performances

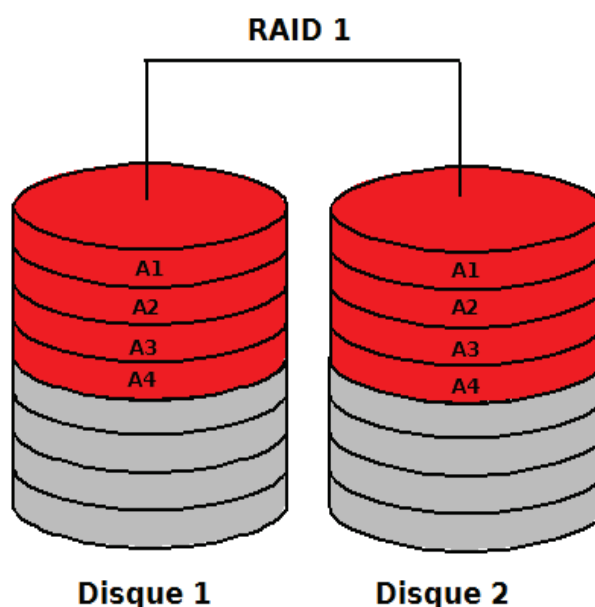
Capacité	plus petit élément x nombre d'éléments
Fiabilité	aucune
Cout	minimal



RAID 1

- redondance
 - "mirroring"
- permet de conserver les données en cas de panne

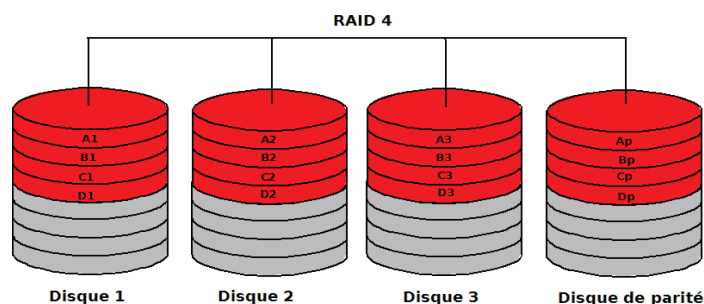
Capacité	plus petit élément
Fiabilité	optimale (tant qu'il reste un disque)
Cout	élevé (directement lié au nombre de miroirs)



RAID 4

- volume agrégé par bandes à parité
 - stripping + un disque de parités
- recalcule des données à partir du bloc de parité en cas de perte
- 3 disques minimum
- peu courant

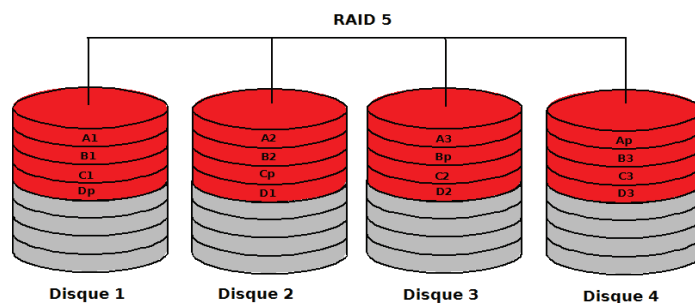
Capacité	de n-1 disques
Fiabilité	perte d'un disque à la fois maximum
Cout	optimal
Performances	très bonnes en lecture faible en écriture



RAID 5

- volume agrégé par bandes à parité répartie
 - RAID 4 réparti
 - répartition circulaire des blocs de parité
- le plus courant
 - meilleur rapport qualité prix

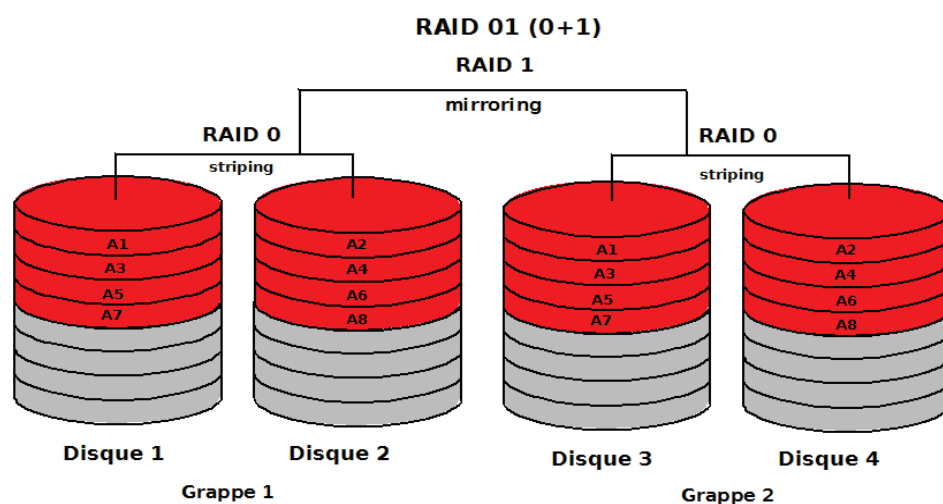
Capacité	de n-1 disques
Fiabilité	perte d'un disque à la fois maximum
Cout	optimal
Performances	très bonnes en lecture faible en écriture



RAID combiné

- Combinaison de différents niveaux de RAID
 - le premier chiffre indiquant le niveau de RAID d'une grappe
 - le second indiquant le niveau de RAID supérieur
- Cas courants
 - RAID 01
 - RAID 10
 - RAID 05
 - RAID 50
 - RAID 51

Exemple : RAID 01



- Minimum
 - 2 grappes
 - 2 disques / grappe

Disque de rechange

- "spare" ou "hotspare"
- disque complémentaire
 - non utilisé
 - prend automatiquement le relais en cas de défaillance d'un des disques du RAID
 - la reconstruction de celui-ci pouvant prendre beaucoup de temps
- après coup, remplacer le disque défaillant
 - qui deviendra un nouveau disque de rechange

Pas à pas

- 1) préparer les partitions pour l'auto-détection
 - partition type : fd (Linux RAID auto)
 - via fdisk (commande t)
- 2) création d'un ensemble RAID
 - périphérique /dev/md[n]
 - via mdadm --create (cf plus loin)
- 3) création du système de fichier
 - via mkfs -t xxx /dev/md[n]
- 4) création du fichier /etc/mdadm.conf
- 5) création du point de montage
- 6) édition de /etc/fstab
- 7) montage

Multiple Devices Admin

```
# mdadm [mode] <raiddevice> [options] <component-devices>
```

- 9 modes : Assemble, Build, Create, Follow (ou Monitor), Grow, Incremental, Manage, Auto-detect & Divers
- pour lancer une commande dans un mode :
 - `--nomdumode`
 - ou `-X` (première lettre du mode, à l'exception d'Auto-detect)
 - Exemple : `--create` ou `-C`

Modes : création et activation

- **create** : créer et activer un ensemble RAID à partir de zéro
- **build** : construire un ensemble RAID sans superbloc pour chaque périphérique
 - ne détruit pas les données pré-existantes
 - utile lors de la récupération de données corrompues
 - ne peut être utilisé avec `mdadm.conf`
- **assemble** : reconstruire un ensemble RAID pré-existante
 - migrer un ensemble vers un autre hôte
 - activer un ensemble au démarrage
- **auto-detect** : activer tout ensemble RAID auto-déecté, via le kernel

Modes : modification et surveillance

- **incremental** : ajouter / supprimer un périphérique d'un ensemble RAID
- **manage** : agir sur les composants spécifiques d'un ensemble RAID
 - suppression de disques défectueux
 - ajout de périphériques de rechange
- **follow / monitor** : surveiller un ou plusieurs périphérique md, et agir sur tout changement d'état
- **grow** : modifier un ensemble RAID existant
 - ajout / suppression de périphérique
- **misc** : "tout le reste" (pas d'option spécifique)
 - opérations sur les ensembles RAID actifs
 - effacer de vieux super-blocks
 - récupération d'informations

Création d'un ensemble RAID

- création d'un ensemble /dev/md0 en RAID1

```
# mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 \  
/dev/sdb1 /dev/sdc1
```

- identique à

```
# mdadm -Cv /dev/md0 -l1 -n2 /dev/sdb1 /dev/sdc1
```

- avec périphérique de rechange

```
# mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 \  
/dev/sdb1 /dev/sdc1 --spare-devices=1 /dev/sdd1
```

- pour surveiller l'état d'avancement de la construction

```
# watch -n 1 cat /proc/mdstat
```

/etc/mdadm.conf

- optionnel
- simplifie des tâches courantes

- génération (mode "Divers")

```
# mdadm --detail --scan --verbose > /etc/mdadm.conf
```

- réassemblage à partir du fichier

```
# mdadm --assemble --scan
```

- opération réalisée au démarrage
- via /etc/rc.d/rc.sysinit ou /etc/init.d/rcS

Résolution de panne

- retirer un disque défectueux d'un ensemble RAID

```
# mdadm --manage /dev/md0 --remove /dev/sdb1
```

- ajout d'un nouveau disque (après remplacement)

```
# mdadm --manage /dev/md0 --add /dev/sdb1
```

- l'ensemble RAID est alors reconstruit

 ne pas oublier de reconstruire le fichier mdadm.conf

/proc/mdstat

- contient les statistiques sur les ensembles RAID
- suivre la (re)construction d'un ensemble RAID

```
# watch -n 1 cat /proc/mdstat
```

Ce qu'on a couvert

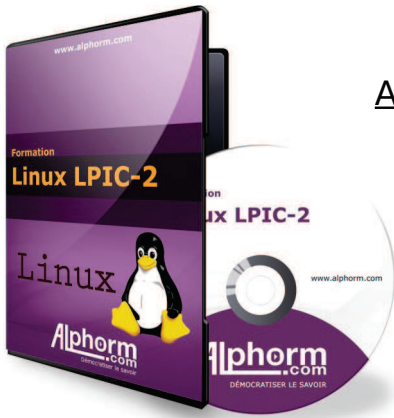
- Configuration et implémentation de RAID logiciel sous GNU/Linux.
- mdadm.conf
- mdadm
- mdstat
- ainsi qu'un rapide rappel de fdisk

204.1 Configuring RAID

Weight : 2

Description : Candidates should be able to configure and implement software RAID. This objective includes using and configuring RAID 0, 1 and 5.





Administration avancée des périphériques de stockage

Ajustement des accès aux périphériques de stockage

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

Plan

- Configurer l'interaction du kernel avec un fs ext
- Paramètres de disques durs PATA
- Paramètres de disques durs SCSI
- Modifier les paramètres du Kernel
- Sysctl



Configurer l'interaction du kernel avec un fs ext

```
# tune2fs [options] device
```

- Options :
 - -e [continue | remount-ro | panic]
 - définie comment le kernel doit réagir dans le cas d'une erreur sur le système de fichier
 - ignorer l'erreur et la reporter à l'application, remonter le fs en lecture uniquement ou kernel panic (arrêt du système)
 - -m reserved_block_percentage
 - 5 % par défaut

Configurer l'interaction du kernel avec un fs ext

```
# tune2fs [options] device
```

- Options :
 - -O [^]mount_option
 - options de montage (mount et fstab étant prioritaires)
 - ^ pour supprimer l'option
 - -s [0|1]
 - active (1) ou désactive (0) la fonctionnalité "sparse superblock"
 - réduire le nombre de copies de sauvegarde du superblock
 - dans groupes de blocks spécifiques au lieux de dans chaque groupe de blocks
 - l'activer permet d'économiser de l'espace sur les fs de très grand taille
 - relancer e2fsck après modification de cette option

Paramètres de disques durs PATA

```
# hdparm [options] [device]
```

- tester les performances des disques ATA
- ajuster leurs paramètres
- la plupart de ses options n'auront aucun effet sur les disques SCSI
 - y compris la plupart des SATA, USB et même PATA pilotés par le sous-système SCSI

Paramètres de disques durs PATA

```
# hdparm [options] [device]
```

- Options
 - -a : obtenir/modifier le nombre de secteurs pour la "lecture en avance" (read-ahead)
 - tampon, améliore les performances lors de la lecture séquentielle de longs fichiers
 - 8 (4ko) par défaut (convient dans la plupart des cas)
 - pour une lecture très aléatoire, ou un disque à read-ahead intégré, baisser cette valeur / supprimer cette fonction peu améliorer les performances
 - -d [0|1] : (dés)activer la fonction "using_dma"
 - Direct Memory Access (cf LPIC1 - Hardware - Introduction)
 - access direct à une zone mémoire
 - améliore quasi systématiquement les performances

Paramètres de disques durs PATA

```
# hdparm [options] [device]
```

- Options
 - -g : Affiche la géométrie du disque
 - cylindres, têtes, secteurs
 - capacité (en secteurs)
 - adresse (en secteurs) du début du périphérique par rapport au début du disque
 - -i : Affiche les informations d'identification
 - fournies par le disque au démarrage
 - -r [0|1] : Obtient/modifie le drapeau de lecture seule pour le périphérique

Paramètres de disques durs PATA

```
# hdparm [options] [device]
```

- Options
 - -t : minutage de lecture (sans mise en cache préalable) du périphérique pour benchmarking.
 - à réaliser 2 ou 3 fois sur un périphérique inactif
 - avec au moins quelques Mo de libre
 - -T : minutage de lecture du cache du périphérique pour benchmarking
 - vitesse de lecture directement depuis le tampon de Linux sans accès disque
 - indication du débit du processeur, cache et mémoire du système testé
 - -v : afficher tout les réglages, sauf -i

Paramètres de disques durs SCSI

```
# sdparm [options] [device]
```

- N'est pas exactement un équivalent SCSI à hdparm
 - Obtenir des informations sur les périphériques SCSI
 - SCSI mode page, VPD (Vital Product Data)
 - Modifier leurs paramètres
 - Envoyer des commandes SCSI au périphérique
- Utile pour tous les disques pilotés via le sous-système SCSI
 - cependant, modifier les paramètres d'un SATA reconnu comme SCSI ne sera pas toujours valable

Paramètres de disques durs SCSI

```
# sdparm [options] [device]
```

- Options
 - -a / --all : afficher tous les champs reconnus pour le type de périphérique
 - -e / --enumerate : afficher des informations sur les pages et champs modifiables via sdparm
 - -g *field* / --get *field* : afficher un champ particulier
 - -i / --inquiry : afficher les pages d'information VPD
 - -l / --long : afficher des informations supplémentaires

Paramètres de disques durs SCSI

```
# sdparm [options] [device]
```

- Options
 - -s STR=n / --set=STR=n : affecter la valeur au champs donné
 - ⚠ à utiliser avec grande précaution
 - -C CMD / --command=CMD : envoyer une commande SCSI au périphérique
 - Exemple : désactiver un périphérique

```
# sdparm --command=stop /dev/sdb
```

Modifier les paramètres du Kernel

- via procfs
 - cf LPIC1 - Hardware - Procfs
- Deux solutions
 - édition directe des pseudo-fichiers

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

- ne persiste pas après redémarrage
- nécessite que ces commandes soit appelées via un init script
- sysctl

Sysctl

```
# sysctl [-n] [-e] [-a | -A | -p filename | -w variable=value ]
```

- Options
 - -a / -A : afficher toutes les valeurs actuellement disponibles
 - -e : ignorer les erreurs liées aux clés inconnues
 - -n : désactiver l'affichage du nom de clé
 - n'affiche que sa valeur
 - -p filename : charger les paramètres à partir du fichier spécifié
 - /etc/sysctl.conf si aucun spécifié
 - "-" pour lire à partir de l'entrée standard
 - -w variable=value : modifier un paramètres

Ce qu'on a couvert

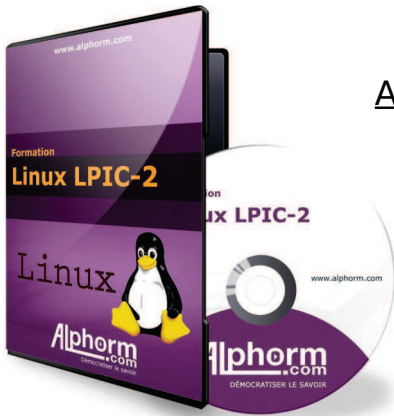
- Afficher et modifier les paramètres des disques durs via
 - tune2fs
 - hdparm
 - sdparm
 - sysctl

204.2 Adjusting Storage Device Access

Weight : 1

Description : Candidates should be able to configure kernel options to support various drives. This objective includes software tools to view & modify hard disk settings.





Administration avancée des périphériques de stockage

Logical Volume Manager

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
- Pas à pas
- Initialiser les volumes physiques
- Créer un groupe de volumes
- Création de volumes logiques
- Étendre un volume logique
- Clichés (Snapshots)
- Effectuer une sauvegarde à partir d'un cliché



Introduction

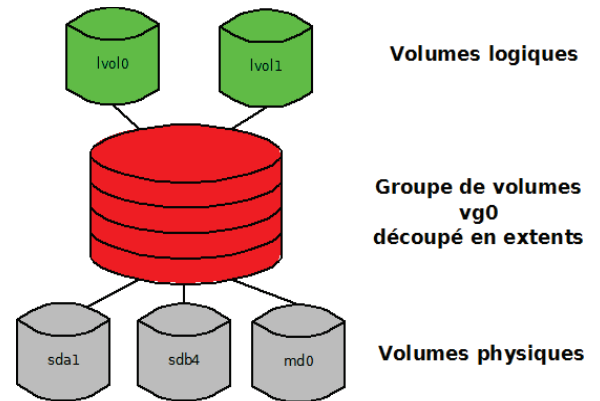
- création et gestion de volumes logiques sous GNU/Linux

- Permet une gestion plus "souple" des périphériques de stockage

- redimensionnement
- fonctionnalités supplémentaires

- fiabilité dépendant de l'ensemble des périphériques utilisés

- ie : un périphérique tombe en panne et tout les volumes logiques sont perdus
- donc, à utiliser avec du RAID



Pas à pas

- 1) optionnel : création des partitions sur les périphériques

- via fdisk
- il est recommandé de bien définir leur type code (8E)

- 2) initialiser les volumes physiques (PV)

- via pvcreate (ou automatiquement à l'étape suivante)

- 3) créer un groupe de volumes (VG)

- via vgcreate

- 4) créer les volumes logiques (LV)

- via lvcreate

- 5) mettre en place les systèmes de fichiers sur les LV

- via mkfs

Initialiser les volumes physiques

```
# pvcreate [options] VolumePhysique [VolumePhysique ...]
```

- Initialise les volumes physiques pour une utilisation ultérieure via LVM
 - partition de disque
 - disque entier
 - doit être remis à zéro via la commande suivante

```
# dd if=/dev/zero of=PhysicalVolume bs=512 count=1
```

- meta périphérique (md) - recommandé
- périphérique de loopback

Créer un groupe de volumes

```
# vgcreate [options] VolumeGroupName PhysicalDevicePath [PhysicalDevicePath...]
```

- si les périphériques n'ont pas été initialisés via pvcreate, ils le seront automatiquement
- Exemple

```
# vgcreate vg0 /dev/sda1 /dev/sdb1
```

- Par défaut, les PE (Physical Extents) sont de 4Mo
 - modifiable via l'option
 - -s, --physicalextentsize PhysicalExtentSize[bBsSkKmMgGtTpPeE]

Création de volumes logiques

```
# lvcreate [options] VolumeGroup{Name|Path}
```

- Options
 - -L, --size LogicalVolumeSize[bBsSkKmMgGtTpPeE]
 - définit la taille du volume logique

- Exemple

```
# lvcreate -L 100M volume01
```

- créé un volume logique de 100Mo
 - nommé par défaut /dev/volume01/lvol0
- Les opérations suivantes sont usuelles (mkfs, mount, etc ...)

Étendre un volume logique

- Si besoin, ajouter un PV au VG

```
# vgextend volume01 /dev/hda6
```

- Étendre le LV

```
# lvextend -L +50M /dev/volume01/lvol0
```

- Puis étendre le système de fichier (démonté)

```
# xfs_growfs /dev/volume01/lvol0
```

- ou, pour l'ext

```
# resize2fs /dev/volume01/lvol0
```

Clichés (Snapshots)

- Copie virtuelle d'un LV
 - facile la sauvegarde
 - accessible en écriture depuis LVM2
 - ouvre de nombreuses possibilités (testing, XEN, etc ...)
- Exemple : créer une snapshot /dev/volume01/snapshot0

```
# lvcreate -L 10g -s -n snapshot0 /dev/volume01/lvol0
```

 n'est **PAS** une sauvegarde

- n'enregistre que les **MODIFICATIONS** apportées au LV, pas les données
- disparaît en cas de redémarrage
- taille évolutive (10Go est donc ici la taille maximum)

Effectuer une sauvegarde à partir d'un cliché

- Monter la snapshot

```
# mount /dev/volume01/snapshot0 /mnt/snap
```

- Copier les données

```
# tar -cvzf /backups/snap.tar.gz /mnt/snap
```

- Démonter et détruire la snapshot

```
# umount /dev/volume01/snapshot0  
# lvremove /dev/volume01/snapshot0
```

Ce qu'on a couvert

- Gestion de LVM
 - création et suppression de LV, PV et VG
 - snapshots
 - redimensionnement

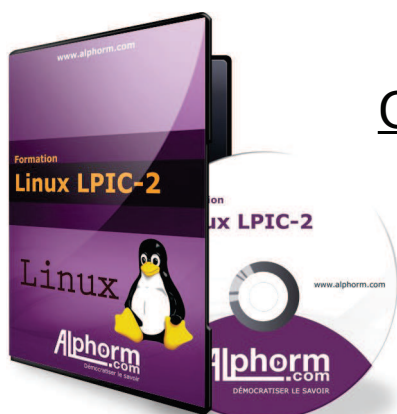
204.3 Logical Volume Manager

Weight : 3

Description : Candidates should be able to create and remove logical volumes, volume groups, and physical volumes. This objective includes snapshots and resizing logical volumes.



Alphorm.com



Configuration Réseau OpenVPN

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

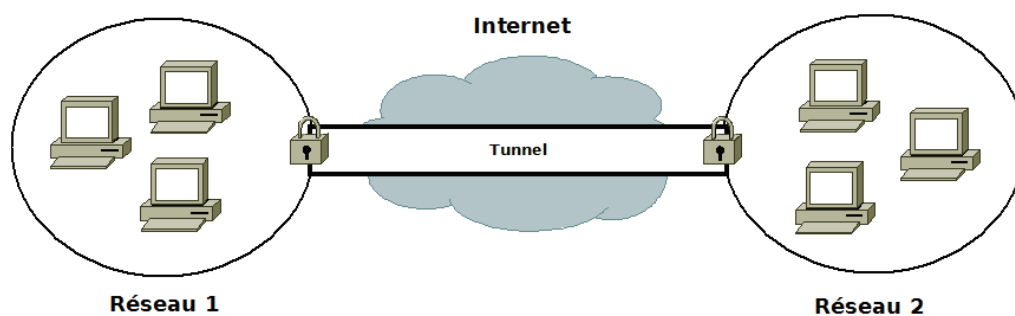
Plan

- Introduction
- OpenVPN
- Exemple simple : point à point
- Configuration serveur
- Configuration client



Introduction

- Virtual Private Network
 - réseau privé virtuel
- Connecter plusieurs réseaux distants
 - de manière sécurisée (tunnel chiffré)
 - via une connexion non-sécurisée (ex : internet)



OpenVPN

- Logiciel Libre (GNU GPL)
- Disponible sur de nombreux OS (GNU/Linux, Windows, BSD, Mac OS X, etc ...)
- Créé en 2002
 - par James Yonan
 - version actuelle : 2.3.2
 - Juin 2013



- Authentification via la bibliothèque OpenSSL
- Sécurisé via chiffrement SSL/TLS

Exemple simple : point à point

- VPN point à point
 - entre un serveur vpn.alphorm.com / 10.1.1.1 et un client 10.1.1.2
 - port par défaut (1194)
- Création de la clé statique

```
$ openvpn --genkey --secret static.key
```

- Copier cette clé sur le serveur et le client

Configuration serveur

- server.conf

```
# type d'interface
dev tun
# adresse IP serveur / client
ifconfig 10.1.1.1 10.1.1.2
# test de connection toutes les 10 secondes, considéré comme indisponible au bout de 60
secondes sans réponse
keepalive 10 60
# relancer la connection si elle semble coupée
ping-timer-rem
# empêcher OpenVPN de fermer et ré-ouvrir le tun/tap à la reception d'un signal SUGSR1
persist-tun
# idem mais pour les fichiers clés
persist-key
# clé secrète partagée pour le chiffrement
secret static.key
```

- tun/tap : interface de communication réseaux entre le kernel et les programmes de l'espace utilisateur

Configuration client

- client.conf

```
# serveur distant
remote vpn.alphorm.com
dev tun
ifconfig 10.1.1.2 10.1.1.1
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
secret static.key
```

Ce qu'on a couvert

- Qu'est ce que le VPN.
- Introduction à la configuration d'OpenVPN

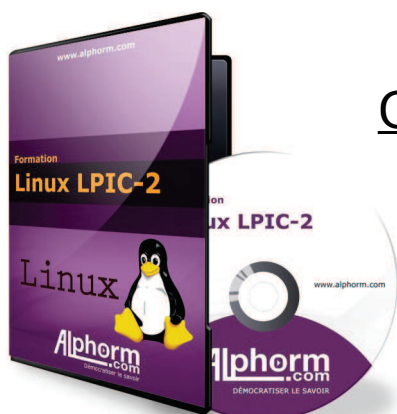
205.2 Advanced Network Configuration and Troubleshooting (Part 1)

Weight : 4

Description : Candidates should be able to configure a network device to implement various network authentication schemes. This objective includes configuring a multi-homed network device, **configuring a VPN client** and resolving communication problems.



