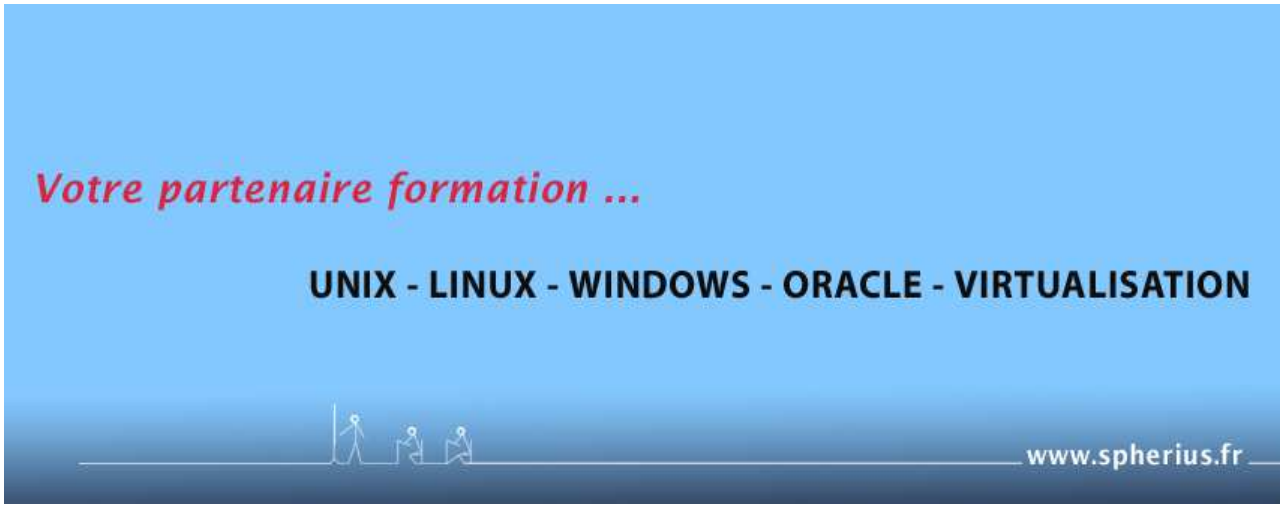
ADMINISTRATION LINUX



SOMMAIRE

Les auteurs de ce document sont :

- Monsieur Baranger Jean-Marc,
- Monsieur Schomaker Theo.

La version du support de cours est:

administration_Linux_version_1.4

La version de Linux utilisée pour les commandes de ce support de cours est :

CentOS et Debian

Les références sont : les documents des sites web de CentOS, de RedHat et de Debian.

Introduction

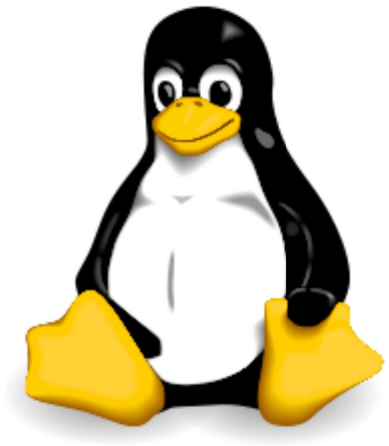
Dans ce chapitre nous allons découvrir les principes généraux d'un système d'exploitation Linux.

Table des matières

Introduction

Présentation

Bienvenue dans l'univers



LINUX

Présentation

Linux est un système d'exploitation. C'est à dire un logiciel qui permet de manipuler des fichiers, d'exécuter des programmes, ...etc via un ordinateur.

Pour utiliser ce système, nous disposons d'une interface graphique, ainsi qu'un terminal de commandes.

Linux appartient à la catégorie «**open source**», ce qui veut dire que son code source est disponible gratuitement par et pour les utilisateurs.

Nous retrouvons ce système d'exploitation principalement dans les entreprises, notamment pour gérer un serveur.

Introduction

L'historique

1970 1991 1994 1996

```
From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: Gcc-1.40 and a posix-question
Message-ID:
Date: 3 Jul 91 10:00:50 GMT

Hello netlanders,

Due to a project I'm working on (in minix), I'm interested in the posix
standard definition. Could somebody please point me to a (preferably)
machine-readable format of the latest posix rules? Ftp-sites would be
nice
```

L'historique

Le système Linux vient du système UNIX.

Les dates importantes

1970 : Création d'Unics (UNIX) par Kenneth Thompson et Dennis Ritchie au sein des laboratoires Bell AT&T.
AT&T souhaite commercialiser son système.

1971 : 23 ordinateurs sont reliés à l'ARPANET. Ray Tomlinson envoi le premier courriel.

1972 : Dennis Ritchie crée le langage C (une évolution du langage B) rendant ainsi Unix portable sur différentes architectures physiques.

1973 : Définition du protocole TCP/IP.

1983 : Adoption du protocole TCP/IP. Premier serveur de noms (DNS).
L'université de Berkeley démarre le développement de Unix BSD.
AT&T prend le nom d'Unix System V.
Richard Stallman annonce le développement de GNU (Gnu is Not Unix) pour créer un système d'exploitation libre.

1985 : Richard Stallman créé la FSF (Free Software Foundation) pour s'assurer que tous les logiciels développés pour GNU restent libres.

1989 : Richard Stallman publie la première licence publique générale GNU.

1990 : Collaboration AT&T et SUN pour créer Unix AT&T System V.4.
Disparition d'ARPANET. Annonce du World Wide Web.

1991 : IBM, DEC et HP créent le groupement OSF (Open Software Foundation).
Démarrage de nombreux projets tel que FreeBSD.

Andrew Tanenbaum développe pour l'enseignement le système Minix. Il s'inspire d'Unix. Les sources sont disponibles mais ne sont pas libres.

Linus Thorvald décide de programmer un remplaçant à Minix qu'il appellera Linux. Le noyau a été publié sous licence GPL ce qui permet en le combinant aux outils GNU d'obtenir un système d'exploitation complet que l'on devrait appeler GNU/Linux au lieu de Linux.

1994 : Noyau Linux 1.0

1995 : Noyau Linux 1.2

1996 : Noyau Linux 2.0
Larry Ewing créé le symbole de linux le manchot **Tux.**
Matthias Ettrich créé le bureau **KDE.**

1997 : Miguel de Icaza créé le bureau **GNOME.**

1998 : Création de l'Open Source Initiative dédiée à la promotion de logiciels open source.

1999 : Entrée en Bourse de Redhat.
Noyau Linux 2.2.

2001 : Noyau Linux 2.4.

2003 : Acquisition de Suse par Novell.
Noyau Linux 2.6.0.

2012 : Noyaux Linux 3.2 LTS à 3.7.
Linus Thorvald optient le prix «Millennium Technology» remis par la Technology Academy Finland .

2015 : Noyaux Linux 3.19 à 4.3.

Premier Message envoyé par Linus Thorvald sur un système minix.

```
From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)

 Newsgroups: comp.os.minix
 Subject: Gcc-1.40 and a posix-question
 Message-ID:
 Date: 3 Jul 91 10:00:50 GMT


 Hello netlanders,

 Due to a project I'm working on (in minix), I'm interested in the posix
 standard definition. Could somebody please point me to a (preferably)
 machine-readable format of the latest posix rules? Ftp-sites would be
 nice
```

Message de Linus Thorvald annonçant l'inclusion de bash et de gcc dans son système.

```
From: torv...@klaava.Helsinki.FI (Linus Benedict Torvalds)

 Newsgroups: comp.os.minix
 Subject: What would you like to see most in minix?
 Summary: small poll for my new operating system
 Keywords: 386, preferences
 Message-ID: <1991Aug25.205708.9541@klaava.Helsinki.FI>
 Date: 25 Aug 91 20:57:08 GMT

 Organization: University of Helsinki

 Lines: 20


 Hello everybody out there using minix -

 I'm doing a (free) operating system (just a hobby, won't be big and
 professional like gnu) for 386(486) AT clones.  This has been brewing
 since april, and is starting to get ready.  I'd like any feedback on
 things people like/dislike in minix, as my OS resembles it somewhat
 (same physical layout of the file-system (due to practical reasons)
 among other things).

 I've currently ported bash(1.08) and gcc(1.40), and things seem to work.
 This implies that I'll get something practical within a few months, and
 I'd like to know what features most people would want.  Any suggestions
 are welcome, but I won't promise I'll implement them :-)

                Linus (torv...@kruuna.helsinki.fi)

 PS.  Yes - it's free of any minix code, and it has a multi-threaded fs.
 It is NOT protable (uses 386 task switching etc), and it probably never
 will support anything other than AT-harddisks, as that's all I have :-(.
```

Introduction

Le type de licences

- Licence
- Open source
- GPL
- Copyleft

Le type de licences

Licence

Une licence est un contrat permettant au titulaire des droits d'auteur, de définir les conditions d'accès à son programme (utilisation, modification et diffusion).

Open source

La désignation «**open source**» permet d'identifier un logiciel sur lequel s'applique une licence établie par l'**Open Source Initiative**.
C'est un logiciel qui a un code source et une distribution libres d'accès et sur lequel nous pouvons créer des travaux dérivés à partir de ce code.

Licence GPL

C'est une licence qui gère la législation ainsi que la distribution des logiciels libres provenant du projet **GNU**.
Elle fut créée par Richard Stallman, fondateur de la **Free Software Foundation**, qui est une organisation américaine pour la promotion du logiciel libre et la défense des utilisateurs.

La licence GPL s'appuie sur la notion de «**copyleft**», un clin d'œil au «**copyright**». Le «**copyleft**» est la liberté d'utiliser les codes sources et de les modifier. La contrainte est que toute adaptation réalisée est soumise à la même licence, donc l'obligation de mettre à disposition le code source.

Les distributions Linux

Red Hat Entreprise Linux

Cette distribution commerciale à été développée par l'entreprise Red Hat.
Red Hat Entreprise Linux est, comme son nom l'indique, destinée aux entreprises.

Plusieurs distributions sont disponibles en fonction de leurs usage : versions serveurs d'entreprise (RHEL), version cloud, version poste de travail.

CentOS (Common ENTrepise Operating System)

Principalement destinée aux serveurs, cette distribution est un dérivé de Red Hat Entreprise Linux.
La première version de CentOS voit le jour en 2004 sur une base RHEL 2.1.

CentOS est une version gratuite de Linux Red Hat et le support est assuré par une communauté.

Debian

Debian est une distribution majeure dans le monde communautaire de Linux. Les distributions proposées sont non commerciales.

Ubuntu

Basée sur une distribution Linux Debian. Ubuntu est disponible sous une version commerciale, mais il existe également une distribution communautaire et grand public.

SUSE

Entreprise allemande du groupe Micro Focus International, elle a développé la distribution Linux «**SUSE Linux Entreprise**».
La première version est apparue en 1994, ce qui fait d'elle la plus ancienne distribution commerciale encore existante.

Compléments

Il existe un grand nombre de versions Linux ayant chacune leurs spécificités. Vous pourrez trouver facilement sur le web la liste complète et actualisée des différentes distributions Linux.

Certaines distributions sont publiées avec l'étiquette LTS (Long Time Support). Le distributeur assure ainsi que la distribution sera maintenue et supportée sur une certaine durée (5 ans usuellement).

Introduction

Les sources de documentation

- Le site officiel de la distribution
- Les KB - Knowledge Base
- Les forums et les communautés
- Le manuel et ses sections

Les sources de documentation

L'administrateur doit s'habituer à utiliser différentes sources d'informations qui vont lui permettre d'assurer une bonne administration du parc de serveurs, de faire de la veille technologique, d'identifier les sources d'informations qu'il pourra exploiter afin de résoudre des problèmes ou de récupérer la bonne procédure de dépannage.

Le site officiel de la distribution Linux doit évidemment être consulté.

On y trouve une grande source de documentations au format web ou pdf. Des documents pour les procédures d'administration ou sur des serveurs en particulier.

Les KB – Knowledge Base – Base de connaissances – est indispensable à l'administrateur. Il doit avoir le réflexe de les consulter lors de problème sur un serveur ou lors d'un comportement anormal d'une commande, processus, service …

Les Kbs sont le point de départ de toutes les investigations d'un administrateur système.

Enfin, toutes les sources pertinentes d'informations doivent être identifiées et référencées, afin d'être exploitées facilement et assurer une veille technologique de votre parc, tels que les communautés ou les blogs.

Premier Pas

La commande «man»

- Manuel d'une commande

man commande

man section commande

La commande «man»

La commande «**man**» est une aide qui permet de visualiser le manuel d'une commande. Le manuel est l'outil indispensable sous Linux. Il existe pour chaque commande une multitude d'options qu'il est impossible de retenir par cœur. Le manuel est divisé en sections. La section 1 contient toutes les commandes, la section 5 contient les fichiers de configuration. Par défaut la section présentée est la 1ère que le système trouve (donc souvent la section 1). Toutes les sections n'existent pas pour chaque commande. Les pages du man sont stockées dans /usr/share/man.

Si des pages de man sont localisées autre part, vous pouvez initialiser la variable MANPATH.

Lors de l'exécution de la commande man, c'est la commande more qui est utilisée pour afficher le contenu. Le déplacement à l'intérieur du man est donc identique à l'exécution de la commande more sur un fichier.

Syntaxe : man commande

Une fois le manuel de commande ouvert, voici ses principales sections :

- **Name :** nom de la commande et son descriptif court,
- **Synopsis :** la syntaxe de la commande,
- **Description :** la description complète de la commande,
- **Options :** la description complète de chaque options,
- **See Also :** «voir aussi» d'autres commandes en rapport avec celle qui est consultée.

Exemple :

```
$ man id

ID(1)                  Manuel de l'utilisateur Linux              ID(1)
NOM
id - Afficher les UIDs et GIDs effectifs et réels
etc ...
```

Interactivité

L'interactivité dans le «**man**» est défini avec des touches du clavier, principalement pour se déplacer au sein de l'aide de la commande ou pour réaliser des recherches.

Raccourci	Action
flèches directionnelles	Permet de naviguer dans la page
espace	Afficher la page suivante
entrée	Afficher la ligne suivante
b	Remonter d'une page
q	Quitter

/	Rechercher en avant
?	Rechercher en arrière
n	Allez à l'occurrence suivante
N	Allez à l'occurrence précédente
h	Afficher l'aide

Sections

Il existe différentes sections pour agencer les pages de manuel.

Numéro de section	Signification
1	Aide des commandes
2	Appels système
3	Librairies
4	Fichiers spéciaux
5	Format de fichiers
6	Jeux
7	Divers
8	Commandes d'administration du système
9	Routines du noyau

Options utiles

-s (section) : permet d'indiquer la section où chercher les pages de manuel. Il est possible de chercher dans plusieurs sections en les séparant par des virgules.

Exemple :

```
$ man      -s      5        passwd
$ man      -s    1,5        passwd
```

Variante :

```
$ man              5        passwd
```

-L (locale) : permet de spécifier les paramètres régionaux pour l'affichage de la page de manuel. Pour afficher la page de manuel «**man**» en anglais taper cette commande :

Exemple :

```
$ man      -L  en      ls
```

Complément

apropos : permet de trouver une commande dont vous ne connaissez pas le nom. Il suffit d'entrer un mot clé à la suite de cette commande, puis celle ci cherchera toutes les commandes ayant ce mot clé dans leur description.

Exemple :

```
$ apropos       sound
esd (1)              - Le démon de son éclairé (Enlightened Sound Daemon)
alsactl (1)          - advanced controls for ALSA soundcard driver
alsaunmute (1)       - a simple script to initialize ALSA sound devices
amixer (1)           - command-line mixer for ALSA soundcard driver
... etc
```

Notes

Installation du système

Dans ce chapitre, nous allons traiter les différentes méthodes d'installation du système d'exploitation Linux.

Table des matières

Installation du système

Les options d'installation – Conseils de partitionnement

- Partitionnement par défaut
- Partitionnement personnalisé
- Démarrage du système

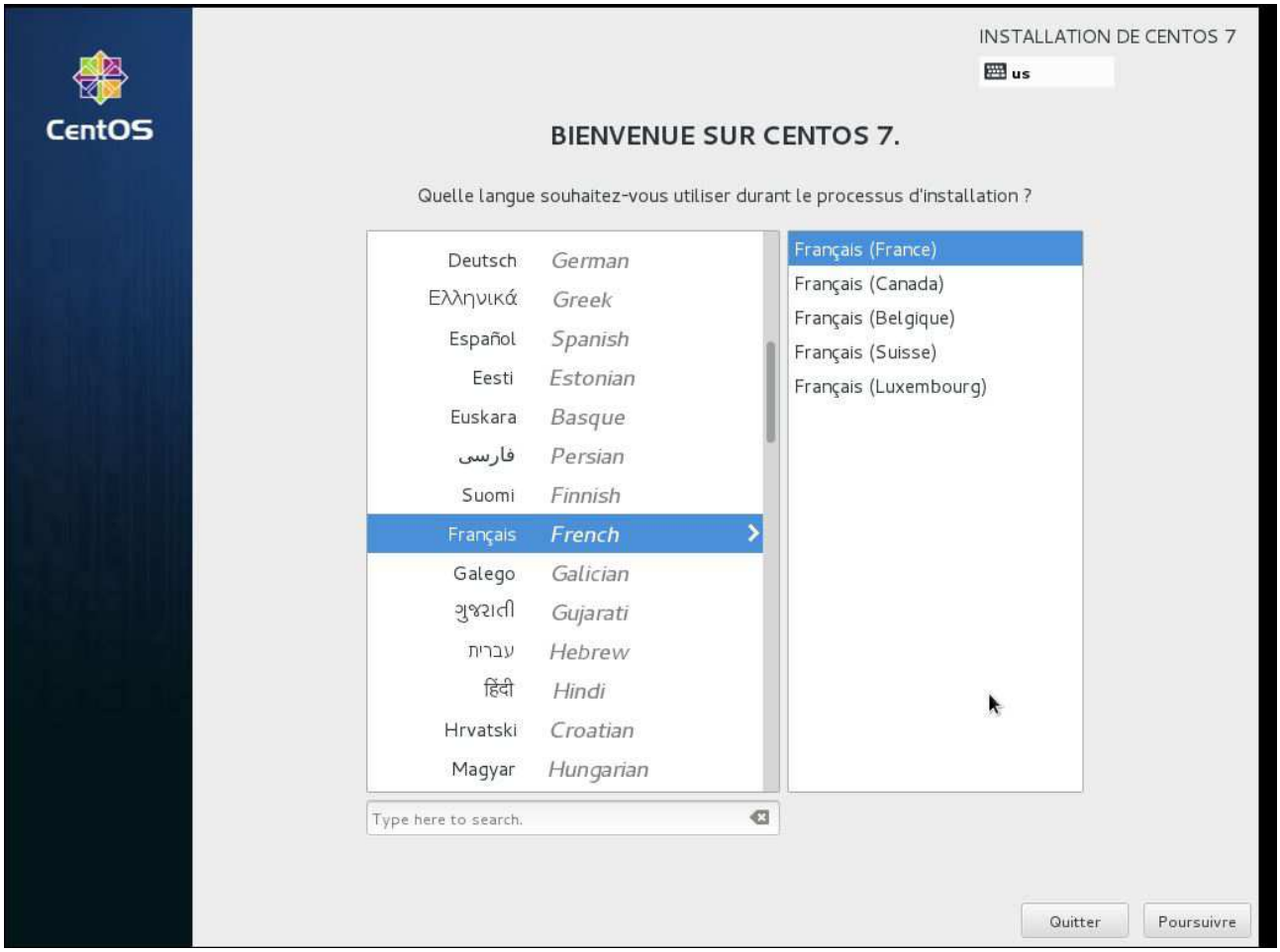
Les options d'installation – Conseils de partitionnement

Le démarrage à partir du DVD ou d'une image ISO propose le menu suivant. Si vous n'êtes pas sûr de l'intégrité du support d'installation vous pouvez le tester. (*Test this media & install CentOS 7*). L'option *Troubleshooting* permet de booter en mode secours. *Install Cent0S7* va lancer la procédure d'installation.

Avant d'installer votre serveur, il est important de savoir quel va être son rôle. En fonction de son rôle le partitionnement devra être adapté (serveur de fichiers, serveur de messagerie, …). Il faudra aussi prévoir que le système puisse être évolutif et notamment prévoir l'agrandissement à chaud des systèmes de fichiers.

Démarrage sur le DVD pour une installation de CentOS 7.

Il faut d'abord préciser en 1er lieu la langue d'installation.

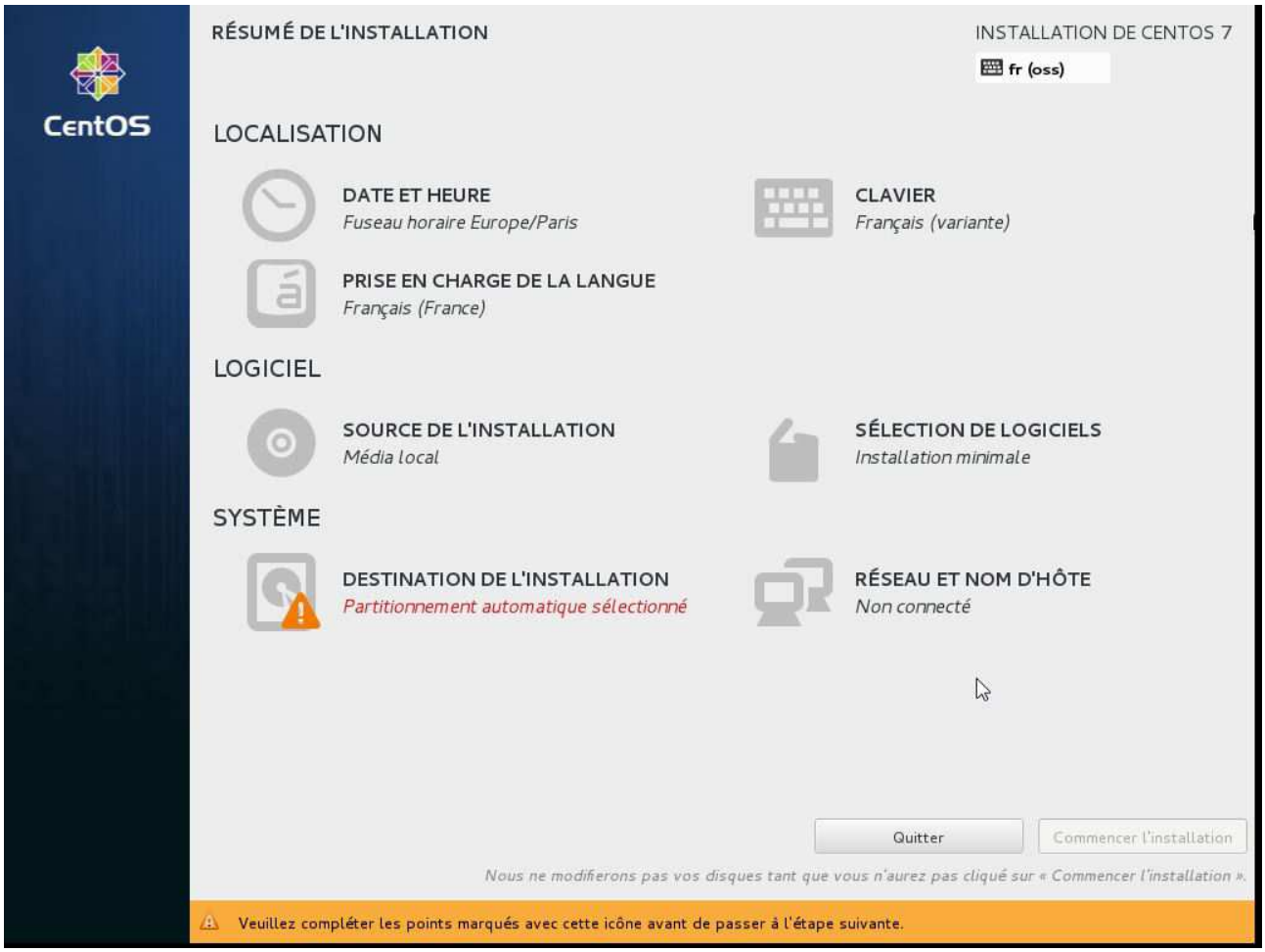


Une fois la langue sélectionnée il faut cliquer sur Poursuivre pour continuer à choisir les options d'installation.

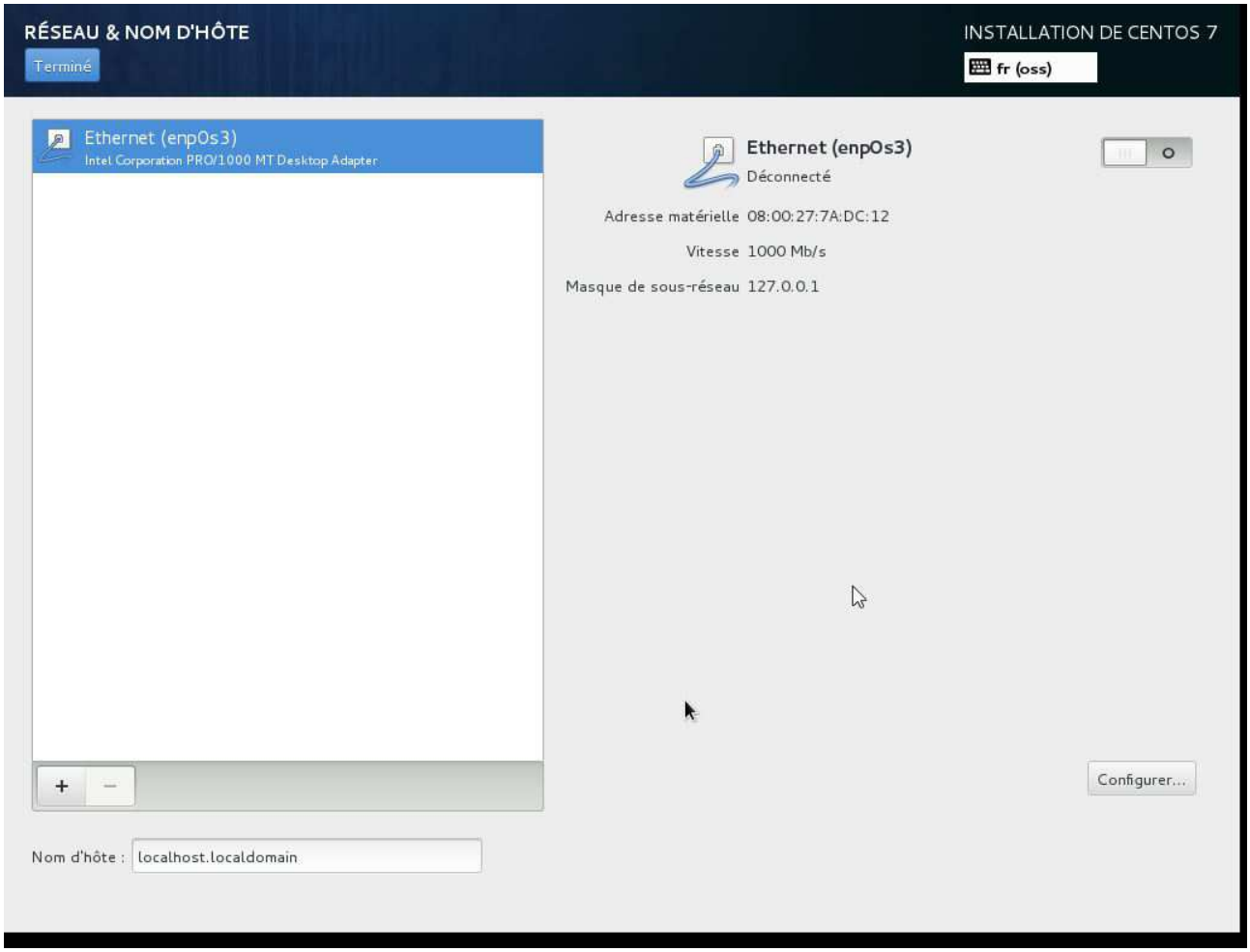
La partie *LOCALISATION* est configurée par défaut avec la langue choisie. En prenant la langue française, la timezone et le clavier sont automatiquement choisis. Il est possible de les modifier en cliquant dessus.

Le champ *LOGICIEL* permet de choisir la source d'installation (DVD par défaut) et le champ *SELECTION DE LOGICIELS* permet de sélectionner les packages à installer.

Le champ *SYSTEME* permet de configurer le partitionnement et de configurer l'adressage IP ainsi que le nom de la machine.



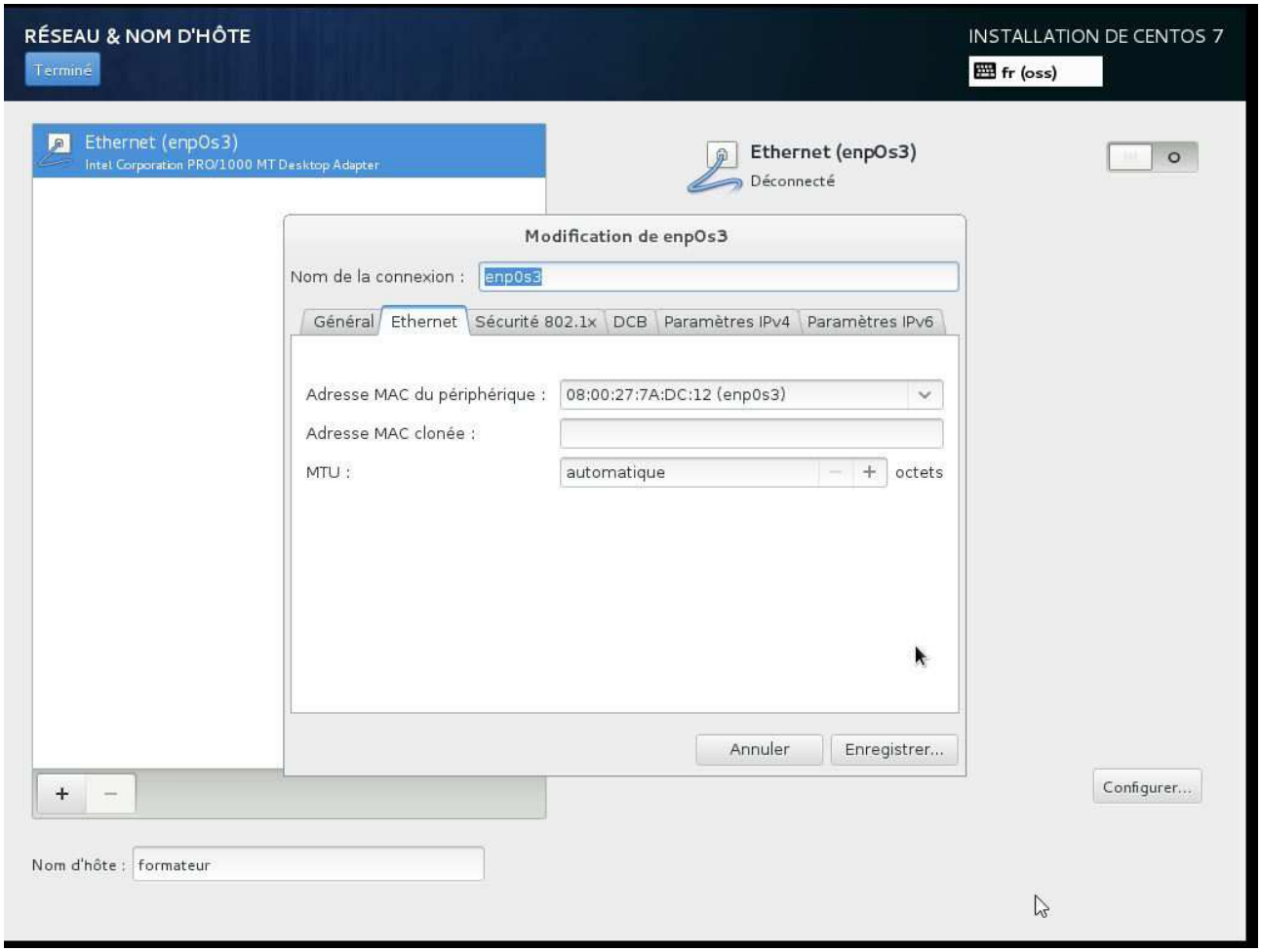
Configuration du nom de la machine et du réseau.