Alphorm.com



Configuration Réseau

Surveillance et analyse de trafic TCP/IP

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- netcat
- netcat : options générales
- Scanner de ports avec netcat
- Netcat client / serveur
- Netstat
- Analyse de paquets avec Tcpdump
- Analyse de paquets avec Wireshark
- nmap : scanner de ports et plus



netcat

```
$ nc [ options ] [ hostname ] [ ports ]
```

- Le couteau suisse du TCP/IP
 - gestion des sockets (peu établir n'importe quelle connexion)
 - s'utilise aussi bien en tant que client que serveur
 - scriptable
 - multiplateforme (disponible sous Windows et Mac OS X)
 - nombreux usages
 - capture de bannière
 - scan de ports
 - etc ...

netcat : options générales

```
$ nc [ options ] [ hostname ] [ ports ]
```

- Options :
 - -u : passer en mode UDP
 - -i *int* : effectuer l'opération suivant un intervalle de *int* secondes
 - -v : verbose
 - -vv pour plus d'informations
 - -x adresse[:port] : connexion via un proxy

Scanner de ports avec netcat

- Scanner des ports 100 à 1, puis 443

```
$ nc -vv 127.0.0.1 1-100 443
```

- -r pour scanner aléatoirement (plus discret)
- par défaut, se stoppe dès qu'il trouve un port ouvert, et attend une E/S
 - -z pour passer en mode zero I/O

- Exemple

```
$ nc -vv -i 3 -r -z 127.0.0.1 21 23 80-160 1337
```

Netcat client / serveur

- ouvrir netcat en mode listening (serveur) sur le port 1337

```
$ nc -l -p 1337
```

- -k pour continuer à écouter après réception d'une connexion

- se connecter au serveur (coté client)

```
$ nc monserveur 1337
```

- Exemple : transfert de fichiers

- serveur

```
$ cat file.tar.gz | nc -l 1337
```

- client

```
$ nc monserveur 1337 > file.tar.gz
```

Netstat

```
$ netstat [options]
```

- Afficher un grand nombre d'informations

- connections
- tables de routage
- statistiques sur les interfaces
- connexions masquées
- messages netlink
- multicasts

- Considéré comme obsolète

- remplacé par ss et ip

Netstat

```
$ netstat [options]
```

- Options

- aucune : lister les sockets ouverts
- -a : Affiche toutes les connexions TCP actives et les ports TCP et UDP sur lesquels l'ordinateur écoute
- -i *iface* / --interface=*iface* : afficher les informations sur une interface
 - similaire à ifconfig ou ip -s link
- -r / --route : afficher les tables de routage noyau
 - similaire à ip route
- --masquerade / -M : afficher les informations relatives aux connexions masquées
 - fonctionnalité NAT de Linux
 - réseaux "cachés" derrière une unique adresse IP
- -p / --programs : afficher le nom et le PID des processus propriétaires de chaque socket

Analyse de paquets avec Tcpdump

```
# tcpdump [options] [-i interface] [pcap-filter expression]
```

- obtenir les détails sur le trafic visible depuis une interface
 - une ligne par paquet
- date protocole source:port > destination:port : informations
- Exemple

```
# tcpdump -i eth1 host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
11:48:56.922382 IP debian.local > google-public-dns-a.google.com: ICMP echo request, id 2933, seq 1,
length 64
11:48:57.053722 IP google-public-dns-a.google.com > debian.local: ICMP echo reply, id 2933, seq 1,
length 64
11:48:57.922897 IP debian.local > google-public-dns-a.google.com: ICMP echo request, id 2933, seq 2,
length 64
11:48:57.989884 IP google-public-dns-a.google.com > debian.local: ICMP echo reply, id 2933, seq 2,
length 64
```

Analyse de paquets avec Wireshark

- Anciennement dénommé Ethereal (avant mai 2006)
- Disponible sur les systèmes Unix et Windows
- Né en 1998, grâce à Gerald Combs
- Deux solutions :
 - GUI
 - ligne de commande : TShark

```
# tshark [-i interface] [pcap-filter expression]
```

nmap : scanner de ports et plus

- TCP connect scan

```
# nmap -sT hostname
```

- UDP scan

```
# nmap -sU hostname
```

- identification des machines d'un réseau

```
# nmap -sP <cible>
```

- identifier l'OS d'une machine

```
# nmap -O --osscan-guess 127.0.0.1
```

Ⓛ Ce qu'on a couvert

- netcat
- netstat
- tcpdump
- wireshark
- nmap

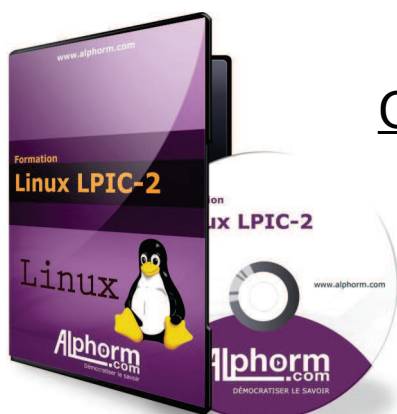
205.2 Advanced Network Configuration and Troubleshooting (Part 2)

Weight : 4

Description : Candidates should be able to configure a network device to implement various network authentication schemes. This objective includes configuring a multi-homed network device, configuring a VPN client and **resolving communication problems**.



Alphorm.com



Configuration Réseau

Dépannage réseau

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Exemple de méthodologie
- Couches physique et liaison
- Couche réseau
- Couche transport
- Couche application
- Problèmes de résolution de nom
- Problèmes de résolution de nom : dig
- Autres éléments à vérifier



Exemple de méthodologie

- 1) lister les composants impliqués
 - interface réseau, routeur, hôte distant, etc ...
- 2) établir leur interaction
 - chemin emprunté par un paquet
 - cf Prime
- 3) Déterminer le contexte du problème
 - Qui, quoi, où, quand, comment, combien (de postes affectés), pourquoi ?
- 4) Déterminer la cause exacte de la panne à partir du modèle TCP/IP
 - a. Couche physique
 - b. Couche liaison de données
 - c. Couche réseau
 - d. Couche transport
 - e. Couche application

Rappel : Modèle TCP/IP

Couche	Description	Exemples
physique	caractéristiques physiques de la communication	câble, fibre optique, radio
liaison	mode de transport des paquets sur la couche physique	Ethernet, Token Ring, SLIP, ATM
réseau	acheminement de paquets à travers un seul réseau	IP
transport	fiabilité des échanges et détermination de l'application à laquelle chaque paquet de données doit être délivré	TCP, UDP
application	programmes réseaux	HTTP, SMTP, FTP, SSH, DNS

Couches physique et liaison

- vérifier que les câbles sont branchés et les hôtes sous-tension
 - contrôle visuel ou logiciels de monitoring
- vérifier que les cartes réseau sont actives
 - ifconfig, ip, ifup

Couche réseau

- Puis-je joindre l'hôte distant ? Le(s) routeur(s) ? Le firewall ?
- Puis-je joindre d'hôtes hôtes du réseau ? D'internet ?
- D'autres hôtes peuvent ils joindre l'hôte distant ?
 - ping, traceroute
- vérifier la configuration ip
 - ifconfig, ip, dhclient
- vérifier la configuration de vos routes
 - ip, route
- Pour aller plus loin : sniffing
 - permet d'analyser en détail les paquets émis ou reçus
 - tcpdump, wireshark, etc ...

Couche transport

- Puis-je joindre l'hôte sur le port désiré ?

```
$ telnet <hote> <port>
```

- Ici encore, sniffing
- Le problème peu alors par exemple être lié à un routeur ou firewall

🐧 Couche application

- Configuration de l'application cliente
 - tester avec un autre client
 - vérifier les paramètres
- Configuration de l'application serveur

🐧 Problèmes de résolution de nom

- Tester via ping, host ou dig
- /etc/resolv.conf : ip des dns
- /etc/hosts : résolution de noms statique
- /etc/hostname ou /etc/sysconfig/network : nom d'hôte d'une machine
- retrouver l'ip / le CNAME d'un hôte (et les MX d'un domaine)

```
$ host <hote ou domaine>
```

- afficher toutes les informations relatives à un domaine / hôte

```
$ host -a <hote ou domaine>
```

Problèmes de résolution de nom : dig

- Vérifier les enregistrements de type A d'un domaine

```
$ dig <domaine>
```

- Connaître l'adresse ip du serveur dns faisant autorité sur un domaine

```
$ dig <domaine> +short
```

- Trouver un nom d'hôte à partir d'une ip

```
$ dig -x 92.121.176.140 +short
```

- Vérifier les enregistrements MX d'un domaine

```
$ dig mx midia.fr +short
```

Autres éléments à vérifier

- Démarrage
 - /var/log/messages
 - dmesg
 - init scripts
- Système
 - /var/log/syslog
- sécurité
 - /etc/host.deny et /etc/host.allow
- configuration réseau
 - /etc/sysconfig/network-scripts ou /etc/network

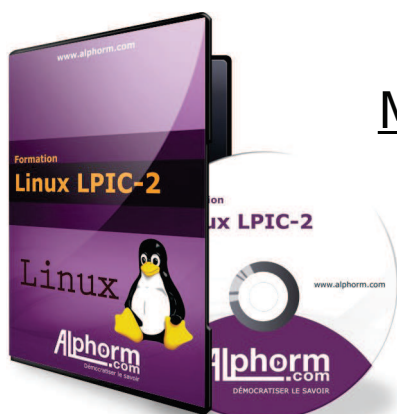
Ce qu'on a couvert

- Comment diagnostiquer les pannes réseau
- Dig, host, telnet
- ainsi que quelques rappels sur la configuration réseau

205.3 Troubleshooting network issues

Weight : 5

Description : Candidates should be able to identify and correct common network setup issues, to include knowledge of locations for basic configuration files and commands.



Maintenance système

Construction et installation de programmes à partir du code source

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Désarchivage et décompression
- Configuration
- Compilation



Introduction

- optimisation
 - personnalisation
 - être à jour
-
- Pourquoi pas dans la LPIC1 ?

Désarchivage et décompression

- tar

```
$ tar xvzf archive.tar.gz
```

```
$ tar xvjf archive.tar.bz2
```

- gunzip

```
$ gunzip archive.gz
```

- bzip2

```
$ bunzip2 archive.bz2
```

Configuration

```
$ ./configure
```

- script GNU autoconf
 - configurer automatiquement le code source d'un logiciel pour l'adapter au système
 - architecture, bibliothèques, dépendances
 - désactivation des fonctionnalités liées à des dépendances optionnelles non satisfaites
 - génération du makefile
- modifier le répertoire d'installation
 - par défaut : /usr/local/

```
$ ./configure --prefix=/opt
```

- afficher les paramètres disponibles

```
$ ./configure --help
```

- Rmq : vous pouvez patcher ces sources comme pour le kernel

Compilation

```
$ make
```

- à partir des éléments du makefile
 - modifiables directement via options

```
$ make DESTDIR=chemin install
```

- rappel kernel : targets
 - all (défaut)
 - clean
 - install

Ce qu'on a couvert

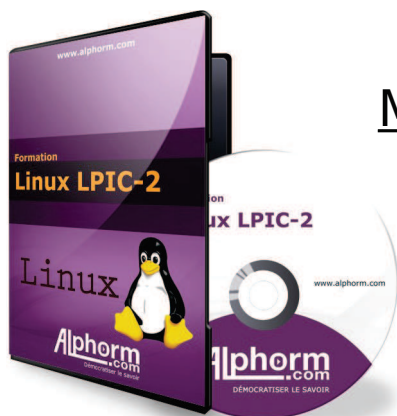
- décompresser et désarchiver
 - tar, gunzip, gzip, bzip2, tar
- personnaliser la configuration de l'installation d'un logiciel
 - configure
- compilation et installation d'un logiciel
 - make

206.1 Make and install programs from source

Weight : 4

Description : Candidates should be able to build and install an executable program from source. This objective includes being able to unpack a file of sources.





Maintenance système

Opérations de sauvegarde

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
- Réflexion préalable
- Supports
- Supports : comparatif
- Manipulation des bandes magnétique
- Rsync
- Autres outils
- Sauvegarde réseau
- Intégrité
- Restauration



Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Introduction

- Pourquoi ?
- Quoi ?
- Quand ?
- Où ?
- Comment ?

Réflexion préalable

- Pourquoi ?
 - importance des données
 - coût de création, information relative à un temps/contexte donné, etc ...
 - fiabilité
 - défaillance matérielle, erreur de manipulation, etc ...
- Quoi ?
 - relativement à leur importance et leur stabilité
 - données personnelles, configuration
 - /home, /etc
 - éventuellement : /var
 - inutiles : /etc/mtab, /proc, /sys, /dev
- Quand ?
 - fonction du rythme de changement des données
 - quotidiennement sur la plupart des systèmes

Supports

- Bande magnétique
 - /dev/st*
 - /dev/nst* (non rewinding tape)
 - ne se rembobine pas automatiquement après chaque opération
- Disque dur
- Médias optiques
- Réseaux

Supports : comparatif

Type	Avantages	Inconvénients	Contextes
bande magnétique	• coût • stockage passif	• temps d'accès	• sauvegarde à long terme
disque dur	• temps d'accès • rapport capacité / prix	• peu adapté à une sauvegarde hors-site	• intermédiaire pour une sauvegarde hors-site • restaurations rapides et fréquentes
média optique	• fiabilité • transport	• capacité de stockage • write-once	• sauvegardes système
réseaux (NAS, SAN)	• adaptabilité • indépendance	• coût • consommation énergétique	

Manipulation des bandes magnétique

```
$ mt [-h] [-f device] operation [count] [arguments...]
```

- Opérations
 - fsf : avancer de count fichiers
 - bsf : reculer de count fichiers
 - eod / seod : avance jusqu'à la fin des données
 - rewind : rembobiner (intégralement)

Rsync

- Rsync (Remote SYNChronisation)
 - synchronisation distante (ou locale) unidirectionnelle

```
$ rsync -avz -e "ssh" source user@destination:dest
```

- -a : mode archivage
 - récursif, conserve les liens symboliques, dates, permissions et périphériques
- -z : compresser les données lors du transfert
- -e : shell distant (ssh par défaut)

Autres outils

- dd : copie bloc à bloc

```
$ dd if=/dev/sda2 of=/tmp/home.img bs=1024 count=1048576
```

- cpio : archivage
 - "ancêtre" de tar (moins connu)
 - 3 modes : -i (input / extraire), -o (output / compression) et -p (pass-through)
 - liste de fichiers à partir de stdin

```
$ find /test | cpio -o > test.cpio
```

- tar

```
# tar -czf /dev/st0 /www /home
```

```
# tar -xvf /dev/st0
```

Sauvegarde réseau

- AMANDA
 - Advanced Maryland Automatic Network Disk Archiver
 - développé par l'université du Maryland
 - basé sur les standards de logiciels de sauvegarde.
 - Unix dump et restore, Gnu tar, autres logiciels ...
 - Le plus populaire
 - sauvegarde séquentielle (lecteur de bande ou disque)
 - modulaire
 - permet une répartition des tâches sur les machines périphériques
 - documentation en français : <http://www.linux-france.org/article/sys/amanda/>

- Bacula
 - serveur disponible uniquement sous Unix (GNU/Linux, Solaris et FreeBSD)
 - repose sur une base de donnée relationnelle
 - enregistre les signatures (SHA-1 ou MD5) de chaque fichier sauvegardé
 - extrêmement complet (chiffrement, gestion des robots changeurs de bandes, scripting, etc ...)
 - administrable via de nombreux GUI

Sauvegarde réseau

- BackupPC
 - via SMB, tar over SSH/rsh/nfs ou rsync
 - administrable via interface web
- Tous sont :
 - disponibles pour Unix (GNU/Linux, BSD, Mac OS X, Solaris) et Windows
 - Libres
 - des références incontournables (mais seulement à "connaître" pour la LPIC2)

Intégrité

- il est important de vérifier l'intégrité des données sauvegardées
 - et de répéter l'opération régulièrement (ex : tout les ans)
- exemple

```
(backup)$ find ./ -type f -exec shasum {} \; > ~/backup_sums.txt
```

```
(origin)$ scp backup:backup_sums.txt .
(origin)$ shasum -c backup_sums.txt
...
./kde/Autostart/.directory: OK
./ssh/authorized_keys: OK
./ssh/id_dsa: OK
...
./rsync-out.txt: FAILED
./try.pl~: OK
shasum: WARNING: 1 of 667 computed checksums did NOT match
```

Restauration

- Toujours vérifier la restauration après sauvegarde
- Établir une procédure de restauration
 - spécifie comment restaurer les données
 - option x de tar, script, rsync ou dd inverse, etc ...

Ce qu'on a couvert

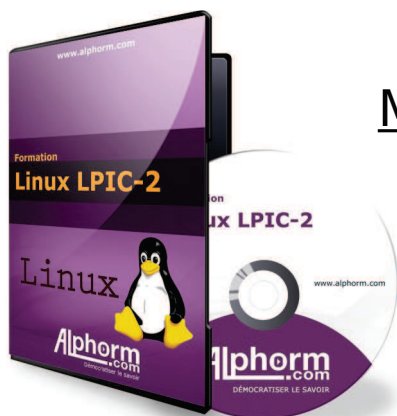
- Établir une stratégie de sauvegarde.
- Les différents supports de sauvegarde.
- cpio, dd, tar, rsync
- Vérifier l'intégrité d'une sauvegarde.
- Restauration

206.2 Backup operations

Weight : 3

Description : Candidates should be able to use system tools to back up important system data.





Maintenance système

Notification aux utilisateurs des problèmes système

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2

tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Messages à l'authentification
- Broadcaster un message à tout les utilisateurs
- Commande shutdown



Linux LPIC-2

tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Messages à l'authentification

- /etc/issue
 - message affiché avant authentification
 - ex : "Bienvenue sur le serveur toto.machin.com - Debian GNU/Linux"
 - mieux : "Attention : utilisateurs autorisés uniquement"
- /etc/issue.net
 - idem, mais pour les connexions distante
- /etc/motd
 - message affiché une fois l'authentification établie
 - particulièrement utile pour informer les utilisateurs d'un événement particulier (ex : extinction planifiée du système)
 - inutile pour les larges environnement
 - particulièrement en cas d'authentification unique
 - attention à sa mise à jour

Broadcaster un message à tout les utilisateurs

- Envoyer un message (22 lignes maximum)

```
$ wall [file]
```

- à partir d'un fichier ou de l'entrée standard (Ctrl-D pour clore)

- Contrôler l'accès en écriture à son terminal par les autres utilisateurs

```
$ mesg [y|n]
```

- Afficher le statut d'accès en écriture des utilisateurs

```
# finger
```

- colonne TTY : précédé de * si accès en écriture désactivé

Commande shutdown

- Exemple

```
# Shutdown -H +10 Server halting in 10 minutes for change change  
number. Expected up at 00:00:00.
```

- Options

- -k : simuler un arrêt du système
 - créé tout de même le fichier /etc/nologin durant son execution
 - interdit la connexion à tout autre utilisateur que root
- -c : annuler (cancel) un arrêt du système

Ce qu'on a couvert

- /etc/issue
- /etc/issue.net
- /etc/motd
- wall
- /sbin/shutdown

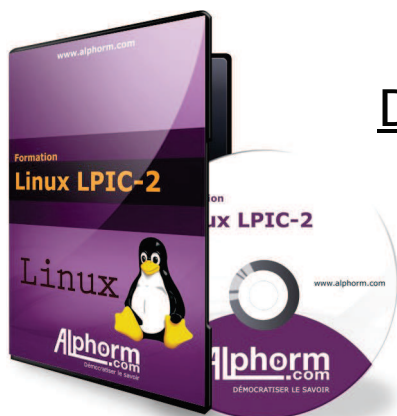
206.3 Notify users on system-related issues

Weight : 1

Description : Candidates should be able to notify the users about current issues related to the system.

Remarque : pour des raisons de cohérence, nous anticipons ici la v4, renumérotant ce sujet du 205.4 au 206.3





Domain Name Server

Configuration élémentaire d'un DNS

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

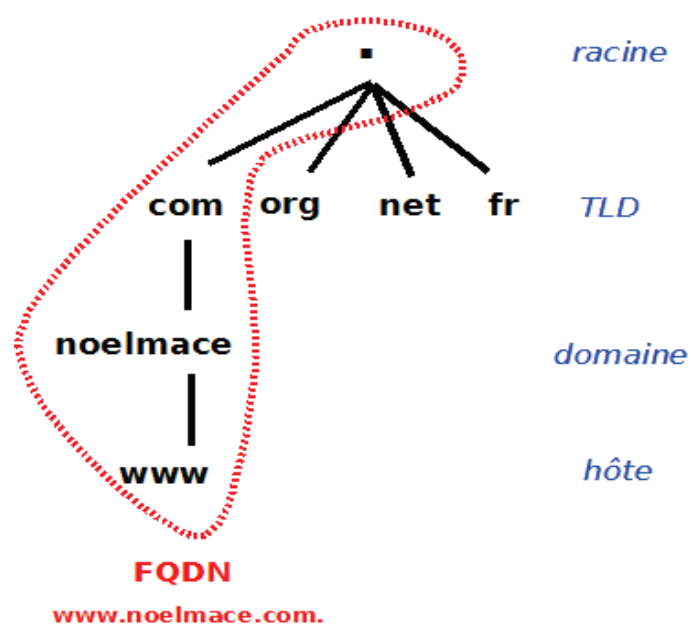
- Introduction
- Hiérarchie
- Fonctionnement
- Vocabulaire
- Bind
- Composants
- Syntaxe du fichier named.conf
- Options
- Logging
- Zones
- Configuration de rndc
- Commandes rndc
- Exemple : serveur de cache



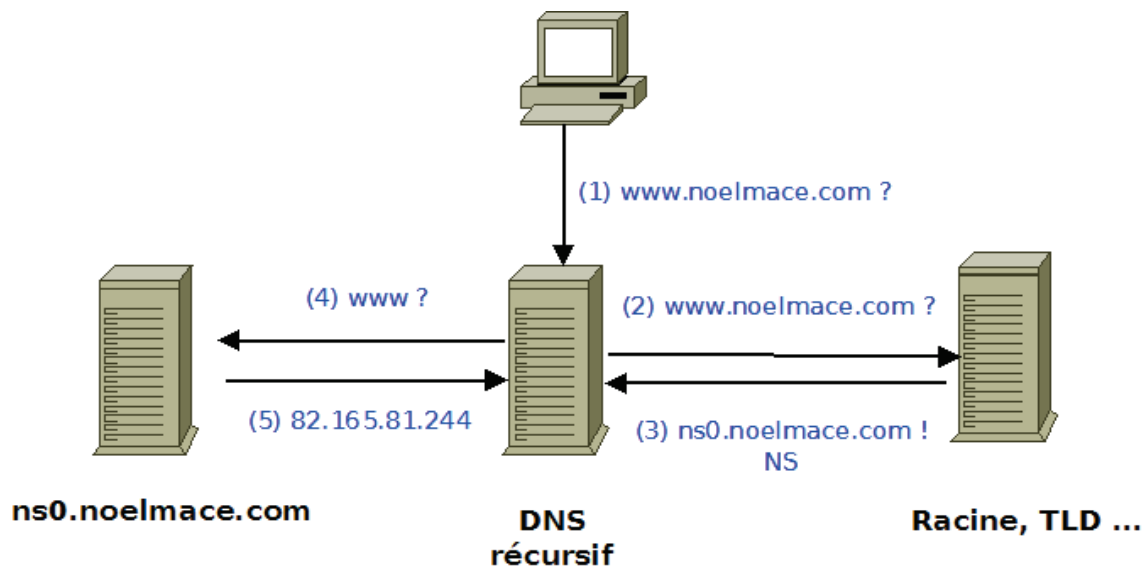
📌 Introduction

- correspondance nom (FQDN) / adresse ip
- autrefois grâce à un fichier HOST.TXT partagé par copie
- Remplace les fichiers hosts depuis 1987
 - "dynamique"
 - centralisé
 - hiérarchisé
 - standard

📌 Hiérarchie



⚠ Fonctionnement



⚠ Vocabulaire

Terme	Définition
Zone	Ensemble des directives associées à un domaine . A chaque zone / domaine correspond un fichier .
DNS récursif	Serveur capable d'interroger de manière récursive les autres serveurs DNS lorsqu'il ne parvient pas à déterminer un serveur faisant autorité sur le nom de domaine recherché.
Serveur primaire / Maître (d'une zone)	Serveur obtenant la configuration de sa zone à partir d'un fichier directement administré. Serveur principal d'un domaine.
Serveur secondaire	Serveur obtenant toutes les informations d'une zone à partir d'un serveur primaire .
Faire autorité sur un domaine	Répondre directement aux requêtes concernant un domaine sans passer par un autre serveur ou un cache. C'est le cas des serveurs primaires et secondaires.

⚠ ne pas confondre "authoritative" (primaire / master) avec "faire autorité"

Bind

- Berkeley Internet Name Daemon
- standard de fait
 - aujourd'hui maintenu par l'Internet Systems Consortium
- Libre : Licence ISC / OpenBSD
- Version 9
 - la plus courante
 - stable, sécurisé et confirmé (plus de 10 ans)
 - objectif LPIC
- Version 10
 - récente (février 2013)
 - **totale**ment différente (réécrit à partir de zéro en 5 ans)
 - intègre également le DHCP



Composants

- /usr/sbin/named
- /usr/sbin/rndc : utilitaire de contrôle
- /etc/bind/named.conf ou /etc/named.conf : fichier de configuration
 - named.conf.local
 - named.conf.options
- /etc/init.d/bind : init script
- /var/named/ : répertoire de travail

Syntaxe du fichier named.conf

- instruction (statements)

```
keyword {  
    ...  
};
```

- options, forwarders, logging, zone "xxx", etc ...
- imbricables
 - ex : forwarders dans options

- instruction "simples"

- ex : inclusion

```
include "/etc/bind/named.conf.options";
```

- doivent toutes se terminer par un ;

Options

- Options de configuration du serveur DNS
- Une seule instruction options par named.conf
 - souvent écrit dans un fichier named.conf.options

Option	Description	Exemple
directory	répertoire de travail	directory "/var/named";
forwarders	serveurs de référence (aucun par défaut)	forwarders { 123.12.135.6 ; }
forward	comportement avec les forwarder first (défaut) : en priorité only : uniquement	forward only ;
version	version du serveur à afficher	version none ;

Logging

```
logging {  
    category cat { channel; };  
    ...  
};
```

- catégorie : type d'information à logger
 - security, lame-server, cname, etc ...
- chaîne : spécifie la sortie
 - null : détruit toutes les informations
 - default_syslog : comportement par défaut du système
- Une seule instruction logging par named.conf
- Configuration par défaut correcte

Zones

- Définit les paramètres généraux d'une zone
 - type (master / slave)
 - nom (dans l'en-tête)
 - fichier (paramètres détaillés de la zone)
 - plus éventuellement d'autres options

```
zone "example.org" {  
    type master;  
    file "/etc/bind/db.example.org";  
};
```

- détails dans le chapitre suivant

Configuration de rndc

rndc.key

```
key "rndc-key" {
    algorithm hmac-md5;
    secret "tyZqsLtPHCNna5SFBLT0Eg==";
};

options {
    default-key "rndc-key";
    default-server 127.0.0.1;
    default-port 953;
};
```

named.conf

```
key "rndc-key" {
    algorithm hmac-md5;
    secret "tyZqsLtPHCNna5SFBLT0Eg==";
};

controls {
    inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { "rndc-key"; };
};
```

Commandes rndc

- générer une clé si aucune n'est disponible sur le système

```
# rndc-confgen
```

- syntaxe de rndc

```
$ rndc [-b source-address] [-c config-file] [-k key-file] [-s server] [-p port] [-V] [-y key_id] {commande}
```

- commandes :
 - reload : recharger la configuration
 - stop : arrêter le serveur
 - flush : vider le cache
 - status : afficher l'état du serveur
 - aucune ou help : liste des commandes possibles

Exemple : serveur de cache

GO !

Ce qu'on a couvert

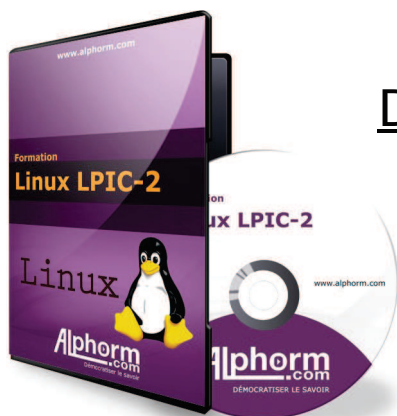
- Ce qu'est un serveur DNS.
- Les quelques principes génériques à connaître.
- Bind
 - named.conf
 - /var/named
 - rndc

207.1 Basic DNS server configuration

Weight : 2

Description : Candidates should be able to configure BIND to function as a caching-only DNS server. This objective includes the ability to convert older BIND configuration files to newer format, managing a running server and configuring logging





Domain Name Server

Création et maintenance de zones DNS

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
- Configuration : maitre / esclave
- Fichiers de zone
- Fichier de zone : exemple
- Instructions
- Enregistrements
 - Adresse (A)
 - Alias (CNAME)
 - Mail Exchange (MX)
 - NameServer (NS)
 - Start Of Authority (SOA)
 - Paramètres SOA
- Zone inverse
- Zone racine
- Délégation de zone
- Tests et vérification avec nslookup



Introduction

- Après avoir appris à configurer un serveur en cache only
 - apprendre à gérer directement des zones
- Deux types de zones : zones et zones inverses
 - à chaque zone **doit** correspondre une zone inverse
 - définition pour chaque dans named.conf
 - permet la résolution adresse ip → nom
 - exemple : 240.123.224.in-addr.arpa

Configuration : maitre / esclave

- fichier named.conf
 - serveur maître

```
zone "example.org" {  
    type master;  
    file "/etc/bind/db.example.org";  
    allow-transfer { 192.168.56.101 ; } ;  
};
```

- serveur esclave

```
zone "example.org" {  
    type slave;  
    masters { 224.123.240.1; };  
    file "db.example.org";  
};
```

Fichiers de zone

- contiennent les informations sur une zone particulière
 - enregistrements
 - directives
- indiqués par l'option **file** d'une directive **zone** dans named.conf
 - chemin complet (/etc/bind/db.example.org)
 - ou chemin relatif
 - par rapport à la directive directory

Fichier de zone : exemple

```
$ORIGIN example.com.
$TTL 86400
@      IN      SOA      dns1.example.com.      hostmaster.example.com. (
                        2001062501 ; serial
                        21600      ; refresh after 6 hours
                        3600       ; retry after 1 hour
                        604800     ; expire after 1 week
                        86400      ; minimum TTL of 1 day

      IN      NS       dns1.example.com.
      IN      NS       dns2.example.com.

      IN      MX       10      mail.example.com.
      IN      MX       20      mail2.example.com.

      IN      A        10.0.1.5

server1      IN      A        10.0.1.5
server2      IN      A        10.0.1.7
dns1         IN      A        10.0.1.2
dns2         IN      A        10.0.1.3

ftp          IN      CNAME    server1
mail         IN      CNAME    server1
mail2        IN      CNAME    server2
www          IN      CNAME    server2
```

Instructions

Instructions	Description	Exemple
\$TTL	Valeur par défaut du temps de vie (Time to live : durée, en secondes, durant laquelle un enregistrement est valide).	\$TTL 86400
\$ORIGIN	Modifier l'origine (<i>current origin</i> : nom de domaine, spécifié dans l'en-tête de la directive zone du named.conf)	\$ORIGIN exemple.com
\$INCLUDE	Permet d'inclure un autre fichier de zone à l'endroit de cette directive. Permet de stocker des configuration de zone à l'écart du fichier de zone principal.	\$INCLUDE /etc/bind/CNAME.exemple.com

Enregistrements

- Syntaxe

www monserveur	7200	IN IN	CNAME A	monserveur 192.168.1.10
-------------------	------	----------	------------	----------------------------

Nom

TTL

Type

Valeur

- La seconde colonne indique la classe
 - ie : le protocole utilisé
 - aujourd'hui, toujours IN (pour internet)
- Nom : absolu (FQN) ou "relatif" (à l'origine)
 - si ne finie pas par un point, l'origine lui sera ajoutée (à droite)
 - @ permet de référencer uniquement l'origine

Adresse (A)

- Nom → IP
- Exemple

monserveur	IN	A	192.168.1.10
------------	----	---	--------------

Alias (CNAME)

- Nom → Nom (A)
- Exemple

www	IN	CNAME	monserveur
monserveur	IN	A	192.168.1.10

Ⓛ Mail Exchange (MX)

- Serveurs mail pour le domaine
- Par priorité (du + petit au + grand)
- Vers une adresse (A)
 - Pas d'Alias (CNAME)
- Exemple

noelmace.com.	IN	MX	10	mail.noelmace.com.
noelmace.com.	IN	MX	50	mail.google.com.

Ⓛ NameServer (NS)

- Spécifier les serveurs faisant autorité sur le domaine
- Vers une adresse (A) (*glue record*)
 - Pas d'Alias (CNAME)
 - éviter de pointer vers l'enregistrement A d'un autre serveur DNS
 - Omettre les furtifs
- Exemple

	IN	NS	ns.noelmace.com.
ns	IN	A	192.168.1.30

Start Of Authority (SOA)

- Informations générales sur la zone
 - Serveur maître
 - Adresse mail de l'admin
 - paramètres
- Exemple

```
@      IN      SOA      ns.noelmace.com. contact.noelmace.com. (
                                2011102402      ; Serial
                                604800      ; Refresh
                                86400      ; Retry
                                2419200      ; Expire
                                604800 )      ; Negative Cache TTL
;
```

Paramètres SOA

Paramètre	Description
Serial	Numéro de série. Permet au serveur secondaire de savoir si il doit se mettre à jour. Incrémenté à chaque modification du fichier. Par convention : yyyyymmdd + numéro de la modification.
Refresh	Fréquence de consultation du serveur primaire par les serveurs secondaires.
Retry	Temps d'attente avant nouvel essai en cas d'echec de refresh.
Expire	Durée d'indisponibilité du serveur primaire après laquelle celui-ci sera considéré comme retiré du service.
Minimum TTL	TTL minimum du cache

- Toutes les durées sont exprimées en secondes !

Ⓛ Zone inverse

- permet la résolution ip → nom
- enregistrements PTR

```
1      IN      PTR      dns1.example.org.
```

⚠ ne pas oublier le point finale (racine)

- déclaration dans named.conf

```
zone "1.168.192.in-addr.arpa" {  
    type master ;  
    file "/etc/bind/db.1.168.192" ;  
} ;
```

Ⓛ Zone racine

- named.conf

```
zone "." {  
    type hint;  
    file "/etc/bind/db.root";  
};
```

- fichier de zone à mettre à jour
 - soit par la distribution
 - soit via ftp.rs.internic.net
 - via dig

```
dig @a.root-servers.net . ns > roothints
```

🔒 Délégation de zone

- Permet de déléguer un sous-domaine à un autre serveur DNS
- Exemple :
 - un serveur ns1.example.com maître sur example.com
 - ip = 192.168.0.1
 - un serveur ns3.sd.example.com maître sur sd.example.com
 - ip = 10.10.0.1

🔒 Délégation de zone

- fichier de zone de example.com sur ns1

```
$ORIGIN example.com.
@           IN      SOA   ns1.example.com. hostmaster.example.com. (
    ...
    )
    IN      NS       ns1.example.com.
ns1         IN      A    192.168.0.1
    ...

$ORIGIN sd.example.com.
@           IN      NS    ns3.sd.example.com.
; il est recommandé, mais non indispensable, d'établir également le serveur
; ns1 en slave de ns3 pour cette zone, et de lui donner autorité sur ce
; sous-domaine (en plus de la configuration dans named.conf)
;           IN      NS    ns1.example.com.

ns3         IN      A    10.10.0.1      ; 'glue' record, obligatoire !
```

Délégation de zone

- fichier de zone de sd.example.com sur ns3

```
$ORIGIN sd.example.com.
@           IN      SOA    ns3.sd.example.com. contact.sd.example.com. (
    ...
    )
           IN      NS     ns3.sd.example.com.
; pour ns1 en slave, voir précédemment
;
;           IN      NS     ns1.example.com.
; ns1.example.com. IN      A      192.168.0.1 ; 'glue' record
ns3         IN      A      10.10.0.1

; exemple d'enregistrement pour ftp.sd.example.com
ftp         IN      A      10.10.0.28

...
```

Tests et vérification avec nslookup

- afficher les enregistrements d'un domaine ou d'un hôte
 - dans le dns configuré

```
$ nslookup www.exemple.org
```

- dans un autre serveur

```
$ nslookup www.exemple.org serveur.de.nom
```

- mode interactif (sans arguments)
 - clause set pour modifier le mode d'interrogation

```
set type=mx
```

- n'est plus maintenu
 - privilégier dig et host
 - cf chapitres précédents

Ce qu'on a couvert

- Configuration des zones dans BIND 9 :
 - fichiers de zone
 - génériques, inverses et racine
 - named.conf
- Comment ajouter un hôte au fichier de zone.
- Comment mettre en place une délégation de zone.
- Comment tester une zone avec nslookup.

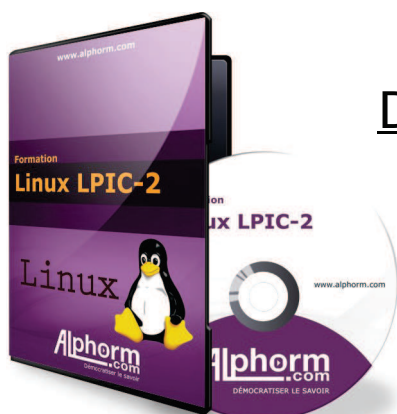
207.2 Create and maintain DNS zones

Weight : 2

Description : Candidates should be able to create a zone file for a forward or reverse zone or root level server. This objective includes setting appropriate values for records, adding hosts in zones and adding zones to the DNS. A candidate should also be able to delegate zones to another DNS server.



Alphorm.com



Domain Name Server

Sécurisation d'un serveur DNS

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Remarque sur le hacking
- Types de requêtes
- Masquer le numéro de version
- ACL
- Limiter les requêtes
- Limiter les transferts de zone
- Limiter les privilèges de BIND
- Chroot
- Chroot : logging
- DNSSEC
 - Introduction
 - Signature des enregistrements
 - DNSKEY et RRSIG
 - Preuves de non-existence
 - Chaîne de confiance
- Mise en pratique
 - Génération de clés avec dnssec-keygen
 - Limitation des transferts avec DNSSEC
 - Signature de zone
 - Configuration du client
 - Enregistrements DS



Introduction

- mettre à jour régulièrement
 - garder un œil sur les nouvelles versions et les annonces de failles de sécurité
 - exemple : <http://lists.debian.org/debian-security-announce/>
- Limiter les informations disponibles
- Limiter l'accès et les transferts de zone
- Isoler/Limiter BIND
- Sécuriser les données (avec DNSSEC)

Remarque sur le hacking

- Ne pas confondre hacking et malveillance
 - black / grey / white hats
- Le hacking n'est d'ailleurs pas uniquement lié aux questions de sécurité, ni même d'informatique
- "aptitude technique et [...] plaisir pris à résoudre des problèmes et à dépasser des limites arbitraires" - Eric Raymond, *Comment devenir un hacker ?*
 - voir aussi [The Jargon File](#), du même auteur, et sa [définition](#) très complète du terme hacker

Types de requêtes

- requêtes "classiques"
 - demande d'une information spécifique
 - contrôlée par l'instruction allow-query
- Transferts de zone
 - envoi de toutes les informations d'une zone à un autre serveur
 - conçues pour les serveurs "esclaves"
 - contrôlées par l'instruction allow-transfer



autorisé par défaut pour tout les hôtes

Masquer le numéro de version

- hack

```
$ dig @target chaos version.bind txt
```

- peu permettre de cibler les attaques en fonction de failles connues

- solution : named.conf

```
options {  
    ...  
    version "hidden";  
};
```

ACL

- Mettre en place un ACL

```
acl "trusted" {  
    localhost;  
    192.168.1.0/24;  
};
```

- utilisable par diverses instructions de contrôle d'accès
 - allow-query, allow-transfer

Limiter les requêtes

- grâce aux instructions allow-query et allow-transfer
 - utilisables dans les instructions zone et options
 - celles des instructions zone surchargeant celles, globales, de l'instruction options
- Exemple

```
acl "my_network" {  
    224.123.240.0/24;  
};  
  
zone "example.org" IN {  
    type master;  
    allow-queries { my_network; };  
};
```

Limiter les transferts de zone

- hacks
 - \$ dig axfr @serveurdns domaine
 - \$ host -l domaine serveurdns
- **DOIT** être limité aux serveurs "esclaves" sur les serveurs maitre
 - totalement interdit (none) sur les serveurs esclaves
- Exemple : named.conf d'un serveur maitre

```
acl "my_slave_servers" {  
    224.123.240.3; // cat.example.org  
};  
  
zone "example.org" IN {  
    type master;  
    allow-transfer { my_slave_servers; };  
};
```



ne pas oublier de faire de même pour les zones inverse

Limiter les privilèges de BIND

- se lance par défaut en tant que root sur certaines distributions
- éviter l'utilisateur/groupe nobody/nogroup
 - trop grand nombre d'applications lancées via cet utilisateur
 - risque de communication entre ces application → faille
- privilégier un utilisateur/groupe spécifique
 - ex : named / named

```
# named -u named -g named
```

- Exemple de init script sous Debian

```
start-stop-daemon ... --exec /usr/sbin/named -- -u named -g named
```



vérifier que cet utilisateur ai l'accès au dossier de travail (instruction directory)

Chroot

- permet d'isoler l'exécution d'un programme
 - en changeant sa racine (ex : /var/cache/bind)
 - option -t de named

```
start-stop-daemon ... --exec /usr/sbin/named -- -t /var/cache/bind
```

- fichiers requis par BIND
 - dossiers etc, dev, lib, sbin (ou usr/sbin) et var/run
 - périphérique /dev/null

```
$ mknod -m 666 /var/cache/bind/dev/null c 1 3
```

- les fichiers /etc/{passwd,group,shadow,ld.so.cache,localtime} contenant l'utilisateur/groupe named/named
- fichiers de configuration (dans /var/cache/bind/etc/bind/)
 - attention à l'instruction directory, qui sera relative à la nouvelle racine
- toutes les librairies utilisées par BIND

```
$ ldd /usr/sbin/named
```

- les programmes named, named-xfer et rndc

Chroot : logging

- la solution traditionnelle de logging présentée aux chapitres précédents requière des fichiers externes au chroot
 - nous devons donc faire appel à une autre solution
 - voici un exemple

```
logging {  
    channel some_log {  
        file "bind.log" versions 3;  
        severity info;  
    };  
  
    category default { some_log; };  
  
    // ...  
};
```

- le nouveau fichier de log sera donc /var/cache/bind/var/cache/bind/bind.log

DNSSEC

- Introduction
 - Signature des enregistrements
 - DNSKEY et RRSIG
 - Preuves de non-existence
 - Chaîne de confiance
- Mise en pratique
 - Génération de clés avec dnssec-keygen
 - Limitation des transferts avec DNSSEC
 - Signature de zone
 - Configuration du client
 - Enregistrements DS

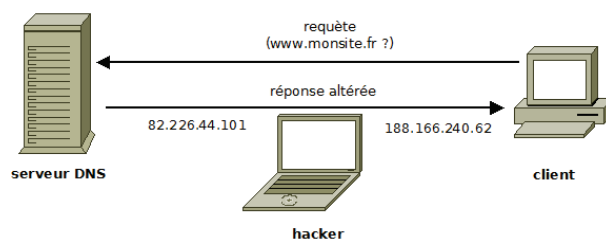


Introduction

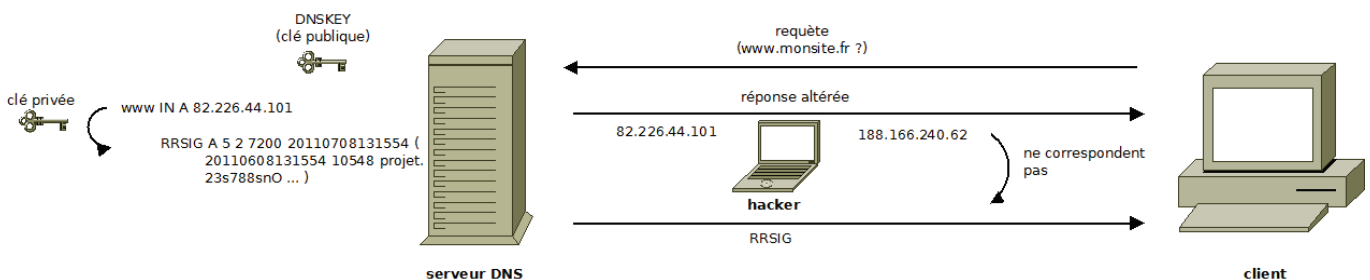
- Permet de sécuriser les réponses d'un serveur DNS
 - par rapport à des informations existante
 - Authentification des données contenues dans les réponses.
 - Intégrité de ces données.
 - ou par rapport à des informations non existantes
 - Preuve de non existence.
- En signant les enregistrements DNS au sein d'une zone
- Permet d'établir une chaîne de confiance basée sur des clés publiques
 - délégation de signatures
 - un DNS de niveau supérieur pouvant annoncer que tel sous-domaine est signé
- Empêche le DNS poisoning
 - intercepter des paquets dns et les modifier

Signature des enregistrements

Danger : le DNS poisoning



Solution : la signature des enregistrements



DNSKEY et RRSIG

- DNSKEY : transmettre une clé publique entre le résolveur (client) et le serveur de nom
 - afin de vérifier la signature du serveur d'autorité
 - vérifier l'intégrité et l'authenticité du message
- RRSIG : signature de l'enregistrement envoyé par le serveur d'autorité
 - pour chaque enregistrement
 - signature du hash de l'enregistrement avec la clé privée du serveur d'autorité

Preuves de non-existence

- pour des noms inexistants
 - par défaut, le serveur répondra par une réponse vide
 - il n'y a donc rien à signer
- NSEC (Next SECure) : preuve de non existence
 - indique les noms n'existant pas !
 - permet ainsi la création d'un RRSIG correspondant
 - Exemple : il n'y a aucun nom entre beta et delta

```
beta.example.net. NSEC delta.example.net. A RRSIG NSEC
```

- problème : à chaque nom existant est associé un NSEC
 - permet donc du "zone walking" (énumération de zone)
 - ie : récupérer l'ensemble des enregistrements existant sur la zone

Preuves de non-existence

- NSEC3 : évite les attaques de type énumération de zone
 - utilise les hashes des noms au lieu des noms eux même
 - Exemple : il n'y a pas de hash valide entre 810c et c73a

```
810c.example.net. NSEC 1 0 5 5A17 c73a A RRSIG
```

- algo (1), salt (5A17), iterations (5)

- NSEC3PARAM : paramètres NSEC3
 - ne sert qu'aux serveur d'autorité
 - afin de calculer le hash des noms qu'il conserve

Chaîne de confiance

- être certain que la clé publique (DNSKEY) du résolveur correspond bien à la bonne clé de la zone
- cf délégation de zone
 - un serveur de confiance indique que l'un de ses serveurs enfants est digne de confiance
- DS : identifier rapidement la clé publique de la zone fille
 - directement lié à l'enregistrement DNSKEY d'une des zones filles
 - envoyé par le serveur fils pour l'enregistrer dans le serveur père
 - hash du nom du détenteur de la clé publique (zone fille)

Mise en pratique

- 2 types de clés :
 - KSK (Key Signing Keys)
 - utilisée uniquement pour signer les clés d'une zone (DNSKEY)
 - ZSK (Zone Signing Keys)
 - utilisée pour signer tout les RRsets d'une zone (RRSIG)

Génération de clés avec dnssec-keygen

```
$ dnssec-keygen -a algo -b size -n nametype [-f flag] nom
```

- *algo* : algorithme cryptographique
 - non sensible à la casse
 - pour DNSSEC : RSAMD5, RSASHA1, DSA ...
 - pour TSIG/TKEY : DH (Diffie Hellman), HMAC-MD5, HMAC-SHA1 ...
- *size* : longueur de la clé (en bits)
 - RSA : entre 512 et 2048
 - DH : entre 128 et 4096
 - DSA : entre 512 et 1024
 - HMAC : entre 1 et 512
- *nametype* : type d'utilisation de la clé
 - non sensible à la casse
 - ZONE, USER ou OTHER
- *flag* : utilisé pour indiquer qu'une clé est une clé KSK
 - ZSK sinon
- créé les fichiers Kname+algorithm+footprint.private and Kname+algorithm+footprint.key

Limitation des transferts avec DNSSEC

- dans named.conf

```
key key.example.com. {  
    algorithm "hmac-md5";  
    secret "5VBiSy...";  
};
```

- limiter les droits d'accès en lecture au seul utilisateur/groupe liés au serveur BIND

- définir les serveurs pouvant se connecter grâce à cette clé

```
server ip_du_serveur_distant {  
    keys key.example.com.;  
};
```

- à inscrire sur **tout** les serveurs

Limitation des transferts avec DNSSEC

- grâce à la clé déclarée précédemment

```
zone "example.com" {  
    type master;  
    file "example.com.zone";  
    allow-transfer { key key.example.com.; };  
};
```

Signature de zone

1) Création des clés (dans /etc/bind/)

```
$ dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE projet  
$ dnssec-keygen -a RSASHA1 -b 1024 -n ZONE projet
```

2) Inclusion des clés dans le fichier de zone

```
$include nom_du_fichier_KSK.key  
$include nom_du_fichier_ZSK.key
```

3) Signature de la zone

- crée le fichier de zone signée projet.signed

```
$ dnssec-signzone -t -k clé_KSK.key db.projet -o projet clé_ZSK.key
```

Signature de zone

4) modification de named.conf

```
zone "projet" {  
    type "master";  
    file "/etc/bind/db.projet.signed";  
};
```

5) modification de named.conf.options

```
dnssec-enable yes;
```

6) relancer bind

```
$ /etc/init.d/bind9 restart
```

Configuration du client

- récupérer la clé KSK
 - de manière sécurisée (scp, sftp ...)
- l'ajouter au fichier /etc/trusted-key.key

```
tail -n 1 KSK.key >> /etc/trusted-key.key
```

- tester la configuration

```
$ dig +dnssec +sigchase papa.projet
```

Signature de zone

1) Création des clés (dans /etc/bind/)

```
$ dnssec-keygen -f KSK -a RSASHA1 -b 1024 -n ZONE projet  
$ dnssec-keygen -a RSASHA1 -b 1024 -n ZONE projet
```

2) Inclusion des clés dans le fichier de zone

```
$include nom_du_fichier_KSK.key  
$include nom_du_fichier_ZSK.key
```

3) Signature de la zone

- créé le fichier de zone signée projet.signed)

```
$ dnssec-signzone -t -k clé_KSK.key db.projet -o projet clé_ZSK.key
```

Enregistrements DS

- Exemple : un serveur A1 fait autorité sur example.org
 - un serveur A2, grâce à une délégation de zone, fait autorité sur sd.example.org
- Nous devons donc transmettre les enregistrements DS générés dans A2 à A1 afin d'établir une chaîne de confiance
- Ces enregistrements ont été créés dans un fichier séparé, dsset-sd.example.org
 - envoyer ce fichier de manière sécurisée à A1
 - l'inclure dans le fichier de zone non signé

Ce qu'on a couvert

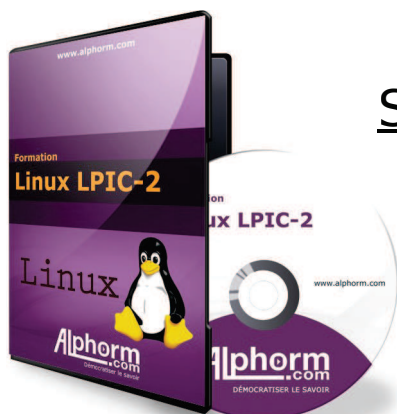
- Principes de base de la sécurisation du DNS.
 - lancement en tant qu'utilisateur non-root
 - Chrooting de bind
 - Transfert de zone
- Signature de zone avec DNSSEC
 - dnssec-keygen et dnssec-signzone

207.3 Securing a DNS server

Weight : 2

Description : Candidates should be able to configure a DNS server to run as a non-root user and run in a chroot jail. This objective includes secure exchange of data between DNS servers.





Services web

Mise en place d'un serveur web

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
 - Apache
 - MPM : prefork ou worker ?
 - Virtual Hosts
- Configuration
 - httpd.conf : exemple
 - Options du serveur Apache
 - Contrôle des répertoires
 - Logging
- Modularité
 - Chargement d'un module Apache
 - mod_perl
 - Installer mod_perl
 - PHP
 - Authentification et autorisation
 - Mise en place
 - Gestion des comptes utilisateur
 - Protection d'un dossier par DAC
 - Protection d'un dossier par MAC
- apache2ctl
- Bonus : les outils Debian



Introduction

- Un des services primordiaux d'Internet
 - certainement le plus connu du grand public
 - beaucoup confondant World Wide Web et Internet
- HTTP
 - HyperText Transfer Protocol
 - Permettre aux utilisateurs d'accéder à des données (pages web) sur un serveur
 - via un client web (ex : Firefox)

Apache

- Né en avril 1995
 - ensemble de correctifs à NCSA HTTPd (du domaine publique)
 - leader de l'époque (plus de 55 % de parts de marché)
 - "mort" (0%) en juillet 1999
- Totalement réécrit en 2000 pour la version 2
 - plus aucune trace de NCSA HTTPd
- Libre (Licence Apache)
 - v2.0 (compatible GPL v3) depuis janvier 2004
- Multi-plateforme
 - GNU/Linux, Mac OS X, BSD, Solaris, Windows
- **LE** serveur web de référence depuis avril 1996
 - 54 % de parts de marché sur les sites actifs en avril 2013 selon netcraft.com
 - contre 13 % pour Nginx, plus léger et performant, qui connaît une progression certaine depuis 2007
 - 12 % pour Microsoft-IIS et 8 % pour Google Servers
 - LAMP : Linux, Apache, MySQL, PHP



MPM : prefork ou worker ?