Le nom d'hôte est par défaut configuré sur localhost.localdomain. La carte réseau est désactivée par défaut. En cliquant sur le bouton, la carte s'active et essaye de communiquer avec un serveur DHCP si elle est configurée en tant que cliente DHCP.

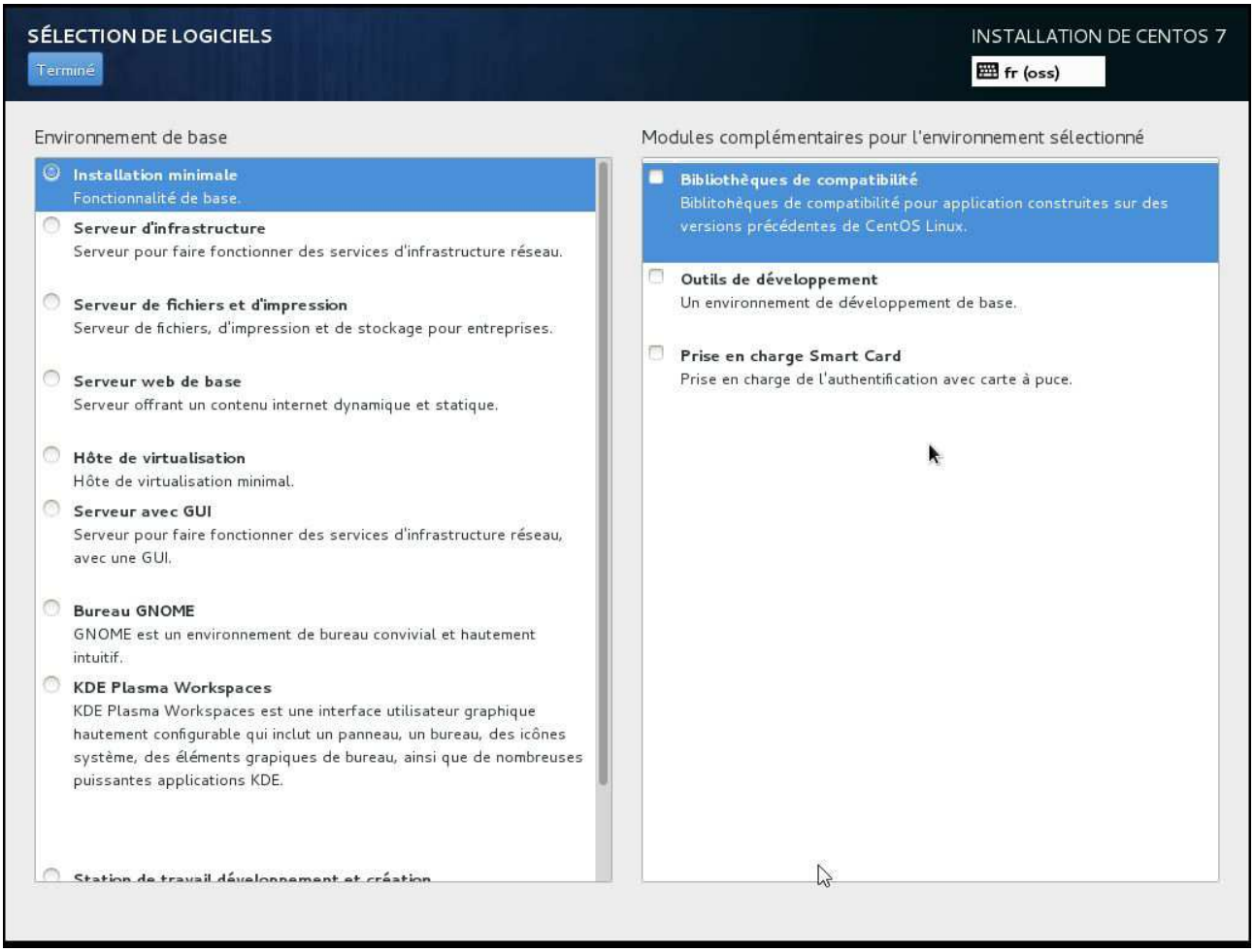
En cliquant sur le bouton *Configurer* vous pouvez paramétrer votre carte réseau et basculer l'adressage IP en fixe.

Configuration de la carte réseau.



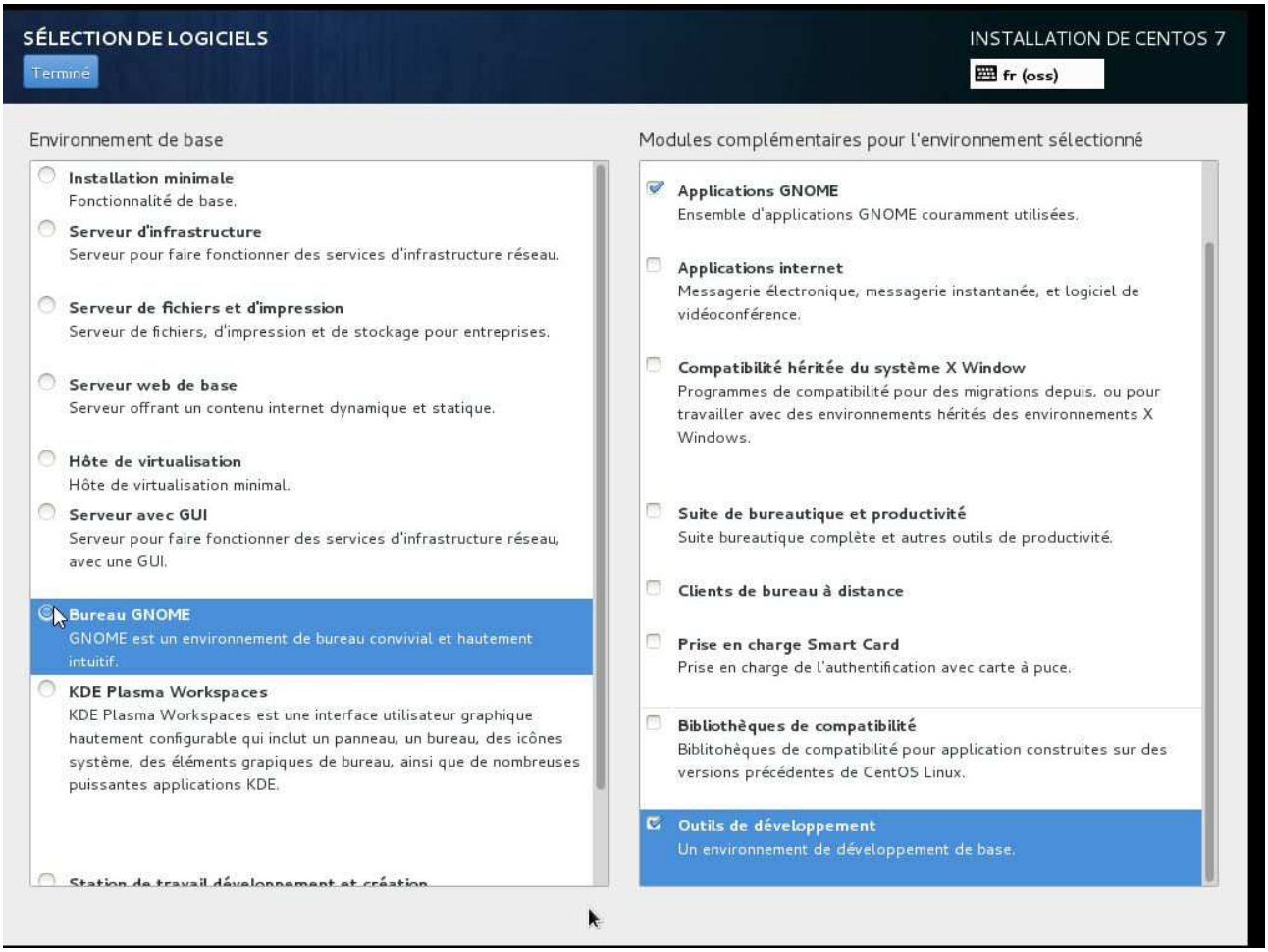
L'onglet *Paramètres Ipv4* permet de basculer en adressage statique. Il faut alors renseigner les champs adressage ip, netmask, passerelle, dns.

Choix des logiciels à installer.



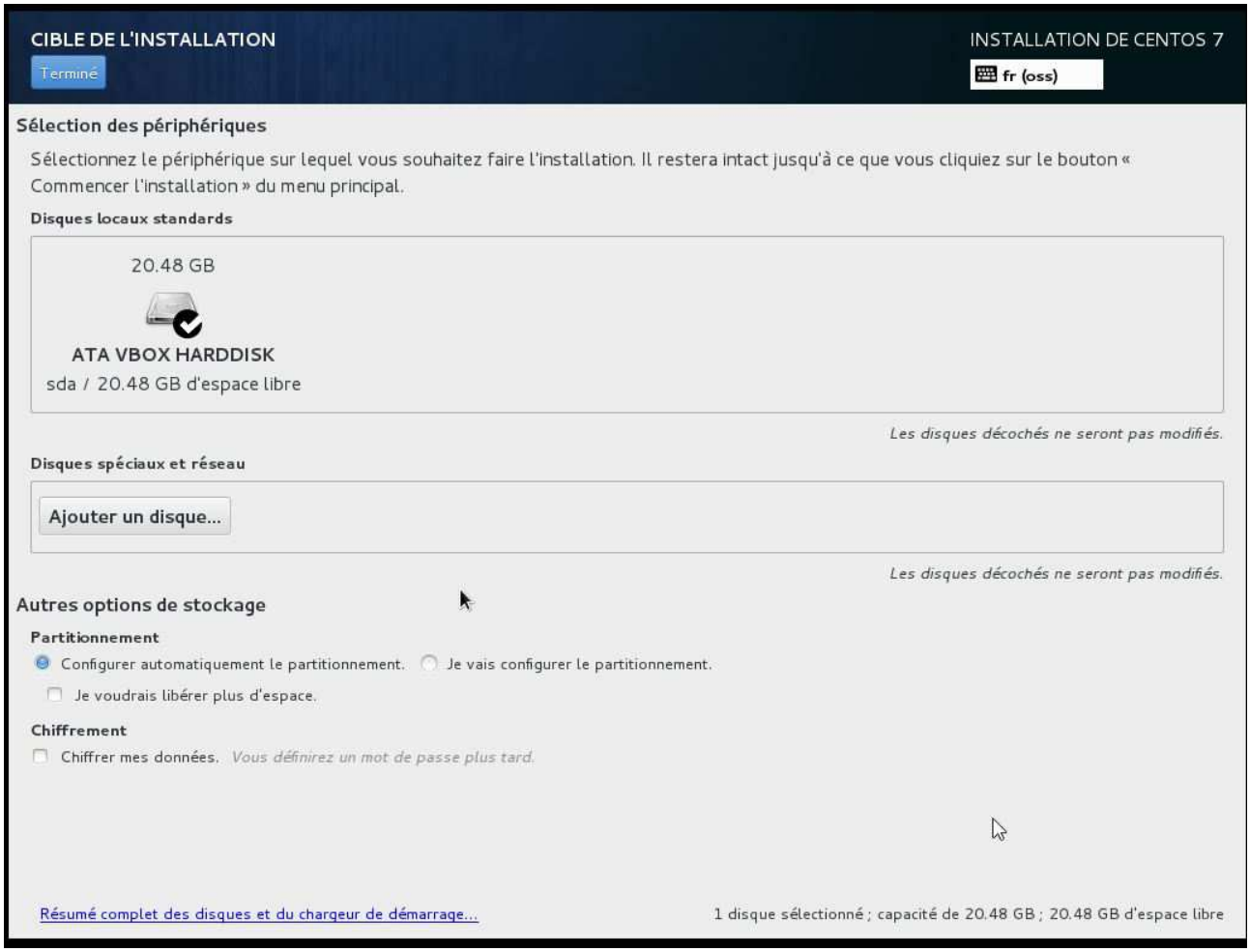
Choisissez le minimum à installer selon vos besoins. Vous pourrez toujours après l'installation, installer d'autres logiciels. La colonne de gauche indique le type d'installation que vous désirez effectuer. La colonne de droite permet d'affiner la sélection.

Le choix Bureau GNOME installe un environnement graphique.



Les outils de développement permettent d'avoir un certain nombre d'outils pré-sélectionnés (compilateur cc, …).

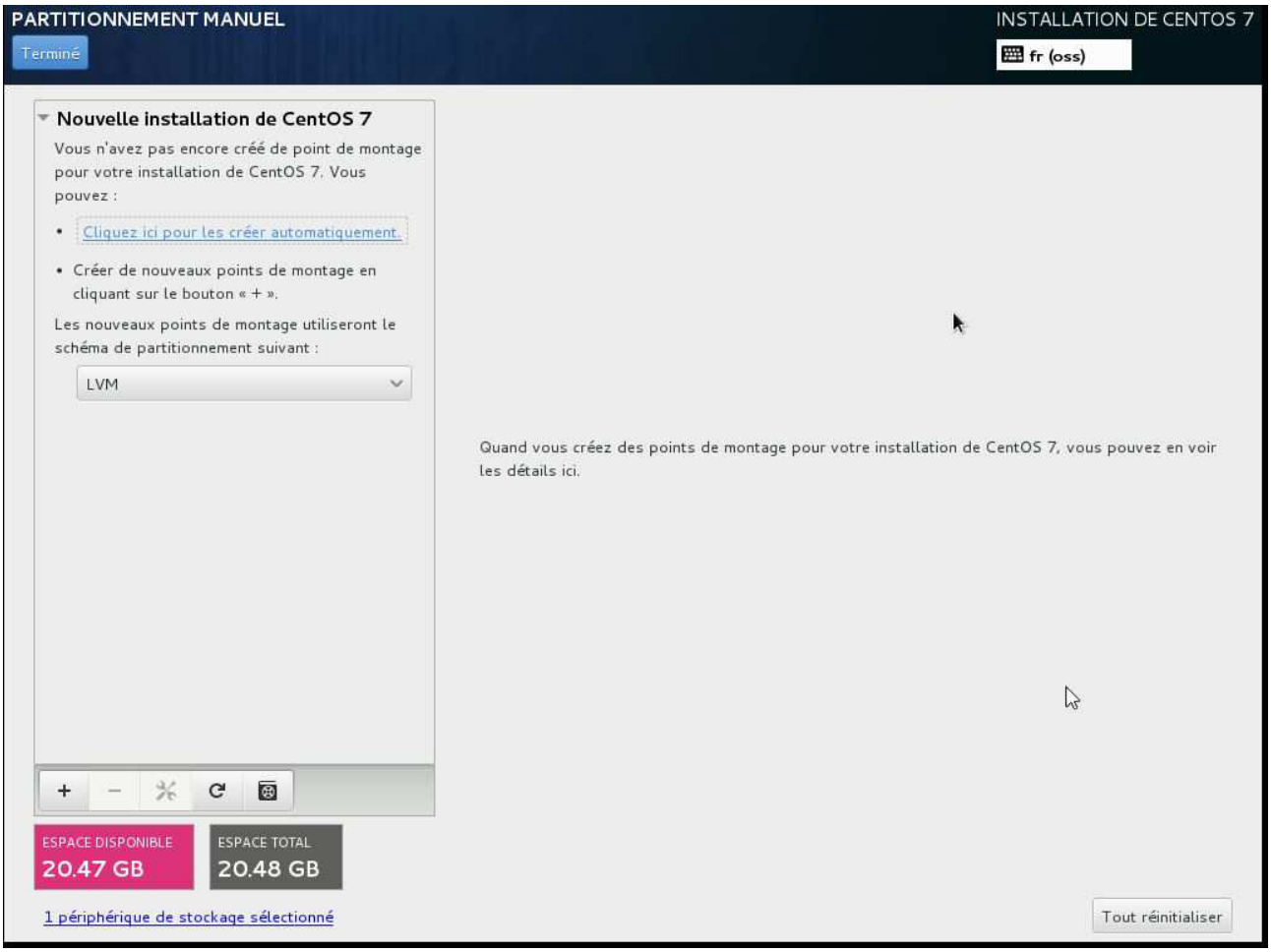
Le partitionnement est la partie la plus délicate. Par défaut une installation avec LVM est sélectionnée ce qui permet d'agrandir facilement la partition. Le bouton *Je vais configurer le partitionnement* permet de choisir un partitionnement personnalisé.



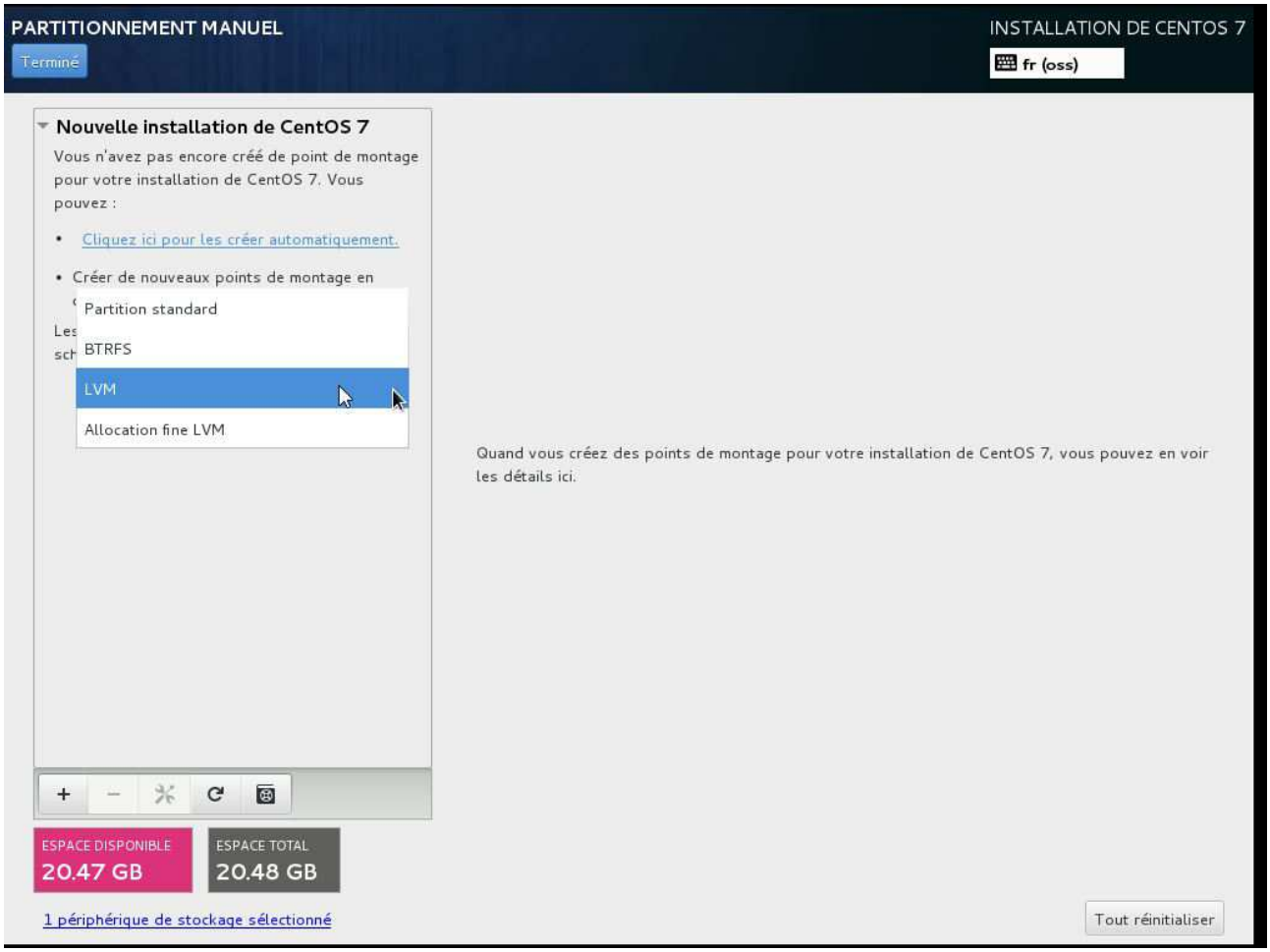
Le bouton *Ajouter un disque* permet de configurer un disque accessible via le réseau avec iscsi ou fcoe.

Le chiffrement des données permet de crypter la partition. Une *pass phrase* est alors demandée lors de l'accès à la partition chiffrée.

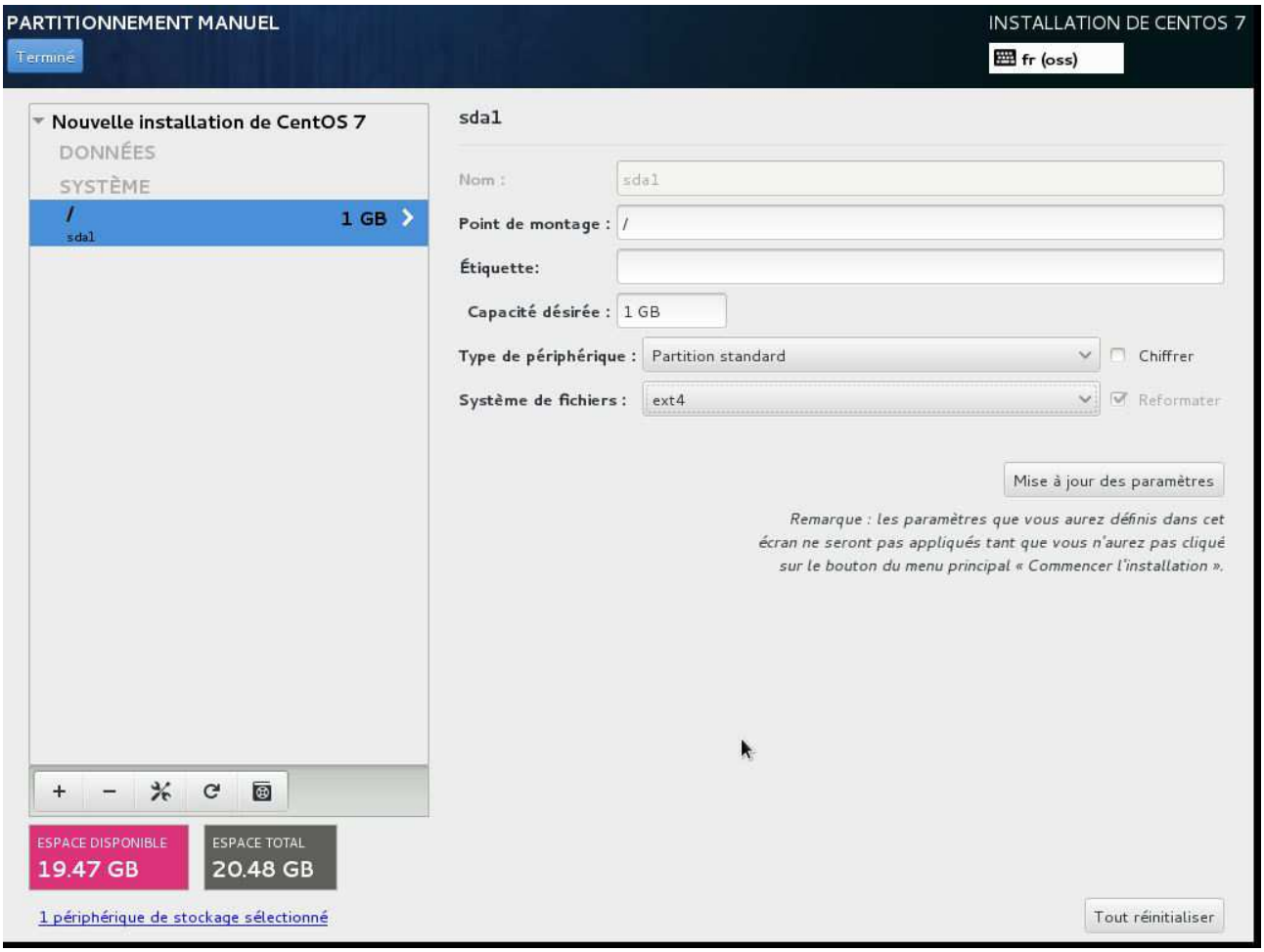
Le partitionnement manuel affiche cette fenêtre. En cliquant sur le bouton '+' nous allons ajouter des partitions.



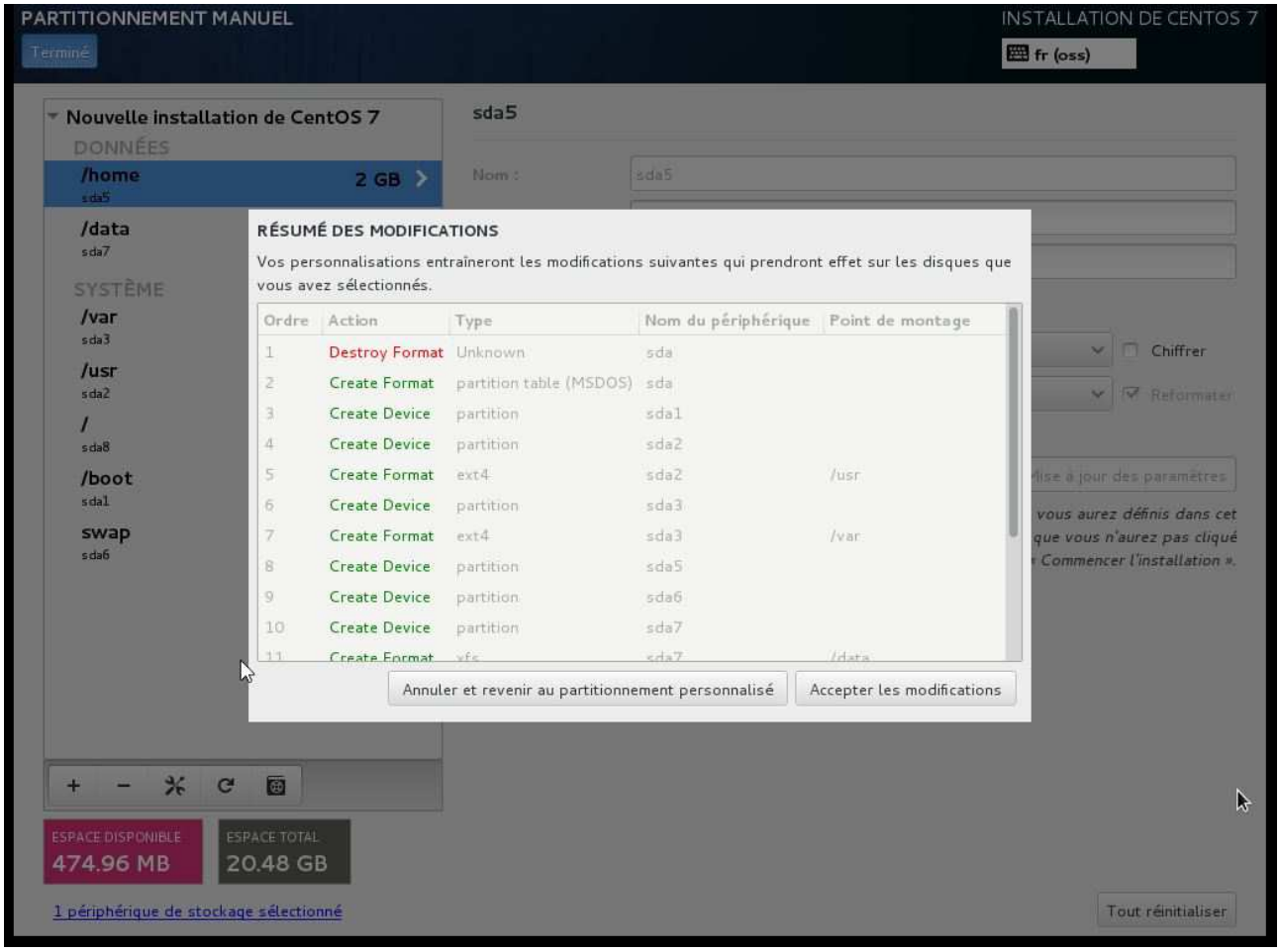
Pour un partitionnement personnalisé il faut choisir la taille des partitions à créer ainsi que le point de montage des partitions.



Création de la partition / d'une taille de 1GB et avec un système de fichiers de type ext4. Pour ajouter d'autres partitions, il faut cliquer sur '+'.

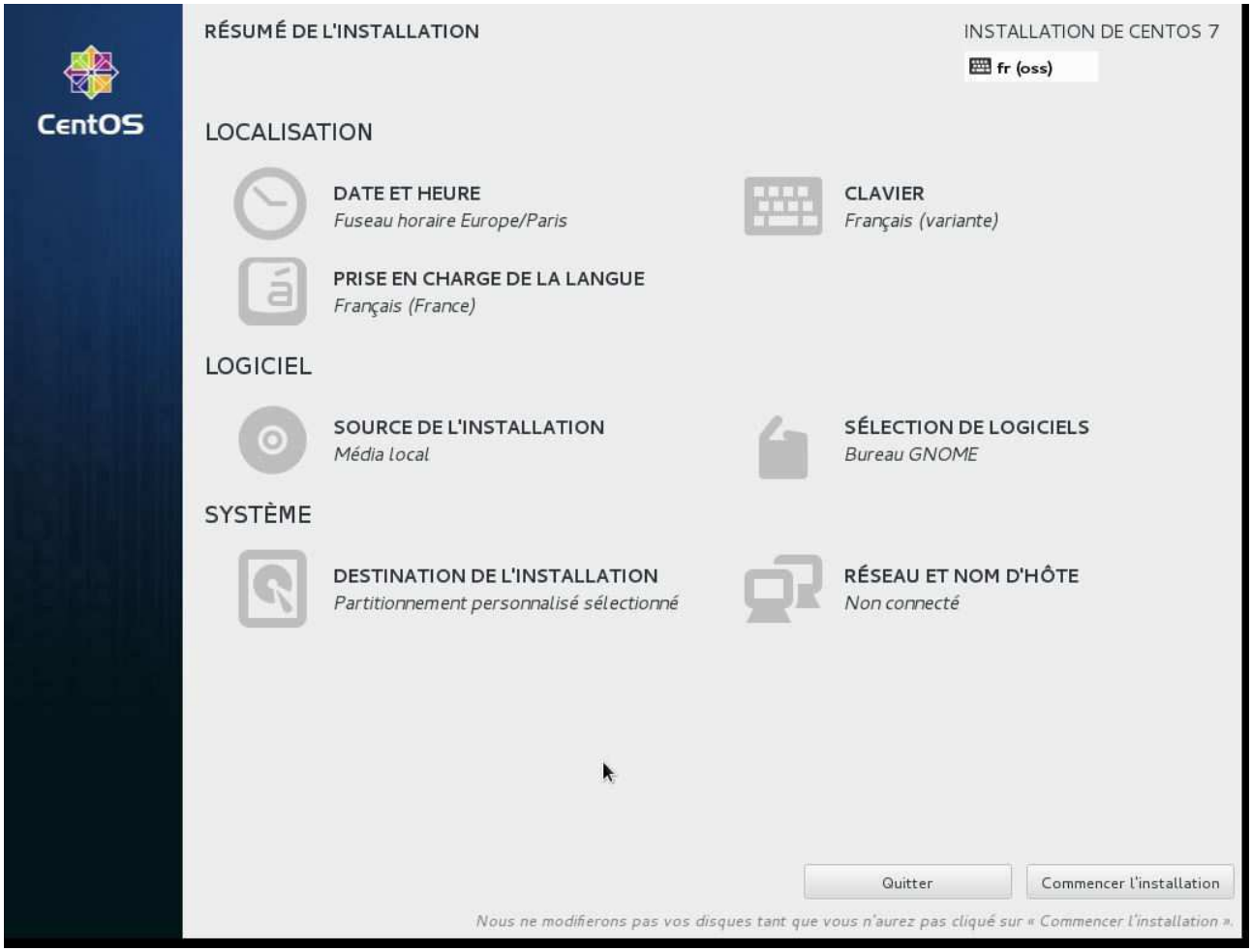


Un résumé est affiché lorsque vous avez terminé le partitionnement de votre disque dur.