- **Multi-Processing Module**

- Moteur de serveur : interprète les requêtes
 - "duplique" apache
- afin de répondre à plusieurs requêtes simultanément
 - 2 principaux paquets : apache2-mpm-prefork ou worker

- **Prefork**

- Mode historique (apache 1.3)
- multi-processing : un processus par connexion
- Meilleure isolation / Faibles performances

- **Worker**

- Multi-threading : un thread par connexion
- Meilleures performances
 - pas ou peu de commutation de contexte
- nécessite des modules compatibles
 - exclue mod_php

Virtual Hosts

- Héberger plusieurs sites sur un même serveur
- Deux types :
 - IP based
 - Nécessite plusieurs interfaces (ou routage)
 - Named based
 - Répond en fonction de l'url appelée
- Configurés dans httpd.conf
 - ou /etc/apache2/sites-available/ sur Debian et dérivés
 - cf cours suivant

Configuration

- Dans (suivant la distribution) :
 - /etc/apache/config/
 - ou /etc/apache2/
 - ou /etc/httpd/config/
- httpd.conf (ou apache2.conf)
 - fichier de configuration principal
 - soit séparé en plusieurs parties (cf "Include")
 - soit d'un bloc
 - s'applique à tout le serveur
 - 3 parties :
 - global environment
 - configuration générale du serveur
 - paramètres du serveur par défaut
 - requêtes non gérées par un virtual host
 - configuration des virtuals hosts
- fichiers .htaccess
 - permettent une configuration spécifique pour chaque dossier
 - à utiliser avec prudence
 - uniquement si vous devez séparer la configuration de certains contextes du fichier principal
 - ie : interdire le droit d'accès à httpd.conf à certains administrateurs
 - « En général, vous ne devriez **jamais** utiliser les fichiers .htaccess à moins que vous n'ayez pas accès au fichier principal de configuration du serveur. Il y a, par exemple, une conception erronée qui prévaut selon laquelle les droits des utilisateurs doivent toujours être gérés dans le fichier .htaccess. Cela n'est simplement pas le cas. Vous pouvez placer les configurations des droits dans la configuration principale du serveur, et cela est, en fait, la manière favorisée de le faire. » - [Documentation Apache](#)

httpd.conf : exemple

GO !

- un exemple sur internet

Options du serveur Apache

- Première section du fichier httpd.conf
 - nombreuses options de type clé valeur

- Nombre maximum de requêtes simultanées autorisées

```
MaxKeepAliveRequests 100
```

- Nombre de serveurs à lancer au démarrage

```
StartServers 5
```

- Nombre minimal et maximal de serveurs "en attente"

```
MinSpareServers 5  
MaxSpareServers 10
```

- trop bas → perte de performance / trop haut → consommation excessive de ressources

- nombre maximal de connections (de clients) simultanées
 - ie : nombre maximal de serveurs

```
MaxKeepAliveRequests 100
```

Contrôle des répertoires

```
<Directory chemin répertoire> ... </Directory>
```

- Regrouper des directives pour qu'elles ne s'appliquent qu'au répertoire concerné

- Exemple

```
<Directory "/usr/local/httpd/htdocs">  
Options Indexes FollowSymLinks  
</Directory>
```

- voir : <https://httpd.apache.org/docs/current/mod/core.html#directory>

Logging

- généralement dans /var/log/apache2 ou httpd
- Configuration (httpd.conf)
 - Messages d'erreurs

```
ErrorLog ${APACHE_LOG_DIR}/error.log
```

- Niveau de logging des messages d'erreurs

```
LogLevel warn
```

- Dans l'ordre : debug, info, notice, warn, error, crit, alert et emerg

- Accès au serveur

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common  
CustomLog ${APACHE_LOG_DIR}/access.log
```

- Pour aller plus loin : [Documentation Apache des Logs](#)

Modularité

- Apache repose sur une architecture modulaire
 - similaire à celle du kernel Linux
 - permet à l'administrateur de choisir les fonctionnalités à inclure
- DSOs (Dynamic Shared Objects)
 - Objets Dynamiques Partagés
 - séparés du fichier binaire principal httpd
 - soit compilés en même temps que le serveur
 - peuvent être intégrés statiquement dans le binaire httpd

```
$ ./configure --prefix=/chemin/vers/installation --enable-foo  
$ make install
```

- soit ajoutés ultérieurement
 - grâce à apxs (Apache Extension Tool)

```
$ cd /chemin/vers/module_tiers  
$ apxs -cia mod_foo.c
```

Chargement d'un module Apache

- Dans le fichier httpd.conf

```
LoadModule module filename
```

- Remarque (pour ceux ayant travaillé sous Apache1) :
 - la directive AddModule n'est plus nécessaire

- Exemple

```
LoadModule alias_module /usr/lib/apache2/modules/mod_alias.so
```

- Comportement conditionnel pour un module

```
<IfModule [!]fichier module|identificateur module>  
...  
</IfModule>
```

mod_perl

- Interpréteur Perl pour Apache
 - permet, grâce à des scripts Perl, de :
 - produire du contenu dynamique
 - gérer Apache
 - et bien d'autres choses encore
 - sans faire appel à un interpréteur externe
 - gain de performance significatif
 - accès complet à l'API Apache

- *"mod_perl is more than CGI scripting on steroids. It is a whole new way to create dynamic content by utilizing the full power of the Apache web server to create stateful sessions, customized user authentication systems, smart proxies and much more. Yet, magically, your old CGI scripts will continue to work and work very fast indeed. With mod_perl you give up nothing and gain so much!"* - [Lincoln Stein](#), un des principaux contributeurs de mod_perl

Installer mod_perl

- Sous Debian :

```
# apt-get install libapache2-mod-perl2
```

- Sous CentOS :

```
# yum install mod_perl
```

- Pour aller plus loin :
 - installation : <https://perl.apache.org/docs/2.0/user/install/install.html>
 - configuration : <https://perl.apache.org/docs/2.0/user/config/config.html>

PHP

- Langage de script, coté serveur, orienté Web et multi-plateforme
 - une référence (cf LAMP)

```
# apt-get install libapache2-mod-php5
```

```
# yum install php
```

- Pour tester l'installation, créer une PHP info page

```
# echo -e "<?php\n\tphpinfo();\n?>" > /var/www/html/info.php
```

- Pour aller plus loin : [documentation complète de l'installation](#)

Authentification et autorisation

- Deux méthodes :
 - discretionary access control (DAC) - Contrôle d'accès discrétionnaire
 - où "un sujet avec une certaine autorisation d'accès est capable de transmettre cette permission (peut-être indirectement) à n'importe quel autre sujet" - Trusted Computer System Evaluation Criteria
 - ici : login + mot de passe
 - mandatory access controls (MAC) - Contrôle d'accès obligatoire
 - décisions de protections imposées (non prises par les objets concernés)
 - ici : Adresse IP, nom d'hôte, etc ...
- Géré par des modules
 - `mod_auth_basic` : le plus courant - stock les informations dans des fichiers texte
 - `mod_auth_dbd` : stockage dans une base SQL
 - `mod_auth_dbm` : stockage dans des fichiers sous un format DBM
 - `mod_auth_digest` : authentification basée sur les condensés MD5
 - `mod_auth_anon` : comportement similaire à un FTP anonymisé
 - `mod_authz_host` : restriction de l'accès en fonction du nom d'hôte ou de l'ip (depuis 2.3)
 - pour les versions précédentes, voir `mod_access`
- Pour aller plus loin : <https://httpd.apache.org/docs/current/howto/auth.html>

Mise en place

- Soit dans `httpd.conf` (recommandé)
 - directives `<Directory>` ou `<Limit>`
- Soit dans des fichiers `.htaccess`
 - dans le répertoire à contrôler
 - non recommandé
- Pour autoriser la surcharge de ces directives

AllowOverride AuthConfig

- peu concerner les `.htaccess`, les sous-répertoires avec `<Directory>`, et autres

Gestion des comptes utilisateur

- Création d'un utilisateur

```
# htpasswd [-c] /usr/local/apache/passwd/passwords monutilisateur
```

- -c pour créer automatiquement le fichier si n'existe pas

 le fichier ne DOIT pas être accessible aux autres utilisateurs

- et encore moins au web !

- Supprimer un utilisateur

```
# htpasswd -D /usr/local/apache/passwd/passwords monutilisateur
```

- Créer un ou plusieurs groupes d'utilisateurs
 - Créer un fichier de groupe selon la syntaxe suivante

```
Nom-de-groupe: user1 user2 user3
```

Protection d'un dossier par DAC

- Dans une directive <Directory *mondossier*> ou un fichier .htaccess dans le dossier

```
AuthType Basic
# message à afficher
AuthName "Restricted Files"
AuthBasicProvider file
AuthUserFile /usr/local/apache/passwd/passwords
AuthGroupFile /usr/local/apache/passwd/groups
Require user monutilisateur
Require group mongroupe
```

- Autoriser l'accès à tout les utilisateurs enregistrés

```
Require valid-user
```

Protection d'un dossier par MAC

- Grâce au module `mod_authz_host`
- Dans une directive `<Directory mondossier>` ou un fichier `.htaccess` dans le dossier

- adresse IP

```
Require ip 10.1.2.3
Require ip 192.168.1.104 192.168.1.205
```

- sous-réseau

- ip partielle

```
Require ip 10.1
Require ip 10 172.20 192.168.2
```

- réseau / masque

```
Require ip 10.1.0.0/255.255.0.0
Require ip 10.1.0.0/16
```

- Hôte

```
Require host example.org
Require host .net example.edu
```

- Local

```
Require local
```

apache2ctl

- Interface de contrôle du démon Apache

```
# apache2ctl [commande] ...
```

- Commandes

- start
- stop
- restart
- fullstatus : statut complet à partir de `mod_status`
 - nécessite un navigateur web texte (comme Lynx)
 - url d'accès modifiable (variable `STATUSURL`)
- status : idem, sans la liste des requêtes actuellement traitées
- graceful : redémarrage par l'envoi d'un `SIGUSR1`
 - ne clos pas les connections actuellement ouvertes
- configtest : teste de syntaxe des fichiers de configuration
- help

Bonus : les outils Debian

- activer / désactiver un site

```
$ a2ensite [site]
```

```
$ a2dissite [site]
```

- créé / supprimer un lien symbolique de sites-availability/site dans sites-enabled

- activer / désactiver un module

```
$ a2enmod [module]
```

```
$ a2dismod [module]
```

- créé / supprimer un lien symbolique de sites-availability/site dans sites-enabled

Ce qu'on a couvert

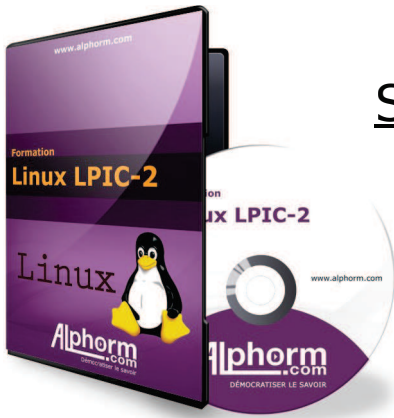
- Installation et configuration de Apache2
 - httpd.conf et .htaccess
 - fichiers journaux
 - nombre maximum de requêtes, nombres minimums et maximums de serveurs et de clients
- Gestion des modules
 - mod_perl
 - mod_php
 - mod_auth
 - htpasswd
- Apache2ctl

208.1 Implementing a web server

Weight : 3

Description : Candidates should be able to install and configure a web server. This objective includes monitoring the server's load and performance, restricting client user access, configuring support for scripting languages as modules and setting up client user authentication. Also included is configuring server options to restrict usage of resources.





Services web

Mise en place de serveurs virtuels Apache 2

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
- Deux solutions
- Directive VirtualHost
- Serveurs virtuels par IP
- Serveurs virtuels par nom d'hôte
- Mécanisme de sélection de serveur virtuel



Introduction

- Héberger plusieurs sites sur un même serveur
- Deux types :
 - IP based
 - Nécessite plusieurs interfaces (ou routage)
 - Named based
 - Répond en fonction de l'url appelée
- Configurés dans httpd.conf
 - ou /etc/apache2/sites-available/ sur Debian et dérivés
- Documentation officielle : <https://httpd.apache.org/docs/current/vhosts/>



Deux solutions

- Faire tourner un processus httpd pour chaque domaine
 - plusieurs installations séparées
 - répartition de sécurité
 - directives **User**, **Group** et **ServerRoot** différentes

```
User httpd1
Group httpd1
ServerRoot "/etc/httpd/server1"
```

- répartition des interfaces (adresses ip)
 - via des directives **Listen** différentes

```
Listen 192.170.2.1:80
```

- Utiliser un unique processus résident
 - partage de configuration des serveurs virtuels
 - meilleures performances

Directive VirtualHost

```
<VirtualHost adresse IP[:port] [adresse IP[:port]] ...> ... </VirtualHost>
```

- Contexte : Configuration du serveur
- rassemble des directives qui ne s'appliqueront qu'à un serveur virtuel particulier
 - La plupart des directives (toutes celles acceptant le contexte "Serveur Virtuel" - cf [doc](#)) sont compatibles

• Exemple

```
<VirtualHost *:80>
  ServerAdmin contact@example.org
  DocumentRoot /www/docs/www.example.org
  ServerName www.example.org
  ErrorLog logs/example.org-error_log
  TransferLog logs/example.org-access_log
</VirtualHost>
```

Serveurs virtuels par IP

• Directive VirtualHost

- définition des directives `ServerAdmin`, `ServerName`, `DocumentRoot`, `ErrorLog` ainsi que `TransferLog` ou `CustomLog`

▪ Exemple

```
<VirtualHost 172.20.30.40:80>
  ServerAdmin webmaster@www1.example.com
  DocumentRoot /www/vhosts/www1
  ServerName www1.example.com
  ErrorLog /www/logs/www1/error_log
  CustomLog /www/logs/www1/access_log combined
</VirtualHost>
```

Serveurs virtuels par nom d'hôte

- Directive **VirtualHost**

- grâce à la directive **ServerName**, permettant de définir le nom auquel répondra le serveur virtuel
 - peu répondre à plusieurs noms grâce à la directive **ServerAlias**

- Exemple

```
<VirtualHost *:80>
# Le premier serveur virtuel de la liste est aussi le
# serveur par défaut pour *:80
ServerName www.example.com
ServerAlias example.com
DocumentRoot /www/domain
</VirtualHost>

<VirtualHost *:80>
ServerName other.example.com
DocumentRoot /www/otherdomain
</VirtualHost>
```

Mécanisme de sélection de serveur virtuel

1) Par couple adresse IP / port

- Les chaînes sans caractères génériques l'emportent sur celles qui en contiennent
- Le port est également pris en compte
 - ie : il peu exister deux hôtes virtuels 192.168.1.1:80 et 192.168.1.1:8080
- la configuration du serveur principale sera utilisée si aucune correspondance n'est trouvée

2) Par nom d'hôte

- Si (et seulement si) plusieurs hôtes virtuels correspondent au couple adresse IP / Port
- Comparaison des directives **ServerName** et **ServerAlias** avec le nom de serveur dans la requête
 - Le premier correspondant est utilisé
 - Y compris si un caractère générique (*) est présent (aucune priorité particulière)
 - Si aucune correspondance n'est trouvée, le **premier** hôte virtuel correspondant au couple IP / Port sera employé

Remarque : il est bien entendu nécessaire d'avoir configuré votre DNS en conséquent

Ce qu'on a couvert

- Qu'est ce qu'un hôte virtuel.
- Mise en place des serveurs virtuels Apache 2
 - avec ou sans adresse IP dédiée
- Comment sont sélectionnés les hôtes virtuels.

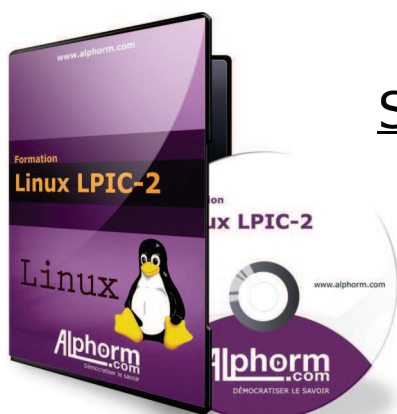
208.2 Maintaining a web server (Part 1)

Weight : 2

Description : Candidates should be able to configure a web server to use **virtual hosts**, Secure Sockets Layer (SSL) and customise file access.



Alphorm.com



Services web

Sécurisation d'un serveur web avec SSL

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Secure Socket Layer
- mod_ssl
- Chiffrement par clés asymétriques
- Signature
- Certificat
- Installation
- /etc/ssl/*
- Création du certificat auto-signé
- Création d'un certificat signé par un CA
- Configuration d'un virtual host SSL



Secure Socket Layer

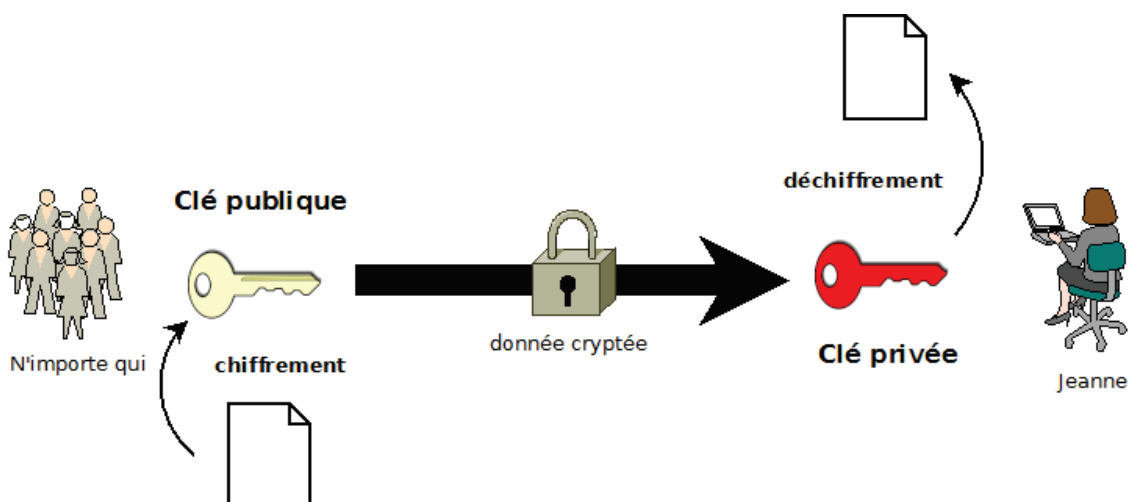
- protocole se situant entre un protocole réseau orienté connexion (TCP/IP) et un protocole de la couche applicative (HTTP)
- sécurisation des communications entre un serveur et un client
 - authentification mutuelle
 - intégrité par signature digitale
 - chiffrement par clés asymétriques
- Port 443

```
Listen 443
```

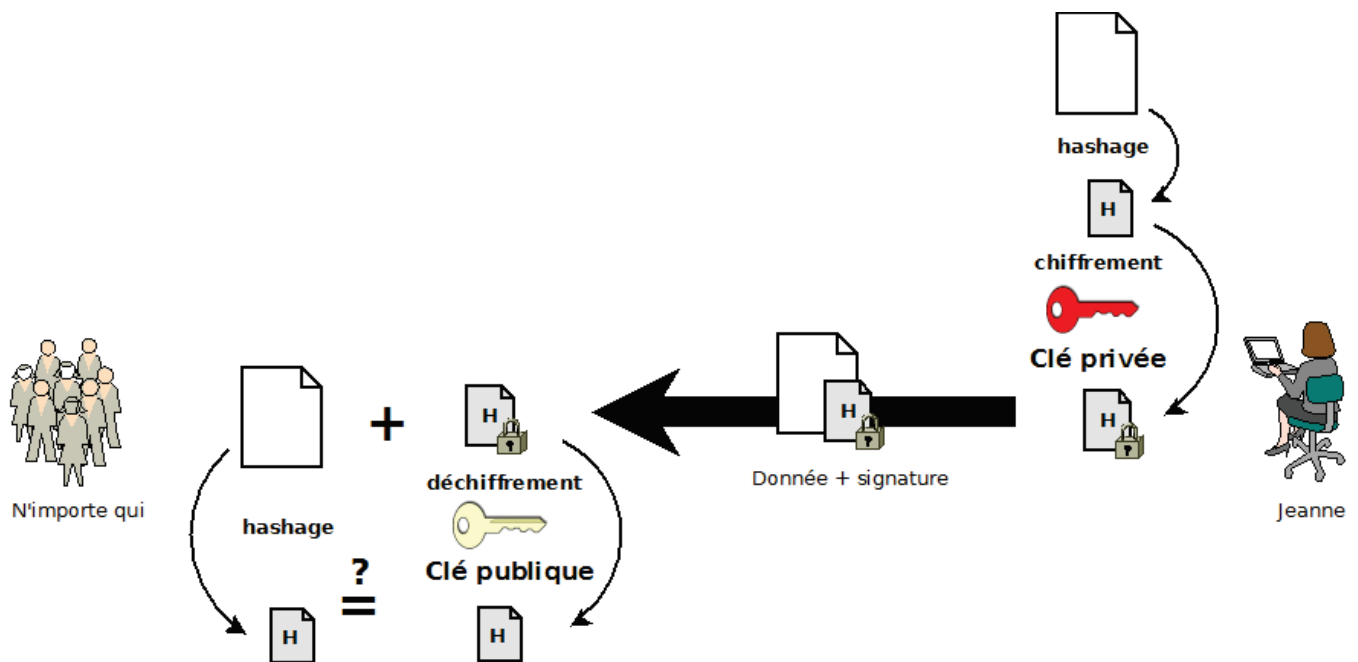
mod_ssl

- Utilisation de SSL pour Apache via OpenSSL
 - d'autres solutions dérivées existent
 - Secure Web Server de Red Hat
 - Raven SSL Module de Raven
 - Stronghold de C2Net
 - mais leur conception est assez similaire dans l'ensemble, et leur usage spécifique (non couverts par la LPIC2 et donc par ce cours)

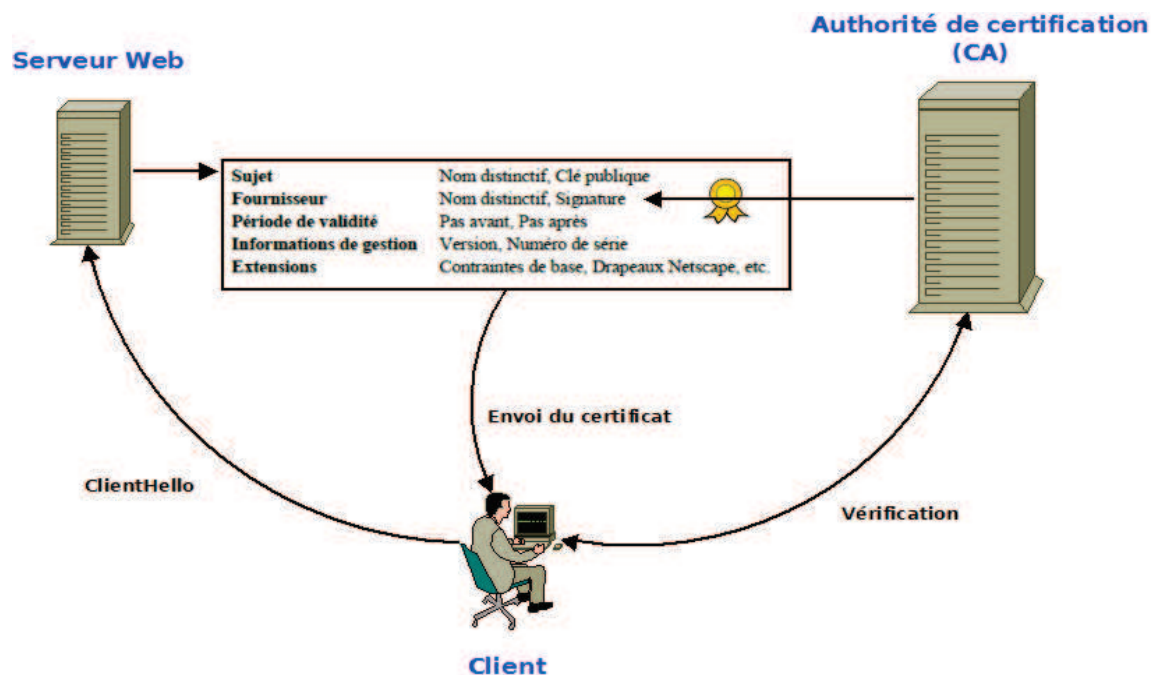
Chiffrement par clés asymétriques



Signature



Certificat



Installation

- Debian : installé par défaut

```
# a2enmod ssl
```

- CentOS

```
# yum install mod_ssl
```

- configuration complète dans conf.d/ssl.conf
 - Directives LoadModule et Listen
 - Contexte global de ssl
 - virtual host par défaut

/etc/ssl/*

- Configuration de OpenSSL
 - certs/ : certificats SSL
 - openssl.cnf : Configuration de OpenSSL
 - date d'expiration des clés
 - nom de l'organisation
 - adresse, etc ...
 - private/ : clés privées

Création du certificat auto-signé

```
# openssl req -x509 -nodes -days 365 -newkey rsa:1024 \  
> -out /etc/ssl/certs/noelmace.com.crt \  
> -keyout /etc/ssl/private/noelmace.com.key
```

```
# chmod 400 /etc/ssl/private/noelmace.com.key
```

- Options
 - -x509 -nodes : type de certificat
 - -days 365 : durée de validité du certificat (en jours)
 - -newkey rsa:1024 : clé RSA de 1024 bits
 - il est déconseillé de créer une clé plus grosse pour des histoires de compatibilité
 - -out /etc/apache2/server.crt : certificat
 - -keyout /etc/apache2/server.key : clé privée
- Interactif : suite de questions (Pays, Ville, Organisation, CN et Adresse mail)
 - ⚠ pour Common Name : indiquer le **nom de domaine** à protéger

Création d'un certificat signé par un CA

- génération de la clé privée

```
# openssl genrsa 1024 > noelmace.com.key
```

- création du CSR
 - Certificate Signing Request ou fichier de demande de signature de certificat

```
# openssl req -new -key servwiki.key > servwiki.csr
```

- Envoyer le CSR au CA (Autorité de certification)
 - par exemple gandi.net, [tustico](https://tustico.com) ou [StartSSL](https://startssl.com) (gratuit)
 - permet d'obtenir un certificat signé par la clé privée de l'organisme
- Déposer les certificats fournis aux bons emplacements
 - votre certificat ainsi que celui de votre CA dans /etc/ssl/certs/
 - votre clé dans le dossier /etc/ssl/private/ avec les droits 400

Configuration d'un virtual host SSL

```
<VirtualHost *:443>
    ServerName noelmace.com
    DocumentRoot /var/www/noelmace.com

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/noelmace.com.crt
    SSLCertificateKeyFile /etc/ssl/private/noelmace.com.key
    SSLCACertificateFile /etc/ssl/certs/GandiXXXSSLCA.pem
    SSLVerifyClient none

    Require ssl
</VirtualHost>
```

- Directives
 - SSLEngine on/off : active / désactive le SSL pour ce serveur virtuel
 - SSLCertificateFile *file* : chemin vers le certificat
 - SSLCertificateFile *file* : chemin vers la clé privée
 - SSLVerifyClient none/optional/require/optional_no_ca : niveau de vérification du certificat pour l'authentification du client
 - Require ssl : les clients ne peuvent se connecter à ce serveur virtuel que via ssl

Ce qu'on a couvert

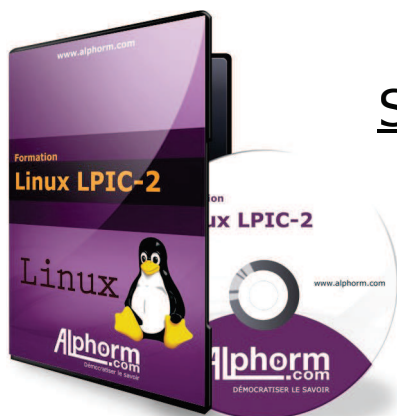
- Qu'est ce que le SSL ?
 - Ainsi que les principes liés.
- Les fichiers de configuration, outils et utilitaires pour SSL
 - openssl, /etc/ssl/*
- Gestion des certificats SSL
- Configuration d'un virtual host pour le ssl

208.2 Maintaining a web server (part 2)

Weight : 2

Description : Candidates should be able to configure a web server to use virtual hosts, Secure Sockets Layer (SSL) and customise file access.





Services web

Mise en place d'un serveur mandataire (proxy)

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Introduction
 - Squid
- Configuration
 - Paramètres généraux
- ACLs
 - ACLs : Exemples
- Restriction d'accès
- Authentification utilisateur
 - Authentification utilisateur pour Squid 2.4-



Introduction

- Serveur mandataire (proxy)
 - intermédiaire entre deux réseaux (ex : local / internet)
- Avantages et fonctionnalités
 - performances
 - mémoire cache, compression
 - sécurité
 - anonymisation
 - surveillance (journalisation)
 - filtrage
 - des publicités et contenus lourds (performance)
 - des contenus indésirables

Squid

- Proxy libre de référence
 - Licence GNU GPL
 - créé en Juillet 1996
 - Notamment utilisé par Wikimedia Fondation et Flickr
 - version actuelle (au 13 Juillet 2013) : 3.3.8
- Support des protocoles HTTP, HTTPS, FTP et Gopher
- Nombreuses fonctionnalités
 - mémoire cache
 - contrôle étendu des accès
 - cache DNS
 - mandataire inverse



Configuration

- squid.conf
 - /etc/squid (CentOS et Debian Squid 2) ou /etc/squid3 (Debian Squid 3)
 - Ensemble de directive complexes
 - ligne par ligne
 - Fonctionnel à l'installation
- Exemple (Extrait) :

```
visible_hostname ubuntu
http_port 3128
...
acl allowedips src 192.168.1.1/255.255.255.0
...
forwarded_for off
...
```

Paramètres généraux

- Définition du port d'écoute HTTP (3128 par défaut)

```
http_port 3177
```

- Interface d'écoute HTTP (toutes par défaut)
 - limiter aux réseaux locaux pour des raisons de sécurité

```
http_port 192.168.1.1:3177
```

- Nom de la machine (obtenu via gethostname()) par défaut)

```
visible_hostname nom_machine
```

ACLs

- Syntaxe

```
acl aclname acltype string[string2]
```

- acltype :

- src : adresse IP de la source (ie. le client) (adresse/masque) ou d'une place d'adresses (adresse_IP_debut-adresse_IP_fin)
- dst : adresse IP de la destination (ie. ordinateur cible)
- srcdomain : domaine du client
- dstdomain : domaine de destination.
- url_regex : chaîne contenu dans l'URL
 - possibilité d'utiliser les jokers ou un fichier
 - sensible à la casse
- urlpath_regex : chaîne comparée avec le chemin de l'URL
 - possibilité d'utiliser les jokers
- proto : protocole.

ACLs : Exemples

```
acl mon_domaine_dst dstdomain noelmace.com
```

```
acl clients src 192.168.0.0/255.255.0.0
```

```
acl url_interdit url_regex forbidden
```

```
acl url_interdites url_regex "/etc/squid/denied_url"
```

Restriction d'accès

- A partir d'une acl pré-définie
 - doit être placé après la définition de cette acl
- Syntaxe

```
http_access allow|deny [!]aclname
```

- Exemples

- interdire l'accès au domaine noelmace.com

```
http_access    deny        mon_domaine_dst
http_access    allow       all
```

- interdire l'accès aux pages contenant le mot forbidden

```
http_access    deny        url_interdit
http_access    allow       all
```

- Restreindre l'accès au proxy au seul réseau 192.168.0.0

```
http_access    allow       localhost
http_access    allow       clients
http_access    deny        all
```

Authentification utilisateur

- 4 types d'authentification HTTP possible
 - Basic, NTLM (SMB LM, v1 and v2), Digest, et Negotiate.
- Nombreuses solutions disponibles
 - APM, LDAP, NCSA auth, SMB ...
- Avec NCSA auth
 - à partir des mêmes outils (htpasswd) que pour Apache2 mod_auth_basic
 - Exemple

```
auth_param basic program /usr/local/squid/bin/ncsa_auth /usr/local/squid/etc/passwd
acl          auth_users      proxy_auth REQUIRED
http_access  allow          auth_users
http_access  deny           all
```

- Documentation : <http://wiki.squid-cache.org/Features/Authentication>

Authentification utilisateur pour Squid 2.4-

- Avec NCSA auth

```
authenticate_program /usr/lib/ncsa_auth /etc/squid/passwd
acl                  auth_users      proxy_auth REQUIRED
acl                  all             src 0/0
http_access          allow          auth_users
http_access          deny           all
```

- Avec LDAP

```
acl          identification proxy_auth      REQUIRED
http_access  allow          identification
authenticate_program /usr/lib/squid/squid_ldap_auth -b $LDAP_USER -u uid SERVEUR_LDAP
```

- LDAP_USER : ou (organizational unit) contenant les clients
 - exemple ou=people, ou= ac-limoges, ou=education, ou=gouv, c=fr

Test : configuration du client Debian

- Pour tester votre serveur, vous pouvez utiliser n'importe quel client http (firefox, epiphany, etc ...)
- La configuration peut se faire au niveau de l'OS client ou du logiciel client web
 - pour configurer firefox : [Documentation officielle](#)
 - pour configurer le proxy sur votre client Debian

```
$ gnome-network-preferences
```

Ce qu'on a couvert

- Gestion et configuration du serveur mandataire Squid
- Restriction d'accès grâce aux ACLs
- Authentification utilisateur

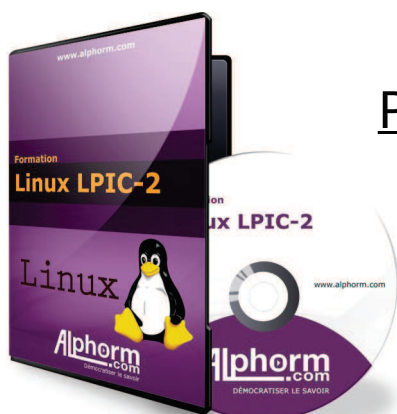
208.3 Implementing a proxy server

Weight : 1

Description : Candidates should be able to install and configure a proxy server, including access policies, authentication and resource usage.



Alphorm.com



Partage de fichiers

Configuration du serveur SAMBA

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Server Message Block
- SAMBA
 - Installation
 - Structure
 - Configuration
 - Paramètres généraux
 - Partage de fichiers
 - Politique d'accès à un partage
 - Droits des fichiers créés
- Gestion des utilisateurs
 - Identificateurs Windows
- Gestion des groupes
- smbclient
- Monter un partage SMB
- Partage d'imprimante
- Utilitaires



Server Message Block

- Protocole de partage réseau de ressources
 - développé en 1985 par IBM pour OS/2
 - nommé alors LAN Manager
 - puis popularisé par Microsoft qui l'intègre à Windows après de nombreuses améliorations, créant ainsi SMB
 - temporairement dénommé CIFS (Common Internet File System) entre 1998 et 2006
 - notamment dans Windows NT 4
 - puis renommé SMB2, une nouvelle version plus rapide
 - Depuis Windows Vista
 - nouvelle version 3.0 introduite avec Windows 8
- Propriétaire
 - spécifications fermées à l'origine
 - puis distribuées via le [MSDN Open Specifications Developer Center](http://MSDN)
- Permet le partage de fichiers et d'imprimante sur tout réseau local Windows



SAMBA

- Développé par rétro-ingénierie grâce à un renifleur de paquets
 - par [Andrew Tridgell](#) depuis 1992
 - aujourd'hui en "partenariat" avec Microsoft, contraint à signé un [accord d'information technique](#) après avoir perdu leur procès en appel contre l'Union Européenne en 2007
 - 2,5 fois [plus performant](#) que Microsoft Windows Server 2003
- version actuelle (au 2 Juillet 2013) : 4.0.7
 - réécriture complète
 - offre un contrôleur de domaine Active Directory
- Dans le cadre de la LPIC2, nous étudierons cependant la version 3, encore parfaitement d'actualité
- Libre (Licence GNU GPL v3)



- Supporte les principaux produits réseau propriétaires Microsoft
 - SMB/CIFS pour le partage de fichiers et imprimantes
 - NetBIOS sur TCP/IP (NBT) pour le nommage WINS (rendu obsolète par DNS) et l'établissement de sessions
 - MSRPC pour les appels de procédure à distance

Installation

- Serveur
 - Debian

```
# apt-get install samba
```

- CentOS

```
# yum install samba
```

- Client

- Debian

```
# apt-get install smbclient
```

- CentOS

```
# yum install samba-client
```

Structure

- via Inetd ou des démons
 - inetd pour plus de sécurité via tcpwrappers et moins d'utilisation de la mémoire
 - démons pour plus de performance
- Deux démons :
 - smbd : Server Message Block Daemon
 - gestion du partage réseau SMB
 - nmbd : NetBIOS Name Service Daemon
 - gestion du serveur WINS
- Ports logiciels
 - TCP et UDP 137 : NetBIOS Name Service
 - UDP 138 : NetBIOS Datagram Service
 - TCP 139 : NetBIOS Session Service
 - TCP et UDP 445 : Services de dossiers partagés Windows

Configuration

- /etc/samba/smbd.conf
 - découpé en sections
 - [global] : paramètres généraux (indiqués par un G dans le man) et paramètres par défaut
 - [printers] et [print\$] : partage d'imprimantes
 - [homes] : partage du répertoire personnel des utilisateurs
 - [partage] : nom d'un partage (tout les paramètres indiqués par un S dans le man, également compatibles avec la section global)
 - vérifié par smbd toutes les 3 minutes pour prendre en compte les modifications
- Exemple :

```
[global]
workgroup = "Mon_Workgroup"
server string = (%Samba %v)
# commentaire
...

[homes]
comment = Home Directories
preexec = /bin/sh -c 'echo "Repertoire_source_samba"/bin/smbclient -M %m -I %I'&
browseable = yes
...

["Nom_De_Partage"]
comment = "Commentaire"
...
```

Paramètres généraux

- section [global] de smb.conf
 - groupe de travail (Domaine NetBIOS)

```
workgroup = MON_WG
```

- Nom NetBIOS

```
netbios name = SERVEUR1
```

- Description

```
server string = serveur %h (Samba %v, GNU/Linux)
```

- % permet la substitution de variables (cf [man](#))
- %h pour le nom d'hôte et %v pour le numéro de version du serveur
- limiter le partage à certaines interfaces

```
bind interfaces only = Yes  
interfaces = 127.0.0.1 eth0:0 192.168.1.20/24
```

Partage de fichiers

- une section par partage
 - chemin vers le répertoire à partager

```
path = /data/Documents
```

- description

```
comment = mon commentaire
```

Politique d'accès à un partage

- Lecture / écriture pour tous

```
read only = No
```

- Lecture seule pour tous

```
read only = Yes
```

- restriction de l'écriture à une liste d'utilisateurs

```
read only = Yes  
write list = user1, user2, @grp1, @grp2
```

- restriction de l'accès à une liste d'utilisateurs

```
valid users = utilisateur1, utilisateur2, @groupe12000
```

Droits des fichiers créés

- Droit des fichiers à la création

```
create mask = 0775
```

- Droit des dossiers à la création

```
directory mask = 700
```

- Forcer tout les utilisateurs à être reconnus comme un seul et même utilisateur sur le système

```
force user = nobody  
force group = nogroup
```

Authentication

- Mode

```
security = mode
```

- share : contrôle d'accès au niveau ressources
 - un mot de passe par partage
- contrôle d'accès au niveau utilisateur
 - user : utilisateur / mot de passe
 - par défaut depuis Samba 2.2.X
 - domain : centralisés sur un domaine
 - délègue toute requête d'authentification au contrôleur de domaine

```
workgroup = WG
```

- server : déprécié (mis en place lorsque par le passé Samba n'était pas capable d'agir en tant que serveur membre d'un domaine)
- ADS : via Active Directory

```
realm = your.kerberos.REALM  
password server = your.kerberos.server
```

Base des utilisateurs Samba

- stocker la **base des utilisateurs** dans
 - un fichier (par défaut, mais déconseillé)

```
passdb backend = smbpasswd  
smb passwd file = /etc/samba/smbpasswd
```

- une base de donnée **TDB** (Trivial DataBase)

```
passdb backend = tdbsam
```

- une base ldap

```
passdb backend = ldapsam:url
```

- pour une description détaillé de la configuration de ldap et Samba, voir la **documentation officielle**

Gestion des utilisateurs

- Gestion de la synchronisation des utilisateurs grâce à smbpasswd
 - utilitaire client/serveur (pouvant modifier à distance les comptes Windows NT)
 - Ajouter ou modifier un utilisateur Samba

```
# smbpasswd -a utilisateur
```

- cet utilisateur **doit** être un utilisateur existant sur le système
 - ie. dans le fichier /etc/passwd
- le mot de passe pourra cependant être différent
- Désactiver un utilisateur Samba

```
# smbpasswd -d utilisateur
```

- Lister les utilisateurs

```
# pdbedit -L
```

Identificateurs Windows

- SID (Security Identifier)
 - censé être unique dans le monde
 - permet d'identifier les serveurs, utilisateurs ou objets (groupes)
 - Format : S-1-5-12-7623811015-3361044348-030300820-1013
 - S - indique que ceci est un SID
 - 1 - niveau de révision
 - 5 - valeur d'autorité de l'identificateur
 - 12-7623811015-3361044348-030300820 - Identificateur de domaine ou d'ordinateur
 - 1013 - Un identificateur relatif (RID : Relative ID)
 - unique au sein d'un domaine

Gestion des groupes

- Grâce à l'utilitaire `net` (permet d'administrer Samba et les serveurs CIFS distants, très complet)
 - commande `groupmap`

- Arguments
 - `unixgroup` : nom du groupe Unix
 - `ntgroup` : nom du groupe Windows NT (doit être associé à un SID)
 - `rid, sid`
 - `type` - type de groupe ('domain', 'local', ou 'builtin')
 - `comment` : description du groupe

- Ajouter une nouvelle entrée de mapping de groupe

```
# net groupmap add {rid=int|sid=string} unixgroup=string \  
[type={domain|local}] [ntgroup=string] [comment=string]
```

- Supprimer une entrée

```
# net groupmap delete {ntgroup=string|sid=SID}
```

- Lister les entrées

```
# net groupmap list [verbose] [ntgroup=string] [sid=SID]
```

smbclient

- Connexion

```
$ smbclient [-L nom_netbios | nom_du_service] [-W workgroup] [-U username[%password]]
```

- Options
 - `-L` : lister les partages disponibles pour un utilisateur (avec `-U`)
 - `-W` : nom de domaine SMB (workgroup) de l'utilisateur
 - utilise par défaut celui défini dans `smb.conf`
 - `-U` : nom de l'utilisateur
- Commandes internes "ftp like"
 - `put`, `get`, `ls`, `cd`, `mkdir`, `help`, etc ...

- Exemples

- lister les partages disponibles

```
# smbclient -L \\serveur1 -W monwg -U noel
```

- se connecter à un partage

```
# smbclient \\\\serveur1\\Documents -W monwg -U noel
```

Monter un partage SMB

- Deux solutions

- smbfs

- déprécié depuis Linux 2.6.20
 - outils externes : smbclient, smbmount, smb.conf

```
# smbmount {service} {mount-point} [-o options]
```

- CIFS VFS

- parfaitement intégré au kernel
 - configuration via /proc/fs/cifs/ et les options de module (via insmod et modprobe)
 - ne nécessite aucun outils externe (smbmount remplacé par un simple helper mount.cifs)

```
# mount -t cifs //192.168.1.10/monpartage /mnt/smb -o user=noel,pass=monmdp
```

- Montage automatique

- dans le fichier /etc/fstab

```
//192.168.1.10/monpartage /mnt/smb cifs user,user=noel,pass=monmdp 0 0
```

Partage d'imprimante

- Partager toutes les imprimantes

```
[printers]
comment = Printer %p on Server1
path = /var/spool/samba
printable = yes
```

- Partager une imprimante spécifique

```
[HP LaserJet]
printer name = lp
comment = HP LaserJet 5 on Server1
path = /var/spool/lpd/samba
printable = yes
writeable = no
```

Utilitaires

- Tester la syntaxe de smb.conf

```
# testparm
```

- Lister les connections au serveur

```
# smbstatus
```

Ce qu'on a couvert

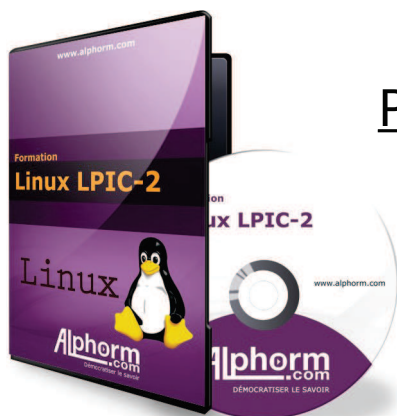
- Samba 3
 - configuration
 - outils et utilitaires
 - partage de fichiers et d'imprimantes
 - montage des partages de fichiers sous GNU/Linux
 - sécurité et mise en correspondance des utilisateurs

209.1 SAMBA Server Configuration

Weight : 4

Description : Candidates should be able to set up a SAMBA server for various clients. This objective includes setting up Samba for login clients and setting up the workgroup in which a server participates and defining shared directories and printers. Also covered is a configuring a Linux client to use a Samba server. Troubleshooting installations is also tested.





Partage de fichiers

Configuration du serveur NFS

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

Plan

- Introduction
- Options du noyau
- RPC et Portmap
- rpcinfo
- Démons
- Sécurité
- Configuration des exports
- Options de partage NFS
- exportfs
- showmount
- Montage
- Options de montage NFS
- nfsstat



Introduction

- Network File System
 - un des plus anciens protocoles de partage de fichiers
 - développé par Sun en 1985 pour Unix
 - pour plus d'infos voir [ce document](#)
 - aujourd'hui également adapté pour Windows
 - standard ouvert
 - basé sur
 - ONC/RPC (Open Network Computing Remote Procedure Call) ou Sun RPC ([RFC 5531](#))
 - protocole d'appel de procédures distant
 - couche 5 (session) du modèle OSI (synchronisation des communications et gestion des transactions)
 - pour plus d'infos sur le système d'authentification ONC/RPC, voir [ce document](#)
 - XDR (eXternal Data Representation)
 - couche 6 (présentation) du modèle OSI (codage)
 - [site officiel](#)
- Versions
 - v1 : uniquement pour un usage expérimental en interne de Sun
 - v2 ([RFC 1094](#), Mars 1989)
 - non sécurisé, sur UDP
 - v3 ([RFC 1813](#), Juin 1995)
 - prise en charge du TCP, des écritures asynchrones
 - encore très utilisé, nous l'étudierons ici
 - v4 ([RFC 3010](#), Décembre 2000 - révisé par la [RFC 3530](#), Avril 2003)
 - réécriture complète avec l'IETF
 - sécurisé (notamment avec [Kerberos](#)), support statefull, meilleures performances
 - v4.1 ([RFC 5661](#), Janvier 2010)
 - parallélisation des accès, introduction du concept de session
 - pour en savoir plus sur NFSv4, lire [ce document](#)

Options du noyau

- NFS file system support (CONFIG_NFS_FS)
 - support client (ou serveur en espace utilisateur) NFSv2
 - NFSv3 client support (CONFIG_NFS_V3)
 - support client NFSv3
 - dépend de CONFIG_NFS_FS
- NFS server support (CONFIG_NFSD)
 - support serveur NFSv2 en espace noyau
 - NFSv3 server support (CONFIG_NFSD_V3)
 - support serveur NFSv3 en espace noyau

RPC et Portmap

- Procédures (fonctions) RPC
 - identifiées par un numéro
 - regroupées en programmes
 - eux même identifiés par un numéro ainsi qu'un numéro de version
 - Les appels à un fonctions peuvent donc ce faire via l'association de ces 3 numéros
 - Tous référencés dans /etc/rpc (à ne pas modifier)
- **Portmap** : démon permettant la conversion de numéros de programmes RPCs en numéros de port logiciel DARPA
 - destiné (sans grand succès) à limiter le nombre de ports logiciels utilisés
 - aujourd'hui uniquement utilisé par :
 - NFS
 - FAM (moniteur de modification de fichier)
 - NIS (logiciel d'annuaire devenu obsolète)

rpcinfo

- utilitaire permettant d'effectuer des appels à un serveur RPC
 - rapporter les informations obtenues
 - man : <http://linux.die.net/man/8/rpcinfo>
- Afficher la liste de tout les programmes RPC enregistrés

```
# rpcinfo -p [host]
```

- Tester un programme RPC par l'appel à sa procédure 0
 - déprécié : via udp

```
# rpcinfo [-n portnum] -u host prognum [versnum]
```

- déprécié : via tcp

```
# rpcinfo [-n portnum] -t host prognum [versnum]
```

- recommandé

```
# rpcinfo -T transport host prognum [versnum]
```

Démons

- `rpc.nfsd`
 - si installé en espace utilisateur (v2 seulement) : serveur complet
 - si installé en espace noyau : simple programme de contrôle
 - relié au "processus" [`nfsd`]
- `rpc.mountd`
 - gestion des requêtes de montage NFS entrantes
 - configuré via `/etc/exports`
- `rpc.lockd`
 - démon de verrouillage
 - non nécessaire pour les kernel 2.4.X et plus
 - intégré en interne ([`lockd`])
- `rpc.statd`
 - service de notification de redémarrage

Sécurité

- NFS n'a pas été conçu à une époque où les questions de sécurité étaient au premier plan
 - sa conception n'est donc pas adapté à ce type de contexte
- Toute authentification utilisateur repose sur les UID et GID
 - tout hôte ayant les droits root sur sa machine a donc, en théorie, les mêmes droits sur les partages auxquels il peu accéder
 - il est donc nécessaire d'utiliser le mapping des utilisateurs
 - ie. associer l'utilisateur root ou tout utilisateur se connectant au partage à un compte (UID/GID) donné
- La restriction des accès se fait donc uniquement sur l'authentification des machines clientes
 - nom d'hôte (dangereux en cas d'attaque sur les DNS), ip ou groupe réseau NIS
- NFSv4 cependant a été totalement repensé
 - rend obligatoire l'implémentation du module noyau `RPCSEC_GSS` (RFC 2203) (voir [man](#))
 - GSS-API (RFC 2743), lié à Kerberos
 - documentation complète sur [ce document](#)
 - orienté vers l'authentification individuelle des utilisateurs
 - d'autres problèmes de sécurité ont également été résolus, comme par suppression du démons `rpc.mountd`

Configuration des exports

- Fichier /etc/exports

```
<dossier partagé> <hôte>(<options>) <hôte2>(<options>)...
```

- <dossier partagé> : chemin du dossier partagé
- <hôte> : hôte pouvant accéder au partage
 - une IP
 - un nom d'hôte ou un domaine grâce à un joker (*)
 - exemple : *.noelmace.com
 - un nom de groupe réseau NIS (NIS netgroup - sous la forme @<netgroup>)
 - un intervalle d'IP avec masque de sous-réseau
 - exemple : 192.168.0.0/24 ou 192.168.0.*

Options de partage NFS

- rw : lecture et l'écriture sur un partage pour l'hôte défini
 - ro par défaut
- Synchronicité
 - async : mode asynchrone
 - répondre aux requêtes avant que les changements effectués par celle-ci n'aient été appliqués sur l'unité de stockage
 - améliore les performances
 - danger pour l'intégrité des données en cas de redémarrage brutal (crash)
 - sync : mode synchrone
- mapping des utilisateurs
 - root_squash : (par défaut) mapping de l'utilisateur root vers l'utilisateur anonyme
 - no_root_squash : pas de mapping pour l'utilisateur root
 - all_squash : mapping de tous les utilisateurs vers l'utilisateur anonyme.
 - anonuid : UID de l'utilisateur anonyme (considéré comme tel dans les précédentes options de mapping).
 - anongid : GID de l'utilisateur anonyme (considéré comme tel dans les précédentes options de mapping).

exportfs

- Il est indispensable d'exporter les exports après les avoir configurés
 - seul /var/lib/nfs/xtab et lu par mountd
- Pour relancer le partage de tout les répertoires
 - ie. synchroniser /var/lib/nfs/xtab avec /etc/exports

```
# exportfs -r
```

- Interrompre tout partage

```
# exportfs -ua
```

showmount

- Afficher des informations de montage sur un serveur NFS

```
# showmount [ -adehv ] [ --all ] [ --directories ] [ --exports ] [ host ]
```

- Options
 - -a ou --all : nom du client et répertoire monté (machine:répertoire)
 - -d ou --directories : uniquement les répertoires montés par un client.
 - -e ou --exports : liste des répertoires exportés par le serveur NFS.
 - -h ou --help : aide
 - --no-headers : supprimer les en-têtes de description de l'affichage.

Montage

- Montage manuel

```
# mount -t nfs server:/share /mountpoint -o options
```

- Montage automatique

- dans /etc/fstab

```
server:/share /mountpoint nfs options 0 0
```

Options de montage NFS

- `rsize=xxx` et `wsiz=xxx`
 - taille des blocs de données échangés
 - pour la lecture et l'écriture
 - permet d'optimiser les vitesses de transfert
 - voir [ce document](#)
- `udp` et `tcp`
 - spécifier le protocole de transport à utiliser
 - seulement UDP pour NFSv2, les deux pour NFSv3, seulement TCP pour NFSv4
- `retry=n`
 - Nombre d'essais effectués pour un montage NFS en arrière-plan avant d'abandonner
 - en minutes (1000 par défaut)
- `nfsvers=n`
 - version de NFS à utiliser
- `timeo=n`
 - délai avant de déclencher la première retransmission d'une RPC
 - en 10èmes de secondes (7 par défaut)
- `hard` (par défaut) ou `soft`
 - Si une opération sur un fichier NFS arrive à une expiration majeure de délai
 - `hard` : réessayer indéfiniment
 - `soft` : renvoyer une erreur au programme appelant
- Voir [man](#) pour la liste complète des options

nfsstat

- Afficher des statistiques NFS