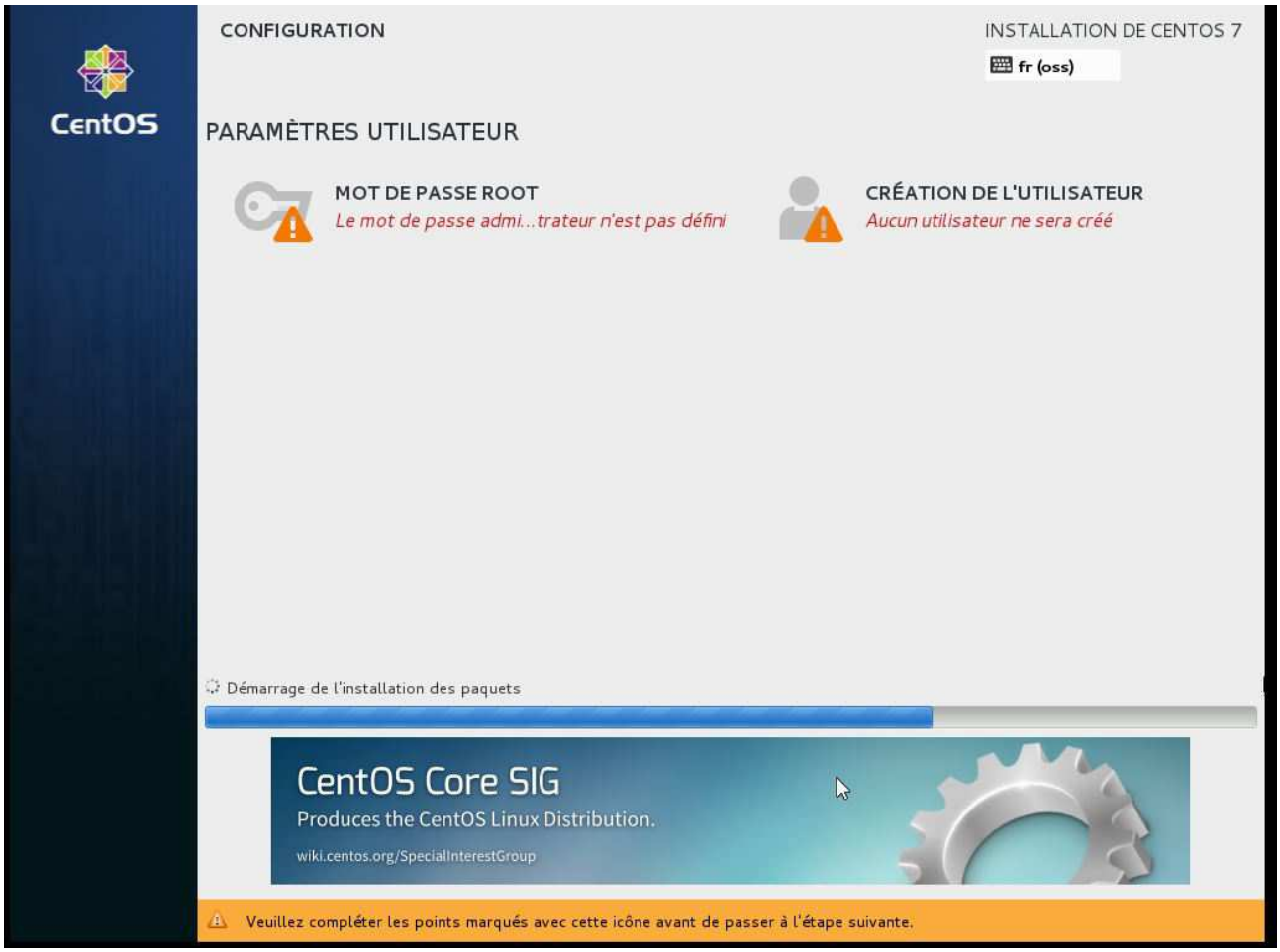
Après que les modifications aient été acceptées, le système affiche la fenêtre permettant de commencer l'installation.

Résumé des options d'installation choisies.

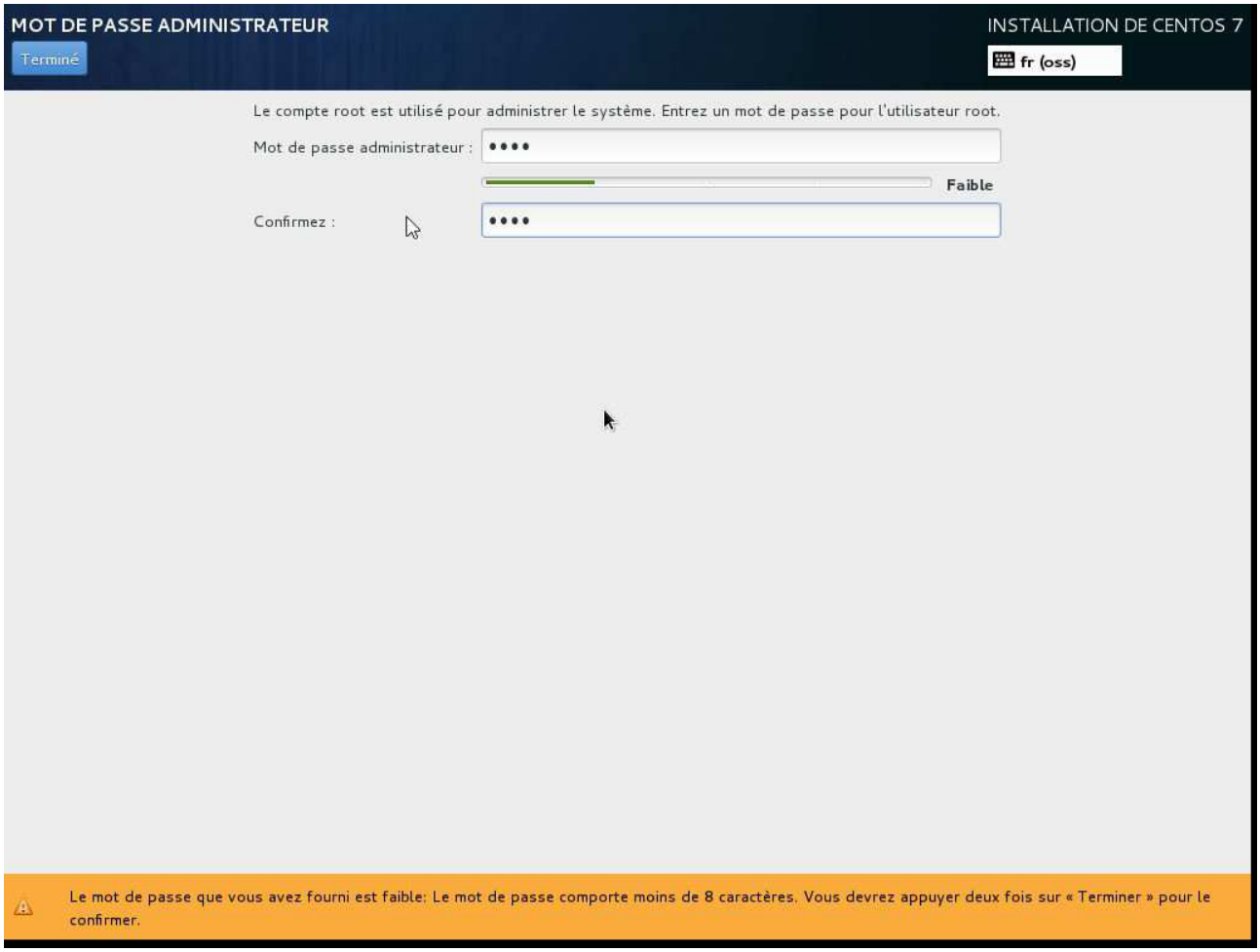


Pour lancer l'installation, il faut cliquer sur 'commencer l'installation'.

L'installation commence mais nous devons encore configurer le mot de passe de l'administrateur et créer un compte utilisateur.

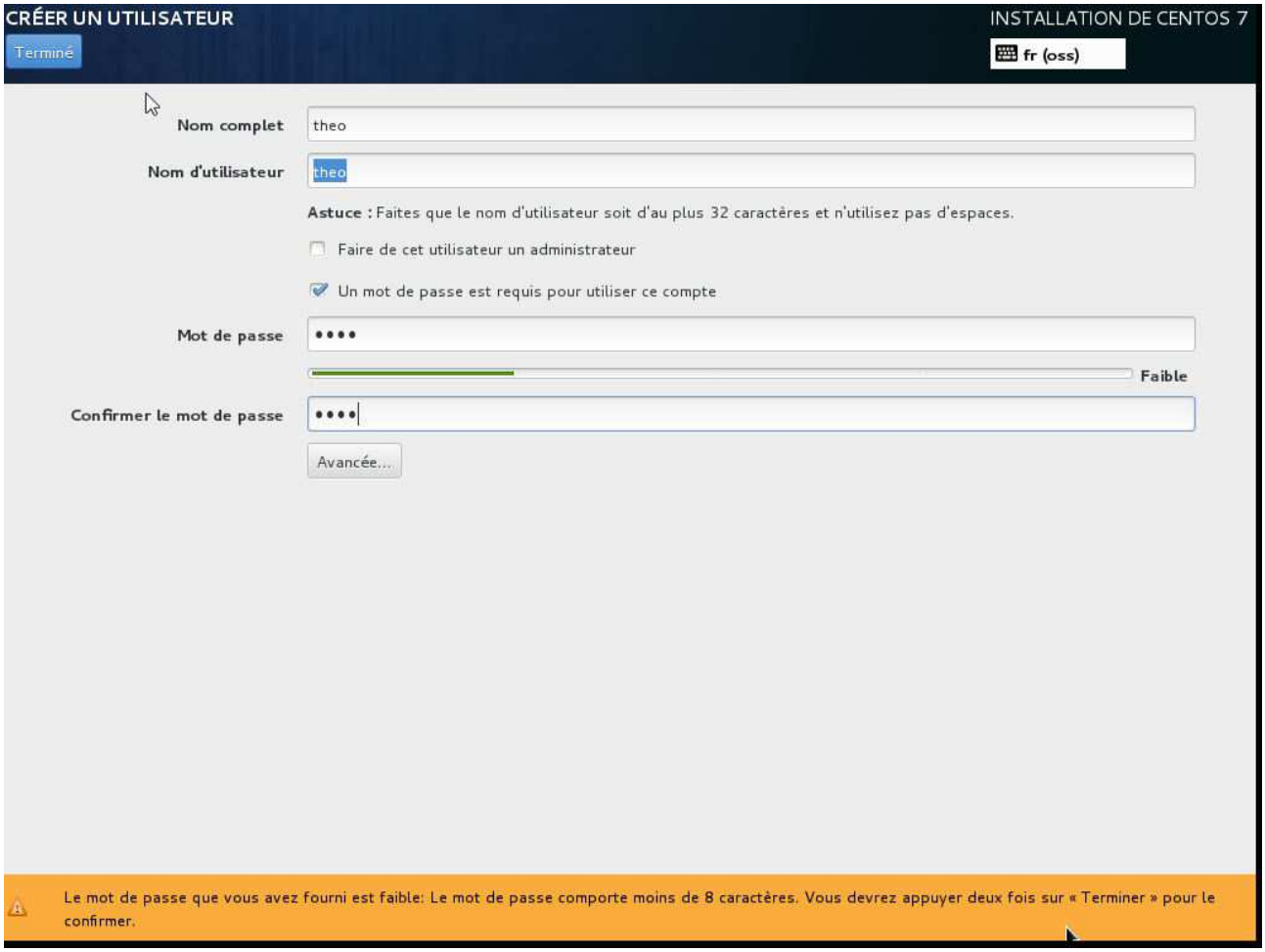


Choix du mot de passe de l'administrateur. Choisissez un mot de passe robuste.



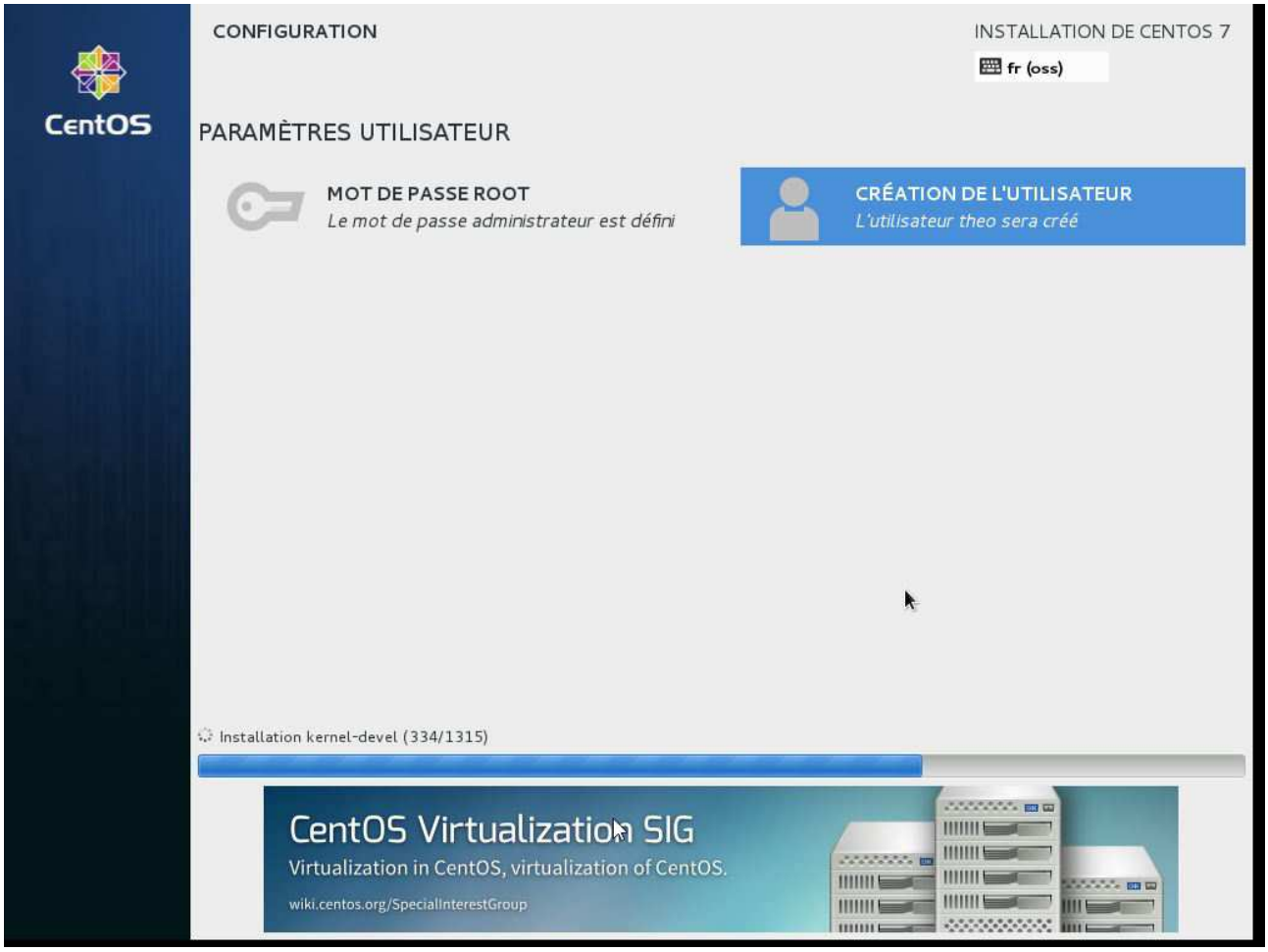
Si vous choisissez un mot de passe considéré comme faible, le système demande de cliquer deux fois sur *Terminé* pour valider le mot de passe saisie.

Création d'un compte utilisateur.

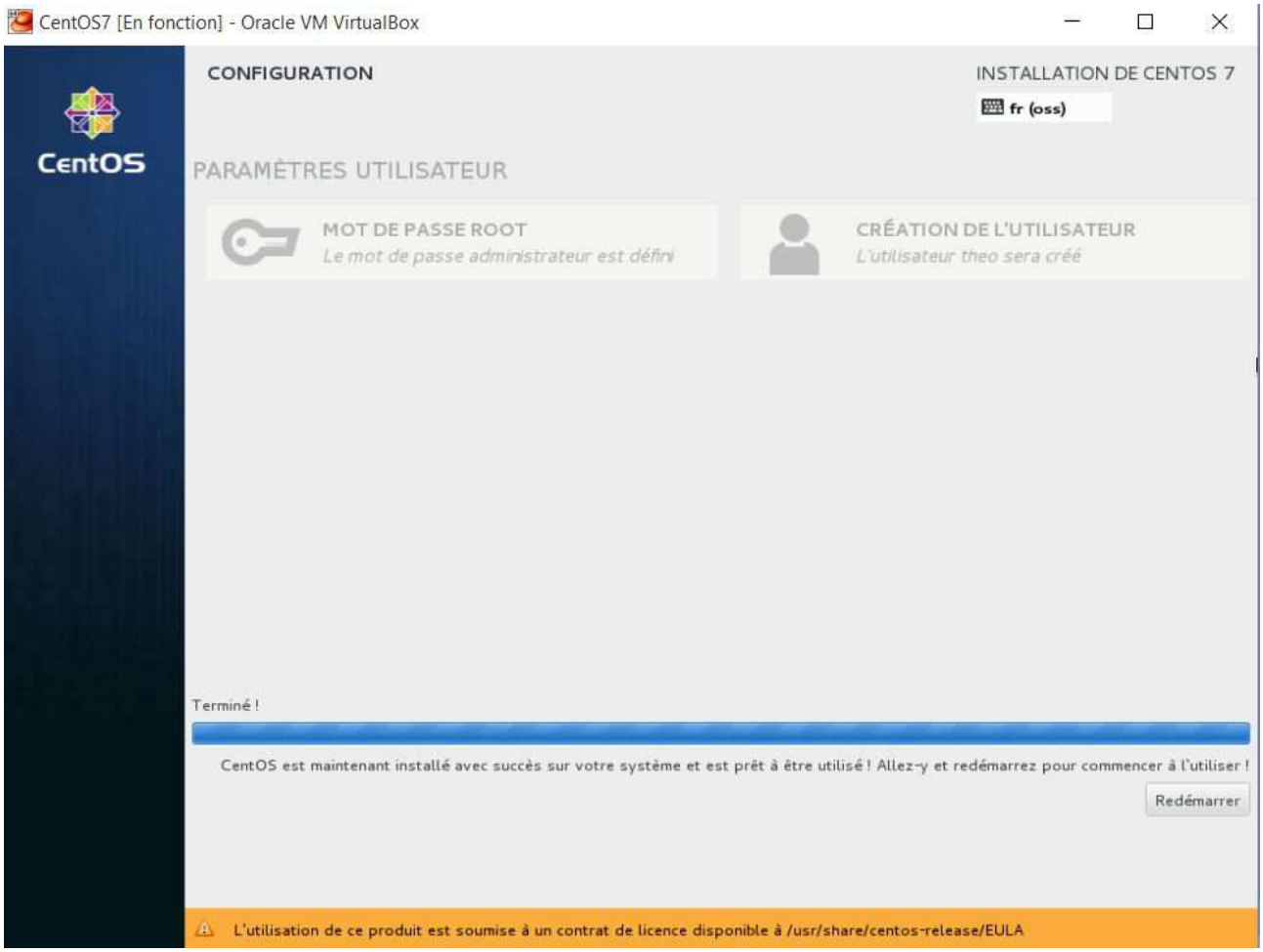


Cocher la case '*Faire de cet utilisateur un administrateur*' permet d'ajouter l'utilisateur au groupe wheel. Selon la configuration de pam, on peut n'autoriser que les utilisateurs du groupe wheel à utiliser la commande su.

Fin de l'installation.



A la fin de l'installation, il faut redémarrer. La fenêtre de login s'affiche alors.



Remarquez que le système nous indique que le produit est soumis à un contrat de Licence. En cliquant dessus une fenêtre s'ouvre pour accepter ou refuser la licence.

Le système nous demande par la suite de configurer Kdump avant de finaliser l'installation.

Le système va redémarrer. Il ne reste plus qu'à vous connecter.

Installation du système

La mise à jour du système après l'installation

- Partitionnement par défaut
- Partitionnement personnalisé
- Démarrage du système

La mise à jour du système après l'installation

Une fois l'installation effectuée, des dépôts logiciels par défaut ont été configuré. Leur définition est stockée dans le répertoire /etc/yum.repos.d ou /etc/apt/sources.list.

Il est important d'effectuer une mise à jour pour avoir la dernière version des logiciels ainsi que les derniers correctifs de sécurité.

Sur les systèmes à base de RedHat, la commande 'yum update' ou 'yum upgrade' permet d'effectuer la mise à jour.

Sur les systèmes dérivés de Debian, la commande 'apt-get upgrade' permet d'effectuer cette mise à jour.

Installation du système

Les méthodes d'installation alternatives

- DVD
- Net Install
- Minimal Install

Les méthodes d'installation alternatives

Il existe différents types d'installation possible. Le plus commun étant d'installer Linux à partir d'un DVD d'installation ou d'une image iso contenant le DVD si vous faites l'installation dans un environnement virtualisé.

Lors de l'installation via le DVD, vous devez répondre à certains nombre de questions comme la langue d'installation, le type de clavier, etc....
Par défaut l'installation propose un partitionnement standard et met la racine sous le contrôle de LVM (Logical Volume Manager). Cela permet d'étendre à chaud la taille du système de fichiers.

Un partitionnement personnalisé est toutefois possible.
Le type de partitionnement dépendra surtout de l'usage que vous allez faire de votre système. Pour un serveur de fichiers contenant les données des utilisateurs, on fera en sorte que /home soit bien dimensionné (Nombre d'utilisateurs fois la taille pour chaque utilisateur). Pour un serveur web la partition qui contient les cookies est /var.

Une installation Net Install est similaire à une installation à partir du DVD. La grande différence est qu'au lieu de copier les packages depuis le DVD, le système va les récupérer sur des dépôts logiciels existants.

L'installation Minimal Install comme son nom l'indique, installe le minimum nécessaire. A vous d'installer au fur et à mesure de vos besoins les différents logiciels.

Installation du système

Les environnements graphiques

- Les différents types de bureau
- Basculer d'un bureau à un autre
- Paramétrage d'une session X

Les environnements graphiques

Les systèmes Linux proposent des environnements graphiques que l'on peut installer (plutôt sur un poste de travail que sur un serveur). Le bureau le plus connu et utilisé est GNOME. D'autres interfaces graphiques existent, notamment KDE ou XFCE.

Lorsque vous installez le système d'exploitation, vous allez sélectionner l'environnement graphique que vous désirez installer (vous pouvez en choisir plusieurs). On peut aussi les installer au fur à mesure.

Si vous avez plusieurs environnements graphiques de disponible, vous devez sélectionner celui que vous utiliserez lors de la demande de connexion sur le système.

Installation du système

La connexion en mode graphique et ligne de commande

- ssh 10.20.30.40
- ssh root@10.20.30.40
- telnet, ftp

La connexion en mode graphique et ligne de commandes

La connexion via l'interface graphique se fait en cliquant sur le nom de l'utilisateur avec lequel on veut se connecter. Le mot de passe est alors demandé et la connexion s'établit si celui-ci est correct.

En ligne de commandes il existe plusieurs utilitaires pour se connecter. Il est recommandé d'exploiter que ceux qui utilisent un protocole sécurisé qui crypte la communication. Les outils tels que ftp et telnet sont dépréciés car leur connexion n'est pas sécurisée.

L'option -X de la commande ssh permet de déporter les applications graphiques exécutées sur le serveur en les affichant en local. L'option X11Forwarding doit être activée.

Notes

La gestion des logiciels

Dans ce chapitre, nous allons étudier l'installation et l'administration des packages, via les commandes rpm, yum et l'exploitation des sources.

Table des matières

La gestion des logiciels

Présentation

- Le format rpm (RedHat)
- Le format dpkg (Débian)
- Un dépôt logiciel : yum et apt-get
- Utilisation des sources

Présentation

Les logiciels sont fournis sous forme de packages. Il existe deux formats principaux de packages qui sont le format rpm (RedHat Package Manager) et le format dpkg (Debian Package).

Le format rpm est utilisé sur les distributions RedHat et leur dérivés (CentOS , Fedora, …) tandis que le format dpkg est utilisé pour les distributions Débian et leur dérivées (Ubuntu,...).

Une base de données des packages installés est interrogeable sur toutes les distributions. Elle est souvent localisée dans /var/lib.

L'installation des logiciels se fait grâce à la commande rpm ou dpkg. Ces commandes ne résolvent pas les dépendances entre les paquets. Cette méthode d'installation peut donc être très fastidieuse. Pour résoudre cette contrainte, des gestionnaires de paquets ont été développés. Ils intègrent notamment la résolution des dépendances, rendant ainsi l'installation beaucoup moins complexe. Les paquets sont téléchargés à partir d'internet ou d'une source locale (dépôt local, DVD).

Le gestionnaire de paquets redhat est yum (Yellow Update Manager) tandis que celui de Débian est apt-get (aptitude-get).

Il existe des interfaces graphiques utilisant ces gestionnaires pour une administration graphique.

Administration des packages

Administration des rpm

- Installation d'un rpm
- Désinstallation d'un rpm
- Interroger la base rpm

La gestion d'un package rpm

Installation du rpm ksh à partir du dvd d'installation :

Vérifions s'il est déjà installé :

```
# rpm -qa | grep ksh
```

Vérifions le chemin d'accès au lecteur DVD :

```
# df -h
Sys. de fichiers Taille UtilisÃ© Dispo Uti% MontÃ© sur
/dev/sda7          969M     31M  872M   4% /
devtmpfs           913M       0  913M   0% /dev
tmpfs              921M     92K  921M   1% /dev/shm
tmpfs              921M    8,8M  912M   1% /run
tmpfs              921M       0  921M   0% /sys/fs/cgroup
/dev/sda2          7,6G    3,5G  3,7G  49% /usr
/dev/sda6          1,9G     10M  1,8G   1% /home
/dev/sda1          969M     77M  826M   9% /boot
/dev/sda3          3,8G    596M  3,0G  17% /var
/dev/sda8          2,0G     33M  2,0G   2% /data
/dev/sr0           3,9G    3,9G     0 100% /run/media/theo/CentOS 7 x86_64
```

Déplacement vers le répertoire contenant les packages :

```
# cd /run/media/theo/CentOS\ 7\ x86_64/
# cd Packages/
# ls | grep ksh
ksh-20120801-19.el7.x86_64.rpm
```

Installation du rpm :

```
# rpm -i ksh-20120801-19.el7.x86_64.rpm
attention: ksh-20120801-19.el7.x86_64.rpm: Entête V3 RSA/SHA256 Signature, clé ID
f4a80eb5: NOKEY
```

Vérification de l'installation :

```
# rpm -qa | grep ksh
ksh-20120801-19.el7.x86_64
```

Suppression du rpm :

```
# rpm -e ksh-20120801-19.el7.x86_64
```

Vérification de la suppression :

```
# rpm -qa | grep ksh
```

Interrogation de la base de données rpm :

A quel package appartient un fichier :

```
# rpm -qf /etc/passwd
setup-2.8.71-4.el7.noarch
```

Quels fichiers sont contenus dans un package :

```
# rpm -ql setup-2.8.71-4.el7.noarch
/etc/aliases
/etc/bashrc
/etc/csh.cshrc
/etc/csh.login
/etc/environment
/etc/exports
/etc/filesystems
/etc/fstab
/etc/group
/etc/gshadow
/etc/host.conf
/etc/hosts
/etc/hosts.allow
/etc/hosts.deny
/etc/inputrc
/etc/motd
/etc/passwd
/etc/printcap
/etc/profile
/etc/profile.d
/etc/protocols
/etc/securetty
/etc/services
/etc/shadow
```

```
/etc/shells
/usr/share/doc/setup-2.8.71
/usr/share/doc/setup-2.8.71/COPYING
/usr/share/doc/setup-2.8.71/uidgid
/var/log/lastlog
```

Afficher des informations sur le package :

```
# rpm -qi setup-2.8.71-4.el7.noarch
Name        : setup
Version     : 2.8.71
Release     : 4.el7
Architecture: noarch
Install Date: jeu. 24 sept. 2015 10:48:17 CEST
Group       : System Environment/Base
Size        : 696310
License     : Public Domain
Signature   : RSA/SHA256, ven. 04 juil. 2014 06:59:13 CEST, Key ID 24c6a8a7f4a80eb5
Source RPM  : setup-2.8.71-4.el7.src.rpm
Build Date  : mar. 10 juin 2014 04:04:36 CEST
Build Host  : worker1.bsys.centos.org
Relocations : (not relocatable)
Packager    : CentOS BuildSystem <http://bugs.centos.org>
Vendor      : CentOS
URL         : https://fedorahosted.org/setup/
Summary     : A set of system configuration and setup files
Description :
The setup package contains a set of important system configuration and
setup files, such as passwd, group, and profile.
```

Afficher les dépendances du package :

```
# rpm -qR setup-2.8.71-4.el7.noarch
config(setup) = 2.8.71-4.el7
rpmlib(BuiltinLuaScripts) <= 4.2.2-1
rpmlib(CompressedFileNames) <= 3.0.4-1
rpmlib(FileDigests) <= 4.6.0-1
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
system-release
rpmlib(PayloadIsXz) <= 5.2-1
```

Afficher l'état des fichiers du package (normal, non installé ou remplacé) :

```
# rpm -qls setup-2.8.71-4.el7.noarch
normal        /etc/aliases
normal        /etc/bashrc
normal        /etc/csh.cshrc
normal        /etc/csh.login
normal        /etc/environment
normal        /etc/exports
normal        /etc/filesystems
normal        /etc/fstab
normal        /etc/group
normal        /etc/gshadow
normal        /etc/host.conf
normal        /etc/hosts
normal        /etc/hosts.allow
normal        /etc/protocols
normal        /etc/securetty
normal        /etc/services
normal        /etc/shadow
normal        /etc/shells
normal        /usr/share/doc/setup-2.8.71
normal        /var/log/lastlog
```

La gestion des logiciels

La gestion des logiciels avec yum

- Les dépôts logiciels
- Les fichiers de configuration
- La commande yum

La gestion des logiciels avec yum

L'utilisation d'un dépôt logiciel permet de simplifier l'installation des packages avec la résolution des dépendances.