```
# nfsstat [OPTION]...
```

- Options
 - -s : uniquement les statistiques du serveur
 - -c : uniquement les statistiques du client
 - -n : uniquement les statistiques NFS
 - -r : uniquement les statistiques RPC
 - -m : lister les partages NFS montés

Ce qu'on a couvert

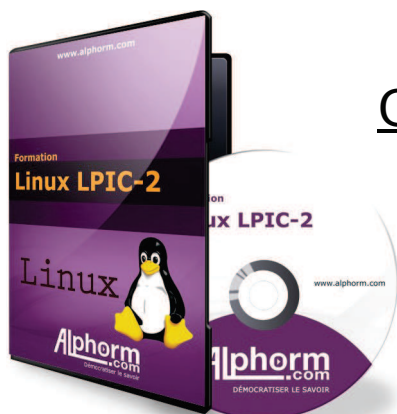
- NFS version 3
 - outils, utilitaires et configuration
 - restrictions d'accès
 - options de montage
- sensibilisation à NFSv4

209.2 NFS Server Configuration

Weight : 4

Description : Candidates should be able to export filesystems using NFS. This objective includes access restrictions, mounting an NFS filesystem on a client and securing NFS.





Gestion des clients réseau

Configuration DHCP

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

Plan

- Bootstrap Protocol
- Dynamic Host Configuration Protocol
- ISC DHCP
- Installation
- Configuration
- Paramètres et options
- Réseaux partagés
- Sous-réseaux
- Groupes
- Hôtes
- Client BOOTP
- Maintenance
- Agent relais DHCP



Bootstrap Protocol

- BOOTP
 - protocole d'amorçage (boot)
 - pour la configuration de stations de travail sans disque disposant de capacités de démarrage limitées
 - adresse IP
 - adresse serveur
 - fichier (image) de démarrage
 - défini en Septembre 1985 ([RFC 951](#))
 - en remplacement de RARP (Reverse Address Resolution Protocol - [RFC 903](#) - Juin 1984)
 - très limité
- Ports UDP :
 - server : 67
 - client : 68

Dynamic Host Configuration Protocol

- Octobre 1993 : première définition ([RFC 1531](#))
 - comme extension de BOOTP (Bootstrap Protocol)
 - couvre l'ensemble des configurations IP
 - adresse IP, masque, passerelle par défaut
 - adresses des serveurs de noms (DNS et NBNS (WINS))
 - mécanisme de récupération des adresses IP inutilisées
- modifié et complété par la [RFC 2131](#) (Mars 1997)
 - référence ipv4 actuelle
- adapté à l'ipv6 depuis Juillet 2003 ([RFC 3315](#))



ISC DHCP

- Développé par Ted Lemon et Vixie Enterprises
 - pour l'Internet Systems Consortium
 - alpha release en Mars 1999
 - première version stable en Janvier 2003



- Maintenu depuis 2004 par une équipe dédiée de l'ISC
 - aujourd'hui en version 4.2.5 (Janvier 2013)
- Libre : Licence ISC également dénommée Licence OpenBSD)

Installation

- Debian
 - version 3 (obsolète)

```
# apt-get install dhcp3-server
```

- version 4

```
# apt-get install isc-dhcp-server
```

- CentOS
 - client et serveur

```
# yum install dhcp
```

Configuration

- /etc/dhcpd.conf
 - voir [man dhcpd.conf](#)
- 6 types de directives
 - paramètres : valeurs internes du serveur, son comportement et informations fournies aux clients
 - options : options de configuration réseau et des divers services réseaux depuis le serveur DHCP
 - déclarations : topologie réseau, clients et adresses ou groupement de paramètres pour un contexte particulier
 - réseaux partagés
 - sous-réseaux
 - groupes
 - hôtes

Paramètres et options

- durée du bail (en secondes)

```
default-lease-time time;
```

```
max-lease-time time;
```

- Option (voir [man dhcpd-options](#))

- masque de sous-réseau

```
option subnet-mask ip-address;
```

- serveur DNS

```
option domain-name-servers ip-address [, ip-address... ];
```

Réseaux partagés

- informer le serveur DHCP que certains sous-réseau IP partagent en réalité le même réseau physique

- Syntaxe

```
shared-network name {  
    [ paramètres ]  
    [ déclarations ]  
}
```

- Exemple

```
shared-network ISC-BIGGIE {  
    paramètres spécifiques au réseau partagé...  
    subnet 204.254.239.0 netmask 255.255.255.224 {  
        paramètres spécifiques au sous-réseau...  
        range 204.254.239.10 204.254.239.30;  
    }  
    subnet 204.254.239.32 netmask 255.255.255.224 {  
        paramètres spécifiques au sous-réseau...  
        range 204.254.239.42 204.254.239.62;  
    }  
}
```

Sous-réseaux

- fournir des paramètres spécifiques au sous-réseau
- spécifier quelles adresses peuvent être dynamiquement allouées aux clients de ce sous-réseau
 - déclaration range

- Exemple

```
subnet 204.254.239.64 netmask 255.255.255.224 {  
    paramètres spécifiques au sous-réseau...  
    range 204.254.239.74 204.254.239.94;  
}
```

Groupes

- appliquer un ou plusieurs paramètres à un groupe de déclaration
 - hôtes, réseaux partagés, sous-réseaux, ou même d'autres groupes
- Exemple

```
group {  
    paramètres spécifiques au groupe...  
    host zappo.test.isc.org {  
        paramètres spécifiques à l'hôte...  
    }  
    host beppo.test.isc.org {  
        paramètres spécifiques à l'hôte...  
    }  
    host harpo.test.isc.org {  
        paramètres spécifiques à l'hôte...  
    }  
}
```

Hôtes

- Permet de spécifier des paramètres spécifiques pour un hôte
 - comme une adresse IP fixe
- au moins une déclaration d'hôte pour chaque client BOOTP
- Exemple

```
host client1 {  
    hardware ethernet DD:GH:DF:E5:F7:D7;  
    fixed-address 192.168.1.20;  
}
```

Client BOOTP

- Exemple de configuration

```
host clientname {  
    filename "/tftpboot.img";  
    server-name "servername";  
    next-server servertftp;  
    hardware ethernet 01:23:45:67:89:AB;  
    fixed-address 192.168.1.90;  
}
```

- nécessite l'installation d'un serveur TFTP sur *servertftp*
- pour une documentation complète de cette configuration sous Debian, voir [ce document](#)

Maintenance

- /var/lib/dhcpd/dhcpd.leases (voir [man dhcpd.leases](#))
 - base de données persistante des baux attribués

Agent relais DHCP

- les trames ARP et BOOTP ne traversent pas les routeurs
 - nécessite donc des serveurs DHCP ou des serveurs relais sur chaque segment
 - transforme les requêtes multicast en de l'unicast
- défini par la [RFC 1542](#)
- agent dhcrelay
 - développé par l'ISC
 - paquet Debian isc-dhcp-relay ou dhcp3-relay
 - inclus dans le paquet dhcp de CentOS

Configuration du relais DHCP

- fichier /etc/default/isc-dhcp-relay

```
# Adresse du serveur DHCP
SERVERS="192.168.1.2"

# Interface utilisée par le relais DHCP
INTERFACES="eth1"

# Options additionnelles pour le démon dhcp-relay
OPTIONS="-q"
```

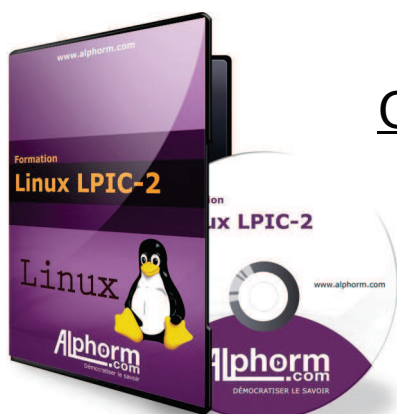
Ce qu'on a couvert

- Configuration du serveur ISC DHCP
 - paramètres
 - mise en place d'un réseau et d'un sous réseau
 - hôtes statiques et hôtes BOOTP
- Maintenance
- Configuration d'un relais DHCP

210.1 DHCP configuration

Weight : 2

Description : Candidates should be able to configure a DHCP server. This objective includes setting default and per client options, adding static hosts and BOOTP hosts. Also included is configuring a DHCP relay agent and maintaining the DHCP server.



Gestion des clients réseau

Authentification PAM

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction
- Configuration des services
- Modules et services
- Types de fonctionnalités
- Contrôle
- Modules
 - pam_unix
 - pam_cracklib
 - pam_cracklib : exemples
 - pam_limits
 - pam_limits : configuration
 - pam_listfile



Introduction

- Pluggable Authentication Modules
 - librairies + API pour l'authentification
 - standard sous GNU/Linux
 - permet de définir la politique d'authentification d'une application indépendamment de celle-ci
 - et de manière centralisée
 - utilisé par un grand nombre de programmes
 - ex : login et su
- Un peu d'histoire
 - /etc/passwd → /etc/shadow
 - /etc/passwd → autres bases de données (ex : ldap)
 - nécessité de réécrire login et chaque logiciel utilisant l'authentification
 - externalisation du processus d'authentification

Configuration des services

- /etc/pam.d/
 - un fichier par service
 - ou pam.conf le cas échéant
 - ajout d'une première colonne "service"

• Syntaxe

```
type control module-path module-arguments
```

- évaluées dans leur ordre d'apparition

• Exemple

```
#%PAM-1.0 : login service
auth required pam_nologin.so
auth required pam_access.so
...
account required pam_stack.so service=system-auth password
required pam_stack.so
...
```

Modules et services

- PAM est (comme son nom l'indique) divisé en modules
 - chacun couvrant une fonction particulière
 - capable d'être liée dynamiquement à une application fournissant un service
- La configuration consiste donc à déterminer quel sera le comportement d'un (ou plusieurs) modules pour un service
 - ex : le service login nécessite l'absence du fichier no_login (module pam_nologin)

```
auth required pam_nologin.so
```

Types de fonctionnalités

- un module offre des fonctionnalités
 - réparties en groupes
 - chaque module pouvant offrir des fonctionnalités dans un ou plusieurs de ces groupes
- 4 groupes indépendants
 - **Account**: vérification des comptes
 - validité du mot de passe, autorisations d'accès, etc ...
 - **Authentication** : vérification de l'identité de l'utilisateur
 - mot de passe, carte à puce, contrôle rétinien, etc ...
 - **Password** : mise à jour des mécanismes d'authentification
 - ex : entrer un nouveau mot de passe
 - fortement lié au groupe Authentication
 - **Session** : tâches à effectuer avant et après un service
 - ex : montage du répertoire personnel de l'utilisateur
- définit le périmètre d'action de chaque fonctionnalité d'un module

Contrôle

- 4 types :
 - **requisite** : termine immédiatement le service en cas d'échec
 - **required** : en cas d'échec, retourne une erreur après que tout les autres modules aient été invoqués
 - **sufficient** : valide le processus d'authentification en cas de succès
 - même si d'autres modules ont auparavant échoués
 - **optional** : n'est pris en compte que si il s'agit de l'unique module associé au service

Modules

- pam_unix
 - authentification via /etc/passwd et /etc/shadow
- pam_cracklib
 - vérification de la sécurité d'un mot de passe
 - dictionnaire et autres paramètres
- pam_limits
 - limite des ressources accessibles via une session
 - à partir de /etc/security/limits.conf puis limits.d/
- pam_listfile
 - autorise ou interdit une action en fonction d'un listfile

pam_unix

Type	Description
account	établir le statut du compte et du mot de passe en se basant sur les éléments shadow (expire, last_change, max_change, min_change, warn_change)
auth	vérification du mot de passe (n'autorise aucun accès en cas de mot de passe vide)
password	mise à jour du mot de passe
session	journalisation des accès

- Documentation (sag) :
http://www.linux-pam.org/Linux-PAM-html/sag-pam_unix.html

pam_cracklib

- Module password uniquement
- Options
 - difok : nombre minimum de caractères permettant de différencier un nouveau mot de passe d'un ancien
 - 5 par défaut
 - minlen : taille minimale du nouveau mot de passe
 - 9 par défaut
 - Crédits : nombre minimal d'occurrence d'un certain type de caractère
 - si N>0 : permet de diminuer la taille minimale requise de maximum N caractères si le type de caractère est utilisé
 - si N< 0 : indique exactement le nombre minimum de caractères du type, sans impacte sur la taille minimale total
 - 1 par défaut
 - dcredit : nombre minimal de chiffres
 - ucredit : nombre minimal de lettres majuscules
 - lcredit : nombre minimal de lettres minuscules
 - ocredit : nombre minimal de caractères spéciaux (autre que majuscule, minuscule ou chiffre)
- Documentation : http://www.linux-pam.org/Linux-PAM-html/sag-pam_cracklib.html

pam_cracklib : exemples

- crédits positifs
 - le mot de passe doit être composé de
 - 14 caractères si il n'est composé que de caractères minuscules
 - 9 caractères si, en plus des lettres minuscules, il est composé d'au moins une majuscule, deux chiffres et deux caractères

```
password required pam_cracklib.so difok=3 minlen=15 dcredit= 2 ocredit=2
password required pam_unix.so use_authok nullok md5
```

- crédits négatifs
 - le mot de passe doit être composé d'au moins un caractère spécial, un chiffre et une lettre majuscule, pour une taille minimale de 8 caractères

```
password required pam_cracklib.so \
    dcredit=-1 ucredit=-1 ocredit=-1 lcredit=0 minlen=8
password required pam_unix.so use_authok nullok md5
```

pam_limits

- fichiers /etc/security/limits.conf et /etc/security/limits.d/*.conf
 - cf LPIC1 - Sujet 110.1 : Tâches d'administration de sécurité
 - affecte tout les utilisateurs, y compris root
- module session uniquement
- Documentation : [sag-pam_limits](#)

pam_limits : configuration

```
<domain> <type> <item> <value>
```

- | | |
|--|---|
| <ul style="list-style-type: none">• domain : entité pour laquelle les limites s'appliquent<ul style="list-style-type: none">▪ nom d'utilisateur▪ nom de groupe (@groupname)▪ tout le monde (*)• type : hard ou soft limit<ul style="list-style-type: none">▪ hard : ne peut être dépassée<ul style="list-style-type: none">• mise en place par l'admin▪ soft : peut être dépassée temporairement▪ - : hard ET soft• value : valeur à appliquer | <ul style="list-style-type: none">• item : quel type d'item est affecté (généralement en Ko)<ul style="list-style-type: none">▪ core : taille des "core files"<ul style="list-style-type: none">• dump de l'état d'un processus en mémoire lors d'un arrêt brutal• pour debugging▪ data : taille des données programme▪ fsize : taille des fichiers créés par l'utilisateur▪ nofile : nombre de fichiers ouverts▪ rss : resident set size maximal<ul style="list-style-type: none">• portion de la mémoire processus stockée en mémoire▪ nproc : nombre de processus concurrents▪ maxlogins : nombre maximum de sessions simultanées▪ priority : process priority▪ cpu : temps cpu d'un seul processus, en minutes |
|--|---|

• Exemple :

```
@limited hard cpu 2
```

pam_listfile

- Options

- `item=[tty|user|rhost|ruser|group|shell]`
 - types d'éléments contenus par le fichier et devant être vérifiés
- `file=/path/filename`
 - fichier liste
- `sense=[allow|deny]`
 - action à réaliser si l'élément est présent dans le fichier
- `onerr=[succeed|fail]`
 - que faire en cas d'erreur
 - ex : ouverture du fichier impossible

- Exemples

- interdire l'accès à une liste d'utilisateurs

```
auth required pam_listfile.so onerr=succeed item=user sense=deny file=/etc/ftpusers
```

- autoriser l'accès à une liste d'utilisateurs

```
auth required pam_listfile.so onerr=fail item=user sense=allow file=/etc/loginusers
```

- Documentation : [sag-pam_listfile](#)

Ce qu'on a couvert

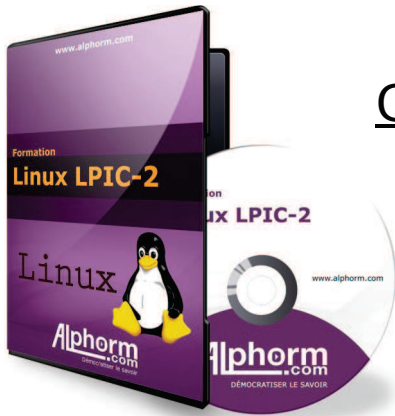
- Fichiers, termes et utilitaires de configuration de PAM
 - `/etc/pam.d` et `pam.conf`
- Modules essentiels de PAM
 - `pam_unix`, `pam_cracklib`, `pam_limits` et `pam_listfile`

210.2 PAM authentication

Weight : 3

Description : The candidate should be able to configure PAM to support authentication using various available methods.





Gestion des clients réseau Clients LDAP

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

Contact : alphorm@noelmace.com

Plan

- Introduction : les annuaires
- Lightweight Directory Access Protocol
- Entrées LDAP
- Attributs
- Filtres LDAP
- Opérateurs
- Clients LDAP sous GNU/Linux
 - installation
- Recherche
- Modification du mot de passe d'un utilisateur
- Ajout et modification d'une entrée
- Suppression d'une entrée



Introduction : les annuaires

- stockage de données hiérarchisées
- destiné au stockage de données pérennes
 - plus rapide en consultation qu'en mise à jour des données qu'une base de donnée "classique"
 - utilisateurs (le plus souvent), matériel, ressources, etc ...
- Les principaux serveurs d'annuaire
 - OpenLDAP (Libre - The OpenLDAP Project)
 - Active Directory (Microsoft)
 - eDirectory (Novell)
 - Open Directory (Apple)
- Tous sont aujourd'hui basés sur (ou compatibles) LDAP

Lightweight Directory Access Protocol

- norme pour les systèmes d'annuaires
 - données
 - nommage
 - modèle fonctionnel
 - sécurité
 - réplication
- créé par Tim Howes (Université du Michigan), Steve Kille (ISODE) et Wengyik Yeong (Performance Systems International) en 1993
 - initialement pour simplifier l'accès (interrogation et modification) aux services d'annuaires X.500 (DAP)
- très nombreuses RFCs (cf [liste](#))

Entrées LDAP

- identifiée par un nom distinct
 - DN, distinguished name
 - Relative Distinguished Name (RDN) suivi du DN de son parent
 - organisation hiérarchique
 - ex : cn=Richard Stallman,ou=people,dc=noelmace,dc=com
- Chaque entrée est constituée d'un ensemble d'attributs
 - nom + type + une ou plusieurs valeurs
 - normaux : définissant l'objet
 - nom, prénom, etc ...
 - opérationnels : réservés au serveur
 - ex : date de modification

Attributs

- Quelques exemples d'attributs courants
 - uid (userid) : identifiant
 - cn (common name) : nom
 - givenname : prénom
 - sn (surname) : surnom
 - o (organization) : entreprise
 - ou (organizational unit) : service
 - mail : adresse mail

Filtres LDAP

- définis par la [RFC 2254](#)
- permettent la récupération (recherche) des entrées LDAP
 - "semblables" à une clause WHERE de requête SQL
- s'écrit sous la forme : attribut OPERATEUR valeur

Opérateurs

Type	Opérateur	Description
Égalité	=	le champs doit avoir la valeur donnée
Présence	*	Joker (tout hormis NULL)
Groupement	()	Permet de séparer / grouper des filtres afin d'employer d'autres opérateurs logiques
Et	&	Tout les filtres doivent être vrais
Ou inclusif		Au moins un filtre doit être vrais
Négation	!	Exclusion de tout les objets correspondant au filtre
Égalité approximative	~=	-
Plus grand ou égal	>=	-
Plus petit ou égal	<=	-

Clients LDAP sous GNU/Linux

- Recherche
 - `ldapsearch`
- Manipulation des entrée
 - `ldappasswd`
 - `ldapadd` & `ldapmodify`
 - `ldapdelete`
- Options communes
 - obsolètes (remplacées par `-H`)
 - `-h` : hôte
 - `-p` : port
 - `-H` : URI du serveur LDAP
 - `-D binddn` : DN de l'utilisateur permettant la connexion au serveur
 - `-w passwd` : mot de passe de l'utilisateur permettant la connexion au serveur

Installation

- Debian

```
# apt-get install ldapscripts
```

- CentOS

```
# apt-get install openldap-clients
```

Recherche

```
$ ldapsearch [options] filtre [attrs...]
```

- récupération des entrées d'un annuaire LDAP à l'aide de filtres
- Options
 - -s {base|one|sub|children} : portée de la recherche
 - respectivement : sur un objet de base, un niveau, la sous-arborescence (par défaut) ou les enfants (LDAPv3)
 - -b : point de départ de la recherche
- Exemple

```
$ ldapsearch -h myhost -p 389 -s base -b "ou=people,dc=example,dc=com" "objectclass=*"
```

Modification du mot de passe d'un utilisateur

```
$ ldappasswd [options] [user]
```

- opération définie par la RFC 3062
 - sur l'attribut userPassword (RFC 2256 section 5.36)
- Options
 - -x : authentification simple (au lieu de SASL)
 - -s newpasswd : nouveau mot de passe
 - -W : demander un nouveau mot de passe de manière interactive (au lieu de -s)
 - sera sinon généré par le serveur

- Exemple

```
$ ldappasswd -x -h localhost -D "cn=root,dc=example,dc=com" \  
-s secretpassword uid=admin,ou=users,ou=horde,dc=example,dc=com
```

Ajout et modification d'une entrée

- Ajout d'une entrée :

```
$ ldapadd [options]
```

- lien vers ldapmodify activant l'option -a

- Modification d'une entrée :

```
$ ldapmodify [options]
```

- Options

- -f : lire les informations de modification à partir du fichier au lieu de l'entrée standard

- Exemple

```
$ ldapadd -c -x -W -D cn=root,dc=example,dc=com -H ldaps://ldap1.example.com/ -f grclient.ldif
```

```
dn: cn=clients,ou=Group,dc=example,dc=com
cn: clients
gidNumber: 10001
memberUid: pierre
memberUid: paul
memberUid: jacque
description: Clients de l'entreprise
objectClass: posixGroup
```

Suppression d'une entrée

```
$ ldapdelete [options] [DN ...]
```

- Exemple :

```
$ ldapdelete -H ldaps://ldap1.example.com -D "cn=root" \
"uid=rmachin,ou=sales,ou=people,dc=example,dc=com"
```

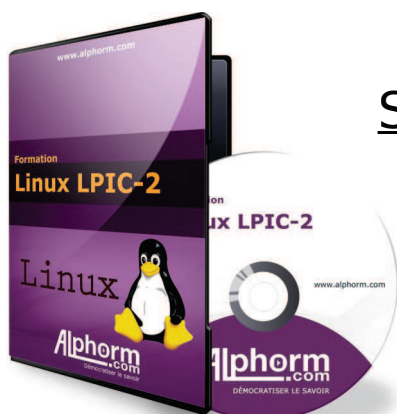
Ce qu'on a couvert

- Introduction au LDAP
 - objectif, contexte et structure
- interrogation et de mise à jour des données d'un serveur LDAP
 - ajout et gestion d'utilisateurs
 - import, ajout et modification des entrées
- Utilitaires
 - Idapsearch, Idapadd, Idapmodify, Idappasswd et Idapdelete)

210.3 LDAP client usage

Weight : 2

Description : Candidates should be able to perform queries and updates to an LDAP server. Also included is importing and adding items, as well as adding and managing users.



Services de courrier électronique

Utilisation des serveurs de messagerie

Site : <http://www.alphorm.com>
Blog : <http://www.alphorm.com/blog>
Forum : <http://www.alphorm.com/forum>

Noël Macé

Formateur et Consultant indépendant
Expert Unix et FOSS

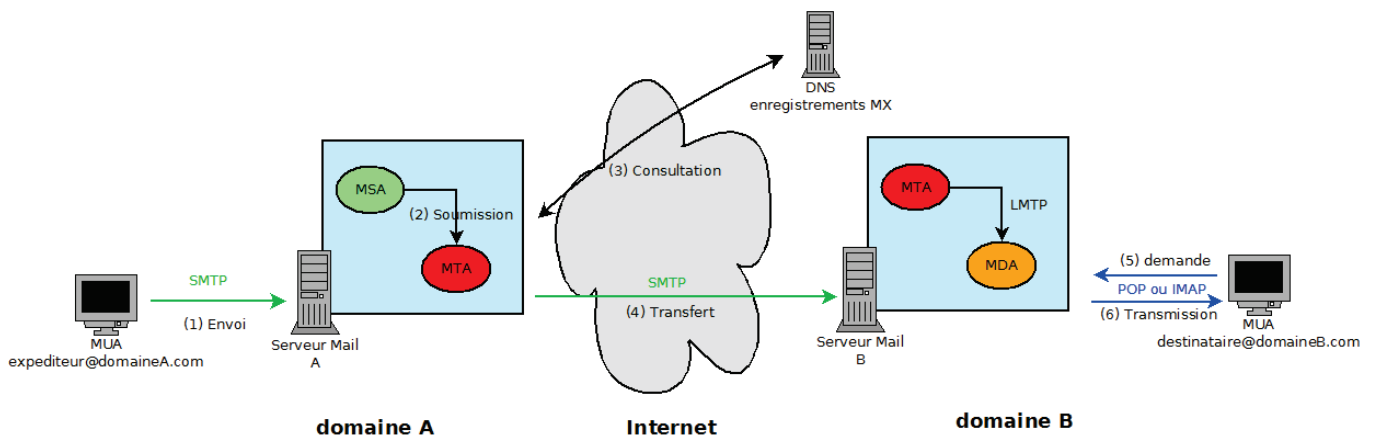
Contact : alphorm@noelmace.com

Plan

- Rappel : Fonctionnement
- Simple Mail Transfer Protocol
- Postfix
 - Configuration de Postfix
 - Paramètres essentiels
 - Journalisation
 - Postfix et les domaines
 - Domaines virtuels
 - Commandes utiles
 - Émulation des commandes sendmail



Rappel : Fonctionnement



Simple Mail Transfer Protocol

- Transfert des mails vers les serveur
 - ports 25, 465 (SSL) et 587 (avec authentification)
- Développé à partir de 1980 en remplacement de FTP Mail et de Mail Protocol (nés en 1973)
 - publié en Novembre 1981 ([RFC 788](#))
 - mis à jour par les [RFC 821](#) (Août 1982) et [5321](#) (Octobre 2008)
 - pour plus de détails, voir [wikipedia\(en\)](#)
- Sendmail (distribué avec BSD 4.1c dès 1981) est alors un des premiers MTA à implémenter ce protocole
 - devient très rapidement le MTA de référence sur Internet

Postfix

- MTA par défaut de Mac OS X, NetBSD et de nombreuses distributions GNU/Linux (comme Ubuntu)
 - un MTA de référence : 25 % de [parts de marché en 2012](#)
 - seconde place derrière Exim (46 %), MTA par défaut de Debian
 - devant Sendmail (11%), le MTA historique, encore par défaut pour CentOS, et Microsoft (10%) depuis 2009
- Libre : IBM Public Licence 1.0 (non compatible GPL)
 - développé dès 1997 par [Wietse Venema](#) (également à l'origine de TCP Wrapper)
 - au [IBM Thomas J. Watson Research Center](#)
 - première distribution en Décembre 1998
 - version actuelle (Juin 2013) : 2.10.1
- Documentation officielle [en français](#) (grâce à Traduc.org) et [en anglais](#)
- Pour une comparaison en détail des différents MTA du marché, voir [ce tableau](#)

Configuration de Postfix

- par défaut dans `/etc/postfix/`
 - `main.cf` : paramètres de configuration de Postfix
 - Syntaxe semblable aux scripts shell (sans les apostrophes)
 - notamment pour les variables (\$)
 - `master.cf` : configuration du démon master
 - définit la manière dont un programme client se connecte à un service, et quel démon s'exécute lorsqu'un service est demandé
- **Doivent** (répertoire et fichiers) appartenir à root sans droit d'écriture pour les autres utilisateurs

Syntaxe des paramètres Postfix

- `main.cf` a une syntaxe semblable aux scripts shells, à quelques différences notables près
 - les variables (paramètres) notamment peuvent sembler proche, mais offrent quelques spécificités
- Déclaration / affectation
 - classique