Le fichier de configuration principal de yum est '/etc/yum.conf' :

```
# more /etc/yum.conf
[main]
cachedir=/var/cache/yum/$basearch/$releasever
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
installonly_limit=5
bugtracker_url=http://bugs.centos.org/set_project.php?project_id=23&ref=http://b
ugs.centos.org/bug_report_page.php?category=yum
distroverpkg=centos-release

#  This is the default, if you make this bigger yum won't see if the metadata
# is newer on the remote and so you'll "gain" the bandwidth of not having to
# download the new metadata and "pay" for it by yum not having correct
# information.
#  It is esp. important, to have correct metadata, for distributions like
# Fedora which don't keep old packages around. If you don't like this checking
# interupting your command line usage, it's much better to have something
# manually check the metadata once an hour (yum-updatesd will do this).
# metadata_expire=90m

# PUT YOUR REPOS HERE OR IN separate files named file.repo
# in /etc/yum.repos.d
```

Si un paramètre est égale à 0 cela signifie qu'il est désactivé, s'il est égal à 1 alors il est activé.

Les différents dépôts sont listés dans /etc/yum.repos.d :

```
# ls /etc/yum.repos.d/
CentOS-Base.repo  CentOS-Debuginfo.repo  CentOS-Sources.repo  CentOS-Vault.repo
```

La configuration du dépôt CentOS-Base :

```
# more CentOS-Base.repo
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client.  You should use this for CentOS updates
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#

[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=os
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=updates
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=extras
#baseurl=http://mirror.centos.org/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo
=centosplus
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

Les différentes commandes yum

Information sur un package :

```
# yum info ksh
Modules complÃ©mentaires chargés : fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
Paquets disponibles
Nom                 : ksh
Architecture        : x86_64
Version             : 20120801
Révision            : 22.el7_1.2
Taille              : 880 k
Dépôt               : updates/7/x86_64
Résumé              : The Original ATT Korn Shell
URL                 : http://www.kornshell.com/
Licence             : EPL
Description         : KSH-93 is the most recent version of the KornShell by
                    : David Korn of AT&T Bell Laboratories.
                    : KornShell is a shell programming language, which is upward
                    : compatible with "sh" (the Bourne Shell).
```

Vérifier si un package est disponible sur un dépôt :

```
# yum list ksh
Modules complémentaires chargés: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
Paquets disponibles
ksh.x86_64                      20120801-22.el7_1.2                     updates
```

Vérifier si un package est installé :

```
# yum list installed | grep ksh
```

Liste des packages récemment installés :

```
# yum list recent
Modules complémentaires chargés: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
Paquets récemment ajoutés
firefox.i686                    38.3.0-2.el7.centos                     updates
firefox.x86_64                  38.3.0-2.el7.centos                     updates
grub2.x86_64                    1:2.02-0.17.0.1.el7.centos.4            updates
grub2-efi.x86_64                1:2.02-0.17.0.1.el7.centos.4            updates
grub2-efi-modules.x86_64        1:2.02-0.17.0.1.el7.centos.4            updates
grub2-tools.x86_64              1:2.02-0.17.0.1.el7.centos.4            updates
libstoraged.x86_64              2.2.0-2.el7                             extras
libstoraged-devel.x86_64        2.2.0-2.el7                             extras
storaged.x86_64                 2.2.0-2.el7                             extras
storaged-iscsi.x86_64           2.2.0-2.el7                             extras
storaged-lvm2.x86_64            2.2.0-2.el7                             extras
```

Lister les dépôts logiciels disponibles :

```
# yum repolist
Modules complémentaires chargés: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
id du dépôt                          nom du dépôt                          statut
base/7/x86_64                        CentOS-7 - Base                       8 652
extras/7/x86_64                      CentOS-7 - Extras                       214
updates/7/x86_64                     CentOS-7 - Updates                    1 486
repolist: 10 352
```

Obtenir des informations sur un groupe de packages :

```
# yum groupinfo kde
Modules complémentaires chargés: fastestmirror, langpacks
Aucun fichier de groupe n'est installé.
Maybe run: yum groups mark convert (see man yum)
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr

Groupe: KDE
 ID du groupe: kde-desktop
 Description : KDE Plasma Workspaces est une interface utilisateur graphique hautement
configurable qui inclut un panneau, un bureau, des icônes système, des éléments
graphiques de bureau, ainsi que de nombreuses puissantes applications KDE.
 Paquets obligatoires:
    abrt-desktop
   +akonadi
   +akonadi-mysql
   +ark
   +bluedevil
   +colord-kde
    cups-pk-helper
    firewall-config
    firstboot
    gdm
   +gwenview
    initial-setup
   +initial-setup-gui
   +kamera
   +kcalc
   +kcharselect
   +kcm-gtk
   +kcm_touchpad
   +kcolorchooser
   +kde-base-artwork
   +kde-baseapps
   +kde-plasma-networkmanagement
   +kde-print-manager
   +kde-runtime
   +kde-settings-pulseaudio
   +kde-wallpapers
   +kde-workspace
   +kdeaccessibility
   +kdeadmin
   +kdegraphics-strigi-analyzer
   +kdegraphics-thumbnailers
   +kdelibs
   +kdenetwork-kdnssd
   +kdenetwork-kget
```

```
   +kdenetwork-krfb
   +kdepim
   +kdeplasma-addons
   +kdeutils-minimal
   +kgpg
   +kmix
   +konsole
   +kruler
   +ksaneplugin
   +ksnapshot
   +ksshaskpass
   +kwrite
   +okular
   +oxygen-gtk
   +phonon-backend-gstreamer
   +plasma-scriptengine-python
   +redhat-access-gui
    setroubleshoot
   +sweeper
   +system-config-date
   +xsettings-kde
   +xterm
 Paquets conditionnels:
   +pinentry-qt
```

Afficher quel package fournit une fonctionnalité :

```
# yum provides ksh
Modules complÃ©mentaires chargÃ©sÂ : fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
ksh-20120801-22.el7.x86_64 : The Original ATT Korn Shell
Dépôt                : base



ksh-20120801-22.el7_1.1.x86_64 : The Original ATT Korn Shell
Dépôt                : updates



ksh-20120801-22.el7_1.2.x86_64 : The Original ATT Korn Shell
Dépôt                : updates
```

Afficher les dépendances d'un package :

```
# yum deplist bash
Modules complÃ©mentaires chargÃ©sÂ : fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
paquet : bash.x86_64 4.2.46-12.el7
  dépendance    : libc.so.6(GLIBC_2.15)(64bit)
   provider: glibc.x86_64 2.17-78.el7
  dépendance    : libdl.so.2()(64bit)
   provider: glibc.x86_64 2.17-78.el7
  dépendance    : libdl.so.2(GLIBC_2.2.5)(64bit)
   provider: glibc.x86_64 2.17-78.el7
  dépendance    : libtinfo.so.5()(64bit)
   provider: ncurses-libs.x86_64 5.9-13.20130511.el7
  dépendance    : rtld(GNU_HASH)
   provider: glibc.x86_64 2.17-78.el7
   provider: glibc.i686 2.17-78.el7
```

Installation d'un package :

Avec l'option -y sur la ligne de commande, la confirmation n'est pas demandée.

```
# yum install nmap
Modules complémentaires chargés: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: mirrors.atosworldline.com
 * updates: mirror.in2p3.fr
Résolution des dépendances
--> Lancement de la transaction de test
---> Le paquet nmap.x86_64 2:6.40-4.el7 sera installé
--> Résolution des dépendances terminée

Dépendances résolues

================================================================================
 Package            Architecture         Version                     Dépôt       Taille
================================================================================
Installation :
 nmap               x86_64               2:6.40-4.el7                base        3.9 M

Résumé de la transaction
================================================================================
Installation   1 Paquet

Taille totale des téléchargements: 3.9 M
Taille d'installation: 16 M
Is this ok [y/d/N]: y
Downloading packages:

nmap-6.40-4.el7.x86_64.rpm       12% [==-              ]  0.0 B/s | 507 kB  --:--:-- ETA

nmap-6.40-4.el7.x86_64.rpm       35% [=======-         ] 875 kB/s | 1.4 MB  00:00:02 ETA

nmap-6.40-4.el7.x86_64.rpm       60% [============      ] 1.0 MB/s | 2.4 MB  00:00:01 ETA

nmap-6.40-4.el7.x86_64.rpm       85% [============-     ] 1.1 MB/s | 3.4 MB  00:00:00 ETA
attentionÂ : /var/cache/yum/x86_64/7/base/packages/nmap-6.40-4.el7.x86_64.rpm: Entête V3
RSA/SHA256 Signature, clé ID f4a80eb5: NOKEY
La clé publique pour nmap-6.40-4.el7.x86_64.rpm n'est pas installée

nmap-6.40-4.el7.x86_64.rpm                                          | 3.9 MB  00:00:01
Récupération de la clé à partir de file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importation de la clef GPG 0xF4A80EB5Â :
ID utilisateur: CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>
Empreinte     : 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8 0eb5
Paquet        : centos-release-7-0.1406.el7.centos.2.3.x86_64 (@anaconda)
Provient de   : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Est-ce correct [o/N]Â : o
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

  Installation : 2:nmap-6.40-4.el7.x86_64                                   1/1
  Vérification : 2:nmap-6.40-4.el7.x86_64                                   1/1

Installé :
  nmap.x86_64 2:6.40-4.el7

Terminé !
```

Vérification de l'installation du package :

```
# yum list installed | grep nmap
nmap.x86_64                             2:6.40-4.el7                    @base
nmap-ncat.x86_64                        2:6.40-4.el7                    @anaconda
```

Suppression d'un package :

```
# yum erase nmap
Modules complémentaires chargés :fastestmirror, langpacks
Résolution des dépendances
--> Lancement de la transaction de test
---> Le paquet nmap.x86_64 2:6.40-4.el7 sera effacé
--> Résolution des dépendances terminée

Dépendances résolues

================================================================================
 Package            Architecture         Version                   Dépôt         Taille
================================================================================
Suppression :
 nmap               x86_64               2:6.40-4.el7              @base          16 M

Résumé de la transaction
================================================================================
Supprimer  1 Paquet

Taille d'installation : 16 M
Est-ce correct [o/N] : o
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

  Suppression  : 2:nmap-6.40-4.el7.x86_64
1/1

  Vérification : 2:nmap-6.40-4.el7.x86_64
1/1

Supprimé :
  nmap.x86_64 2:6.40-4.el7

Terminé !
```

Installer un groupe de package :

```
# yum  groupinstall  kde-desktop
```

La gestion des logiciels

La gestion d'un package dpkg

- Le format dpkg (debian)
- dpkg -l -i -r
  -L -S -s

La gestion d'un package dpkg

Installation du package ksh à partir du dvd 2 de Débian:

Vérifions s'il est déjà installé :

```
# dpkg -l | grep ksh
```

Vérifions le chemin d'accès au lecteur DVD :

```
# df -h
Sys. de fichiers                    Taille Utilisé Dispo Uti% Monté sur
/dev/dm-0                             7,0G    3,5G  3,2G  53% /
udev                                   10M       0   10M   0% /dev
tmpfs                                 405M    5,9M  399M   2% /run
tmpfs                                1012M     92K 1012M   1% /dev/shm
tmpfs                                 5,0M    4,0K  5,0M   1% /run/lock
tmpfs                                1012M       0 1012M   0% /sys/fs/cgroup
/dev/mapper/poste--debian8--vg-var    2,7G    337M  2,3G  13% /var
/dev/mapper/poste--debian8--vg-tmp    360M    2,1M  335M   1% /tmp
/dev/mapper/poste--debian8--vg-home   7,9G     23M  7,5G   1% /home
/dev/sda1                             236M     32M  192M  15% /boot
tmpfs                                 203M    8,0K  203M   1% /run/user/1000
/dev/sr0                              4,3G    4,3G     0 100% /media/cdrom0
```

Déplacement vers le répertoire contenant les packages :

```
# cd /media/cdrom/pool/main/k/ksh
# ls
ksh_93u+20120801-1_i386.deb
```

Installation du package:

```
# dpkg -i ksh_93u+20120801-1_i386.deb
Sélection du paquet ksh précédemment désélectionné.
(Lecture de la base de données... 139083 fichiers et répertoires déjà installés.)
Préparation du dépackage de ksh_93u+20120801-1_i386.deb ...
Dépackage de ksh (93u+20120801-1) ...
Paramétrage de ksh (93u+20120801-1) ...
update-alternatives: utilisation de « /bin/ksh93 » pour fournir « /bin/ksh » (ksh) en
mode automatique
Traitement des actions différées (« triggers ») pour man-db (2.7.0.2-5) ...
```

Vérification de l'installation :

```
# dpkg -l | grep ksh
ii  ksh       93u+20120801-1       i386         Real, AT&T version of the Korn shell
```

Suppression du package:

```
# dpkg -r ksh
(Lecture de la base de données... 139103 fichiers et répertoires déjà installés.)
Suppression de ksh (93u+20120801-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.7.0.2-5) ...
```

Vérification de la suppression :

```
# dpkg -l | grep ksh
rc  ksh       93u+20120801-1     i386         Real, AT&T version of the Korn shell
```

Le package a été supprimé mais il a gardé la définition des fichiers de configuration en cas de réinstallation. Il faut utiliser l'option purge pour tout supprimer.

```
# dpkg -P ksh
(Lecture de la base de données... 139082 fichiers et répertoires déjà installés.)
Suppression de ksh (93u+20120801-1) ...
Purge des fichiers de configuration de ksh (93u+20120801-1) …
```

```
# dpkg -l | grep ksh
```

Interrogation de la base de données Débian:

A quel package appartient un fichier :

```
# dpkg -S /usr/bin/passwd
passwd: /usr/bin/passwd
```

Quels fichiers sont contenus dans un package :

```
# dpkg -L passwd
/.
/sbin
```

```
/sbin/shadowconfig
/etc
/etc/pam.d
/etc/pam.d/newusers
/etc/pam.d/chpasswd
/etc/pam.d/chsh
/etc/pam.d/chfn
/etc/pam.d/passwd
...
```

Afficher des informations sur le package :

```
# dpkg -s passwd
Package: passwd
Status: install ok installed
Priority: required
Section: admin
Installed-Size: 2156
Maintainer: Shadow package maintainers <pkg-shadow-devel@lists.alioth.debian.org>
Architecture: i386
Multi-Arch: foreign
Source: shadow
Version: 1:4.2-3+deb8u1
Replaces: manpages-tr (<< 1.0.5), manpages-zh (<< 1.5.1-1)
Depends: libaudit1 (>= 1:2.2.1), libc6 (>= 2.8), libpam0g (>= 0.99.7.1), libselinux1 (>=
1.32), libsemanage1 (>= 2.0.3), libpam-modules, debianutils (>= 2.15.2)
Conffiles:
 /etc/cron.daily/passwd db990990933b6f56322725223f13c2bc
 /etc/default/useradd cc9f9a7713ab62a32cd38363d958f396
 /etc/pam.d/chfn 4d466e00a348ba426130664d795e8afa
 /etc/pam.d/chpasswd 9900720564cb4ee98b7da29e2d183cb2
 /etc/pam.d/chsh a6e9b589e90009334ffd030d819290a6
 /etc/pam.d/newusers 1454e29bfa9f2a10836563e76936cea5
 /etc/pam.d/passwd eaf2ad85b5ccd06cceb19a3e75f40c63
Description: change and administer password and group data
 This package includes passwd, chsh, chfn, and many other programs to
 maintain password and group data.
 .
 Shadow passwords are supported.  See /usr/share/doc/passwd/README.Debian
Homepage: http://pkg-shadow.alioth.debian.org/
```

La gestion des logiciels

La gestion des packages avec aptitude

- Les dépôts logiciels
- Les fichiers de configuration
- La commande apt-get

La gestion des packages avec aptitude

L'utilisation d'un dépôt logiciel permet de simplifier l'installation des packages avec la résolution des dépendances.

Aptitude est le gestionnaire de package Débian qui encapsule les commandes dpkg. La commande aptitude permet d'exécuter une interface de gestion des packages.

L'équivalent en ligne de commande est la commande apt-get. La configuration d'apt est stocké dans le répertoire /etc/apt. Les dépôts logiciels sont listés dans le fichier sources.list.

```
# cat /etc/apt/sources.list
#

# deb cdrom:[Debian GNU/Linux 8.2.0 _Jessie_ - Official i386 DVD Binary-1 20150906-
10:02]/ jessie contrib main

deb cdrom:[Debian GNU/Linux 8.2.0 _Jessie_ - Official i386 DVD Binary-1 20150906-10:02]/
jessie contrib main

deb http://ftp.fr.debian.org/debian/ jessie main
deb-src http://ftp.fr.debian.org/debian/ jessie main

deb http://security.debian.org/ jessie/updates main contrib
deb-src http://security.debian.org/ jessie/updates main contrib

# jessie-updates, previously known as 'volatile'
deb http://ftp.fr.debian.org/debian/ jessie-updates main contrib
deb-src http://ftp.fr.debian.org/debian/ jessie-updates main contrib
```

Dans le répertoire /etc/apt/apt.conf.d se trouve une partie de la configuration d'apt. D'autres sources de dépôts sont définis dans /etc/apt/sources.list.d.

Les différentes commandes apt-get

Information sur un package :

```
# apt-cache showpkg  bash
Package: bash
Versions:
4.3-11+deb8u1 (/var/lib/apt/lists/ftp.fr.debian.org_debian_dists_jessie_main_binary-
i386_Packages) (/var/lib/dpkg/status)
 Description Language:
…
Reverse Depends:
  mysql-server-5.5,passwd
  mariadb-server-10.0,passwd
  ziproxy,passwd
…
Dependencies:
1:4.2-3+deb8u1 - libaudit1 (2 1:2.2.1) libc6 (2 2.8) libpam0g (2 0.99.7.1) libselinux1 (2
1.32) libsemanage1 (2 2.0.3) libpam-modules (0 (null)) debianutils (2 2.15.2) manpages-tr
(3 1.0.5) manpages-zh (3 1.5.1-1)
1:4.2-3 - libaudit1 (2 1:2.2.1) libc6 (2 2.8) libpam0g (2 0.99.7.1) libselinux1 (2 1.32)
libsemanage1 (2 2.0.3) libpam-modules (0 (null)) debianutils (2 2.15.2) manpages-tr (3
1.0.5) manpages-zh (3 1.5.1-1)
Provides:
1:4.2-3+deb8u1 -
1:4.2-3 -
Reverse Provides:
```

```
# apt-cache show bash
Package: bash
Version: 4.3-11+deb8u1
Essential: yes
Installed-Size: 5073
Maintainer: Matthias Klose <doko@debian.org>
Architecture: i386
Replaces: bash-completion (<< 20060301-0), bash-doc (<= 2.05-1)
Depends: base-files (>= 2.1.12), debianutils (>= 2.15)
Pre-Depends: dash (>= 0.5.5.1-2.2), libc6 (>= 2.15), libncurses5 (>= 5.5-5~), libtinfo5
…
```

Installation d'un package :

```
# apt-get install ksh
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  ksh
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1 548 ko dans les archives.
Après cette opération, 3 138 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://ftp.fr.debian.org/debian/ jessie/main ksh i386 93u+20120801-1 [1
548 kB]
1 548 ko réceptionnés en 0s (5 983 ko/s)
Sélection du paquet ksh précédemment désélectionné.
(Lecture de la base de données... 139083 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../ksh_93u+20120801-1_i386.deb ...
Dépaquetage de ksh (93u+20120801-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.7.0.2-5) ...
```

```
Paramétrage de ksh (93u+20120801-1) ...
update-alternatives: utilisation de « /bin/ksh93 » pour fournir « /bin/ksh » (ksh) en
mode automatique
```

Suppression d'un package :

```
# apt-get remove nmap
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants seront ENLEVÉS :
  gnome gnome-nettool nmap
0 mis à jour, 0 nouvellement installés, 3 à enlever et 0 non mis à jour.
Après cette opération, 20,7 Mo d'espace disque seront libérés.
Souhaitez-vous continuer ? [O/n] O
(Lecture de la base de données... 139103 fichiers et répertoires déjà installés.)
Suppression de gnome (1:3.14+3) ...
Suppression de gnome-nettool (3.8.1-1) ...
Suppression de nmap (6.47-3+deb8u2) ...
Traitement des actions différées (« triggers ») pour hicolor-icon-theme (0.13-1) ...
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.22-1) ...
Traitement des actions différées (« triggers ») pour gnome-menus (3.13.3-6) ...
Traitement des actions différées (« triggers ») pour mime-support (3.58) ...
Traitement des actions différées (« triggers ») pour libglib2.0-0:i386 (2.42.1-1+b1) ...
Traitement des actions différées (« triggers ») pour man-db (2.7.0.2-5) …
```

Administration des packages

Installation et compilation à partir des fichiers sources

- Le fichier source
- Le fichier Makefile
- Le compilateur gcc
- Les étapes de la compilation

Installation et compilation à partir des fichiers sources

L'installation à partir des sources permet d'installer un programme correspondant au plus près de votre architecture matérielle. Il faut d'abord récupérer le fichier source.

Un compilateur est nécessaire. Si besoin installer 'gcc' (Gnu Compiler Collection).

Récupération des sources sur le site gnu.org :

```
# wget  ftp://ftp.gnu.org/gnu/hello/hello-2.9.tar.gz
--2015-09-24 15:21:33--  ftp://ftp.gnu.org/gnu/hello/hello-2.9.tar.gz
           => «hello-2.9.tar.gz»
RÃ©solution de ftp.gnu.org (ftp.gnu.org)... 208.118.235.20, 2001:4830:134:3::b
Connexion vers ftp.gnu.org (ftp.gnu.org)|208.118.235.20|:21...connecté.
Ouverture de session en anonymous...Session établie!
==> SYST ... complété.    ==> PWD ... complété.
==> TYPE I ... complété.  ==> CWD (1) /gnu/hello ... complété.
==> SIZE hello-2.9.tar.gz ... 723645
==> PASV ... complété.    ==> RETR hello-2.9.tar.gz ... complété.
Longueur: 723645 (707K) (non certifiée)


 0% [                                       ] 0           --.-K/s
 5% [=>                                     ] 42 944       204KB/s
35% [============>                          ] 256 296      409KB/s
78% [==========================>            ] 567 120      676KB/s
100%[======================================>] 723 645      412KB/s
100%[======================================>] 723 645      412KB/s   ds 1,7s

2015-09-24 15:21:36 (412 KB/s) - «hello-2.9.tar.gz» sauvegardé [723645]
```

```
# ls
anaconda-ks.cfg  hello-2.9.tar.gz  initial-setup-ks.cfg
```

Extraction de l'archive :

```
# tar zxf hello-2.9.tar.gz

# ls
anaconda-ks.cfg  hello-2.9  hello-2.9.tar.gz  initial-setup-ks.cfg
# cd hello-2.9/
# ls
ABOUT-NLS   ChangeLog.O   COPYING      m4           NEWS            src
aclocal.m4  config.in     doc          maint.mk     po              tests
AUTHORS     configure     GNUmakefile  Makefile.am  README          THANKS
build-aux   configure.ac  INSTALL      Makefile.in  README-dev      TODO
ChangeLog   contrib       lib          man          README-release
```

Le fichier 'README' contient les instructions pour compiler ce programme. Lisez-le si vous n'êtes pas sûr des différentes étapes à effectuer.

Le script 'configure' va s'appuyer sur les fichiers 'Makefile.am' et 'Makefile.in' pour générer un fichier 'Makefile' correspondant à notre architecture matérielle.

```
# ./configure
checking for a BSD-compatible install... /bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
..............
..............
configure: creating ./config.status
config.status: creating Makefile
config.status: creating contrib/Makefile
config.status: creating doc/Makefile
config.status: creating lib/Makefile
config.status: creating man/Makefile
config.status: creating po/Makefile.in
config.status: creating src/Makefile
config.status: creating tests/Makefile
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing po-directories commands
config.status: creating po/POTFILES
config.status: creating po/Makefile
```

Le script 'configure' a généré le fichier 'Makefile' sur lequel va s'appuyer la commande 'make' pour compiler notre programme.

```
# ls
ABOUT-NLS     config.h        contrib      m4           NEWS             stamp-h1
aclocal.m4    config.in       COPYING      maint.mk     po[              tests
AUTHORS       config.log      doc          Makefile     README           THANKS
build-aux     mconfig.status  GNUmakefile  Makefile.am  README-dev       TODO
ChangeLog     configure       INSTALL      Makefile.in  README-release
ChangeLog.O   configure.ac    lib          man          src
```

Exécution de la commande 'make' pour compiler le programme :

```
# make
make  all-recursive
make[1]: Entering directory `/root/hello-2.9'
Making all in contrib
make[2]: Entering directory `/root/hello-2.9/contrib'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/hello-2.9/contrib'
Making all in lib
make[2]: Entering directory `/root/hello-2.9/lib'
....................
....................
Making all in tests
make[2]: Entering directory `/root/hello-2.9/tests'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/hello-2.9/tests'
make[2]: Entering directory `/root/hello-2.9'
make[2]: Leaving directory `/root/hello-2.9'
make[1]: Leaving directory `/root/hello-2.9'
```

Il ne reste plus qu'à installer le programme grâce à la commande 'make install'.

```
# make install
make[2]: Entering directory `/root/hello-2.9/tests'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/hello-2.9/tests'
make[2]: Entering directory `/root/hello-2.9'
make[2]: Leaving directory `/root/hello-2.9'
make[1]: Leaving directory `/root/hello-2.9'
.................
```

Par défaut, le binaire est installé dans /usr/local/bin/hello.

```
# whereis hello
hello: /usr/local/bin/hello
```

Notre variable PATH contient le répertoire /usr/local/bin, nous pouvons donc utiliser la commande directement.

```
# echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
# hello
Hello, world!
```

Notes

La gestion du stockage

Dans ce chapitre, nous allons étudier l'administration et la maintenance des disques.

Table des matières

Gestion des disques

Types et nommage des disques

- Les différents types de disques
- Les règles de nommage des disques
- Les unités de stockage USB

Terminologie

Les disques de type IDE seront nommés de la façon suivante :

/dev/hd**a** → **1**er disque IDE

/dev/hd**b** → **2**ème disque IDE

Si les disques sont partitionnés, le numéro de la partition suit la lettre du disque :

/dev/hd**c2** → **2**ème partition du **3**ème disque IDE

Les disques de type de SATA, SCSI, USB sont nommés de la façon suivante :

/dev/sd**a** → **1**er disque de type SCSI

/dev/sd**b** → **2**ème disque de type SCSI

Comme pour les disques IDE, un numéro suivant la lettre du disque indique le numéro de la partition :

/dev/sd**d5** → **5**ème partition du **4**ème disque SCSI

Les disques USB sont détectés comme des disques SCSI. Il sont nommés /dev/sdXY où X représente la lettre affecté au disque. Le système utilise la 1ère lettre disponible (b si vous avez un seul disque). Y représente la partition sur le disque (1 en général car les clefs USB ne sont pas partitionnées).

Lorsque vous branchez un disque sur des systèmes récents, il est monté automatiquement. Dans un environnement graphique, une icône est créée sur le bureau. Pour savoir sous quel nom le disque est détecté, il faut consulter le fichier /var/adm/messages.

Si le disque USB n'est pas monté automatiquement, la commande suivante permet de le faire.

```
# mount –t vfat /dev/sdb1 /mnt/usb

# mount –t ntfs /dev/sdb1 /mnt/usb
```

Remarque : Pour utiliser des périphériques amovibles contenant un système de fichiers NTFS, il faut installer le package ntfs-3g.

La gestion du stockage

La table de partition MBR

- Présentation de la MBR
- Les partitions primaires
- Les partitions étendues

La table de partition MBR

La MBR (Master Boot Record) contient les informations sur la structure de votre disque (nombre de secteurs, de pistes, de cylindres, taille, géométrie,...)

Elle est toujours située sur le 1er secteur du disque. Un secteur représente 512 octets. Dans la MBR un chargeur de démarrage est installé (LILO, GRUB, GRUB 2) qui a pour tâche de charger le noyau en mémoire.

Les 446 premiers octets contiennent la géométrie du disque et le chargeur de démarrage. Les 64 octets suivants contiennent la table de partitionnement.

Les 2 derniers octets contiennent un code hexadécimal normalement égale à 'aa55' indiquant que la MBR est valide.

Les disques ne peuvent que contenir 4 partitions principales dû à l'architecture du disque lors de sa fabrication. Ainsi si vous créez 4 partitions principales et qu'il reste de l'espace disponible sur le disque, cet espace n'est pas utilisable. La taille d'une partition est limitée à 2.2 To.

Pour dépasser la limitation de 4 partitions , il faut créer une partition étendue. Dans cette dernière, les partitions créées sont appelées partitions logiques.

La partition étendue jouera le rôle d'une base de données pour adresser les partitions logiques.

Le nombre maximum de partitions que l'on peut créer, toutes partitions confondues, est de 15.

Le fichiers spéciaux sont des fichiers qui représentent des périphériques. Sur un système Linux, le terminal ou le disque dur sont vus comme des fichiers qu'on appelle fichiers spéciaux. A la place de la taille du fichier, deux chiffres indiquent le numéro de majeur et le numéro de mineur du périphérique.

Les disques durs utilisent un driver de type 'sd'. Chaque disque dur pouvant contenir jusqu'à 15 partitions, le premier disque verra les numéros de mineur 1 à 15 affectés à ces partitions (le 0 est réservé pour le disque entier). Le numéro de mineur 16 représente le deuxième disque et les numéros 17 à 31 seront utilisés pour les partitions. Le 'b' pour le type de fichier indique que le périphérique fonctionne en mode bloc.

```
# ls -l /dev/sd*
brw-rw---- 1 root disk 8,  0 sept. 24 16:49 /dev/sda
brw-rw---- 1 root disk 8,  1 sept. 24 16:49 /dev/sda1
brw-rw---- 1 root disk 8,  2 sept. 24 16:49 /dev/sda2
brw-rw---- 1 root disk 8,  5 sept. 24 16:49 /dev/sda5
brw-rw---- 1 root disk 8,  6 sept. 24 16:49 /dev/sda6
brw-rw---- 1 root disk 8,  7 sept. 24 16:49 /dev/sda7
brw-rw---- 1 root disk 8,  8 sept. 24 16:49 /dev/sda8
brw-rw---- 1 root disk 8, 16 sept. 24 16:49 /dev/sdb
brw-rw---- 1 root disk 8, 32 sept. 24 16:49 /dev/sdc
brw-rw---- 1 root disk 8, 48 sept. 24 16:49 /dev/sdd
brw-rw---- 1 root disk 8, 64 sept. 24 16:49 /dev/sde
brw-rw---- 1 root disk 8, 80 sept. 24 16:49 /dev/sdf
```

Correspondance entre le driver et le numéro de majeur :

```
# more /proc/devices
Character devices:
  1 mem
  4 /dev/vc/0
  4 tty
  4 ttyS
  5 /dev/tty
  5 /dev/console
  5 /dev/ptmx
  6 lp
  7 vcs
 10 misc
 13 input
116 alsa
128 ptm
136 pts
180 usb
189 usb_device
251 hidraw
252 bsg
253 watchdog
254 rtc

Block devices:
259 blkext
  8 sd
 11 sr
 65 sd
 66 sd
 67 sd
 68 sd
 69 sd
 70 sd
 71 sd
...
```

Affichage des partitions détectées par le noyau :

```
# more /proc/partitions
major minor  #blocks  name

  11        0    4476888 sr0
   8       64    2097152 sde
   8       32    2097152 sdc
   8       16    2097152 sdb
   8        0   20971520 sda
   8        1    7629824 sda1
   8        2          1 sda2
   8        5    2928640 sda5
   8        6    1376256 sda6
   8        7     389120 sda7
   8        8    8641536 sda8
   8       48    2097152 sdd
   8       80    2097152 sdf
```

Pour identifier ses partitions, le système utilise un UUID ou un label. Le principal intérêt réside dans le fait que l'UUID ou le label d'un disque n'est pas modifié lorsque son emplacement physique est modifié.

Pour avoir la correspondance entre l'UUID ou le label d'un disque avec son nom, il faut consulter les répertoires présents dans /dev/disks.

```
# ls -l /dev/disk/by-uuid/
total 0
lrwxrwxrwx 1 root root  9 sept. 28 10:35 2015-09-06-10-27-28-00 -> ../../sr0
lrwxrwxrwx 1 root root 10 sept. 28 10:35 2c5e6590-cbc4-42c9-bd31-d482720fa183 -> ../../sda8
lrwxrwxrwx 1 root root 10 sept. 28 10:35 53e59d78-4a46-4bcc-9d28-0e315d23f49d -> ../../sda5
lrwxrwxrwx 1 root root 10 sept. 28 14:21 84b75605-e60d-4dff-8dea-537f8c49c795 -> ../../sdd1
lrwxrwxrwx 1 root root 10 sept. 28 10:35 977c9c97-7821-4b2e-aed9-7b97ab3871f2 -> ../../sda1
lrwxrwxrwx 1 root root 10 sept. 28 10:35 f9e2f47b-1a30-4cb6-b2ba-e632b5f6e805 -> ../../sda6
lrwxrwxrwx 1 root root 10 sept. 28 10:35 fd07275b-c82a-4aea-a69f-7b36288846d5 -> ../../sda7
```

```
# ls -l /dev/disk/by-label/
total 0
lrwxrwxrwx 1 root root 9 sept. 28 10:35 Debian\x208.2.0\x20i386\x201 -> ../../sr0
```

La commande blkid permet d'afficher les informations sur les partitions.

```
# blkid /dev/sda1
/dev/sda1: UUID="7c74fc34-c368-428a-a806-a8f3258da52c" TYPE="swap" PARTUUID="000d15e6-01"
# blkid /dev/sda2
/dev/sda2: UUID="02127890-e0fe-48bc-b903-123c4d655e23" UUID_SUB="0874dfd3-ddc7-4fbc-9df4-
0bf999bd443b" TYPE="btrfs" PTTYPE="dos" PARTUUID="000d15e6-02"
# blkid /dev/sda3
/dev/sda3: UUID="9ca23d55-5a3b-4460-b9a9-ff71594d5fd0" TYPE="xfs" PARTUUID="000d15e6-03"
```

La commande findfs permet de faire la correspondance entre le nom de la partition et l'UUID ou le label.

```
# findfs UUID="9ca23d55-5a3b-4460-b9a9-ff71594d5fd0"
/dev/sda3
```

La gestion du stockage

La table de partition GPT

- GUID Partition Table (GPT)
- Les partitions jusqu'à 9,4 Zo (2^73 octets)
- GPT primaire et GPT secondaire

La table de partition GPT

La table de partitionnement GPT remplace au fur à mesure la MBR dû aux limitations de cette dernière.
A l'inverse de la MBR, la table de partition GPT est stockée dans un en-tête GPT. IL n'y a plus de notions de partitions primaires ou partitions logiques. Ce sont toutes des partitions primaires si on utilise une terminologie MBR. Le nombre de partitions est limité à 128.

GPT utilise l'adressage logique des blocs (LBA) et non plus l'adressage en cylindres-pistes-secteurs. Chaque LBA fait une taille de 512 octets. Chaque partition est adressée sur 128 octets.

La structure interne de la GPT est la suivante :

LBA0 : Protective MBR
LBA1 : En-tête primaire GPT
LBA2 : Table de partitionnement (partition 1 à 4)
LBA3 : Table de partitionnement (partition 5 à 8)
…
LBA33 : Table de partitionnement (partition 125 à 128)

GPT Primaire

LBA34 : Partition 1
….
LBA X : Partition N-1
….
LBA Y : Partition N

N <= 128

….
LBA -33 : Table de partitionnement (partition 1 à 4)
LBA -32 : Table de partitionnement (partition 5 à 8)
…
LBA -2 : Table de partitionnement (partition 125 à 128)
LBA -1 : En-tête secondaire GPT

GPT Secondaire

Remarque : LBA -33 signifie LBA 33 à partir de la fin du disque

Gestion des disques

Le partitionnement avec fdisk

- Visualiser le partitionnement avec fdisk -l
- L'utilitaire fdisk en mode interactif
- La commande partprobe

Le partitionnement avec fdisk

La commande 'fdisk' sert à partitionner un disque. Il existe un mode interactif pour créer de nouvelles partitions sur un disque.

Lister les disques d'un système :

```
# fdisk -l

Disque /dev/sde : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Disque /dev/sdc : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Disque /dev/sda : 20 GiB, 21474836480 octets, 41943040 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0xee2fa967

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 15261695 15259648  7,3G 83 Linux
/dev/sda2       15263742 41940991 26677250 12,7G  5 Extended
/dev/sda5       15263744 21121023  5857280  2,8G 83 Linux
/dev/sda6       21123072 23875583  2752512  1,3G 82 Linux swap / Solaris
/dev/sda7       23877632 24655871   778240  380M 83 Linux
/dev/sda8       24657920 41940991 17283072  8,2G 83 Linux

Disque /dev/sdd : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
```

```
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Disque /dev/sdf : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
```

Remarque : la commande 'lsblk' liste les disques avec un affichage assez convivial :

```
# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   20G  0 disk
├─sda1   8:1    0  7,3G  0 part /
├─sda2   8:2    0    1K  0 part
├─sda5   8:5    0  2,8G  0 part /var
├─sda6   8:6    0  1,3G  0 part [SWAP]
├─sda7   8:7    0  380M  0 part /tmp
└─sda8   8:8    0  8,2G  0 part /home
sdb      8:16   0    2G  0 disk
sdc      8:32   0    2G  0 disk
sdd      8:48   0    2G  0 disk
sde      8:64   0    2G  0 disk
sdf      8:80   0    2G  0 disk
sr0     11:0    1  4,3G  0 rom
```

```
# lsblk --fs
NAME   FSTYPE  LABEL               UUID                                 MOUNTPOINT
sda
├─sda1 ext4                        977c9c97-7821-4b2e-aed9-7b97ab3871f2 /
├─sda2
├─sda5 ext4                        53e59d78-4a46-4bcc-9d28-0e315d23f49d /var
├─sda6 swap                        f9e2f47b-1a30-4cb6-b2ba-e632b5f6e805 [SWAP]
├─sda7 ext4                        fd07275b-c82a-4aea-a69f-7b36288846d5 /tmp
└─sda8 ext4                        2c5e6590-cbc4-42c9-bd31-d482720fa183 /home
sdb
sdc
sdd
sde
sdf
sr0    iso9660 Debian 8.2.0 i386 2 2015-09-06-10-41-49-00
```

Pour partitionner un disque :

```
# fdisk /dev/sdb

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Created a new DOS disklabel with disk identifier 0xd58f0f39.

Commande (m pour l'aide) : m

Aide :

  DOS (secteur d'amorçage)
   a   modifier un indicateur d'amorçage
   b   éditer l'étiquette BSD imbriquée du disque
   c   basculer l'indicateur de compatibilité DOS

  Générique
   d   supprimer la partition
   l   afficher les types de partitions connues
   n   ajouter une nouvelle partition
   p   afficher la table de partitions
   t   modifier le type d'une partition
   v   vérifier la table de partitions

  Autre
   m   afficher ce menu
   u   modifier les unités d'affichage et de saisie
   x   fonctions avancées (réservées aux spécialistes)

  Sauvegarder et quitter
   w   écrire la table sur le disque et quitter
   q   quitter sans enregistrer les modifications

  Créer une nouvelle étiquette
   g   créer une nouvelle table vide de partitions GPT
   G   créer une nouvelle table vide de partitions SGI (IRIX)
   o   créer une nouvelle table vide de partitions DOS
   s   créer une nouvelle table vide de partitions Sun


Commande (m pour l'aide) :
```

Afficher la table de partitionnement : option p
Nous constatons que le disque n'est pas partitionné et qu'il a une taille de 2Go.

```
# fdisk /dev/sdb

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Created a new DOS disklabel with disk identifier 0x92557139.

Commande (m pour l'aide) : p
Disque /dev/sdb : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x92557139
```

Création de nouvelles partitions : options n, p, e, l

```
# fdisk /dev/sdb

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Created a new DOS disklabel with disk identifier 0x3ed112b5.

Commande (m pour l'aide): n
Type de partition
   p   primaire (0 primaire, 0 étendue, 4 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) :ENTREE
Premier secteur (2048-4194303, 2048 par défaut) :ENTREE
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2048-4194303, 4194303 par défaut) :
+500M

Une nouvelle partition 1 de type « Linux » et de taille 500 MiB a été créée.

Commande (m pour l'aide) : p
Disque /dev/sdb : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x3ed112b5

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1        2048 1026047 1024000  500M 83 Linux


Commande (m pour l'aide) : n
Type de partition
   p   primaire (1 primaire, 0 étendue, 3 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (2-4, 2 par défaut) :ENTREE
Premier secteur (1026048-4194303, 1026048 par défaut) :ENTREE
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (1026048-4194303, 4194303 par défaut) :
+400M
```

```
Une nouvelle partition 2 de type « Linux » et de taille 400 MiB a été créée.

Commande (m pour l'aide) : n
Type de partition
   p   primaire (2 primaire, 0 étendue, 2 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : e
Numéro de partition (3,4, 3 par défaut) :ENTREE
Premier secteur (1845248-4194303, 1845248 par défaut) :ENTREE
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (1845248-4194303, 4194303 par défaut) :
+800M

Une nouvelle partition 3 de type « Extended » et de taille 800 MiB a été créée.

Commande (m pour l'aide) : n
Type de partition
   p   primaire (2 primaire, 1 étendue, 1 libre)
   l   logique (numéroté à partir de 5)
Sélectionnez (p par défaut) : l

Ajout de la partition logique 5
Premier secteur (1847296-3483647, 1847296 par défaut) :ENTREE
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (1847296-3483647, 3483647 par défaut) :
+400M

Une nouvelle partition 5 de type « Linux » et de taille 400 MiB a été créée.

Commande (m pour l'aide) : p
Disque /dev/sdb : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x3ed112b5

Device     Boot   Start     End Sectors  Size Id Type
/dev/sdb1          2048 1026047 1024000  500M 83 Linux
/dev/sdb2       1026048 1845247  819200  400M 83 Linux
/dev/sdb3       1845248 3483647 1638400  800M  5 Extended
/dev/sdb5       1847296 2666495  819200  400M 83 Linux


Commande (m pour l'aide) :
```

Tant que l'on n'a pas écrit la table de partitionnement sur le disque, le partitionnement est en mémoire. Si vous utilisez la lettre q pour quitter l'utilitaire fdisk, vous perdez la configuration du partitionnement. La lettre w (write) permet d'écrire le partitionnement sur le disque.

```
Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

Vérification du partitionnement :

```
# fdisk -l /dev/sdb

Disque /dev/sdb : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x3ed112b5

Device     Boot   Start     End Sectors  Size Id Type
/dev/sdb1          2048 1026047 1024000  500M 83 Linux
/dev/sdb2       1026048 1845247  819200  400M 83 Linux
/dev/sdb3       1845248 3483647 1638400  800M  5 Extended
/dev/sdb5       1847296 2666495  819200  400M 83 Linux
```

Vérification que le noyau ait bien pris en compte les nouvelles partitions :

```
# more /proc/partitions
major minor  #blocks  name

  11        0    4476888 sr0
   8       64    2097152 sde
   8       32    2097152 sdc
   8       16    2097152 sdb
   8       17     512000 sdb1
   8       18     409600 sdb2
   8       19          1 sdb3
   8       21     409600 sdb5
   8        0   20971520 sda
   8        1    7629824 sda1
   8        2          1 sda2
   8        5    2928640 sda5
   8        6    1376256 sda6
   8        7     389120 sda7
   8        8    8641536 sda8
   8       48    2097152 sdd
   8       80    2097152 sdf
```

Partitionnement d'un disque alors qu'il est en cours d'utilisation (un système de fichiers monté) :

```
# lsblk /dev/sdb
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sdb      8:16   0    2G  0 disk
├─sdb1   8:17   0  500M  0 part /data
├─sdb2   8:18   0  400M  0 part
└─sdb5   8:21   0  400M  0 part
```

Création d'une partition sur le deuxième disque.

```
# fdisk /dev/sdb

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.


Commande (m pour l'aide) : n
Type de partition
   p   primaire (2 primaire, 1 étendue, 1 libre)
   l   logique (numéroté à partir de 5)
Sélectionnez (p par défaut) : l

Ajout de la partition logique 6
Premier secteur (2668544-3483647, 2668544 par défaut) :ENTREE
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2668544-3483647, 3483647 par
défaut) :ENTREE

Une nouvelle partition 6 de type « Linux » et de taille 398 MiB a été créée.

Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Échec de relecture de la table de partitions.: Périphérique ou ressource occupé

Le noyau continue à utiliser l'ancienne table. La nouvelle sera utilisée lors du prochain
démarrage ou après avoir exécuté partprobe(8) ou kpartx(8).
```

La partition a bien été créée comme indiqué par le résultat de fdisk.

```
# fdisk -l /dev/sdb

Disque /dev/sdb : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x3ed112b5

Device     Boot   Start     End Sectors  Size Id Type
/dev/sdb1          2048 1026047 1024000  500M 83 Linux
/dev/sdb2       1026048 1845247  819200  400M 83 Linux
/dev/sdb3       1845248 3483647 1638400  800M  5 Extended
/dev/sdb5       1847296 2666495  819200  400M 83 Linux
/dev/sdb6       2668544 3483647  815104  398M 83 Linux
```

La partition n'est pas utilisable par le noyau (elle n'apparaît pas dans /proc/partitions).

```
# more /proc/partitions | grep sdb
   8       16    2097152 sdb
   8       17     512000 sdb1
   8       18     409600 sdb2
   8       19          1 sdb3
   8       21     409600 sdb5
```

La commande '*partprobe*' force le noyau à relire sa table de partitionnement. Le noyau détecte maintenant la nouvelle partition.

```
# partprobe /dev/sdb
# more /proc/partitions | grep sdb
   8       16    2097152 sdb
   8       17     512000 sdb1
   8       18     409600 sdb2
   8       21     409600 sdb5
   8       22     407552 sdb6
```

Remarque : Dans une machine virtuelle la commande *partprobe* ne fonctionne pas toujours. La commander *partx* permet de détecter de nouvelle partition (option -a) ou d'en supprimer (option -d).

```
# partx –a /dev/sdb
# partx –d /dev/sdb
```

L'utilisation de *fdisk* dans des scripts d'administration permet d'automatiser le partitionnement d'un disque.

Exemple avec la commande *echo*.

```
# (echo n;echo p;echo 1;echo ;echo ;echo t;echo 8e;echo w ) | fdisk
/dev/sdc
```

Exemple avec les étiquettes.

```
# fdisk /dev/sdb << EOF
> n
> p
> 1
>
>
> t
> 8e
> w
> EOF
```

Gestion des disques

La gestion de la swap

- Description de la swap
- Ajout d'une partition de swap supplémentaire
- Configurer la partition de swap qui sera utilisée en premier
- Ajout d'un fichier de swap

La gestion de la swap

La swap permet de pallier un manque de mémoire vive. Lorsque la RAM est saturée, le système bascule une ou plusieurs pages mémoire sur un espace disque spécifique appelé l'espace de swap.

Lors de l'installation d'un système Linux, une partition de swap est requise.

La mémoire virtuelle est la somme de l'espace de swap plus la RAM.

Affichage de la swap existante :

```
# swapon -s
Nom de fichier                          Type            Taille  Utilisé Priorité
/dev/sda6                               partition       1376252 0       -1

# more /proc/swaps
Filename                                Type            Size    Used    Priority
/dev/sda6                               partition       1376252 0       -1
```

Affichage de la mémoire virtuelle :

```
# free
              total        used        free      shared  buff/cache   available
Mem:        1883880      640876      743528        9780      499476     1051500
Swap:       2097148           0     2097148
```

Ajout d'une partition de swap :

- Création d'une partition de type swap :

```
# fdisk /dev/sdc

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Created a new DOS disklabel with disk identifier 0xcc7df692.

Commande (m pour l'aide) : n
Type de partition
   p   primaire (0 primaire, 0 étendue, 4 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) :ENTREE
Premier secteur (2048-4194303, 2048 par défaut) :ENTREE
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2048-4194303, 4194303 par défaut) : +1G

Une nouvelle partition 1 de type « Linux » et de taille 1 GiB a été créée.

Commande (m pour l'aide) : t
Partition 1 sélectionnée
Code Hexa (taper L pour afficher tous les codes) :L

 0  Vide            24  NEC DOS         81  Minix / Linux a bf  Solaris
 1  FAT12           27  TFS WinRE masqu 82  partition d'éch c1  DRDOS/sec (FAT-
 2  root XENIX      39  Plan 9          83  Linux           c4  DRDOS/sec (FAT-
 3  usr XENIX       3c  récupération Pa 84  OS/2 masquée di c6  DRDOS/sec (FAT-
 4  FAT16 <32M      40  Venix 80286     85  Linux étendue   c7  Syrinx
 5  Étendue         41  PPC PReP Boot   86  NTFS volume set da  Non-FS data
 6  FAT16           42  SFS             87  NTFS volume set db  CP/M / CTOS / .
 7  HPFS/NTFS/exFAT 4d  QNX4.x          88  Linux plaintext de  Dell Utility
 8  AIX             4e  2e partie QNX4. 8e  LVM Linux       df  BootIt
 9  Amorçable AIX   4f  3e partie QNX4. 93  Amoeba          e1  DOS access
 a  Gestionnaire d' 50  OnTrack DM      94  Amoeba BBT      e3  DOS R/O
 b  W95 FAT32       51  OnTrack DM6 Aux 9f  BSD/OS          e4  SpeedStor
 c  W95 FAT32 (LBA) 52  CP/M            a0  IBM Thinkpad hi eb  BeOS fs
 e  W95 FAT16 (LBA) 53  OnTrack DM6 Aux a5  FreeBSD         ee  GPT
 f  Étendue W95 (LB 54  OnTrackDM6      a6  OpenBSD         ef  EFI (FAT-12/16/
10  OPUS            55  EZ-Drive        a7  NeXTSTEP        f0  Linux/PA-RISC b
…

Code Hexa (taper L pour afficher tous les codes) :82
Type de partition « Linux » modifié en « Linux swap / Solaris ».

Commande (m pour l'aide) : p
Disque /dev/sdc : 2 GiB, 2147483648 octets, 4194304 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0xcc7df692

Device     Boot Start     End Sectors Size Id Type
/dev/sdc1        2048 2099199 2097152   1G 82 Linux swap / Solaris


Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

- Initialiser l'espace de swap :

```
# mkswap /dev/sdc1
Configure l'espace d'échange (swap) en version 1, taille = 1048572 Kio
pas d'étiquette, UUID=e3a15619-ea03-4fe4-8b07-3bd6a6d3c154
```

- Activer l'espace de swap :

```
# swapon /dev/sdc1
# swapon -s
Nom de fichier                          Type            Taille  Utilisé Priorité
/dev/sda6                               partition       1376252 0       -1
/dev/sdc1                               partition       1048572 0       -2
```

- Modifier la priorité de l'espace de swap :

```
# swapoff /dev/sdc1
# swapon -p 0 /dev/sdc1
# swapon -s
Nom de fichier                          Type            Taille  Utilisé Priorité
/dev/sda6                               partition       1376252 0       -1
/dev/sdc1                               partition       1048572 0       0
```

Remarque : les espaces de swap avec la même priorité sont utilisées de manière alternatives (round-robin).

Pérenniser la swap au démarrage

Pour activer les espaces de swap au démarrage de la machine, il faut ajouter des entrées dans le fichier /etc/fstab.

```
# grep swap /etc/fstab
# swap was on /dev/sda6 during installation
UUID=f9e2f47b-1a30-4cb6-b2ba-e632b5f6e805 none        swap    sw              0       0
/dev/sdc1                                 none        swap    sw              0       0
```

Remarque : L'option pri=valeur permet de positionner la priorité de l'espace de swap dans le fichier /etc/fstab.

Ajout d'un fichier de swap :

- Création d'un fichier de la taille de la swap :

```
# dd if=/dev/zero of=/swapfile bs=1024 count=600000
600000+0 enregistrements lus
600000+0 enregistrements écrits
614400000 octets (614 MB) copiés, 1,87515 s, 328 MB/s
```

```
# ls -lh /swapfile
-rw-r--r-- 1 root root 586M sept. 25 14:19 /swapfile
```

- Initialisation et activation de l'espace de swap :

```
# mkswap /swapfile
Configure l'espace d'échange (swap) en version 1, taille = 599996 Kio
pas d'étiquette, UUID=3c61f3f2-b7f2-4e00-873e-7248a3842e71
```

```
# swapon /swapfile
swapon: /swapfile : droits 0644 non sûrs, 0600 conseillées.
```

```
# swapoff /swapfile
# chmod 600  /swapfile
# swapon /swapfile
# swapon -s
Nom de fichier                          Type            Taille  Utilisé Priorité
/dev/sda6                               partition       1376252 0       -1
/dev/sdc1                               partition       1048572 0       0
/swapfile                               file            599996  0       -2
```

Notes

La gestion des systèmes de fichiers

Dans ce chapitre, nous allons étudier l'administration et la maintenance des systèmes de fichiers, ainsi que les quotas.

Table des matières

La gestion des systèmes de fichiers

Les types de systèmes de fichiers

- ext2, ext3, ext4
- reiserfs
- HPFS
- UFS
- JFS
- XFS
- ZFS
- vfat
- NTFS

Les types de systèmes de fichiers

ext2 : 2nd Extended File System : le système de fichiers historique de Linux qui corrige les erreurs de l'Extended File System (ext).

ext3 : Third Extended File System : ajoute la journalisation à ext2.

ext4 : Fourth Extended File System : ajoute l'index à ext3 pour un meilleur stockage des données.

Reiserfs : Système de fichiers journalisé créé par Monsieur Reiser.

HPFS : Système de fichiers de HP.

UFS : Unix File System.

JFS : Système de fichiers d'IBM.

XFS : Système de fichiers journalisé créé par Silicon Graphics (SGI).

ZFS : Système de fichiers de Solaris Oracle.

VFAT : Implémentation de FAT sous Linux.

NTFS : Système de fichiers de Windows.

Remarque : Sous Linux, les modules pour le support ntfs sont rarement compilés dans le noyau.

Les systèmes de fichiers

Le système de fichiers xfs

- système de fichiers 64 bits
- système de fichiers journalisé
- système de fichiers par défaut sur RHEL7

Le système de fichiers XFS

Le système de fichiers xfs est un système de fichiers 64 bits journalisé. Il a été crée par Silicons Graphics pour son système d'exploitation Irix.
Il est basé sur des extensions (comme ext4) ce qui permet un accès rapide aux données. Il fut pendant longtemps un des systèmes de fichiers les plus performants. La taille maximale d'un volume est de 16 EO, celui d'un fichier de 8EO.

C'est le système de fichiers utilisé par défaut à partir de la RHEL 7.

Les systèmes de fichiers

Le système de fichiers xfs

- Création d'un système de fichiers : mkfs.xfs
- Accès au système de fichiers: mount
- Péréniser l'accès: ajout au fichier /etc/fstab
- Supprimer l'accès au système de fichiers: umount

Création d'un système de fichiers

```
# mkfs.xfs /dev/sdc1
meta-data=/dev/sdc1              isize=512    agcount=4, agsize=65536 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=262144, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Accéder au système de fichiers

```
# mount /dev/sdc1 /rep1
```

Pérenniser l'accès au système de fichiers

```
# grep sdc1 /etc/fstab
/dev/sdc1               /rep1                   xfs     defaults        0 0
```

Supprimer l'accès au système de fichiers

```
# umount /rep1
      ou
# umount /dev/sdc1
```

Les systèmes de fichiers

Le système de fichiers xfs

- Option -f pour forcer la création
- Option -b pour la taille de blocs
- Option -i pour les inodes
- Option -l pour la journalisation

Création d'un système de fichiers avec un taille de blocs de 1024 octets.

```
# mkfs.xfs -f -b size=1024 /dev/sde1
meta-data=/dev/sde1              isize=256    agcount=4, agsize=2096896 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0
data     =                       bsize=1024   blocks=8387584, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=1024   blocks=10240, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Remarque : l'option -f permet de forcer la création du système de fichiers si la partition en contient déjà un.

La gestion des systèmes de fichiers

Le montage et le démontage d'un système de fichiers

- Montage d'un système de fichiers

  mount /etc/fstab

- Démontage d'un système de fichiers

  umount umount -f fuser -cu fuser -ck

- Informations sur un système de fichiers

  mount /etc/mtab findmnt

Le montage et le démontage d'un système de fichiers

L'opération de montage consiste à attacher un système de fichiers à un répertoire vide appelé point de montage. Lorsque l'on se déplace sur ce point de montage, on se trouve à la racine du système de fichier qui y a été rattaché.

La commande pour réaliser un montage est '*mount*'. Lors de l'opération de montage, des options peuvent être spécifiées. La commande pour réaliser un démontage est '*umount*'.

Pour monter automatiquement le système de fichiers au démarrage, il faut ajouter une entrée au fichier /etc/fstab.

Exemple1 :

```
# mkdir /rep1
# mkdir /rep2
```

```
# mount /dev/sdb1 /rep1
# mount -o noatime /dev/sdc1 /rep2
```

```
# cp /etc/passwd /rep1
# cp /etc/passwd /rep2
```

```
# cat /rep1/passwd
# cat /rep2/passwd
```

```
# ls -lu /rep1 /rep2
/rep1:
total 20
drwx------ 2 root root 16384 sept. 28 14:09 lost+found
-rw-r--r-- 1 root root  2266 sept. 28 14:52 passwd

/rep2:
total 20
drwx------ 2 root root 16384 sept. 28 14:16 lost+found
-rw-r--r-- 1 root root  2266 sept. 28 14:50 passwd
```

On constate que la date de dernière consultation n'a pas été modifiée dans rep2 à cause de l'option de montage noatime.

Exemple2 :

```
# mount -o ro,remount /dev/sdb1 /rep1
# touch /rep1/fic1
touch: impossible de faire un touch « /rep1/fic1 »: Système de fichiers accessible en
lecture seulement
```

Le système de fichiers étant monté en lecture seule, il n'est pas possible de créer des fichiers (même en tant que root).

Pour démonter un système de fichiers, il faut utiliser la commande *umount*. Elle ne fonctionne que s'il n'y a aucun processus qui accède au système de fichiers. L'option -a démonte tous les systèmes de fichiers qui sont démontables.

```
# umount /rep1
# umount -a
umount: /run/user/0 : cible occupée
       (Dans certains cas, des renseignements sur les processus utilisant
        le périphérique sont accessibles avec lsof(8) ou fuser(1).)
...
```

La commande '*mount -a*' monte tous les systèmes de fichiers présents dans /etc/fstab avec l'option auto de positionnée.

- Forcer le démontage d'un système de fichiers :

```
# umount /rep1
umount: /rep1 : cible occupée
```

Si on force le démontage, il peut y avoir une perte de données si jamais des écritures se font en même temps. L'option -f de *umount* permet de forcer l'opération mais cela s'avère souvent insuffisant.

```
# umount -f /rep1
umount: /rep1 : cible occupée
```

La commande fuser permet de savoir quels processus accèdent au système de fichiers :

```
# fuser -cu /rep1
/rep1:                1448c(root)  2688c(theo)
```

L'option -k de fuser permet de tuer tous les processus accédant au système de fichiers :

```
# fuser -ck /rep1
/rep1:                1448c  2688c
# fuser -cu /rep1
# umount /rep1
```

- Visualiser ce qui est monté :

La commande *df* :

```
# df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/sda1          7,1G    4,6G  2,1G  69% /
udev                10M       0   10M   0% /dev
tmpfs              405M    6,0M  399M   2% /run
tmpfs             1012M     92K 1012M   1% /dev/shm
tmpfs              5,0M       0  5,0M   0% /run/lock
tmpfs             1012M       0 1012M   0% /sys/fs/cgroup
/dev/sda7          360M    2,1M  335M   1% /tmp
/dev/sda8          8,0G     25M  7,6G   1% /home
/dev/sda5          2,7G    388M  2,2G  15% /var
tmpfs              203M    8,0K  203M   1% /run/user/1000
tmpfs              203M       0  203M   0% /run/user/0
/dev/sdb1          2,0G    3,1M  1,9G   1% /rep1
/dev/sdc1          2,0G    3,1M  1,9G   1% /rep2
```

La commande *mount* sans options :

```
# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
...
```

Le fichier /etc/mtab (la commande *mount* s'appuie dessus) :

```
# more /etc/mtab
rootfs  /  rootfs  rw  0  0
sysfs  /sys  sysfs  rw,seclabel,nosuid,nodev,noexec,relatime  0  0
proc  /proc  proc  rw,nosuid,nodev,noexec,relatime  0  0
...
```

La commande *findmnt* permet de lister tous les systèmes de fichiers, leur point de montage et les options de montage, le type de système de fichiers.

```
# findmnt
TARGET                     SOURCE     FSTYPE      OPTIONS
/           /dev/mapper/centos-root  xfs        rw,relatime,seclabel,attr2,inode64,noquota
├─/sys                     sysfs      sysfs       rw,nosuid,nodev,noexec,relatime,seclabel
│ ├─/sys/kernel/security   securityfs securityfs  rw,nosuid,nodev,noexec,relatime
│ ├─/sys/fs/cgroup         tmpfs      tmpfs       ro,nosuid,nodev,noexec,seclabel,mode=755
...
```

L'option -l permet d'avoir un affichage non arborescent.

```
# findmnt -l
 TARGET                   SOURCE     FSTYPE      OPTIONS
/sys                      sysfs      sysfs       rw,nosuid,nodev,noexec,relatime,seclabel
/proc                     proc       proc        rw,nosuid,nodev,noexec,relatime
/sys/kernel/security      securityfs securityfs  rw,nosuid,nodev,noexec,relatime
```

L'option -t permet de filtrer sur le type de système de fichiers.