```
mavariabale = valeur
```

- à partir du contenu d'un fichier

```
mavariabale = /chemin/du/fichier
```

- à partir du contenu d'une table de correspondance
 - paramètres définis dans un fichier séparé à la syntaxe identique

```
mavariabale = type:/chemin/du/fichier
```

- Ce fichier n'étant pas évalué de manière séquentielle, une variable peut être employée avant sa "déclaration"
 - Postfix est "paresseux", et ne consulte la valeur d'un paramètre que lorsqu'il est utilisé

```
mavariabale = $monautrevar
```

Paramètres essentiels

- domaine des courriels sortants

```
myorigin = $myhostname
```

```
myorigin = $mydomain
```

- domaine à partir duquel les courriels sont reçus

```
mydestination = $mydomain, localhost.$mydomain, hash:/etc/postfix/moredomains
```

- défaut (pour les deux) : \$myhostname

- domaines de destination (et leurs sous-domaines) que le système acceptera de relayer

- (défaut : \$mydestination)

```
relay_domains = $mydomain
```

- Indiquer un relais SMTP

- ne sera pris en compte qu'en l'absence de mapping correspondant dans la table optionnelle [transport](#)
- à défaut de valeur, Postfix tentera de transférer le mail au serveur MX du domaine de destination

```
relayhost = mail.myisp.com
```

Journalisation

- via syslog (ou dérivés)
 - cf /etc/syslog.conf ou /etc/rsyslog.conf
 - Exemple :

```
mail.err /dev/console
mail.debug /var/log/maillog
```

- Rapporter les problèmes de permission/appartenance

```
# postfix check
```

- Lister tout les problèmes éventuels

```
# egrep '(reject|warning|error|fatal|panic):' /var/log/maillog
```

Postfix et les domaines

- Postfix offre plusieurs possibilités concernant un domaine
 - destination finale
 - domaines canoniques
 - nom et adresse IP du serveur et parfois le nom du domaine parent
 - classe : domaines locaux
 - domaines hébergés
 - ne sont pas directement associés au nom de la machine
 - classe : domaines virtuels
 - d'alias
 - ou de boîtes au lettres
 - serveur MX de secours d'un (ou plusieurs) domaine(s)
 - conserve les courriels lorsque le serveur MX principal ne fonctionne pas
 - les transfère dès qu'il fonctionne de nouveau
 - classe : domaines relayés
 - relais pour la retransmission des courriels
 - classe : domaines par défaut
- Documentation : voir [Virtual Readme](#) et [Address Class Readme](#)

Domaines virtuels

- spécification des domaines d'alias virtuels
 - par une liste (séparés par des espaces ou des virgules)
- ```
virtual_alias_domains = example.com, autreexemple.com
```
- Table optionnelle faisant correspondre des adresses ou des domaines avec des adresses locales ou distantes
    - via une [table de correspondance](#) "hash" (créé via [postmap](#) ou [postalias](#))

```
virtual_alias_maps = hash:/etc/postfix/virtual
```

- Exemple de fichier

```
postmaster@example.com peter
info@anotherexample.com gerda
sales@example.com petra
@example.com jim
```

## Commandes utiles

---

- Recharger la configuration de Postfix

```
postfix reload
```

- création ou mise à jour d'une table de correspondance "hash"

```
postmap fichier
```

## Émulation des commandes sendmail

---

- Interface de compatibilité de Postfix pour Sendmail

```
$ sendmail [option ...] [recipient ...]
```

- afficher la file d'attente des courriels

```
$ mailq
```

- équivalent à `sendmail -bp`

- initialiser la DB des alias (paramètre `alias_database`)

```
newaliases
```

- équivalent à `sendmail -I`

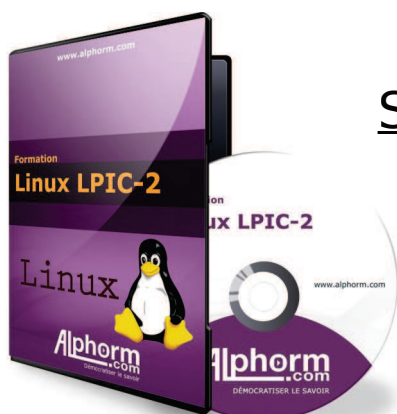
# Ce qu'on a couvert

- Introduction au protocole SMTP et aux MTA
- Configuration de Postfix
  - fichiers de configuration
  - paramètres essentiels
- Gestion de la journalisation des MTA

## 211.1 Using e-mail servers

**Weight :** 3

**Description :** Candidates should be able to manage an e-mail server, including the configuration of e-mail aliases, e-mail quotas and virtual e-mail domains. This objective includes configuring internal e-mail relays and monitoring e-mail servers.



Services de courrier électronique

## Distribution locale des courriels

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

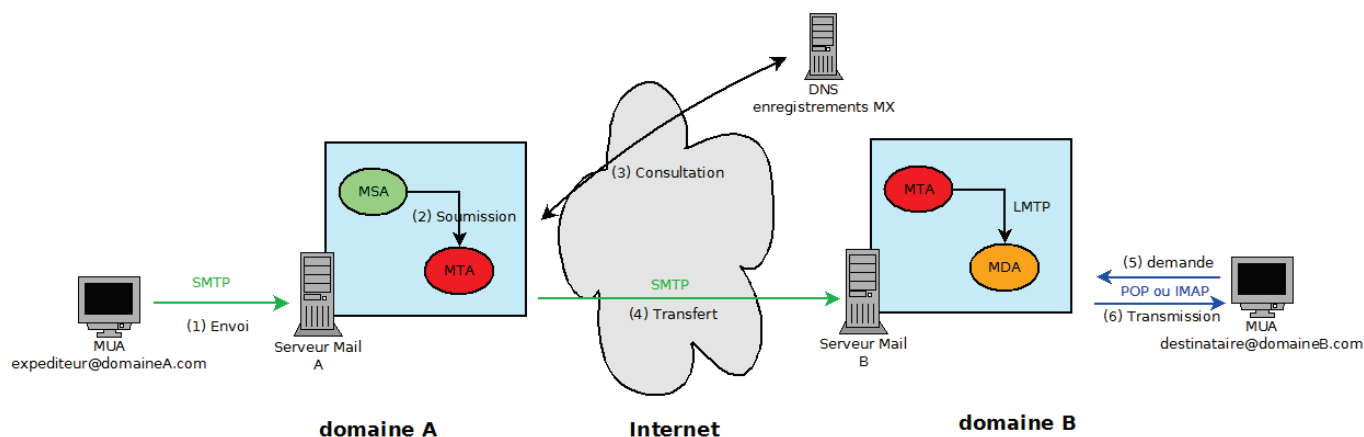
Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

# Plan

- Introduction
- Formats de stockage
  - Mbox
  - Maildir
- Procmail
  - Fonctionnement
  - Configuration
- Recettes procmail
  - En tête d'une recette
    - En tête d'une recette : verrouillage
  - Règles de correspondance
  - Actions
  - Quelques exemples



# Introduction



# Formats de stockage

---

- Définissent la manière de stocker les courriels et les mailbox
  - format des fichiers
  - hiérarchie des éventuels dossiers
  - etc ...
- Nombreux formats
  - Standards : Mbox et Maildir
    - tout deux reconnus par procmail
    - Maildir est cependant recommandé aujourd'hui
  - nmh, MIX, .pst (propriétaire Microsoft), etc ...

## Mbox

---

- apparu avec [Unix V6](#) (AT&T - Mai 1975)
- format ouvert
  - [RFC 4155](#) (Septembre 2005)
- un fichier texte (ASCII 7bits) par mailbox
  - courriels simplement séparés par une ligne vide suivie du mot "From" en début de ligne
- Avantages :
  - universellement supporté
    - nombreuses conversions possibles
      - Outlook .pst via readpst
      - html via Hypermail
  - recherche et écriture au sein d'une mailbox rapides
- Désavantages :
  - problèmes de verrouillage
  - sujet à la corruption

# Maildir

- développé dans le cadre de [QMail](#)
  - MTA léger, modulaire et sécurisé du domaine public
  - par [Daniel J. Bernstein](#) (également à l'origine de [daemontools](#))
  - Décembre 1995

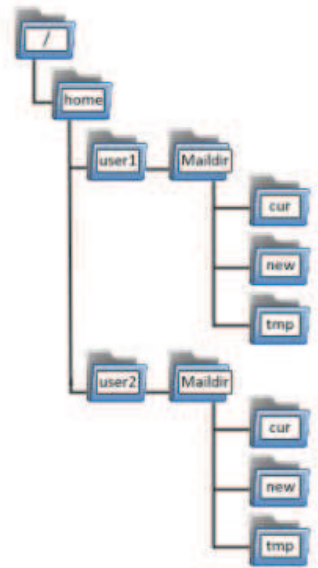
- un dossier par mailbox
  - contenant lui même trois dossiers : new, cur et tmp

- Avantages :

- rapidité de :
  - localisation
  - récupération
  - et suppression des courriels
- peu (voir pas) de verrouillage fichier
- utilisable sur des FS réseaux
- n'est pas sujet à la corruption

- Désavantages :

- nombre de petits fichiers
  - inefficacité de certains FS
- recherche de texte des une ou plusieurs mailbox lente
  - nécessite l'ouverture de tout les fichiers



Structure Maildir  
Wikimedia cc-by-sa

# Procmal

- MDA de référence pour les systèmes Unix
  - Libre (Licence GPL)
- Largement employé
  - en adéquation avec un MTA (Exim, Postfix, Sendmail)
    - et souvent un serveur IMAP / POP tel que Dovecote pour la distribution distante
  - excellentes capacités de filtrage
- première version distribuée en Décembre 1990
  - n'est plus maintenu
    - version finale 3.22 le 10 Septembre 2001
- Documentation : [Procmal Documentation Project](#) et [Procmal Quick Reference Guide](#)

# Fonctionnement

- programme autonome
  - généralement appelé directement par le MTA
    - Rappel : pour Postfix

```
mailbox_command = /usr/bin/procmail
```

- n'est appelé via la ligne de commande que très rarement
  - essentiellement pour des tests
- prétraitement et tri des courriels
  - mailinglists
  - anti-spam
  - réponses automatiques

# Configuration

- /etc/procmailrc
  - prioritaire si présent
  - configuration générale, pour tout les utilisateurs
- \$HOME/.procmailrc
  - pour chaque utilisateur

## • Exemple

```
SHELL=/bin/sh
MAILDIR=$HOME/Mail
LOGFILE=$HOME/Mail/procmail.log

:0:
* ^Subject: test
testing
```

composé de :

- définitions de variables
- recettes

En l'absence de fichier de configuration, procmail écrira tout les courriers dans /var/spool/mail

- pour d'autres exemples, voir dans /usr/share/doc/procmail/exemples/ , [dans la documentation](#) ou à la fin de ce support

# Recettes procmail

---

- décomposées en 3 parties
  - en tête ou "ligne double point" ("colon line")
  - règle(s) de correspondance
    - expression(s) rationnelle(s)
      - sur les en-têtes et corps des messages
    - détermine quels messages seront traités par cette recette
  - action
- à défaut de règle correspondante, les courriers seront livrés dans la mailbox par défaut

## En tête d'une recette

---

• Première ligne de chaque recette

```
:0 [drapeaux] [: [verrou_local]]
```

• le premier double point indique un début de règle

• le 0 est, lui, présent pour des raisons historiques

• Drapeaux : détermine la manière dont la recette sera exécutée

• portée

• des règles de correspondances

• H : en tête du message (par défaut)

• B : corps du message

• HB : les deux

• des actions (ce qui leur est envoyé)

• h : n'envoie que les en-têtes pour traitement

• b : n'envoie que le corps du message pour traitement

• hb : les deux (par défaut)

• contrôle des flux (exemple : c : garde une copie du message pour traitement ultérieur)

• mode d'exécution

• sensibilité à la casse (cf quickref)

## En tête d'une recette : verrouillage

---

```
:0 [drapeaux] [: [verrou_local]]
```

- second double point
  - mettre en place un fichier de verrou
    - afin de ne pas corrompre un fichier en y écrivant simultanément deux courriers
    - nécessaire en cas d'écriture (sauvegarde)
  - [verrou local] : explicite le fichier de verrou à mettre en place

## Règles de correspondance

---

- permettent de déterminer si l'action doit être effectuée sur ce message ou non
- commencent toujours par "\*" (une étoile suivie d'un espace)
- Pour associer les règles de correspondances
  - une par ligne = ET logique
  - sur une même ligne, séparées par des "|" (pipes) = OU logique
    - une seule étoile en début de ligne, non pour chaque expression

# Actions

opération à réaliser en cas de correspondance avec la/les règle(s)

redirection

vers un fichier (mbox) ou un dossier (maildir)

/chemin/du/fichier

chemin/relatif

/chemin/du/dossier/

action la plus courante

permet de délivrer le courrier dans la mailbox indiquée

nécessite un verrou si écrit dans un fichier

si le chemin est relatif (pas de / en début de ligne), il le sera par rapport à \$MAILDIR

vers un programme

| programme

vers une (ou plusieurs) autre(s) adresse(s) électronique

! addr1@site.net addr2@else.com addr3 ...

il est possible de remplacer l'action par une autre ensemble de recettes et de variables en utilisant les caractère { et }

# Quelques exemples

transférer tout courriel de l'expéditeur lui@example.com vers l'adresse moi@noelmace.com

```
:0
* ^From.*lui@example.com
! goodmail@example2.com
```

```
:0
* > 1048576
grosfichiers
```

transférer tout courriel provenant du domaine fsf.org et contenant le mot "Supporter" suivi du mot "Issue" (correspondant au Free Software Supporter, newsletter mensuelle de la FSF) vers la boîte mail de l'utilisateur news, et le copier vers notre dossier forwarded.news

```
:0c
* ^From.*@fsf\ .prg
* ^Subject:.*Supporter.*Issue.*
! news

:0:
forwarded.news
```

# Ce qu'on a couvert

- Configuration de procmail
  - recettes, drapeaux, règles et actions
- Les formats de stockage
  - mbox
  - maildir

## 211.2 Managing Local E-Mail Delivery

**Weight** : 2

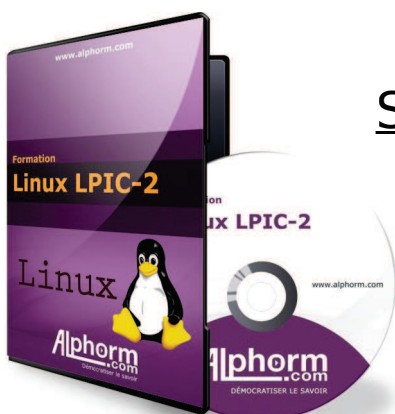
**Description** : Candidates should be able to implement client e-mail management software to filter, sort and monitor incoming user e-mail.



Linux LPIC-2

tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

# Alphorm.com



Services de courrier électronique

## Distribution distante des courriels

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

Linux LPIC-2

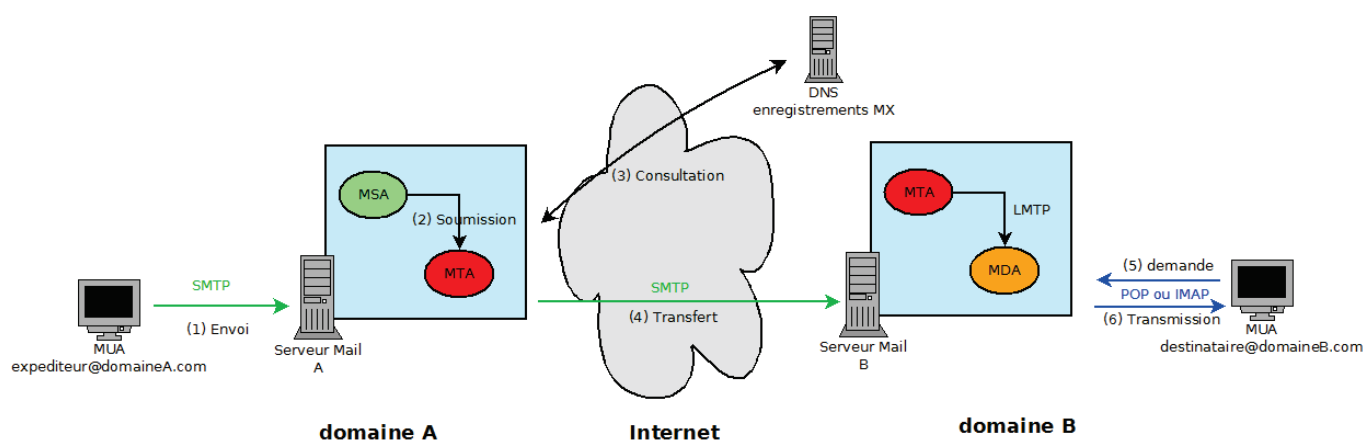
tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site **alphorm.com**

# Plan

- Introduction
- Courier Mail Server
  - Configuration
  - Pré-requis Postfix et Procmail
  - Configuration avec Postfix et Procmail
- Dovecot
  - Authentification
    - Authentification : Configuration
  - Emplacement des mailboxes



# Introduction



# Courier Mail Server

---

- serveur mail / groupware tout en un
  - ESMTP, IMAP, POP3, LDAP, SSL et HTTP
  - webmail (avec calendrier et planning)
  - services mailing list
- constitué de composants individuels
  - activables et désactivables à volonté
  - cf paquets Debian (courier-base, courier-imap, courier-ldap, courier-webadmin, etc ...)
  - nous nous concentrerons ici sur ce dont nous avons besoin : des serveurs POP3 et IMAP pour compléter Postfix et Procmail
    - courier-imap et courier-pop
- stockage natif en maildir
  - possibilité de livraison sous d'autres formats pré-établis
- file d'attente des mails dans /var/spool/mqueue

## Configuration

---

- Deux possibilités (à choisir à l'installation)
  - par dossiers (nécessaire pour webadmin)
  - ou par fichier (à favoriser si administration pour la console)
    - ce que nous présenterons ici dans le cadre de la LPIC2
- /etc/courier/
  - imapd : configuration de courier-imap
  - pop3d : configuration de courier-pop
  - authdaemonrc : configuration de courier-authdaemon (démon d'authentification de courier)

## Pré-requis Postfix et Procmail

- Postfix : fichier main.cf

```
mailbox_command = procmail -a "$EXTENSION"
```

- Procmail : ajouter un fichier \$HOME/.procmailrc ou /etc/procmailrc

```
MAILDIR=$HOME/Maildir/
DEFAULT=$MAILDIR/
```

- créer le(s) dossier(s) \$HOME/Maildir/

```
$ maildirmake ~/Maildir
```

- attention aux droits posix : l'utilisateur doit avoir l'accès à ce dossier en lecture et écriture

- vérifiez également les alias (/etc/aliases)

## Configuration avec Postfix et Procmail

- courier-imap : dans le fichier /etc/courier/imapd

```
MAILDIRPATH=Maildir
```

- courier-authdaemon

```
authmodulelist="authpam"
```

- redémarrer les services

```
/etc/init.d/postfix restart
/etc/init.d/courier-imap restart && /etc/init.d/courier-authdaemon restart
```

- vous pouvez dès à présent vous connecter via votre MUA préféré (Evolution par exemple) en IMAP via un compte de votre système (login : votre identifiant – mdp : idem que sur le système, grâce à PAM)

# Dovecot

---

- Serveur POP3 et IMAP4r1 orienté sécurité
  - libre (Double licence MIT et GPLv2)
  - destiné aux systèmes Unix (Solaris, GNU/Linux, (Free|Open|Net)BSD et Mac OS X)
- Compatible mbox et Maildir
- Inclus son propre MDA (Dovecot Local Delivery Agent)
- Dernière version : 2.2.5 (5 Aout 2013)
  - attention : nombreuses différences de configuration avec Dovecot1, encore par défaut sous Debian
- Documentation officielle [ici](#)
- Configuration : /etc/dovecot.conf ou /etc/dovecot/dovecot.conf

# Authentification

---

- Dovecot peu stocker les comptes utilisateurs de nombreuses manières
  - PAM, BDSAuth, LDAP, passwd
  - bases de données SQL : MySQL, PostgreSQL et SQLite
- 4 parties
  - le mécanisme d'authentification
    - définit le protocole utilisé pour la communication des informations d'authentification
    - PLAIN (en clair, à utiliser via SSL/TLS) ou non (CRAM-MD5, NTLM, etc ...)
  - le mécanisme de chiffrement des mots de passe
    - en clair (PLAIN) ou via une fonction de hachage (par exemple via MD5-CRYPT)
    - la plupart du temps, imposé par la base des mots de passe
    - PAM ne laissant même pas voir les mots de passe à Dovecot, la question ne se pose pas dans ce cas
  - la base des utilisateurs
    - Passwd, Passwd-file, LDAP, SQL, etc ...
  - la base des mots de passe
    - PAM, IMAP, Passwd, Passwd-file, SQL,

# Authentication : Configuration

---

• Dovecot v1 :

```
auth default {
 mechanisms = plain cram-md5
 passdb pam {
 }
 userdb passwd {
 }
}
```

• Dovecot v2

```
auth_mechanisms = plain cram-md5
passdb {
 driver = pam
}
userdb {
 driver = passwd
}
```

# Emplacement des mailboxes

---

- paramètre mail\_location
  - format Maildir

```
mail_location = maildir:~/Maildir
```

- format mbox

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

- identique v1 et v2

# Ce qu'on a couvert

---

- Configuration des serveurs IMAP et POP
  - courier
  - Dovecot

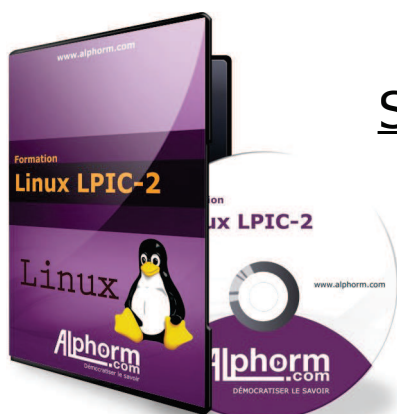
## 211.3 Managing Remote E-Mail Delivery

**Weight** : 2

**Description** : Candidates should be able to install and configure POP and IMAP daemons.



# Alphorm.com



Sécurité du système

# Configuration d'un routeur

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

# Plan

---

- Netfilter
- Vocabulaire
- Tables
- Cibles
- Options essentielles de iptables
- Règles simples
  - Exemples de règles simples
- Extensions de correspondance
  - Options des extensions de correspondance
- Extensions de cibles
  - traduction d'adresse réseau



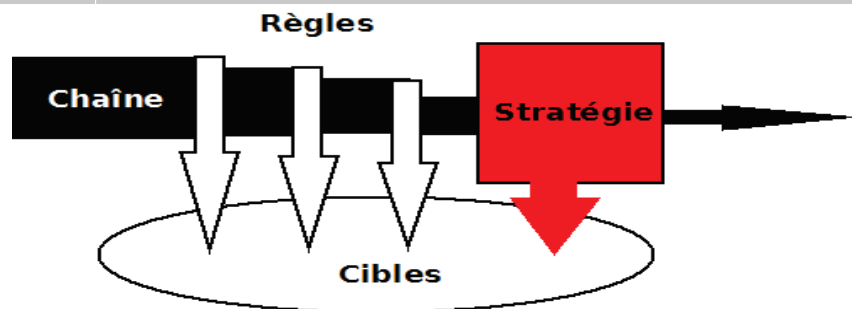
# Netfilter

---

- Framework
  - Pare-feu Linux
  - Projet lancé en 1998
  - Intégré à Linux 2.3 en mars 2000
    - en remplacement de ipchains (lui aussi développé par Rusty Russell)
- Manipulable par divers programmes en espace utilisateur
  - Le plus courant étant iptables, développé par l'équipe Netfilter
    - Mais il en existe d'autres, comme ufw ou gufw

## Vocabulaire

| Élément            | Définition                                        |
|--------------------|---------------------------------------------------|
| Chaîne             | Trafic réseaux                                    |
| Table              | Regroupement de chaînes par catégorie             |
| Règle              | Instructions appliquées à un trafic               |
| Cible              | Action effectuée en cas de validation d'une règle |
| Stratégie (Policy) | Cible par défaut d'une chaîne                     |



## Tables

| table  | usage                                      | chaînes     |
|--------|--------------------------------------------|-------------|
| FILTER | Filtrage classique                         | INPUT       |
|        |                                            | OUTPUT      |
|        |                                            | FORWARD     |
| NAT    | Translation d'ip                           | PREROUTING  |
|        |                                            | POSTROUTING |
|        |                                            | OUTPUT      |
| MANGLE | Modification de paquets                    | PREROUTING  |
|        |                                            | OUTPUT      |
| RAW    | Marquage (nécessite le module iptable_raw) | PREROUTING  |
|        |                                            | OUTPUT      |

# Cibles

| cible  | Effet                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------|
| ACCEPT | autorisation                                                                                                    |
| DROP   | destruction                                                                                                     |
| QUEUE  | transmission en espace utilisateur                                                                              |
| RETURN | cesser de parcourir la chaîne et retourner dans la chaîne précédente (appelante) en passant à la règle suivante |

## Options essentielles de iptables

- Création d'une règle