```
# findmnt -t xfs
TARGET  SOURCE                  FSTYPE OPTIONS
/       /dev/mapper/centos-root xfs    rw,relatime,seclabel,attr2,inode64,noquota
└─/boot /dev/sdc2               xfs    rw,relatime,seclabel,attr2,inode64,noquota
```

La gestion des systèmes de fichiers

Les options de montage

- mount -o option1,option2,... système_fichiers point_montage
- L'option defaults
- L'option remount
- L'option auto

Les options de montage

Il existe un grand nombre d'options permettant d'effectuer un montage pour activer des fonctionnalités spécifiques au niveau du système de fichiers.

L'option noatime permet de ne pas mettre à jour la date de dernier accès du fichier. Cela permet de gagner un peu de bande passante si le fichier consulté est stocké sur un emplacement réseau.

Les options usrquota et grpquota permettent la prise en charge des quotas pour les systèmes de fichiers ext.

L'option defaults regroupe un certain nombre d'options de montage qui sont souvent utilisés. IL s'agit des options suivantes : rw, suid, dev, exec, auto, nouser et async.

L'option auto permet de monter le système de fichiers automatiquement au démarrage.

Liste des options de montage les plus courantes.

Option	Description
ro	Le système de fichier est monté en lecture seule.
rw	Le système de fichier est monté en lecture écriture.
noatime	ne pas mettre à jour la date de dernier accès au fichier.
remount	remonter le système de fichiers avec les nouvelles options de montage
acl	support des acl linux sur le filesystem
usr_quota	implémentation des quotas pour les utilisateurs.
grp_quota	implémentation des quotas pour les groupes.
defaults	regroupe les options par défaut rw,suid,dev,exec,auto,nouser, async.
suid	autoriser les fichiers qui ont le setuid ou setgid de positionné.
dev	interpréter les périphériques spéciaux de type bloc ou caractère.
exec	autoriser l'exécution de fichiers binaires.
auto	peut être monté avec l'option -a de la commande mount (exécute au démarrage).
nouser	ne pas autoriser un utilisateur ordinaire à monter le système de fichiers
async	Toutes les entrées et sorties seront asynchrones

La gestion des systèmes de fichiers

Les commandes df et du

- La commande df
- La commande du

Les commandes df et du

La commande df (disk free) affiche le taux d'occupation du disque :

```
# df -h
Sys. de fichiers        Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/centos-root    27G    3,5G   24G  13% /
devtmpfs                  905M       0  905M   0% /dev
tmpfs                     920M       0  920M   0% /dev/shm
tmpfs                     920M    8,9M  912M   1% /run
tmpfs                     920M       0  920M   0% /sys/fs/cgroup
/dev/sda1                1014M    233M  782M  23% /boot
tmpfs                     184M    8,0K  184M   1% /run/user/42
tmpfs                     184M     24K  184M   1% /run/user/1000
tmpfs                     184M       0  184M   0% /run/user/0
```

La commande du (disk usage) affiche la taille occupée sur le disque par les fichiers.

```
# du -sh /etc/sysconfig
444K    /etc/sysconfig
```

Remarque : l'option '-h' affiche les tailles de manière plus conviviale pour la lecture.

La gestion des systèmes de fichiers

L'automatisation du montage avec le fichier /etc/fstab

- Le fichier /etc/fstab

filesystem mountpoint type options dump fsck

L'automatisation du montage avec le fichier /etc/fstab

Pour qu'un système de fichiers soit monté au démarrage, il faut que sa définition soit présente dans le fichier /etc/fstab et qu'il ait l'option auto de positionnée :

```
# more /etc/fstab

#
# /etc/fstab
# Created by anaconda on Mon Sep 25 16:30:42 2017
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /                       xfs     defaults        0 0
UUID=518dd6bc-8683-45e4-9bb4-dcd74873b66b /boot xfs     defaults        0 0
/dev/mapper/centos-swap swap                    swap    defaults        0 0
```

Définition des colonnes.

Champ	Signification
filesystem	le système de fichiers à monter, identifié par son nom, son UUID ou son LABEL
mountpoint	le point de montage du système de fichiers
type	le type de système de fichiers
options	les options de montage du système de fichiers
dump	champ utilisé par l'utilitaire dump pour savoir s'il faut effectuer une sauvegarde (si égal à 1) du système de fichiers
pass	champ utilisé par l'utilitaire fsck pour savoir quels systèmes de fichiers doivent être vérifiés au démarrage. La racine doit toujours être vérifiée en 1er.

La commande mount est « intelligente ». S'il manque le nom du périphérique ou le point de montage, la commande va vérifier s'il n'y a pas une entrée correspondante au sein du fichier /etc/fstab.

```
# mount /rep1
# mount /rep2
mount: impossible de trouver /rep2 dans /etc/fstab
```

La gestion des systèmes de fichiers

Le dépannage d'un système de fichiers

- La commande xfs_repair

Le dépannage d'un système de fichiers

La commande xfs_repair vérifie l'intégrité d'un système de fichiers et répare un système de fichiers corrompus.

```
# xfs_repair /dev/sdc2
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
```

La gestion des systèmes de fichiers

La création et le paramétrage de système de fichiers ext

- Les commandes mkfs et mke2fs
- Les options des commandes mkfs et mke2fs
- Les commandes tunefs et dumpe2fs
- Contrôle d'intégrité avec la commande fsck

La création et le paramétrage de système de fichiers ext

La commande mkfs permet de créer un système de fichiers. La structure interne d'un système de fichiers est composé des éléments suivants :

- le super-bloc (commence à l'octet 1024 de la partition et a une taille de 1ko). Il contient les méta-données de la partition. Le super-bloc étant essentiel au bon fonctionnement, il est recopié au début de certains groupes de cylindres.

- le groupe de cylindres. Le système de fichiers est divisé en groupe de cylindres pour une meilleure optimisation de celui-ci

- blocs de groupes de cylindres. Une table de groupe décrit ses caractéristiques (nombre d'inodes, le nombre de blocs de données, le nombre de répertoire, les blocks et les inodes libres,..)

- La tables des inodes.

- Création d'un système de fichiers ext2 :

```
# mkfs –t ext2 /dev/sdb1
```

La commande mke2fs encapsule la commande mkfs :

```
# mke2fs /dev/sdc1
```

- Affichage des caractéristiques du système de fichiers :

```
# tune2fs –l /dev/sdc1
```

- Caractéristiques très détaillées du système de fichiers :

```
# dumpe2fs  /dev/sdc1
```

- Vérifier si la partition contient un système de fichiers :

```
# blkid /dev/sdb1
/dev/sdb1: UUID="a865d209-fbfa-44bc-be8e-62c5417a43b8" TYPE="ext2" PARTUUID="3ed112b5-01"
```

- Création d'un système de fichiers ext2 en modifiant la taille des blocs, le minfree et la densité des inodes :

```
# mkfs.ext2 –b 1024 –i 8192 –m 0 /dev/sdc1
```

Principales options de la commande mkfs.

Option	Définition
-b	Permet d'indiquer la taille des blocs
-i	Permet d'indiquer la densité des inodes
-m	Permet d'indiquer le pourcentage réservé à root

Remarque : les valeurs par défaut de la taille d'un bloc et de la densité des inodes proviennent du fichier /etc/mke2fs.conf.

- Création d'un système de fichiers ext3 :

```
# mke2fs -j /dev/sdb1
```

ou

```
# mkfs -t ext3 /dev/sdc1
```

- Création d'un système de fichiers ext4 :

```
# mkfs -t ext4 /dev/sdb1
```

ou

```
# mkfs.ext4 /dev/sdc1
```

- Modifier le minfree d'un système de fichiers :

```
# tune2fs -m 0 /dev/sdb1
```

- Transformer un système de fichiers ext2 en ext3 :

```
# tune2fs -j /dev/sdb1
```

- Transformer une partition ext3 en ext2 :
  Il faut supprimer la journalisation des caractéristiques de notre système de fichiers.

```
# tune2fs -O ^has_journal /dev/sdb1
```

- Transformer une partition ext3 en ext4 :

```
# tune2fs -O extents,uninit_bg,dir_index /dev/sdc1
```

Remarque : il n'est pas possible de basculer de l'ext4 en ext3, sauf si le système de fichiers n'a jamais été utilisé.

La gestion des systèmes de fichiers

Vérifier la cohérence d'un système de fichiers: fsck

- umount /dev/sdXY
- fsck /dev/sdXY
- fsck -y /dev/sdXY

Vérifier la cohérence d'un système de fichiers : fsck

La commande fsck permet de vérifier l'intégrité d'un système de fichiers et de réparer un système de fichiers corrompus. L'option -y permet de répondre automatiquement 'oui' à chaque correction d'erreur proposée. Cette option est très pratique car lors de la corruption d'un système de fichiers, vous avez souvent plusieurs problèmes à corriger.

REMARQUE : La commande **fsck s'utilise toujours sur un système de fichiers démonté.**

```
# fsck /dev/sdb1
fsck de util-linux 2.25.2
e2fsck 1.42.12 (29-Aug-2014)
/dev/sdb1 : propre, 12/131072 fichiers, 9005/524032 blocs
```

Suppression des 32 premiers ko de /dev/sdb1

```
# dd if=/dev/zero of=/dev/sdb1 bs=1024 count=32
32+0 enregistrements lus
32+0 enregistrements écrits
32768 octets (33 kB) copiés, 0,00771204 s, 4,2 MB/s
```

```
# fsck /dev/sdb1
fsck de util-linux 2.25.2
e2fsck 1.42.12 (29-Aug-2014)
ext2fs_open2: Numéro magique invalide dans le super-bloc
fsck.ext2 : Superbloc invalide, tentons d'utiliser les blocs de sauvetage...
/dev/sdb1 n'a pas été démonté proprement, vérification forcée.
L'i-noeud de changement de taille n'est pas valide. Recréer<o>? oui
Passe 1 : vérification des i-noeuds, des blocs et des tailles
```

```
Passe 2 : vérification de la structure des répertoires
Passe 3 : vérification de la connectivité des répertoires
Passe 4 : vérification des compteurs de référence
Passe 5 : vérification de l'information du sommaire de groupe
Le décompte des i-noeuds libres est erroné pour le groupe n°0 (8181, décompté=8180).
Corriger<o>? oui
Le décompte des i-noeuds libres est erroné (131061, décompté=131060).
Corriger<o>?
/dev/sdb1 : e2fsck a été annulé.

/dev/sdb1: ***** LE SYSTÈME DE FICHIERS A ÉTÉ MODIFIÉ *****
```

```
# fsck -y /dev/sdb1
fsck de util-linux 2.25.2
e2fsck 1.42.12 (29-Aug-2014)
/dev/sdb1 n'a pas été démonté proprement, vérification forcée.
Passe 1 : vérification des i-noeuds, des blocs et des tailles
Passe 2 : vérification de la structure des répertoires
Passe 3 : vérification de la connectivité des répertoires
Passe 4 : vérification des compteurs de référence
Passe 5 : vérification de l'information du sommaire de groupe
Le décompte des i-noeuds libres est erroné (131061, décompté=131060).
Corriger ? oui


/dev/sdb1: ***** LE SYSTÈME DE FICHIERS A ÉTÉ MODIFIÉ *****
/dev/sdb1 : 12/131072 fichiers (0.0% non contigus), 9005/524032 blocs
```

```
# fsck /dev/sdb1
fsck de util-linux 2.25.2
e2fsck 1.42.12 (29-Aug-2014)
/dev/sdb1 : propre, 12/131072 fichiers, 9005/524032 blocs
```

Les systèmes de fichiers

Les quotas sur un système de fichiers xfs

- Options de montage pour activer les quotas
- Positionner des quotas pour des utilisateurs et des groupes
- Informations sur les quotas

Les quotas sur un système de fichiers xfs

Le système de fichiers xfs supporte les quotas pour des utilisateurs, des groupes et des projets. Il faut monter le système de fichiers avec l'option adéquate pour activer les quotas sur le système de fichiers (uquota, gquota, pquota).
Il existe deux types de quotas. Les quotas sur les inodes (nombre de fichiers et de répertoires que l'on peut créer) et les quotas blocs (espace maximum que l'on peut utiliser).
La limite hard d'un quota est la limite infranchissable. La limite soft est la limite que l'on peut dépasser durant un certain temps appelé temps de grâce.

```
# grep /users /etc/fstab
/dev/sde1               /users     xfs        defaults             1 2
```

```
# mount | grep users
/dev/sde1 on /users type xfs (rw,relatime,attr2,inode64,noquota)
```

Activation des quotas pour les utilisateurs et les groupes.

```
# grep /users /etc/fstab
/dev/sde1               /users     xfs        defaults,uquota,gquota               1 2
```

```
# mount | grep users
/dev/sde1 on /users type xfs (rw,relatime,attr2,inode64,usrquota,grpquota)
```

Pour afficher les informations relatives aux quotas, utiliser les options de la commande xfs_quota.

```
# xfs_quota -x -c quot
/dev/sda3 (/home) User:
     668    theo
      40    user1
      40    user2
      40    user3
/dev/sde1 (/users) User:
      23    pim
      23    pam
      23    poum
```

```
# xfs_quota -x -c state
User quota state on /users (/dev/sde1)
  Accounting: ON
  Enforcement: ON
  Inode: #90 (2 blocks, 2 extents)
Group quota state on /users (/dev/sde1)
  Accounting: ON
  Enforcement: ON
  Inode: #91 (2 blocks, 2 extents)
Project quota state on /users (/dev/sde1)
  Accounting: OFF
  Enforcement: OFF
  Inode: #91 (2 blocks, 2 extents)
Blocks grace time: [7 days 00:00:30]
Inodes grace time: [7 days 00:00:30]
Realtime Blocks grace time: [7 days 00:00:30]
```

L'option -x de la commande cfs_quota permet de positionner les limites pour les utilisateurs.

```
# xfs_quota -x /dev/sde1
xfs_quota> path
      Filesystem          Pathname
[000] /users              /dev/sde1 (uquota, gquota
```

```
xfs_quota> limit bsoft=400m bhard=500m pim
xfs_quota> quota pim
Disk quotas for User pim (1004)
Filesystem             Blocks      Quota      Limit  Warn/Time      Mounted on
/dev/sde1                  23     409600     512000   00 [--------] /users
xfs_quota> quota -h pim
Disk quotas for User pim (1004)
Filesystem   Blocks  Quota  Limit Warn/Time    Mounted on
/dev/sde1       23K   400M   500M  00 [------] /users
```

```
xfs_quota> limit isoft=30 ihard=35 pam
xfs_quota> quota pam
Disk quotas for User pam (1005)
Filesystem             Blocks      Quota      Limit  Warn/Time      Mounted on
/dev/sde1                  23          0          0   00 [--------] /users
xfs_quota> quota -i pam
Disk quotas for User pam (1005)
Filesystem              Files      Quota      Limit  Warn/Time      Mounted on
/dev/sde1                  16         30         35   00 [--------] /users
```

L'option '-h' permet d'afficher la sortie dans un format plus lisible. L'option '-i' permet de visualiser les quotas sur les inodes.

La sous commande « report » permet d'afficher un rapport des quotas.

```
# xfs_quota -x /dev/sde1
xfs_quota> report
User quota on /users (/dev/sde1)
                                Blocks
User ID          Used       Soft       Hard    Warn/Grace
---------- --------------------------------------------------
root                0          0          0     00 [--------]
pim                23     409600     512000     00 [--------]
pam                23          0          0     00 [--------]
poum               23          0          0     00 [--------]

Group quota on /users (/dev/sde1)
                                Blocks
Group ID         Used       Soft       Hard    Warn/Grace
---------- --------------------------------------------------
root                0          0          0     00 [--------]
users              69          0          0     00 [--------]
```

```
xfs_quota> report -h
User quota on /users (/dev/sde1)
                        Blocks
User ID      Used   Soft   Hard Warn/Grace
---------- ---------------------------------
root            0      0      0  00 [------]
pim           23K   400M   500M  00 [------]
pam           23K      0      0  00 [------]
poum          23K      0      0  00 [------]

Group quota on /users (/dev/sde1)
                        Blocks
Group ID     Used   Soft   Hard Warn/Grace
---------- ---------------------------------
root            0      0      0  00 [------]
users          69K      0      0  00 [------]
```

Remarque : Les commandes peuvent-être exécutées directement depuis le shell sans entrer dans l'utilitaire xfs_quota.

```
# xfs_quota -x -c report /users
User quota on /users (/dev/sde1)
                                Blocks
User ID          Used       Soft       Hard    Warn/Grace
---------- --------------------------------------------------
root                0          0          0     00 [--------]
pim                23     409600     512000     00 [--------]
pam                23          0          0     00 [--------]
poum               23          0          0     00 [--------]

Group quota on /users (/dev/sde1)
                                Blocks
Group ID         Used       Soft       Hard    Warn/Grace
---------- --------------------------------------------------
root                0          0          0     00 [--------]
users              69          0          0     00 [--------]
```

```
# xfs_quota -x -c 'report -h' /users
User quota on /users (/dev/sde1)
                        Blocks
User ID      Used   Soft   Hard Warn/Grace
---------- --------------------------------
root            0      0      0  00 [------]
pim           23K   400M   500M  00 [------]
pam           23K      0      0  00 [------]
poum          23K      0      0  00 [------]

Group quota on /users (/dev/sde1)
                        Blocks
Group ID     Used   Soft   Hard Warn/Grace
---------- --------------------------------
root            0      0      0  00 [------]
users          69K      0      0  00 [------]
```

```
# xfs_quota -x -c 'limit bsoft=900m bhard=1000m isoft=50 ihard=60
poum' /users
```

Les commandes de quotas pour les systèmes de fichiers classiques fonctionnent avec XFS.

Affichage des quotas sur un système de fichiers.

```
# repquota /users
*** Report for user quotas on device /dev/sde1
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --       0       0       0              3     0     0
pim       --      23  409600  512000             16     0     0
pam       --      23       0       0             16    30    35
poum      --      23  921600 1024000             16    50    60
```

Affichage des quotas de l'utilisateur poum.

```
# quota poum
Disk quotas for user poum (uid 1006):
     Filesystem  blocks   quota   limit   grace   files   quota   limit   grace
      /dev/sde1      23  921600 1024000              16      50      60
```

Un utilisateur peut visualiser ses quotas.

```
pam@formateur:~> quota
Disk quotas for user pam (uid 1005):
Système fichiers   blocs   quota  limite  sursisfichiers   quota  limite  sursis
      /dev/sde1      23       0       0              16      30      35
```

Cas de dépassement de la limite soft.

```
pam@formateur:~> touch f5
pam@formateur:~> touch f6
pam@formateur:~> quota
Disk quotas for user pam (uid 1005):
Système fichiers   blocs   quota  limite  sursisfichiers   quota  limite  sursis
      /dev/sde1      24       0       0              31*     30      35   7days
```

Lorsque la limite soft est dépassée, le décompte pour le temps de grâce est enclenché.

```
# xfs_quota -x -c 'report -ih' /users
User quota on /users (/dev/sde1)
                        Inodes
User ID      Used   Soft   Hard Warn/Grace
---------- ---------------------------------
root            3      0      0  00 [------]
pim            16      0      0  00 [------]
pam            31     30     35  00 [6 days]
poum           16     50     60  00 [------]

Group quota on /users (/dev/sde1)
                        Inodes
Group ID     Used   Soft   Hard Warn/Grace
---------- ---------------------------------
root            3      0      0  00 [------]
users          63      0      0  00 [------]
```

```
# repquota /users
*** Report for user quotas on device /dev/sde1
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --       0       0       0              3     0     0
pim       --      24  409600  512000             16     0     0
pam       -+      24       0       0             31    30    35  6days
poum      --      23  921600 1024000             16    50    60
```

Lorsque la limite hard est atteinte, il n'est plus possible de créer des fichiers.

```
pam@formateur:~> touch f11
touch: impossible de faire un touch « f11 »: Débordement du quota d'espace disque
```

```
pam@formateur:~> quota
Disk quotas for user pam (uid 1005):
Système fichiers   blocs   quota  limite  sursisfichiers   quota  limite  sursis
      /dev/sde1      24       0       0              35*     30      35   6days
```

Copier les quotas d'un utilisateur vers un autre utilisateur.

```
# useradd -d /users/toto -m toto
# repquota /users
*** Report for user quotas on device /dev/sde1
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --       0       0       0              3     0     0
pim       --      24  409600  512000             16     0     0
pam       -+      24       0       0             35    30    35  6days
poum      --      23  921600 1024000             16    50    60
toto      --      23       0       0             16     0     0
```

L'option '-p' de la commande edquota permet de copier les quotas d'un utilisateur.

```
# edquota -p poum toto
# repquota /users
*** Report for user quotas on device /dev/sde1
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --       0       0       0              3     0     0
pim       --      24  409600  512000             16     0     0
pam       -+      24       0       0             35    30    35  6days
poum      --      23  921600 1024000             16    50    60
toto      --      23  921600 1024000             16    50    60
```

La gestion des systèmes de fichiers

Les quotas sur les systèmes de fichiers ext

- Les quotas utilisateurs et groupes
- Les limites soft et hard
- Les commandes de gestion des quotas

Les quotas sur les systèmes de fichiers ext

Les quotas permettent de limiter l'espace disque disponible pour un utilisateur ou pour un groupe d'utilisateurs.
On peut implémenter des quotas sur les blocs de données (taille) ou sur le nombre d'inodes (nombre de fichiers et de répertoires qu'on pourra créer).

La limite hard est la limite que l'utilisateur ne pourra jamais dépasser.

La limite soft est la limite qu'il peut dépasser durant le délai de grâce (7 jours par défaut). Si au bout du délai de grâce l'utilisateur n'est pas en dessous de sa limite soft, il ne pourra plus créer de fichiers (même si la limite hard n'est pas atteinte).

Mise en œuvre :

- Monter le système de fichiers avec les options usrquota et grpquota :

```
# grep quota /etc/fstab
UUID=2c5e6590-cbc4-42c9-bd31-d482720fa183 /home           ext4
defaults,usrquota,grpquota 0 2
```

```
# mount -o remount /home
```

```
# mount | grep quota
/dev/sda8 on /home type ext4 (rw,relatime,quota,usrquota,grpquota,data=ordered)
```

- Créer la base de données qui va contenir les quotas :

```
# quotacheck -cug /home
quotacheck: Impossible de remonter le système de fichier monté sur /home en lecture
seule, les valeurs comptabilisées riquent d'être fausses.
Veuillez interrompre tous les programmes qui écrivent sur ce système de fichiers ou
utilisez l'option -m pour forcer la vérification.
```

```
# quotacheck -cugm /home
# ls /home
aquota.group  aquota.user  lost+found  theo
```

Cette commande a créé les fichiers /home/aquota.group et /home/aquota.user.

- Activer les quotas sur le système de fichiers :

```
# quotaon /home
```

Définir les quotas pour des utilisateurs ou pour des groupes :

La commande 'edquota' édite le fichier avec l'éditeur par défaut (vi en général). Pour définir un autre éditeur, il faut configurer la variable EDITOR.

```
# edquota theo
Quotas disque pour user theo (uid 1000) :
 Système de fichiers          blocs       souple     stricte   inodes    souple   stricte
  /dev/sda8                     5900          0          0        138        0        0
```

Une fois le fichier édité, il suffit de définir vos limites souples (soft) et strictes (hard).

```
# edquota theo
Quotas disque pour user theo (uid 1000) :
 Système de fichiers          blocs       souple     stricte   inodes    souple   stricte
  /dev/sda8                     5900          0          0        138      142      145
```

Lors de la création des fichiers, il y a un avertissement lors du débordement de la limite soft. La limite hard ne peut pas être dépassée.

```
theo@formateur:~$ touch f1
theo@formateur:~$ touch f2
sda8: warning, user file quota exceeded.
theo@formateur:~$ touch f3
theo@formateur:~$ touch f4
theo@formateur:~$ touch f5
sda8: write failed, user file limit reached.
touch: impossible de faire un touch « f5 »: Débordement du quota d'espace disque
```

Un simple compte utilisateur peut afficher les quotas qui lui sont affectés :

```
theo@formateur:~$ quota
Disk quotas for user theo (uid 1000):
Système fichiers   blocs   quota  limite  sursisfichiers   quota  limite  sursis
      /dev/sda8    5944       0       0             145*    142     145   6days
```

L'administrateur peut afficher les quotas des utilisateurs :

```
# quota theo
Disk quotas for user theo (uid 1000):
Système fichiers   blocs   quota  limite  sursisfichiers   quota  limite  sursis
      /dev/sda8    5944       0       0             145*    142     145   6days
```

L'administrateur peut afficher les quotas par système de fichiers :

```
# repquota /home
*** Rapport pour les quotas user sur le périphérique /dev/sda8
Période de sursis bloc : 7days ; période de sursis inode : 7days
                        Block limits                File limits
Utilisateur     utilisé souple stricte sursis utilisé souple stricte sursis
------------------------------------------------------------------------
root      --      20       0       0              2     0     0
theo      -+    5944       0       0            145   142   145  6days
user1     --       4       0       0              4     0     0
```

Recopier les quotas d'un utilisateur vers un autre :

```
# edquota -p theo user1
```

```
# repquota /home
*** Rapport pour les quotas user sur le périphérique /dev/sda8
Période de sursis bloc : 7days ; période de sursis inode : 7days
                        Block limits                File limits
Utilisateur     utilisé souple stricte sursis utilisé souple stricte sursis
---------------------------------------------------------------------------
root      --      20       0       0              2     0     0
theo      -+    5944       0       0            145   142   145  6days
user1     --      16       0       0              4   142   145
```

Notes

LE LVM

Dans ce chapitre, nous allons étudier l'administration avancée des disques avec LVM .

Table des matières

LE LVM

Présentation du LVM Linux

- Les volumes physiques
- Les groupes de volumes
- Les volumes logiques
- Extension d'un groupe de volumes
- Extension d'un volume logique
- Extension du système de fichiers

Présentation du LVM Linux

Logical Volume Manager est un gestionnaire de volumes. Il permet notamment d'étendre à chaud des volumes logiques et les systèmes de fichiers.

Dans un premier temps, les partitions sont transformées en volumes physiques. Cela crée des étendues physiques (PE : Physical Extend) qui font 4Mo.

Un groupe de volumes va être construit au-dessus des volumes physiques. Un groupe de volumes regroupe plusieurs volumes physiques. Un groupe de volumes peut-être étendu en cours de fonctionnement pour ajouter un volume physique.

Dans le groupe de volumes va être créée un volume logique qui sera constituée d'étendues logiques (LE :Logical Extend). Le LE est identique au PE. Le volume logique peut-être étendu à chaud avec certains systèmes de fichiers (pour ext2, il faut démonter le système de fichiers).

Création d'un volume physique

Mise en œuvre de LVM :

- Création de partitions sur chaque disque :

Nous créons une partition faisant la totalité du disque. Pour se souvenir qu'elle fait partie de LVM, nous la marquons avec le type (« Linux LVM ») via le code 8e de la commande fdisk.

```
# fdisk /dev/sdb << EOF
> n
> p
> 1
>
>
> t
> 8e
> w
> EOF

Bienvenue dans fdisk (util-linux 2.25.2).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.


Commande (m pour l'aide) : Type de partition
   p   primaire (0 primaire, 0 étendue, 4 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : Numéro de partition (1-4, 1 par défaut) : Premier secteur
(2048-4194303, 2048 par défaut) : Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2048-
4194303, 4194303 par défaut) :
Une nouvelle partition 1 de type « Linux » et de taille 2 GiB a été créée.

Commande (m pour l'aide) : Partition 1 sélectionnée
Code Hexa (taper L pour afficher tous les codes) :Type de partition « Linux » modifié en
« Linux LVM ».

Commande (m pour l'aide) : La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

Vérification que les partitions ont bien été créées :

```
# fdisk -l /dev/sd[bcd]
```

- Transformation des partitions en volumes physiques :

```
# pvcreate /dev/sd[bcd]1
  Physical volume "/dev/sdb1" successfully created
WARNING: swap signature detected on /dev/sdc1. Wipe it? [y/n]: y
  Wiping swap signature on /dev/sdc1.
  Physical volume "/dev/sdc1" successfully created
  Physical volume "/dev/sdd1" successfully created
```

```
# pvs
  PV         VG   Fmt  Attr PSize PFree
  /dev/sdb1       lvm2 ---  2,00g 2,00g
  /dev/sdc1       lvm2 ---  2,00g 2,00g
  /dev/sdd1       lvm2 ---  2,00g 2,00g
```

```
# pvdisplay -C
  PV         VG   Fmt  Attr PSize PFree
  /dev/sdb1       lvm2 ---  2,00g 2,00g
  /dev/sdc1       lvm2 ---  2,00g 2,00g
  /dev/sdd1       lvm2 ---  2,00g 2,00g
```

```
# pvdisplay
  "/dev/sdb1" is a new physical volume of "2,00 GiB"
  --- NEW Physical volume ---
  PV Name               /dev/sdb1
  VG Name
  PV Size               2,00 GiB
  Allocatable           NO
  PE Size               0
  Total PE              0
  Free PE               0
  Allocated PE          0
  PV UUID               q6gKI9-EdWL-gnox-hqn0-OKHj-t5QJ-Zz4KZ2

  "/dev/sdc1" is a new physical volume of "2,00 GiB"
  --- NEW Physical volume ---
  PV Name               /dev/sdc1
  VG Name
  PV Size               2,00 GiB
  Allocatable           NO
  PE Size               0
  Total PE              0
  Free PE               0
  Allocated PE          0
  PV UUID               guDjW2-kcZK-hCJ7-Dm0C-XbPV-l2j1-K1pFGK

  "/dev/sdd1" is a new physical volume of "2,00 GiB"
  --- NEW Physical volume ---
  PV Name               /dev/sdd1
  VG Name
  PV Size               2,00 GiB
  Allocatable           NO
  PE Size               0
  Total PE              0
  Free PE               0
  Allocated PE          0
  PV UUID               gnF9Zo-H8Dv-XOCW-VADZ-5cwS-9UJm-aKXXnt
```

```
# pvscan
  PV /dev/sdb1         lvm2 [2,00 GiB]
  PV /dev/sdc1         lvm2 [2,00 GiB]
  PV /dev/sdd1         lvm2 [2,00 GiB]
  Total: 3 [6,00 GiB] / in use: 0 [0   ] / in no VG: 3 [6,00 GiB]
```

Création d'un groupe de volumes

- Création d'un groupe de volumes à partir de 2 partitions :

```
# vgcreate vgtest /dev/sd[bc]1
  /proc/devices: No entry for device-mapper found
  /proc/devices: No entry for device-mapper found
  Volume group "vgtest" successfully created
```

```
# vgs
  VG     #PV #LV #SN Attr   VSize VFree
  vgtest   2   0   0 wz--n- 3,99g 3,99g
```

La commande 'vgs' indique que le groupe de volumes 'vgtest' est constitué de 2 PV (volume physique). Il n'y a pas de LV (volume logique) dans le VG (groupe de volumes).

```
# pvs
  PV         VG     Fmt  Attr PSize PFree
  /dev/sdb1  vgtest lvm2 a--  2,00g 2,00g
  /dev/sdc1  vgtest lvm2 a--  2,00g 2,00g
  /dev/sdd1         lvm2 ---  2,00g 2,00g
```

```
# vgdisplay -C
  VG     #PV #LV #SN Attr   VSize VFree
  vgtest   2   0   0 wz--n- 3,99g 3,99g
```

```
# vgdisplay
  --- Volume group ---
  VG Name               vgtest
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               3,99 GiB
  PE Size               4,00 MiB
  Total PE              1022
  Alloc PE / Size       0 / 0
  Free  PE / Size       1022 / 3,99 GiB
  VG UUID               5WDM31-BDqu-CXJx-LMGQ-oc8u-dPtc-o5sGnj
```

Création d'un volume logique

- Création de volumes logiques dans un groupe de volumes :

Création d'un volume logique nommé lv_test1 de 1024Mo dans le groupe de volume vgtest :

```
# lvcreate -L 1024M -n lv_test1 vgtest
  Logical volume "lv_test1" created
```

Visualisation :

```
# lvs
  LV       VG     Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  lv_test1 vgtest -wi-a----- 1,00g
```

```
# lvdisplay -C
  LV       VG     Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  lv_test1 vgtest -wi-a----- 1,00g
```

```
# lvdisplay
  --- Logical volume ---
  LV Path                /dev/vgtest/lv_test1
  LV Name                lv_test1
  VG Name                vgtest
  LV UUID                VzY7Qw-lA20-mpLV-Oe9I-7GAp-dSno-64utiR
  LV Write Access        read/write
  LV Creation host, time formateur, 2015-09-25 15:21:33 +0200
  LV Status              available
  # open                 0
  LV Size                1,00 GiB
  Current LE             256
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           254:0
```

La commande vgdisplay nous confirme qu'il ne reste plus que 766 PE de disponible :

```
# vgdisplay
  --- Volume group ---
  VG Name               vgtest
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  2
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               0
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               3,99 GiB
  PE Size               4,00 MiB
  Total PE              1022
  Alloc PE / Size       256 / 1,00 GiB
  Free  PE / Size       766 / 2,99 GiB
  VG UUID               5WDM31-BDqu-CXJx-LMGQ-oc8u-dPtc-o5sGnj
```

Création d'un volume logique nommé lv_test2 de 766PE dans le groupe de volume vgtest :

```
# lvcreate -l 766 -n lv_test2 vgtest
  Logical volume "lv_test2" created
```

```
# lvdisplay /dev/vgtest/lv_test2
  --- Logical volume ---
  LV Path                /dev/vgtest/lv_test2
  LV Name                lv_test2
  VG Name                vgtest
  LV UUID                lk3O6x-Ooe7-a7tA-lUiX-g8G5-Fbzb-0nebYd
  LV Write Access        read/write
  LV Creation host, time formateur, 2015-09-25 15:27:35 +0200
  LV Status              available
  # open                 0
  LV Size                2,99 GiB
  Current LE             766
  Segments               2
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           254:1
```

```
# vgdisplay
  --- Volume group ---
  VG Name               vgtest
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  3
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                2
  Open LV               0
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               3,99 GiB
  PE Size               4,00 MiB
  Total PE              1022
  Alloc PE / Size       1022 / 3,99 GiB
  Free  PE / Size       0 / 0
  VG UUID               5WDM31-BDqu-CXJx-LMGQ-oc8u-dPtc-o5sGnj
```

Création d'un système de fichiers xfs sur lv_test1 et montage sur /test1 :
Copie de données sur /test1 pour augmenter le taux d'occupation du système de fichiers.

```
# mkfs -t xfs -m 0 /dev/vgtest/lv_test1
```

```
# mkdir /test1
# mount /dev/vgtest/lv_test1 /test1
# cp -r /etc /var /test1
```

Nous constatons que le taux d'occupation du système de fichiers est de 41% :

```
# df -h /test1
Sys. de fichiers            Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/vgtest-lv_test1   976M    393M  568M  41% /test1
```

Ajouter une entrée dans le fichier /etc/fstab si vous désirez le volume logique soit automatiquement monté au démarrage.

Extension d'un groupe de volumes

- Extension du groupe de volume par l'ajout d'un volume physique :

```
# vgextend vgtest /dev/sdd1
  Volume group "vgtest" successfully extended
```

```
# vgs
  VG     #PV #LV #SN Attr   VSize VFree
  vgtest   3   2   0 wz--n- 5,99g 2,00g
```

```
# pvs
  PV         VG     Fmt  Attr PSize PFree
  /dev/sdb1  vgtest lvm2 a--  2,00g    0
  /dev/sdc1  vgtest lvm2 a--  2,00g    0
  /dev/sdd1  vgtest lvm2 a--  2,00g 2,00g
```

```
# vgdisplay
  --- Volume group ---
  VG Name               vgtest
  System ID
  Format                lvm2
  Metadata Areas        3
  Metadata Sequence No  4
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                2
  Open LV               1
  Max PV                0
  Cur PV                3
  Act PV                3
  VG Size               5,99 GiB
  PE Size               4,00 MiB
  Total PE              1533
  Alloc PE / Size       1022 / 3,99 GiB
  Free  PE / Size       511 / 2,00 GiB
  VG UUID               5WDM31-BDqu-CXJx-LMGQ-oc8u-dPtc-o5sGnj
```

Extension d'un volume logique

Extension du volume logique lv_test1 de 511 PE :

```
# lvextend -l +511 /dev/vgtest/lv_test1
  Size of logical volume vgtest/lv_test1 changed from 1,00 GiB (256 extents) to 3,00 GiB
(767 extents).
  Logical volume lv_test1 successfully resized
```

Remarque : N'omettez pas le signe '+' qui indique qu'il faut ajouter 511 PE à la taille existante. Sans ce signe, vous indiquez la taille totale de votre volume logique.

La taille du LV est bien de 3Go :

```
# lvdisplay /dev/vgtest/lv_test1
  --- Logical volume ---
  LV Path                /dev/vgtest/lv_test1
  LV Name                lv_test1
  VG Name                vgtest
  LV UUID                VzY7Qw-lA20-mpLV-Oe9I-7GAp-dSno-64utiR
  LV Write Access        read/write
  LV Creation host, time formateur, 2015-09-25 15:21:33 +0200
  LV Status              available
  # open                 1
  LV Size                3,00 GiB
  Current LE             767
  Segments               2
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           254:0
```

Vérifions le taux d'occupation du système de fichiers :

```
# df -h /test1
Sys. de fichiers            Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/vgtest-lv_test1   976M    393M  568M  41% /test1
```

Le taux d'occupation est toujours identique car le volume logique a été étendu mais pas le système de fichiers (Il fait toujours 976 Mo). Il faut donc étendre le système de fichiers du volume logique.

```
# xfs_growfs /test1
resize2fs 1.42.12 (29-Aug-2014)
Le système de fichiers de /dev/vgtest/lv_test1 est monté sur /test1 ; le changement de
taille doit être effectué en ligne
old_desc_blocks = 1, new_desc_blocks = 1
Le système de fichiers sur /dev/vgtest/lv_test1 a maintenant une taille de 785408 blocs
(4k).
```

Remarque : il faut utiliser la commande resize2fs nom_systeme_fichiers pour étendre un système de fichiers ext.

```
# df -h /test1
Sys. de fichiers            Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/vgtest-lv_test1   3,0G    393M  2,6G  14% /test1
```

Suppression de la configuration

- Suppression de la configuration LVM :

```
# umount /test1
# lvremove /dev/vgtest/lv_test1
Do you really want to remove active logical volume lv_test1? [y/n]: y
  Logical volume "lv_test1" successfully removed
```

```
# vgremove vgtest
Do you really want to remove volume group "vgtest" containing 1 logical volumes? [y/n]: y
Do you really want to remove active logical volume lv_test2? [y/n]: y
  Logical volume "lv_test2" successfully removed
  Volume group "vgtest" successfully removed
```

```
# pvremove /dev/sd[bcd]1
  Labels on physical volume "/dev/sdb1" successfully wiped
  Labels on physical volume "/dev/sdc1" successfully wiped
  Labels on physical volume "/dev/sdd1" successfully wiped
```

Notes

Le démarrage du système et des services

Dans ce chapitre, nous allons étudier le processus complet de démarrage et d'arrêt d'un serveur Linux.

Table des matières

Le démarrage du système et des services

Le processus de démarrage

- La phase de boot : de l'allumage du système au chargement du noyau
- BIOS et UEFI
- démarrage sysVinit et systemd

Le processus de démarrage

Séquence de démarrage BIOS et MBR

Le BIOS est une puce qui est localisée sur la carte mère avec une mémoire de type EEPROM (Electric Erasable Programmable Read-Only Memory).

Lors du démarrage d'un système, le BIOS (Basic Input Output System) exécute ses POST (Power On Self Test) puis cherche parmi les périphériques indiqués dans la séquence de démarrage celui dont le premier secteur est une MBR.

Le BIOS lit la MBR (Maser Boot Record) qui se trouve sur le 1er secteur du 1er disque dur. Le BIOS lance le chargeur de démarrage primaire qui est stocké dans la MBR (GRUB stage1 en général qui pointe sur grub stage2).

Le chargeur de démarrage (bootloader) primaire (grub stage 1) lance le chargeur de démarrage secondaire (grub stage2) qui est localisé sous /boot.

Le chargeur de démarrage secondaire charge le noyau et les modules en mémoire, monte l'image initrd (initial ram disk).

Le noyau monte la partition contenant la racine en lecture seule.

Le noyau exécute le programme /sbin/init qui lit le fichier /etc/inittab. Le processus init a un PID de 1. Le mécanisme init charge le reste des services.

Ce rôle peut-être dévolu à systemd qui remplace le démarrage historique SysVinit. Dans ce cas le noyau exécute /usr/lib/systemd/systemd qui aura un PID 1. Le démarrage des services est effectué

par systemd.

Enfin, le système d'exploitation est opérationnel. La connexion devient possible par la présentation de l'invite de login.

Il existe deux implémentation de GRUB :

GRUB 0.9x : ancien GRUB présent sur les distributions CentOS 5 et 6 qui sera appelé grub legacy.

GRUB 2 : le nouveau GRUB présent à partir de la distribution CentOS7.

Remarque : Le fichier /proc/cmdline indique le noyau qui a été chargé en mémoire.

Séquence de démarrage UEFI et GPT

L'interface UEFI à l'instar de la MBR est chargée de contrôler la séquence de démarrage. Au contraire de la MBR, l'UEFI a sa propre architecture indépendemment de la CPU, et ses propres drivers. UEFI peut monter certaines partitions et lire certains systèmes de fichiers.

Au moment du demarrage l'interface UEFI cherche une partition particulière avec un GUID (Global Unique Identifer) qui la marque comme étant une partition ESP (EFI System Partition). Cette partition est par défaut localisée au début du disque et montée sur /boot/efi. Cette partition contient des applications qui sont compilées pour l'architecture efi, notamment des chargeurs de démarrage pour les systèmes d'exploitation et des utilitaires. La commande *efibootmgr* permet de paramétrer le chargeur de démarrage à exécuter (EFI DVC/CDROM ; EFI Hard Drive ; EFI Internal Shell).
GRUB est chargé en mémoire depuis la partition ESP.

Chaque chargeur de démarrage EFI (GRUB 2 souvent) doit-être stocké dans un sous-répertoire du répertoire EFI de la partition ESP (/boot/efi/EFI/centos, /boot/efi/EFI/redhat, /boot/efi/EFI/debian, …).

Partitionnement par défaut d'une distribution CentOS avec UEFI.

```
# df -h
Sys. de fichiers    Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/cl-root    17G    4,1G   13G  25% /
devtmpfs              905M       0  905M   0% /dev
tmpfs                 920M     96K  920M   1% /dev/shm
tmpfs                 920M    8,8M  911M   1% /run
tmpfs                 920M       0  920M   0% /sys/fs/cgroup
/dev/sda2            1014M    164M  851M  17% /boot
/dev/sda1             200M    9,5M  191M   5% /boot/efi
tmpfs                 184M       0  184M   0% /run/user/0
tmpfs                 184M    8,0K  184M   1% /run/user/1000
```

La partition est de type FAT.

```
# blkid /dev/sda1
/dev/sda1: SEC_TYPE="msdos" UUID="4A18-7E1E" TYPE="vfat" PARTLABEL="EFI System Partition"
PARTUUID="5c6c4cc1-dbec-4b75-bc1a-04d107191910"
```

Le répertoire contient le fichier grub.cfg.

```
# ls /boot/efi/EFI/centos/
BOOT.CSV  gcdx64.efi  grubenv      MokManager.efi   shim.efi
fonts     grub.cfg    grubx64.efi  shim-centos.efi
```

Remarque : Sur un système non UEFI, le fichier grub.cfg se trouve dans le répertoire /boot/grub2.

ATTENTION : Dans une machine virtuelle, il se peut d'arriver dans un Shell GPT après un redemarrage. Il faudra créer un fichier startup.nsh dans la partition efi. Évidemment le clavier est en qwerty pour compliquer la tache.

```
Shell> fs0:
FS0:\> edit startup.nsh
```

Cela ouvre le fichier vide startup.nsh dans lequel il faut ajouter la ligne suivante :

```
\EFI\centos\grubx64.efi
```

Avec un clavier azerty il faut donc taper la séquence suivante : *EFI*centos*grubx-':efi

Pour sauvegarder il faut taper CTRL-s ; pour quitter CTRL-a.

Le démarrage du système et des services

La chargement du noyau en mémoire avec grub2

- /boot/grub2/grub.cfg /boot/efi/EFI/centos/grub.cfg
- Le fichier /etc/default/grub
- Le répertoire /etc/grub.d

Le chargement du noyau en mémoire avec GRUB2

Exemple d'un grub2 sur CentOS 7

```
# more /boot/grub2/grub.cfg
#
# DO NOT EDIT THIS FILE
#
# It is automatically generated by grub2-mkconfig using templates
# from /etc/grub.d and settings from /etc/default/grub
#

### BEGIN /etc/grub.d/00_header ###


export menuentry_id_option
.......................

### BEGIN /etc/grub.d/10_linux ###
menuentry 'CentOS Linux, with Linux 3.10.0-229.14.1.el7.x86_64' --class centos --class
gnu-linux --class gnu --class os --unrestricted $menuentry_id_option '
gnulinux-3.10.0-229.14.1.el7.x86_64-advanced-7fce1258-9c75-4ba3-9a3c-4e2a8cf1c1dc' {
        load_video
        set gfxpayload=keep
        insmod gzio
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-
efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1'  80ce1fa7-9b
3e-47eb-992c-7a0b64a8ffbf
        else
          search --no-floppy --fs-uuid --set=root 80ce1fa7-9b3e-47eb-992c-7a0b64a8ffbf
        fi
```

```
        linux16 /vmlinuz-3.10.0-229.14.1.el7.x86_64 root=UUID=7fce1258-9c75-4ba3-9a3c-
4e2a8cf1c1dc ro vconsole.keymap=fr crashkernel=auto  vconsole.font=lata
rcyrheb-sun16 rhgb quiet
        initrd16 /initramfs-3.10.0-229.14.1.el7.x86_64.img
}
..................
```

Contrairement à grub legacy, le fichier de configuration de grub2 n'est pas modifiable directement.
Le fichier 'grub.cfg' est construit à partir de différents fichiers :

- le fichier /etc/default/grub
- les fichiers présents dans /etc/grub.d

Le fichier /etc/grub.d/40_custom permet de spécifier des entrées personnalisées.

Pour modifier les paramètres globaux de grub, il faut mettre à jour le fichier de configuration générique /etc/default/grub, puis exécuter la commande '*grub2-mkconfig*'.

```
# more /etc/default/grub
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="vconsole.keymap=fr crashkernel=auto  vconsole.font=latarcyrheb-sun16
rhgb quiet"
GRUB_DISABLE_RECOVERY="true"
```

Une fois les fichiers modifiés, il faut reconstruire le fichier 'grub.cfg'.
La commande '*grub2-mkconfig*' effectue cette opération.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-229.14.1.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-229.14.1.el7.x86_64.img
Found linux image: /boot/vmlinuz-3.10.0-123.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-123.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-7bf1837498aa45f9a2f731a1cba7b2c0
Found initrd image: /boot/initramfs-0-rescue-7bf1837498aa45f9a2f731a1cba7b2c0.img
done
```

Remarque : si vous utilisez les disques UEFI (non MBR), le fichier de configuration de grub se trouve dans /boot/efi/EFI/centos/grub.cfg. Il faudra donc indiquer le bon fichier de sortie à la commande '*grub2-mkconfig*'.

La ligne contenant set root ='hd0,msdos1' indique la partition qui contient le noyau.
La ligne contenant linux16 permet de localiser le noyau linux à charger. C'est un chemin relatif par rapport à la partition indentifié par set root.

'hd0,msdos1' fait référence à /dev/sda1 qui contient une table MBR.
'hd2,gpt2' fait référence à /dev/sdc2 qui contient une table GPT.

Attention: sur les versions précédentes de GRUB la ligne set root(hd0,1) faisait référence à la partition /dev/sda2 et non /dev/sda1.

Le démarrage du système et des services

Le système de démarrage historique de Linux

- Présentation de sysVinit
- niveaux d'init
- Présentation de upstart

Le système de démarrage historique de Linux

Sous beaucoup de distributions Linux, le système de démarrage est 'SysInit' qui fonctionne avec des niveaux de démarrage correspondant à des services qui sont démarrés selon le niveau.

La commande '*init*' peut prendre en argument un niveau pour l'atteindre.

Les différents niveaux d'init ou runlevel sont :

Niveau de démarrage	Signification
Niveau 0	arrêt électrique.
Niveau 1	mode mono-utilisateur ou Single User. C'est un mode de dépannage. Comme son nom l'indique on est seul sur la machine. Les services réseaux ne sont pas exécutés.
Niveau 2	mode multi-utilisateur sans certains services réseaux comme NFS.
Niveau 3	mode multi-utilisateur complet. Tous les services sont lancés à l'exception de l'interface graphique.
niveau 4	non utilisé. Peut servir pour un niveau personnalisé.
Niveau 5	c'est le niveau 3 avec l'interface graphique.
Niveau 6	mode réinitialisation. C'est le niveau d'init qui permet de rebooter la machine.

Les commandes 'runlevel' ou 'who -r' permettent de savoir à quel niveau de démarrage le système s'exécute.

```
# who -r
         niveau d'exécution 5 2017-10-18 10:29
# runlevel
N 5
```

L'affichage de la commande runlevel indique le niveau de démarrage précédent puis l'actuel. Le N signifie que le niveau de démarrage précédent n'existe pas, donc que la machine vient de démarrer.

```
# init 3
# runlevel
5 3
```

La commande 'shutdown' permet d'arrêter une machine. Des options et arguments de la commande permettent de rebooter la machine (option -r), d'attendre un délai et d'envoyer un message par broadcast à tous les utilisateurs connectés. L'option '-c' permet d'arrêter un shutdown qui a été programmé.

```
# shutdown -r +2  "Reboot de la machine dans deux minutes"
Shutdown scheduled for mer. 2017-10-18 14:03:24 CEST, use 'shutdown -c' to cancel.
```

```
# shutdown -c
Broadcast message from root@cent1708 (Wed 2017-10-18 14:01:51 CEST):
The system shutdown has been cancelled at Wed 2017-10-18 14:02:51 CEST!
```

```
# shutdown 18:30 "Arret de la machine à 18h30"
Shutdown scheduled for mer. 2017-10-18 18:30:00 CEST, use 'shutdown -c' to cancel.
```

Remarque : La commande shutdown exige une heure ou un délai. Le mot clef now permet d'effectuer l'action immédiatement.

Le gestion des services systemd

Présentation de systemd

- La commande systemctl
- mulit-user.targer et graphical.target
- systemctl isolate
- systemctl set-default

Présentation de systemd

Systemd a été développé pour répondre à la problématique du démarrage séquentiel des services. Avec systemd, il faut atteindre une cible (target). Les deux cibles correspondant aux niveaux de démarrage 3 et 5 sont respectivement multi-user.target et graphical.target. Systemd gère les dépendances entre les services. Ainsi le niveau grapical.target dépend du niveau multi-user.target. Lorsque systemd démarre, il veut arriver au niveau default.target qui est un lien symbolique vers le niveau de démarrage désiré.

Afficher le niveau de démarrage par défaut.

```
# systemctl get-default
graphical.target
# ls -l /etc/systemd/system/default.target
lrwxrwxrwx. 1 root root 36 24 sept. 11:31 /etc/systemd/system/default.target ->
/lib/systemd/system/graphical.target
```

La commande *systemctl* permet de modifier la cible par défaut lors du prochain redémarrage.

```
# systemctl set-default multi-user.target
rm '/etc/systemd/system/default.target'
ln -s '/usr/lib/systemd/system/multi-user.target' '/etc/systemd/system/default.target'
```

La commande a supprimé et recréé le lien symbolique.

```
# ls -l /etc/systemd/system/default.target
lrwxrwxrwx 1 root root 41 26 janv. 12:16 /etc/systemd/system/default.target ->
/usr/lib/systemd/system/multi-user.target
```

Le changement de niveau peut s'effectuer avec la commande systemctl.

```
# runlevel
N 5

# systemctl isolate multi-user.target

# runlevel
5 3

# systemctl isolate graphical.target

# runlevel
3 5
```

Tableau de correspondance entre les commandes de SysInit et de systemd.

Commande sysVinit	Équivalence systemd	Observations
`init 0`	`systemctl poweroff` `init 0`	Arrêt du système

`init 1,s`	`systemctl isolate runlevel1.target`
	`systemctl rescue`
	`init 1; init s`
		Mode single-user

`init 2`	`systemctl isolate runlevel2.target`
	`systemctl isolate multi-user.target`
	`init 2`
		Par défaut identique au niveau 3

`init 3`	`systemctl isolate runlevel3.target`
	`systemctl isolate multi-user.target`
	`init 3`
		Mode multi-user sans l'interface graphique

`init 4`	`systemctl isolate runlevel4.target`
	`systemctl isolate multi-user.target`
	`init 4`
		Par défaut identique au niveau 3

`init 5`	`systemctl isolate runlevel5.target`
	`systemctl isolate graphical.target`
	`init 5`
		Identique au niveau 3 avec l'interface graphique

`init 6`	`systemctl reboot` `init 6`	Redémarrage du système

Le démarrage du système et des services

La gestion des services avec systemd

- systemctl stop
- systemctl start
- systemctl restart
- systemctl reload
- systemctl status

- systemctl disable
- systemctl enable

La gestion des services systemd

Arrêter, démarrer, redémarrer, recharger un service :

```
# systemctl stop crond.service
# systemctl start crond.service
# systemctl restart crond.service
# systemctl reload crond.service
```

Remarque : La commande service a été réécrite de façon à prendre en charge la commande systemctl.

```
# service crond stop
Redirecting to /bin/systemctl stop  crond.service
```

Statut d'un service :

Le service est inactif.

```
# systemctl status crond.service
crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled)
   Active: inactive (dead) since mar. 2016-01-26 14:01:41 CET; 27s ago
  Process: 1397 ExecStart=/usr/sbin/crond -n $CRONDARGS (code=exited, status=0/S
UCCESS)
 Main PID: 1397 (code=exited, status=0/SUCCESS)

janv. 26 14:00:02 formateur systemd[1]: Started Command Scheduler.
janv. 26 14:00:02 formateur crond[1397]: (CRON) INFO (RANDOM_DELAY will be s...)
janv. 26 14:00:02 formateur crond[1397]: (CRON) INFO (running with inotify s...)
janv. 26 14:01:41 formateur systemd[1]: Stopping Command Scheduler...
janv. 26 14:01:41 formateur systemd[1]: Stopped Command Scheduler.
Hint: Some lines were ellipsized, use -l to show in full.
```

Le service est actif.

```
# systemctl status crond.service
crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled)
   Active: active (running) since mar. 2016-01-26 14:02:49 CET; 1s ago
 Main PID: 2736 (crond)
   CGroup: /system.slice/crond.service
           └─2736 /usr/sbin/crond -n

janv. 26 14:02:49 formateur systemd[1]: Starting Command Scheduler...
janv. 26 14:02:49 formateur systemd[1]: Started Command Scheduler.
janv. 26 14:02:49 formateur crond[2736]: (CRON) INFO (RANDOM_DELAY will be scaled with
factor 10% if used.)
janv. 26 14:02:49 formateur crond[2736]: (CRON) INFO (running with inotify support)
janv. 26 14:02:49 formateur crond[2736]: (CRON) INFO (@reboot jobs will be run at
computer's startup.)
```

Désactiver un service pour qu'il ne démarre pas lors du démarrage du système

```
# systemctl disable crond.service
rm '/etc/systemd/system/multi-user.target.wants/crond.service'
```

On constate que la désactivation du service est simplement la suppression du lien symbolique.

```
# systemctl status crond.service
crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; disabled)
   Active: active (running) since mar. 2016-01-26 14:07:32 CET; 25s ago
 Main PID: 2841 (crond)
   CGroup: /system.slice/crond.service
           └─2841 /usr/sbin/crond -n

janv. 26 14:07:32 formateur systemd[1]: Starting Command Scheduler...
janv. 26 14:07:32 formateur systemd[1]: Started Command Scheduler.
janv. 26 14:07:32 formateur crond[2841]: (CRON) INFO (RANDOM_DELAY will be scaled with
factor 47% if used.)
janv. 26 14:07:32 formateur crond[2841]: (CRON) INFO (running with inotify support)
janv. 26 14:07:32 formateur crond[2841]: (CRON) INFO (@reboot jobs will be run at
computer's startup.)
```

Activer un service pour qu'il démarre au boot :

```
# systemctl enable crond.service
ln -s '/usr/lib/systemd/system/crond.service' '/etc/systemd/system/multi-
user.target.wants/crond.service'
```

```
# systemctl status crond.service
crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled)
   Active: active (running) since mar. 2016-01-26 14:07:32 CET; 2min 32s ago
 Main PID: 2841 (crond)
   CGroup: /system.slice/crond.service
           └─2841 /usr/sbin/crond -n

janv. 26 14:07:32 formateur systemd[1]: Starting Command Scheduler...
janv. 26 14:07:32 formateur systemd[1]: Started Command Scheduler.
janv. 26 14:07:32 formateur crond[2841]: (CRON) INFO (RANDOM_DELAY will be scaled with
factor 47% if used.)
janv. 26 14:07:32 formateur crond[2841]: (CRON) INFO (running with inotify support)
janv. 26 14:07:32 formateur crond[2841]: (CRON) INFO (@reboot jobs will be run at
computer's startup.)
```

Le démarrage du système et des services

Les fichiers de configuration systemd

- /etc/systemd/system.conf
- /etc/systemd/system/...

Les fichiers de configuration systemd

Les fichiers de configuration de systemd sont situés dans /etc/systemd. Le fichier de configuration principal est /etc/systemd/system.conf. Il se présente sous la forme 'variable=valeur'.

```
# more /etc/systemd/system.conf
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See systemd-system.conf(5) for details.

[Manager]
#LogLevel=info
#LogTarget=journal-or-kmsg
#LogColor=yes
#LogLocation=no
#DumpCore=yes
#CrashShell=no
#ShowStatus=yes
#CrashChVT=1
#CPUAffinity=1 2
#JoinControllers=cpu,cpuacct net_cls,net_prio
#RuntimeWatchdogSec=0
#ShutdownWatchdogSec=10min
#CapabilityBoundingSet=
```

```
#SystemCallArchitectures=
#TimerSlackNSec=
#DefaultTimerAccuracySec=1min
#DefaultStandardOutput=journal
#DefaultStandardError=inherit
#DefaultTimeoutStartSec=90s
#DefaultTimeoutStopSec=90s
#DefaultRestartSec=100ms
#DefaultStartLimitInterval=10s
#DefaultStartLimitBurst=5
#DefaultEnvironment=
#DefaultCPUAccounting=no
#DefaultBlockIOAccounting=no
#DefaultMemoryAccounting=no
#DefaultLimitCPU=
#DefaultLimitFSIZE=
#DefaultLimitDATA=
#DefaultLimitSTACK=
#DefaultLimitCORE=
#DefaultLimitRSS=
#DefaultLimitNOFILE=
#DefaultLimitAS=
#DefaultLimitNPROC=
#DefaultLimitMEMLOCK=
#DefaultLimitLOCKS=
#DefaultLimitSIGPENDING=
#DefaultLimitMSGQUEUE=
#DefaultLimitNICE=
#DefaultLimitRTPRIO=
#DefaultLimitRTTIME=
```

Vous pouvez modifier des paramètres dans ce fichier ou effectuer la modification directement au niveau du noyau. Certains fichiers sont présents aussi bien dans /etc/systemd/system et dans /lib/systemd/system avec un contenu différent. Pour afficher quel répertoire est prioritaire exécuter la commande suivante :

```
# pkg-config systemd --variable=systemdsystemunitdir
/usr/lib/systemd/system
```

Les fichiers de configuration peuvent avoir une ou plusieurs sections en fonction du type de service. La section [Unit] contient les options génériques qui permettent de spécifier le comportement de l'unité en définissant les liens de dépendances avec les autres unités.

Mot clef section [Unit]	Signification
Description	Une description du service.
Documentation	La documentation associée au service.
Requires	Indique ce qui est requis pour considérer que le niveau soit considéré comme actif. Cette section indique donc les dépendances du service. Si le lancement d'une unité échoue, l'unité n'est pas activée.
After	Permet d'indiquer l'ordre d'activation des unités. L'unité n'est lancée qu'après l'activation des unités spécifiées. After n'active pas explicitement les unités spécifées (contrairement à Requires).
Wants	Une version plus légère de Requires. Si une des unités indiquées ne démarre pas, cela n'aura pas de conséquences sur l'unité à activer.
Conflicts	Indique les niveaux pour lequel le service est en conflit c'est dire pour quel niveaux il ne faut pas le démarrer.
AllowIsolate	Permet de simuler le changement de niveau comme avec sysInit

```
# ls -l /etc/systemd/system/default.target
lrwxrwxrwx 1 root root 40 26 janv. 12:18 /etc/systemd/system/default.target ->
/usr/lib/systemd/system/graphical.target
# more /usr/lib/systemd/system/graphical.target
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

[Unit]
Description=Graphical Interface
Documentation=man:systemd.special(7)
Requires=multi-user.target
Wants=display-manager.service
Conflicts=rescue.service rescue.target
After=multi-user.target rescue.service rescue.target display-manager.service
AllowIsolate=yes
```

Pour atteindre le niveau graphical-target il faut que le niveau multi-user.target soit activé (Option Requires). Pour atteindre ce niveau il a besoin que le display manager soit activé (Option Wants). Si le display manager n'est pas démarré cela n'empêche pas le système de démarrer.
Si le système démarre en mode secours l'unité graphical.target n'est pas démarré (Option Conflict).
Le système attend que les unités spécifiés par l'option After soit démarrées avant d'atteindre le niveau d'exécution spécifiée.

La section [Install] indique à systemctl ce qu'il doit effectuer lors de l'activation ou désactivation d'un service dans systemd (enable ou disable).

Mot clef section [Install]	Signification
RequiredBy	Indique la liste des unités qui dépendent de l'unité. Lors de l'activation de cette unité, les unités listées dans RequiredBy recoivent une dépendance Require de l'unité.
WantedBy=XYZ	Indique pour quel niveau le service doit être démarré. Lors de l'activation de cette unité, les unités listées dans WantedBy recoivent une dépendance Want de l'unité.
Also	Indique des unités supplémentaires à installer ou désinstaller avec l'unité.
Alias	Indique une liste d'alias séparés par des espaces pour l'unité. Les commandes systemctl peuvent utiliser ce nom d'alias à la place du nom officiel (à part systemctl enable).
DefaultInstance	Réservé pour les unités instancées. Permet d'indiquer quelle est l'instance par défaut.

La section [type d'unité] regroupent les directives spécifique au type. Pour le démarrage des services linux, les fichiers de configuration contiennent la section [Service].

Mot clef section [Service]	Signification
Type	Indique le type de demarrage des processus constituant l'unité. Cela a une incidence sur le démarrage des processus lancés par la directive ExecStart. **simple** → Valeur par défaut. Le processus lancé par ExecStart est le processus principal du service. **forking** → Le processus lancé par ExecStart engendre un processus fils qui devient le processus principal du service. Le processus parent lorsque le fils a terminé. **oneshot** → Similaire à simple mais le processus s'arrête avant de lancer les unités suivantes. **dbus** → Similaire à simple mais les unitées suivantes ne sont lancés que si le processus principal a obtenu un nom d-bus. **notify** → Similaire à simple mais les unitées suivantes ne sont lancés qu'après l'envoi d'un message de notification grâce à la fonction sd_notify(). **idle** → similaire à simple. L'exécution du binaire se produit après que toutes les tâches soient terminées. Cela évite de mélanger la sortie du status avec la sortie shell des services.
ExecStart	Indique la commande à exécuter avec ses options ou arguments lors du démarrage du service.
ExecStop	Indique la commande à exécuter lors de l'arrêt du service.
ExecReload	Indique la commande à exécuter lors du rechargement du service
Restart	Permet de redémarrer automatiquement le service si le processus a été arreté (excepté pour un arrêt propre avec systemctl)
RemainAfterExit	Valeur booléenne (true ou false) configurée à false par défaut. Positionnée sur true, le service est considéré comme actif même si aucun processus n'est actif. Utilisé quand Type est configuré sur oneshot
KillMode	Indique commente le processus doit être "tué". Les valeurs permises sont: control-group process mixed none
KillSignal	Indique quel signal envoyer en premier pour "tuer" un service lorsqu'il est désactivé. Le signal SIGKILL est utilisé par défaut.

Fichier de configuration du service 'crond'.