```
iptables [-t table] -A chaîne règle -j cible [options]
```

- Suppression d'une règle

```
iptables [-t table] -D chaîne {règle|règlenum} [options]
```

- Définition de la règle par défaut (stratégie) d'une chaîne

```
iptables [-t table] -P chaîne cible [options]
```

- Lister toutes les règles d'une chaîne

```
iptables [-t table] -L chaîne [options]
```

- Vider une chaîne (supprime toutes les règles d'une chaîne)

```
iptables [-t table] -F chaîne [options]
```

## Règles simples

---

- pour une interface
  - -i *interface* : d'entrée
  - -o *interface* : pour une interface de sortie
- pour une adresse ip
  - -s *adresse* : source
  - -d *adresse* : destination

## Exemples de règles simples

---

- Refuser tout les paquets entrant via l'interface eth1

```
iptables -A INPUT -i eth1 -j DROP
```

- Accepter tout les paquets sortant via l'interface eth1

```
iptables -A OUTPUT -o eth1 -j ACCEPT
```

- Refuser tout les paquets en entrée provenant de 192.168.1.10

```
iptables -A INPUT -s 192.168.1.10/24 -j DROP
```

- Autoriser tout les paquets en sortie à destination de 192.168.1.1

```
iptables -A OUTPUT -d 192.168.1.1/24 -j ACCEPT
```

# Extensions de correspondance

---

- modules additionnels de correspondance de paquets
  - Peuvent être chargés de deux manières
    - Implicitement
      - Option `-p protocole` ou `-protocol protocole`
        - udp, tcp, icmp ou all
    - Explicitement
      - Option `-m module` ou `-match module`
- Permettent d'utiliser des options supplémentaires, en fonction du module
- Remarque : pour visualiser l'aide relative à un module, indiquez l'option correspondante suivie de `-h`

## Options des extensions de correspondance

---

- |                                                                                                                                                                     |                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • tcp et udp <ul style="list-style-type: none"><li>▪ <code>--source-port [!] port[:port]</code></li><li>▪ <code>--destination-port [!] port[:port]</code></li></ul> | • icmp <ul style="list-style-type: none"><li>▪ <code>--icmp-type [!] nom_du_type_icmp</code><ul style="list-style-type: none"><li>• numérique ou par nom (cf <code>-h</code>)</li></ul></li></ul> |
| • tcp <ul style="list-style-type: none"><li>▪ <code>--tcp-flags [!] masque comp</code></li><li>▪ <code>[!] --syn</code></li></ul>                                   | • state <ul style="list-style-type: none"><li>▪ <code>--state {NEW ESTABLISHED RELATED INVALID}</code></li></ul>                                                                                  |

# Extensions de cibles

---

- modules de cible additionnels
  - permettre de nouvelles actions sur les paquets
- LOG : journalisation du paquet
- REJECT : supprimer le paquet et répondre par un paquet d'erreur
  - sorte de DROP verbeux
- traduction d'adresse réseau (NAT : Network address translation)
  - DNAT
  - SNAT
  - MASQUERADE
- Et bien d'autres (cf [man iptables](#))

## traduction d'adresse réseau

---

- Uniquement disponibles dans la table nat
- modification de l'adresse de destination

```
iptables -t nat -A {PREROUTING|OUTPUT} règle \
-j DNAT --to-destination adresse-ip[-adresse-ip][:port-port]
```

- modification de l'adresse source
  - personnalisable

```
iptables -t nat -A POSTROUTING règle \
-j SNAT --to-source adresse-ip[-adresse-ip][:port-port]
```

- masquerading : une seule ip (celle du routeur)

```
iptables -t nat -A POSTROUTING règle -j MASQUERADE
```

# Ce qu'on a couvert

- Configuration du pare-feu Netfilter sous GNU/Linux
  - filtrage
  - NAT et IP masquerading
  - logging

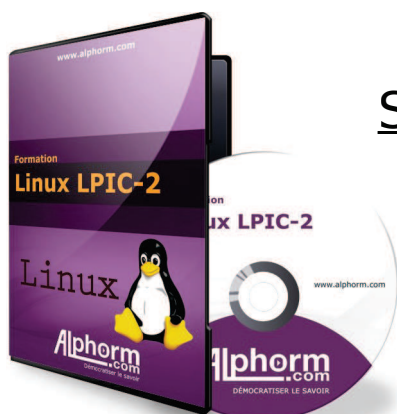
## 212.1 Configuring a router

**Weight** : 3

**Description** : Candidates should be able to configure a system to perform network address translation (NAT, IP masquerading) and state its significance in protecting a network. This objective includes configuring port redirection, managing filter rules and averting attacks.



# Alphorm.com



Sécurité du système

## Sécurisation des serveurs FTP

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

# Plan

---

- Introduction
- Serveurs FTP
- Connexions FTP actives et passives
- Vsftpd
- Pure-ftpd



# Introduction

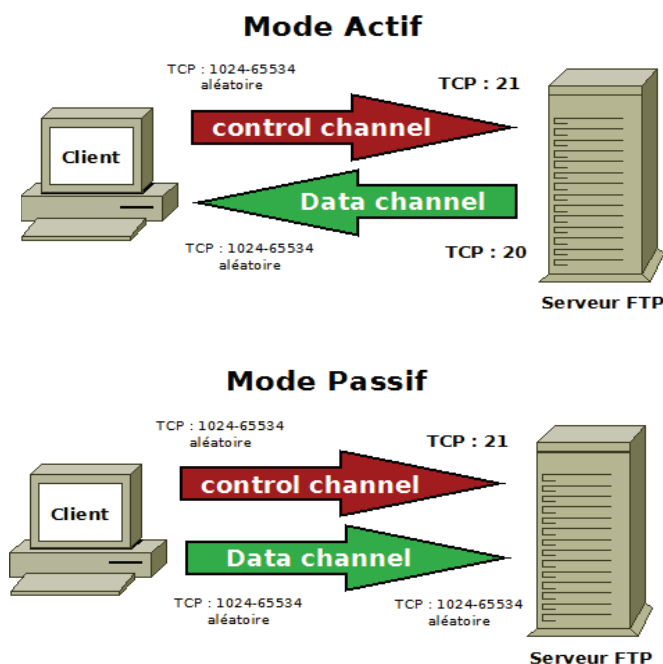
---

- File Transfer Protocol
  - protocole de transfert de fichier de référence
  - relativement ancien
    - RFC 114 - 16 avril 1971
  - remplacée par la RFC 765 (juin 1980) puis 959 (Octobre 1985 - version finale)
    - complétée par
      - la RFC 2228 (Juin 1997) : extensions de sécurité
      - la RFC 2428 (Septembre 1998) : ipv6 et nouveau type de mode passif (commande EPSV)
- Faiblement sécurisé
  - remplacé par du FTP over SSL (FTPS) ou du SFTP (SSH)

# Serveurs FTP

- pure-ftp
  - un serveur libre (licence BSD) de référence
  - fortement orienté sécurité
  - né en 2001 à partir de Troll-FTPd
  - disponible sur la quasi intégralité des systèmes Unix
    - même **Android**
  - version actuelle : 1.0.36 - 21 Mars 2012
- vsftpd : Very Secure FTP Daemon
  - également fortement orienté sécurité et libre (licence GPL)
  - serveur FTP par défaut sur de nombreuses distributions (Ubuntu, CentOS, Slackware ...)
  - version actuelle : 3.0.2 - Septembre 2012)
- proftpd
  - libre (GPL), puissant, sécurisé et fortement documenté
  - configuration similaire à Apache
    - fichier proftpd.conf
  - version actuelle : 1.3.4d - 14 Juin 2013

## Connexions FTP actives et passives



- Control channel (connexion de contrôle)
  - mode texte : commande / réponse
- Data channel (connexion de donnée)
  - transmission de données (contenu ou liste de fichiers)
  - généralement établie pour le transfert de données relatives à une seule commande
    - Mode actif : est établie par le serveur
    - Mode passif (commande PASV)
      - met le serveur en attente de connexion sur le port aléatoire qu'il aura envoyé en réponse

## Vsftpd

- Configuration
  - fichier /etc/vsftpd.conf (cf [man](#))
  - syntaxe : clé=valeur
  - Exemple

```
listen=NO : via inetd
listen=YES
write_enable=YES
anonymous_enabled=YES
anon_root=/var/ftp/pub
anon_upload_enable=YES # nécessite write_enable=YES
restreindre l'utilisateur anonyme à la lecture sur les fichiers
accessibles à tout le monde uniquement
anon_world_readable_only=NO
...
```

## Pure-ftpd

- N'est pas directement configuré par des fichiers
  - mais par des options (de la commande pure-ftpd)
- Cependant un [wrapper](#) permet de récupérer ces options à partir
  - d'un fichier /etc/pure-ftpd/pure-ftpd.conf sous CentOS

| Paramètre     | valeur |
|---------------|--------|
| # commentaire |        |

- ou d'un dossier /etc/pure-ftpd/conf sous Debian
  - un fichier par option
    - le nom de ce fichier correspondant à l'option dans son format long
    - et son contenu à la valeur à donner
  - Exemple

```
$ cat /etc/pure-ftpd/conf/NoAnonymous
yes
```

- correspond à l'option -E ou --noanonymous

# Ce qu'on a couvert

- Configuration des serveurs FTP
  - vsftpd
  - pure-ftpd
- Sensibilisation à ProFTPD
- Compréhension des différences entre les connexions FTP passives et les connexions actives.

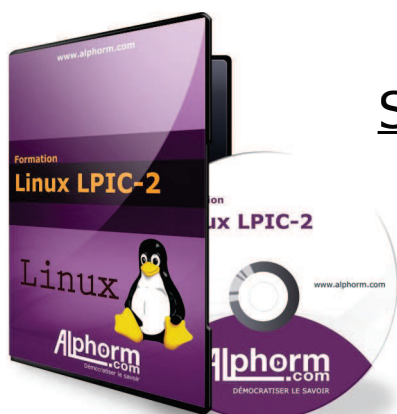
## 212.2 Managing FTP servers

**Weight** : 2

**Description** : Candidates should be able to configure an FTP server for anonymous downloads and uploads. This objective includes precautions to be taken if anonymous uploads are permitted and configuring user access.



# Alphorm.com



Sécurité du système

## Shell sécurisé (SSH)

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

# Plan

---

- Rappels
- Rappel : Configuration
- Restrictions des connexions root
- Restriction des connexions



# Rappels

---

- Ce qui a déjà été vu dans la LPIC1 :
  - fonctionnement et principes du SSH
  - client SSH : connexion
  - copie de fichier avec scp
  - configuration basique du serveur
  - gestion des clés coté serveur et coté client
    - ssh-agent
  - redirection de port (aka TCP Forwarding / tunneling)
- Nous allons donc ici nous concentrer sur les questions de sécurité, particulièrement sur les restrictions d'accès

## Rappel : Configuration

- fichier `/etc/ssh/sshd-config`

```
Port 22
Protocol 2,1
ListenAddress 0.0.0.0
KeepAlive Yes
HostKey ssh_host_dsa.key
HostKey ssh_host_rsa.key
PermitRootLogin no
PasswordAuthentication yes
PubkeyAuthentication yes
PermitEmptyPasswords no
X11Forwarding yes
```

## Restrictions des connexions root

```
PermitRootLogin {yes|no|without-password|forced-commands-only}
```

- `yes` : autoriser (par défaut)
- `no` : interdire (recommandé)
- `without-password` : désactiver l'authentification par mot de passe
  - donc restreindre aux authentifications par clé
- `forced-commands-only` : n'autoriser les connexions que via le(s) couple(s) de clés pour lesquels l'option « `command` » est définie
  - définie dans le fichier `/root/.ssh/authorized_keys` du serveur
  - permet de lancer cette commande automatiquement lors d'une connexion via la clé associée, et empêcher ainsi l'usage de toute autre commande
  - Exemple (voir à ce propos l'excellent article de [admin-linux.fr](http://admin-linux.fr))

```
command="ls" ssh-dss
ACABB3N2aC1ld2...XC2/D47x2= root@SERVEUR1
```

## Restriction des connexions

- Autoriser / interdire authentication par

- clé publique

```
PubkeyAuthentication {yes|no}
```

- mot de passe

```
PaswordAuthentication {yes|no}
```

- Restreindre l'accès à une liste d'utilisateurs / groupes

```
{Allow|Deny}Users user1,user2
```

```
{Allow|Deny)Groups group1,group2
```

- il est possible d'utiliser les caractères ' ? ' et ' \* ' comme joker pour ces paramètres

- Limiter les versions de protocole SSH disponibles

```
Protocol {2,1|1|2}
```

## Ce qu'on a couvert

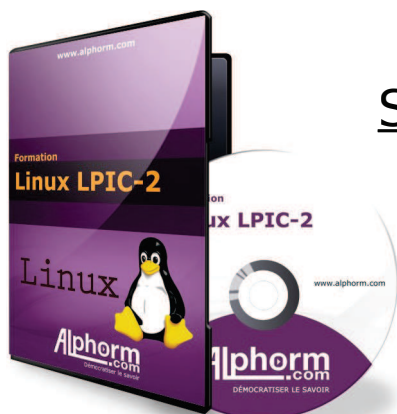
- Bref rappel des éléments relatifs à la LPIC1
- Configuration du serveur OpenSSH
  - restriction d'accès

### 212.3 Secure shell (SSH)

**Weight** : 4

**Description** : Candidates should be able to configure and secure an SSH daemon. This objective includes managing keys and configuring SSH for users. Candidates should also be able to forward an application protocol over SSH and manage the SSH login.





## Sécurité du système

# Tâches de sécurité

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

Linux LPIC-2 tout droits réservés **noelmace.com**© autorisation d'exploitation exceptionnellement délivrée pour le site [alphorm.com](http://www.alphorm.com)

## Plan

- Rappels
- Introduction
- Se tenir au courant
  - Bugtraq
  - CERT
  - CIAC
  - Autres ressources
- fail2ban
  - Configuration de fail2ban
- Le scanner de vulnérabilité OpenVAS
- Détection d'intrusion avec Snort



# Rappels

---

- Ce que nous avons déjà vu
  - surveillance et analyse du trafic réseau (LPIC2 - chapitre 5.2)
    - netcat, nmap
  - gestion du pare-feu Linux (LPIC2 - chapitre 12.1)
    - utilisable à des fins de détection d'intrusion (cible LOG)
- Nous allons donc ici approfondir ces sujets en mettant l'accent sur l'audit et la détection de problèmes de sécurité afin de pouvoir y répondre rapidement

# Introduction

---

- La sécurité n'est pas une affaire de feignant
  - de par son principe même, tout y change en permanence
    - vulnérabilité → annonce → résolution, le tout dans un délais très court
  - il est donc très important de se tenir en permanence à jour
    - audit, suivit de l'actualité, etc ...
- Dans la pratique, elle est également une affaire de chaque instant
  - criticité des systèmes
  - surveillance permanente
    - pour un temps de réactivité minimal

## Se tenir au courant

---

- un volume gigantesque de vulnérabilités sont découvertes chaque jour
  - de nombreuses solutions permettent de les surveiller
  - mailing lists, sites spécialisés, magazines, etc ...
- Seule la connaissance d'une vulnérabilité permet de s'en protéger
  - faire entièrement confiance aux mises à jour et à vos protections généralistes ne peu suffire dans un environnement critique

## Bugtraq

---

- mailing list ouverte à tous
  - crée le 5 Novembre 1993 (modéré depuis le 5 Juin 1995)
- fondée sur le principe de Full Disclosure
  - divulgation publique totale de toute vulnérabilité
  - opposé à la sécurité par l'obscurité
- traite de quasiment toutes (dans les 150/jours) les dernières vulnérabilités
  - annonce, description, méthodes d'exploitation, solutions, etc ...
- site officiel : <https://www.securityfocus.com> - FAQ
  - pour souscrire, envoyer un mail à [bugtraq-subscribe@securityfocus.com](mailto:bugtraq-subscribe@securityfocus.com)

- Les CERT (Computer Emergency Response Team)
  - Organismes officiels
  - Centres d'alerte et de réaction aux attaques informatiques
    - prévention des risques et assistance aux traitements d'incidents
    - généralement ouverts à tous
  - Quelques exemple :
    - [US-CERT](#) (United States Department of Homeland Security)
    - [CERT-RENATER](#) (France - Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche)
- CERT Coordination Center (ou CERT/CC)
  - premier CERT
  - aujourd'hui le centre principal de coordination des CERT
  - fondé par le DARPA en novembre 1988
    - suite à la frappe du « premier » ver, Moris (ou Rogue)
  - site officiel : <https://www.cert.org/> - mailing lists et flux d'actualité

## CIAC (ancienne version)

---

- [Computer Incident Advisory Capability](#)
  - fondé par le département de l'énergie des États-Unis d'Amérique
  - en Février 1989
- Nombreuses mailing lists
  - CIAC-BULLETIN : Avis et informations de haute priorité
  - CIAC-NOTES : collection d'articles sur la sécurité informatique
  - SPI-ANNOUNCE : actualité de Security Profile Inspector (SPI)
    - mises à jour, nouvelles fonctionnalités, etc ...
  - SPI-NOTES : discussions sur l'utilisation de SPI et les problèmes rencontrés
- Pour souscrire, envoyer un mail avec pour contenu un message comme suit à [ciac-listproc@llnl.gov](mailto:ciac-listproc@llnl.gov)
  - `subscribe list-name LastName, FirstName, PhoneNumber`
- *cf modifications, ces mailing lists ne semblent plus exister*

- [Computer Incident Advisory Capability](#)
  - fondé par le département de l'énergie des États-Unis d'Amérique
  - en Février 1989
- Membre fondateur
  - du [GFIRST](#)
    - Government Forum of Incident Responders and Security Teams
    - communautés de plus de 50 équipes de divers agences fédérales des USA
    - hébergée par le US-CERT
  - et du [FIRST](#) (Forum of Incident Response and Security Teams)
- Anciennement chargé d'informer largement sur les incidents informatiques
  - vulnérabilités, virus et hoarx pour l'essentiel
- Renommé DOE-CIRC / JC3 (Joint Cybersecurity Coordination Center) en Octobre 2008
  - pour se tenir au courant, voir ses [communiqués](#)
  - travail aujourd'hui essentiellement avec l'US-CERT

## Autres ressources

---

- [MISC](#) : « le magazine consacré 100% à la sécurité informatique »
  - mensuel français de Unix Garden, des Editions DIAMOND
    - également éditeur de l'excellent [Gnu/Linux Magazine France](#)
  - actualité, perspectives techniques, questions juridiques, etc ...
- Informations de sécurité Debian
  - mailing list : [debian-security-annonce](#)
- Voir aussi les ressources Red Hat
  - notifications : <https://access.redhat.com/security/updates/advisory/>
  - mises à jour : <https://access.redhat.com/security/updates/>
  - dans un autre registre, le [guide de sécurité Red Hat](#)

# fail2ban

---

- Solution de protection active
  - parcourt les journaux systèmes
    - à la recherche d'activités indiquant une attaque de type DOS ou bruteforce
  - banni automatiquement l'adresse IP source de ces attaques
    - en établissant une règle iptables
    - de manière temporaire
- Ne permet pas de prévenir les attaques DDOS
  - Aucun véritable support de l'ipv6 à ce jour (patch expérimental)



## Configuration de fail2ban

---

- fichier /etc/fail2ban/jail.conf
  - un bloc par service à surveiller

```
bloc du service ssh
[ssh]
activer le service
enabled = true
ports à surveiller
port = ssh,sftp
filtre de détection pour les logs
filter = sshd
fichier de log à surveiller
logpath = /var/log/auth.log
nombre maximum d'essais autorisés avant bannissement
maxretry = 6
bannir durant 15 minutes
bantime = 900
```

## Le scanner de vulnérabilité OpenVAS

- Open Vulnerability Assessment System
  - fork libre (GPL) de Nessus (propriétaire)
- Analyse un équipement, un ensemble d'équipements, voir même un réseau entier
  - afin d'y détecter les vulnérabilités éventuelles
- Affiche une synthèse indiquant
  - une liste des vulnérabilités détectées, par niveau de criticité
  - une description de celles-ci
  - ainsi qu'une méthode (ou un lien) permettant d'y remédier
- Pour plus de détails, voir notamment [ce document](#)



## Détection d'intrusion avec Snort



- système de détection d'intrusion pour le réseau (NIDS)
  - référence en la matière
  - Libre (GPL)
- Maintenu par Sourcefire
  - propose un programme de [certifications professionnelles](#) dédié
- Configurable via des règles
  - à la manière de iptables
  - nombreuses sont celles partagées librement par les utilisateurs sur le net (cf [Emerging Threats](#))
- Peut être amélioré par / associé à
  - un IPS (système de prévention d'intrusion)
    - Snort Inline, Guardian, SnortSam, etc...
  - un logiciel de monitoring
  - acidbase, Prelude-IDS, etc ... ajouter un texte
- voir la [documentation officielle](#)

# Ce qu'on a couvert

- Sites et organisations informant des alertes de sécurité
  - Bugtraq, CERT, CIAC et d'autres sources
- Détection et protection contre les intrusions et attaques
  - Snort
  - OpenVAS
  - fail2ban

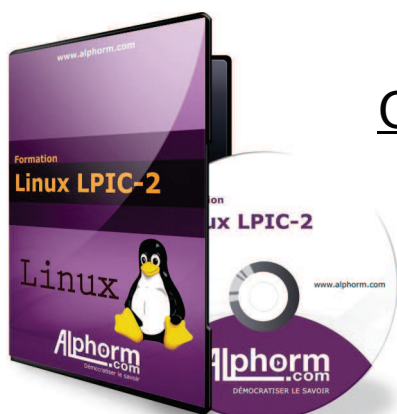
## 212.5 Security tasks

**Weight :** 3

**Description :** Candidates should be able to receive security alerts from various sources, install, configure and run intrusion detection systems and apply security patches and bugfixes.



# Alphorm.com



## Conclusion

# Conclusion

Site : <http://www.alphorm.com>  
Blog : <http://www.alphorm.com/blog>  
Forum : <http://www.alphorm.com/forum>

**Noël Macé**

Formateur et Consultant indépendant  
Expert Unix et FOSS

Contact : [alphorm@noelmace.com](mailto:alphorm@noelmace.com)

# Plan

---

- A propos de la nouvelle version
- Changements opérés
- Les principales modifications
- Chapitre 213 en détail
- Sujets abordés dans le chapitre 213
- S'entraîner au dépannage
- Et pour conclure



## A propos de la nouvelle version

---

- Comme évoqué plus tôt :
  - Nouvelle version 4.0
    - Déjà publiée (voir [ici](#))
    - Prendra effet le 1er Novembre 2013
- Permet une approche plus logique de l'ensemble de l'apprentissage
  - Plus en adéquation avec les problématiques actuelles
  - La dernière version (3.5) datant du 1er Août 2012

# Changements opérés

---

- . Nombreux changements
  - Répertoriés sur [cette page](#)
  - Tout en tâchant de conserver au maximum la numérotation existante
- . Répercussions sur tout les examens (LPIC1 et 3 compris)
  - Éviter la répétition
- . Logiciels et fonctionnalités dépassées
  - Sendmail (en faveur de Postfix)
  - Plus grande importance du kernel et de udev
  - Etc ...
- . En grande parti anticipé dans ce cours

# Les principales modifications

---

- Pour plus de cohérence, quelques chapitres ont donc été revus dans ce cours afin d'anticiper ces changements
  - . chapitre 205.4 : Information des utilisateurs
    - déplacé dans le chapitre 6 : Maintenance système
    - plus cohérent, meilleure répartition entre chapitres en temps et poids
  - . chapitre 212.4 : TCP Wrapper
    - déplacé dans la LPIC1
      - . objectif 110.2
      - . chapitre 14.1 de notre cours : sécurité réseau
    - remplacé, dans la v4, par l'objectif 212.5 (OpenVPN)
      - . abordé au chapitre 5.1 de ce cours
  - chapitre 213 : « supprimé »
    - car la résolution de panne est un sujet transverse
      - . ce qui amenait à de nombreuses répétitions
        - Avec d'autres sujets de la LPIC2
        - Avec la LPIC1
    - nous avons donc abordé ces sujets tout au long de notre cours

# Chapitre 213 en détail

---

- 213.1 : Identification des étapes de démarrage et dépannage des chargeurs d'amorçage
  - Fusionné avec le Sujet 202.2 Récupération du système
  - Suppression des mentions concernant init.d
  - Déjà vu dans
    - Le chapitre 7 de LPIC1 - Linux+
    - La chapitre 2 de ce cours (particulièrement dans la vidéo 3)
- 213.2 : Dépannage général
  - Fusionné avec le chapitre 201.5 Gestion et requêtes sur un noyau et les modules pendant l'exécution
    - lui même fusionné avec le chapitre 203.4 Gestion de périphériques avec udev
    - Renommé en 201.3 Gestion du noyau à chaud et résolution de problèmes
  - Déjà vu dans
    - Le chapitre 1 de ce cours (particulièrement les vidéos 1 et 6)
    - Le chapitre 3 de ce cours (vidéo 6)
- 213.3 Dépannage des ressources système et 213.4 Dépannage de la configuration de l'environnement
  - Supprimés du fait de nombreuses répétitions avec les autres objectifs de la LPIC2 et la LPIC1

# Sujets abordés dans le chapitre 213

---

- Cron
- Syslog
- Passwd, shadow et group
- Uname
- Sysctl (cf procfs)
- Lsof, lsusb, lsdev, lspci
- Procédure de démarrage
  - init
  - Initrd
  - Initramfs
  - GRUB
- Gestion des modules du kernel

Tous déjà vus et revus !

## S'entraîner au dépannage

---

- La pratique, toujours la pratique
- Maîtriser tout les outils présentés
- Petit conseil : en profiter pour explorer les forums
  - Tester ses connaissances en tentant de résoudre les problèmes des autres

## Et pour conclure

---

- Un bonne préparation à tous
  - en vous souhaitant de réussir haut la main vos examens
- Pour avoir toutes les chances de votre côté
  - utilisez GNU/Linux au maximum (et tant qu'à faire, des logiciels libres)
  - tenez vous au courant de l'actualité
    - [UnixGarden](#), [linuxfr](#), listes et sites des distributions, etc ...
  - rejoignez un groupe d'utilisateur
    - sur Paris : [parinux](#), sur Toulouse : le [CULTe](#)
  - approfondissez au maximum
    - grâce aux liens présents dans ce cours, notamment les documentations officielles
    - ainsi que ceux qui vous retrouverez [ici](#), y compris en passant des examens d'entraînement

# Ce qu'on a couvert

---

- Rappel concernant les actuelles versions des objectifs LPIC
  - Modifications principales et anticipations de ce cours
    - objectif 213
      - Comment s'y préparer
      - Raisons de « l'absence » de ce chapitre dans ce cours
- Conclusion de notre cours et petits conseils