```
# more /usr/lib/systemd/system/crond.service
[Unit]
Description=Command Scheduler
After=auditd.service systemd-user-sessions.service time-sync.target

[Service]
EnvironmentFile=/etc/sysconfig/crond
ExecStart=/usr/sbin/crond -n $CRONDARGS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process

[Install]
WantedBy=multi-user.target
```

L'équivalent de la directive 'respawn' proposée par sysinit est réalisé par la directive 'Restart='. La directive 'RestartSec=' permet de configurer la durée au bout duquel il faut relancer le service.

```
# more /etc/systemd/system/getty.target.wants/getty@tty1.service
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

[Unit]
Description=Getty on %I
Documentation=man:agetty(8) man:systemd-getty-generator(8)
Documentation=http://0pointer.de/blog/projects/serial-console.html
After=systemd-user-sessions.service plymouth-quit-wait.service
After=rc-local.service

# If additional gettys are spawned during boot then we should make
# sure that this is synchronized before getty.target, even though
# getty.target didn't actually pull it in.
Before=getty.target
IgnoreOnIsolate=yes

# On systems without virtual consoles, don't start any getty. Note
# that serial gettys are covered by serial-getty@.service, not this
# unit.
ConditionPathExists=/dev/tty0

[Service]
# the VT is cleared by TTYVTDisallocate
ExecStart=-/sbin/agetty --noclear %I $TERM
Type=idle
Restart=always
RestartSec=0
UtmpIdentifier=%I
TTYPath=/dev/%I
TTYReset=yes
TTYVHangup=yes
TTYVTDisallocate=yes
KillMode=process
IgnoreSIGPIPE=no
SendSIGHUP=yes

# Unset locale for the console getty since the console has problems
# displaying some internationalized messages.
Environment=LANG= LANGUAGE= LC_CTYPE= LC_NUMERIC= LC_TIME= LC_COLLATE= LC_MONETARY=
LC_MESSAGES= LC_PAPER= LC_NAME= LC_ADDRESS= LC_TELEPHONE= LC_MEASURE
MENT= LC_IDENTIFICATION=

[Install]
WantedBy=getty.target
DefaultInstance=tty1
```

Visualiser le fichier de configuration d'un service avec systemctl.

```
# systemctl cat crond.service
# /usr/lib/systemd/system/crond.service
[Unit]
Description=Command Scheduler
After=auditd.service systemd-user-sessions.service time-sync.target

[Service]
EnvironmentFile=/etc/sysconfig/crond
ExecStart=/usr/sbin/crond -n $CRONDARGS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process

[Install]
WantedBy=multi-user.target
```

Pour modifier ce fichier de configuration la sous-commande '*edit*' permet de l'éditer.
Par défaut, l'éditeur **nano** est utilisé. Il faut modifier la variable **EDITOR** pour utiliser un autre éditeur.

```
# export EDITOR=/usr/bin/vi
# systemctl edit crond.service
```

Pour éditer le fichier avec sa configuration actuelle, il faut ajouter l'option '--full' à la sous-commande 'edit'.

```
# systemctl edit --full crond.service
```

Visualiser la configuration très détaillée d'un service :

```
# systemctl show crond.service
Id=crond.service
Names=crond.service
Requires=basic.target
Wants=system.slice
WantedBy=multi-user.target
Conflicts=shutdown.target
Before=shutdown.target multi-user.target
After=auditd.service systemd-user-sessions.service time-sync.target systemd-
journald.socket basic.target system.slice
Description=Command Scheduler
LoadState=loaded
ActiveState=inactive
SubState=dead
FragmentPath=/usr/lib/systemd/system/crond.service
UnitFileState=enabled
InactiveExitTimestamp=mar. 2016-01-26 14:07:32 CET
InactiveExitTimestampMonotonic=593225746
…….....
```

Le démarrage du système et des services

Ajout d'un service de démarrage systemd

- Création du script
- Création du fichier systemd
- systemctl --system deamon-reload

Ajout d'un service de démarrage systemd

Création d'un script de démarrage avec systemd.

Le script 'systemd-perso' est localisé dans /usr/lib/systemd

```
# cat /usr/lib/systemd/systemd-perso
#!/bin/sh
case $1 in
        start) echo "Le service perso démarre le $(date)" >> /demarre ;;
         stop) echo "Le service perso s'arrete le $(date)" >> /arret ;;
            *) echo "Usage: $0 {start|stop}" ;;
esac
```

Créer le fichier monservice.service pour mettre le service sous le contrôle de systemd et le rendre exécutable.

```
# cat /usr/lib/systemd/system/perso.service
[Unit]
Description="Test d'un service perso"
After=systemd-user-sessions.service

[Service]
ExecStart=/usr/lib/systemd/systemd-perso start
ExecStop=/usr/lib/systemd/systemd-perso stop

[Install]
WantedBy=multi-user.target
```

Rechargement de systemd :

```
# systemctl --system daemon-reload
```

Vérification :

```
# systemctl start perso.service
# cat /demarre
Le service perso démarre le ven. oct. 20 15:35:31 CEST 2017
```

```
# systemctl stop perso.service
# cat /arret
Le service perso s'arrete le ven. oct. 20 15:35:31 CEST 2017
```

Activation pour le prochain démarrage :

```
# systemctl enable perso.service
Created symlink from /etc/systemd/system/multi-user.target.wants/perso.service to
/usr/lib/systemd/system/perso.service.
```

Le démarrage du système et des services

Procédures d'arrêt et de redémarrage

- systemctl halt
- systemctl poweroff
- systemctl reboot
- systemctl suspend
- systemctl hibernate
- systemctl hybrid-sleep

Pour basculer dans le mode rescue il faut passer cet argument à la commande *systemctl*.

```
# systemctl rescue
```

est équivalent à

```
# systemctl isolate rescue.target
```

Pour basculer en mode emergency il faut passer cet argument à systemctl. Dans ce mode le système montera la racine en lecture sans monter d'autres systèmes de fichiers locaux.

```
# systemctl emergency
```

Par défaut avec cette commande un message est envoyé par broadcast à tous les utilisateurs qui sont connectés sur le serveur. Pour empêcher l'envoi du message il faut utiliser l'option --no-wall.

```
# systemctl --no-wall emergency
```

Arrêter le système et mettre la machine hors tension.

```
# systemctl poweroff
```

Arrêter le système sans mettre la machine hors tension.

```
# systemctl halt
# systemctl --no-wall halt
```

La commande shutdown peut-être utilisé pour envoyer un halt ou un poweroff grace aux options -H (--halt) ou -P (--poweroff).

Le fichier /run/nologin est créé 5 minutes avant la fermeture du système pour éviter de nouvelles connexions. Avec un argument de temps passé à la commande shutdown il est possible d'envoyer un message.

```
# shutdown --poweroff
```

Pour suspendre un arret programmé il faut passer l'option '-c' à la commande shutdown.

```
# shutdown -c
```

Suspendre le système. Cela sauvegarde l'état système en RAM excepté les module RAM et éteint la plupart des périphériques de la machine. Quand vous rallumez la machine, l'état est restauré depuis la RAM sans avoir besoin de booter à nouveau. Etant donné que l'état du système est restauré de puis la RAM, restaurer le système dans état suspendu est plus rapide que dans l'état d'hibernation (restauration depuis le disque) mais reste plus sensible aux problèmes électriques.

```
# systemctl suspend
```

Mettre le système en hibernation. Cela sauvegarde l'état système sur le diques et éteint la machine. Quand vous rallumez la machine, l'état est restauré depuis le disque sans avoir besoin de booter à nouveau. La RAM n'a pas besoin d'etre alimenté électriquement vu que la restauration se fait depuis le disque dur.

```
# systemctl hibernate
```

La commande suivante permet de suspendre le système et de le mettre en hibernation.

```
# systemctl hybrid-sleep
```

Le démarrage du système et des services

Les unités systemd

- Les différents types d'unités
- les unités prédéfinies
- /usr/lib/systemd/system

Les unités systemd

Chaque objet basique qu'administre systemd est une « unité » (unit). Les unités peuvent-être de différents types. Le type le plus courant est le type service (le fichier se termine par l'extension .service). Pour administrer ses services, l'outil principal est la commande systemctl. Chaque unité a un état (active, inactive, failed). Systemd travaille beaucoup avec des liens symboliques. Les fichiers présents dans /etc/systemd/system pointent sur /usr/lib/systemd/system. Systemd intègre la gestion des logs et le contrôle des PID des services lancés. L'avantage de systemd est de pouvoir lancer des services en parallèle dont les services ne sont pas dépendants.

Systemd peut aussi lancer en parallèle des processus inter-dépendants. Pour cela, il va anticiper le démarrage du service en créant une socket unix pour tout service à démarrer. Les services dépendants de ce service vont se connecter sur la socket alors que le service n'est pas encore actif. Une fois actif, systemd lui passera la socket pour que les services dépendants démarrent.

Type d'unité	Description
automount	Permet de gérer l'auto-monteur
mount	Permet de gérer le fichier /etc/fstab
path	Permet de gérer d'autres services
service	Permet de démarrer et de gérer des services lancés par des scripts ou par systemd
snapshot	Permet de revenir à une configuration précédente grâce au mécanisme des snapshots
socket	Une socket est associée à un service. L'accès à la socket va démarrer le service.
target	Permet de regrouper les unités par cible.
timer	Permet d'activer des unités à une date spécifique
swap	Permet l'activation de l'espace de swap

Chaque unité possède un fichier de configuration. Le type d'unité est donné par le suffixe du nom du fichier de configuration. Par exemple, le fichier crond.service est de type service.

Il existe un certain nombre d'unités prédéfinie. Ils permettent entre autres de booter au niveau de démarrage désiré.

Nom de l'unité	Description
basic.target	Taches à exécuter assez tôt
default.target	Lien symbolique vers graphical.target (ou multi-user.target) qui indique le niveau de démarrage par défaut.
Emergency.target, rescue.target, halt.target, poweroff.target reboot.target shutdown.target	Unités exécutées lors du démarrage, arrêt, reboot de la machine. La commande suivante permet d'arriver au mode rescue : **# systemctl rescue.target**
sysinit.target	Target permettant l'initialisation du système. Il est exécuté quelque soit le niveau de démarrage.
runlevelN.target	Permet de simuler les changements de niveaux comme sous sysinit. Ce sont des liens symboliques. Par exemple runlevel5.target pointe sur graphical.target.
local-fs.target	Permet le montage des systèmes de fichiers locaux
remote-fs.target	Permet le montage des systèmes de fichiers distants
swap.target	Permet l'activation des espaces de swap
network.target	Permet la gestion du réseau

Lister toutes les unités de type target.

```
# systemctl list-units --type target
UNIT                   LOAD   ACTIVE SUB    DESCRIPTION
basic.target           loaded active active Basic System
cryptsetup.target      loaded active active Encrypted Volumes
getty.target           loaded active active Login Prompts
graphical.target       loaded active active Graphical Interface
local-fs-pre.target    loaded active active Local File Systems (Pre)
local-fs.target        loaded active active Local File Systems
multi-user.target      loaded active active Multi-User System
network-online.target  loaded active active Network is Online
network-pre.target     loaded active active Network (Pre)
network.target         loaded active active Network
nfs-client.target      loaded active active NFS client services
nss-user-lookup.target loaded active active User and Group Name Lookups
paths.target           loaded active active Paths
remote-fs-pre.target   loaded active active Remote File Systems (Pre)
remote-fs.target       loaded active active Remote File Systems
slices.target          loaded active active Slices
sockets.target         loaded active active Sockets
sound.target           loaded active active Sound Card
swap.target            loaded active active Swap
sysinit.target         loaded active active System Initialization
timers.target          loaded active active Timers

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

21 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

Le démarrage du système et des services

Lister les unités systemd

- systemctl list-units
- systemctl list-units –all
- systemctl list-units-files
- systemctl list-dependencies
- systemctl cat
- systemctl show
- systemctl edit

Lister les unités sytemd

Lister toutes les unités actives de systemd :

```
# systemctl list-units
UNIT                                        LOAD   ACTIVE SUB       DESCRIPTION
proc-sys-fs-binfmt_misc.automount           loaded active running   Arbitrary Executable File Formats File
System
sys-devices-pc...0:0-1:0:0:0-block-sr0.device loaded active plugged   VBOX_CD-ROM
sys-devices-pc...00:00:03.0-net-enp0s3.device loaded active plugged   PRO/1000 MT Desktop Adapter
sys-devices-pc...0:00:05.0-sound-card0.device loaded active plugged   82801AA AC'97 Audio Controller
sys-devices-pc...00:00:08.0-net-enp0s8.device loaded active plugged   PRO/1000 MT Desktop Adapter
sys-devices-pc...:0:0:0-block-sda-sda1.device loaded active plugged   VBOX_HARDDISK
…....
swap.target                                 loaded active active    Swap
sysinit.target                              loaded active active    System Initialization
timers.target                               loaded active active    Timers
systemd-tmpfiles-clean.timer                loaded active waiting   Daily Cleanup of Temporary Directories

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

153 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

Lister toutes les unités chargées en mémoire par systemd (y compris celles qui ne sont pas actuellement actives) :

```
# systemctl list-units --all
UNIT                                    LOAD   ACTIVE   SUB       DESCRIPTION
proc-sys-fs-binfmt_misc.automount       loaded active   running   Arbitrary Executable File Formats File
System
dev-cdrom.device                        loaded active   plugged   VBOX_CD-ROM
dev-disk-by\x2...dROM_VB2\x2d01700376.device loaded active   plugged   VBOX_CD-ROM
dev-disk-by\x2...43b3e45f\x2d0af958ea.device loaded active   plugged   VBOX_HARDDISK
dev-disk-by\x2...7597ecbf\x2d765648a1.device loaded active   plugged   VBOX_HARDDISK
dev-disk-by\x2...7f7a6522\x2d94f27455.device loaded active   plugged   VBOX_HARDDISK
…....
systemd-tmpfiles-clean.timer            loaded active   waiting   Daily Cleanup of Temporary Directories

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

293 loaded units listed.
To show all installed unit files use 'systemctl list-unit-files'.
```

Lister toutes les unités installées sur le système (y compris celles qui ne sont pas chargées en mémoire).

```
# systemctl list-unit-files
UNIT FILE                                   STATE
proc-sys-fs-binfmt_misc.automount           static
dev-hugepages.mount                         static
dev-mqueue.mount                            static
proc-fs-nfsd.mount                          static
proc-sys-fs-binfmt_misc.mount               static
sys-fs-fuse-connections.mount               static
sys-kernel-config.mount                     static
sys-kernel-debug.mount                      static
tmp.mount                                   disabled
var-lib-nfs-rpc_pipefs.mount                static
….............
mdadm-last-resort@.timer                    static
systemd-readahead-done.timer                static
systemd-tmpfiles-clean.timer                static

334 unit files listed.
```

Pour un service particulier :

```
# systemctl list-unit-files crond.service
UNIT FILE     STATE
crond.service enabled

1 unit files listed.
```

La sortie de la commande 'systemctl list-units' peut varier en fonction de la version de systemctl. Il est conseillé de mettre systemd à jour avec yum.

```
# yum upgrade -y systemd
# systemctl list-units
  UNIT                                                LOAD   ACTIVE     SUB       JOB   DESCRIPTION
  proc-sys-fs-binfmt_misc.automount                   loaded active     running         Arbitrary Executable
File Formats File System Automount Po
  sys-devices-pci0000:00-0000:00:01.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.device loaded active     plugged
VBOX_CD-ROM CentOS_7_x86_64
  sys-devices-pci0000:00-0000:00:03.0-net-enp0s3.device     loaded active     plugged         PRO/1000 MT Desktop
Adapter
  sys-devices-pci0000:00-0000:00:05.0-sound-card0.device    loaded active     plugged         82801AA AC'97 Audio
Controller
  sys-devices-pci0000:00-0000:00:08.0-net-enp0s8.device     loaded active     plugged         PRO/1000 MT Desktop
Adapter
  sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sda1.device loaded active
plugged         VBOX_HARDDISK 1
  sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sda2.device loaded active
plugged         VBOX_HARDDISK 2
  sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sda3.device loaded active
plugged         VBOX_HARDDISK 3
…
```

Lister les dépendances d'un service :

```
# systemctl list-dependencies crond.service
crond.service
├─system.slice
└─basic.target
  ├─alsa-restore.service
  ├─alsa-state.service
  ├─firewalld.service
  ├─microcode.service
  ├─rhel-autorelabel-mark.service
  ├─rhel-autorelabel.service
  ├─rhel-configure.service
  ├─rhel-dmesg.service
  ├─rhel-loadmodules.service
  ├─paths.target
  ├─slices.target
  │ ├─-.slice
  │ └─system.slice
  ├─sockets.target
  │ ├─avahi-daemon.socket
  │ ├─cups.socket
  │ ├─dbus.socket
  │ ├─dm-event.socket
  │ ├─iscsid.socket
  │ ├─iscsiuio.socket
  │ ├─lvm2-lvmetad.socket
  │ ├─rpcbind.socket
  │ ├─systemd-initctl.socket
  │ ├─systemd-journald.socket
  │ ├─systemd-shutdownd.socket
  │ ├─systemd-udevd-control.socket
  │ └─systemd-udevd-kernel.socket
```

Lister les dépendances avec l'affichage étendu pour les unités :

```
# systemctl list-dependencies --all crond.service
crond.service
├─system.slice
│ └─-.slice
└─basic.target
  ├─alsa-restore.service
  ├─alsa-state.service
  ├─firewalld.service
  │ ├─dbus.socket
  │ │ ├─-.mount
  │ │ │ └─system.slice
  │ │ │   └─-.slice
  │ │ ├─system.slice
  │ │ │ └─-.slice
  │ │ ├─var.mount
  │ │ │ ├─-.mount
  │ │ │ │ └─system.slice
  │ │ │ │   └─-.slice
  │ │ │ ├─system.slice
```

Lister les unités d'un type spécifique :

```
# systemctl list-unit-files --type=socket
UNIT FILE                    STATE
avahi-daemon.socket          enabled
cups.socket                  enabled
dbus.socket                  static
dm-event.socket              enabled
iscsid.socket                enabled
iscsiuio.socket              enabled
libvirtd.socket              static
lldpad.socket                disabled
lvm2-lvmetad.socket          enabled
rpcbind.socket               enabled
rsyncd.socket                disabled
sshd.socket                  disabled
syslog.socket                static
systemd-initctl.socket       static
systemd-journald.socket      static
systemd-networkd.socket      disabled
systemd-shutdownd.socket     static
systemd-udevd-control.socket static
systemd-udevd-kernel.socket  static
virtlockd.socket             disabled

20 unit files listed.
```

```
# systemctl list-unit-files --type=target
UNIT FILE                 STATE
basic.target              static
bluetooth.target          static
cryptsetup-pre.target     static
cryptsetup.target         static
ctrl-alt-del.target       disabled
default.target            enabled
emergency.target          static
final.target              static
getty.target              static
graphical.target          enabled
halt.target               disabled
hibernate.target          static
hybrid-sleep.target       static
initrd-fs.target          static
initrd-root-fs.target     static
initrd-switch-root.target static
initrd.target             static
iprutils.target           disabled
kexec.target              disabled
local-fs-pre.target       static
local-fs.target           static
machines.target           disabled
multi-user.target         static
network-online.target     static
.................
```

Le démarrage du système et des services

Outils systemd

- systemd-analyze
- systemd-analyze blame
- systemctl -H nom_user@nom_machine commande

Outils systemd

Systemd intègre des outils d'analyse, notamment pour savoir le temps de démarrage global et celui de chaque service.

```
# systemd-analyze
Startup finished in 455ms (kernel) + 4.519s (initrd) + 2min 20.832s (userspace) = 2min
25.806s
```

Avec l'exemple ci-dessus, il a fallu 0,455 seconde pour charger le noyau, 4,519 secondes pour charger l'initial RAM disque (initrd) et 140,832 secondes pour charger l'espace utilisateur.

```
# systemd-analyze blame
      2min 730ms iscsi.service
          5.396s NetworkManager-wait-online.service
          5.064s firewalld.service
          4.141s ModemManager.service
          4.051s tuned.service
          3.650s accounts-daemon.service
          2.970s gssproxy.service
          2.319s plymouth-quit-wait.service
          2.310s avahi-daemon.service
          2.289s kdump.service
          2.124s rsyslog.service
          1.986s systemd-udev-settle.service
          1.273s systemd-fsck-root.service
          1.229s lvm2-monitor.service
          1.124s sysstat.service
          1.056s multipathd.service
           950ms chronyd.service
```

Arborescence des services

```
# systemd-analyze critical-chain
The time after the unit is active or started is printed after the "@" character.
The time the unit takes to start is printed after the "+" character.

graphical.target @39.158s
└─multi-user.target @39.158s
  └─postfix.service @27.754s +7.085s
    └─network.target @27.753s
      └─network.service @26.926s +825ms
        └─NetworkManager-wait-online.service @20.408s +6.507s
          └─NetworkManager.service @19.738s +666ms
            └─firewalld.service @17.131s +2.603s
              └─polkit.service @11.783s +5.328s
                └─basic.target @10.697s
                  └─sockets.target @10.697s
                    └─avahi-daemon.socket @10.696s
                      └─sysinit.target @10.651s
                        └─systemd-update-utmp.service @10.564s +85ms
                          └─auditd.service @9.789s +773ms
                            └─systemd-tmpfiles-setup.service @9.705s +81ms
                              └─rhel-import-state.service @9.263s +442ms
                                └─local-fs.target @9.262s
                                  └─run-user-42.mount @37.586s
                                    └─local-fs-pre.target @7.605s
                                      └─lvm2-monitor.service @2.988s +4.615s
                                        └─lvm2-lvmetad.service @3.950s
                                          └─lvm2-lvmetad.socket @2.988s
                                            └─-.slice
```

Systemd offre la possibilité d'administrer des machines distantes

```
# systemctl -H root@192.168.1.4  status nfs.service
```

Remarque : l'option --host' est équivalente à '-H'

Le démarrage du système et des services

Commandes systemd

- hostnamectl
- hostnamectl set-hostname new_name

- timedatectl
- timedatectl set-time HH:MM

- localectl
- localectl set-locale nom_locale

Afficher le nom de la machine

```
# hostnamectl
   Static hostname: centos-uefi
         Icon name: computer-vm
           Chassis: vm
        Machine ID: e8133b53f7934ab6b0c6cfae1d0726ff
           Boot ID: eeb7258107374d548eeca68fd7609980
    Virtualization: kvm
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-693.2.2.el7.x86_64
      Architecture: x86-64
```

Modifier le nom de la machine

```
# hostnamectl set-hostname newname
# more /etc/hostname
newname
```

Afficher les informations concernant la date et l'heure

```
# timedatectl
      Local time: jeu. 2017-10-26 11:37:48 CEST
  Universal time: jeu. 2017-10-26 09:37:48 UTC
        RTC time: jeu. 2017-10-26 09:37:50
       Time zone: Europe/Paris (CEST, +0200)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: yes
 Last DST change: DST began at
                  dim. 2017-03-26 01:59:59 CET
                  dim. 2017-03-26 03:00:00 CEST
 Next DST change: DST ends (the clock jumps one hour backwards) at
                  dim. 2017-10-29 02:59:59 CEST
                  dim. 2017-10-29 02:00:00 CET
```

Désactiver ntp

```
# timedatectl set-ntp no
```

Modifier l'heure locale

```
# timedatectl set-time 10:00
```

Modifier la date

```
# timedatectl set-time "2017-12-31 23:59:59"
```

Afficher les timezones

```
# timedatectl list-timezones | grep Europe
```

Modifier la timezone

```
# timedatectl set-timezone Europe/Rome
```

Par défaut le système utilise le temps UTC. Pour configurer le système afin qu'il utilise l'heure locale il faut positionner l'option set-local-rtc à yes.

```
# timedatectl set-local-rtc yes
```

Modifier la localisation.

Afficher la localisation actuellement

```
# localectl
   System Locale: LANG=fr_FR.UTF-8
       VC Keymap: fr-oss
      X11 Layout: fr
     X11 Variant: oss
```

Afficher les localisation disponibles

```
# localectl list-locales
```

Afficher ceux concernant les Etats-Unis.

```
# localectl list-locales | grep US
```

Modifier la localisation

```
# localectl set-locale LANG=en_US.utf8
```

Afficher les types de clavier disponibles.

```
# localectl list-keymaps | grep fr
```

Modifier la configuration du clavier.

```
# localectl set-keymap fr-latin9
```

Démarrage et arrêt d'un serveur

Le démarrage en mode secours

- Procédure pour booter en mode rescue
- Procédure pour booter en mode single-user

Le démarrage en mode secours

Pour démarrer en mode secours, il faut passer l'argument 'S' au noyau. Si le système est en cours d'utilisation, la commande 'init' permet d'atteindre le niveau S. Ce niveau est le mode secours, il n'y a que les systèmes de fichiers critiques qui sont montés et le réseau n'est pas démarré.

Lors du démarrage de la machine, il est aussi possible d'éditer le noyau à lancer depuis grub et de passer l'argument S au noyau. On est ensuite directement connecté en root sur la machine et pour certains systèmes sans avoir besoin d'entrer un mot de passe. C'est pour cette raison que la plupart des administrateurs positionnent un mot de passe sur grub.

Si le système ne démarre pas, on peut booter en mode secours sur le DVD d'installation. Dans ce cas, le système recherchera la partition ou le volume contenant le slash et essaiera de le monter sur le répertoire /mnt/sysimage. A travers ce répertoire, vous aurez accès au contenu de votre slash.

Il est d'usage de « chrooter » le répertoire /mnt/sysimage pour accéder directement à notre environnement.

Démarrage et arrêt d'un serveur

Présentation de GRUB legacy

- /boot/grub/grub.conf
- /etc/inittab

  initdefault

Présentation de GRUB legacy

Exemple d'un grub legacy sur CentOS 6.5

```
# more /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/vg_formateur-lv_root
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-431.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-431.el6.x86_64 ro root=/dev/mapper/vg_formateur-l
v_root rd_NO_LUKS rd_LVM_LV=vg_formateur/lv_swap rd_NO_MD LANG=fr_FR.UTF-8 SYSFO
NT=latarcyrheb-sun16 crashkernel=128M  KEYBOARDTYPE=pc KEYTABLE=fr-latin9 rd_LVM
_LV=vg_formateur/lv_root rd_NO_DM rhgb quiet
        initrd /initramfs-2.6.32-431.el6.x86_64.img
```

Chaque système d'exploitation à démarrer est référencé par le mot clef 'title' (un seul OS dans notre cas).

default=0 indique l'OS à démarrer référencé par 'title'.
timeout=5 indique le temps qu'a l'utilisateur avant que l'OS par défaut soit sélectionné.
splashimage indique l'image à charger lors du démarrage.
hiddenmenu indique qu'il faut cacher le menu par défaut (il faut appuyer sur ENTREE pour qu'il s'affiche).
root (hd0,0) indique qu'elle est la partition qui contient le noyau. Le 1er chiffre indique la lettre de la partition, la deuxième indique le numéro de la partition. Ainsi hd0,0 fait référence à la partition /dev/sda1.

kernel indique un chemin relatif par rapport à la partition qui contient le noyau. C'est cette ligne qui monte la partition racine en lecture seule (ro) au moment du démarrage. Des options sont spécifiées pour indiquer comment le noyau va démarrer.
- rhgb : redhat graphical boot : indique un démarrage graphique
- quiet : silencieux : supprime certains messages du démarrage.

initrd indique qu'elle est l'image à charger au démarrage qui contient notamment certains drivers.

Fichier /etc/inittab d'une CentOS 6.5 :

```
# more /etc/inittab
# inittab is only used by upstart for the default runlevel.
#
# ADDING OTHER CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.
#
# System initialization is started by /etc/init/rcS.conf
#
# Individual runlevels are started by /etc/init/rc.conf
#
# Ctrl-Alt-Delete is handled by /etc/init/control-alt-delete.conf
#
# Terminal gettys are handled by /etc/init/tty.conf and /etc/init/serial.conf,
# with configuration in /etc/sysconfig/init.
#
# For information on how to write upstart event handlers, or how
# upstart works, see init(5), init(8), and initctl(8).
#
# Default runlevel. The runlevels used are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:5:initdefault:
```

Le fichier indique que le niveau de démarrage par défaut est le niveau 5.

Gestion des services avec SysInit

Les commandes service et chkconfig pour gérer les services

- service nom_service {stop|start|restart|reload}
- La commande chkconfig
- Le répertoire /var/lock/subsys

Les commandes service et chkconfig pour gérer les services

Les scripts des différents services sont localisés dans le répertoire /etc/init.d.

On peut faire appel à un script en lui passant des arguments (start, stop, restart, status,...). La commande '*service*' effectue la même chose sans taper le chemin absolu du service.

Il est possible d'invoquer les scripts directement avec le chemin absolu ou en utilisant la commande *service*.

```
# /etc/init.d/crond status
crond (pid  3222) en cours d'exécution...
# /etc/init.d/crond stop
Arrêt de crond :                                           [  OK  ]
# service crond start
Démarrage de crond :                                       [  OK  ]
#
```

Pour chaque niveau d'exécution, un répertoire /etc/rc.d/rc<niveau>.d existe. Les services sont démarrés ou arrêtés dans l'ordre alpha-numérique.

```
# ls /etc/rc.d/rc5.d
K01numad          K75quota_nld          S10network            S26haldaemon
K01smartd         K76ypbind             S11auditd             S26udev-post
K02oddjobd        K84wpa_supplicant     S11portreserve        S28autofs
K05wdaemon        K85ebtables           S12rsyslog            S50bluetooth
K10psacct         K86cgred              S13cpuspeed           S55sshd
K10saslauthd      K87restorecond        S13irqbalance         S56xinetd
K15htcacheclean   K88sssd               S13iscsi              S70spice-vdagentd
K15httpd          K89rdisc              S13rpcbind            S80postfix
K46radvd          K95firstboot          S15mdmonitor          S82abrt-ccpp
K50dnsmasq        K99rngd               S20kdump              S82abrtd
K50netconsole     S01sysstat            S22messagebus         S84ksm
K50snmpd          S02lvm2-monitor       S23NetworkManager     S85ksmtuned
K50snmptrapd      S05cgconfig           S24nfslock            S90crond
K60nfs            S06multipathd         S24rpcgssd            S95atd
K69rpcsvcgssd     S07iscsid             S25blk-availability   S97libvirtd
K73winbind        S08ip6tables          S25cups               S99certmonger
K74ntpd           S08iptables           S25netfs              S99libvirt-guests
K75ntpdate        S09netcf-transaction  S26acpid              S99local
```

Ces répertoires contiennent des liens symboliques débutant par S (start) ou par K (kill) qui sont respectivement des scripts de démarrage ou des scripts d'arrêt.

```
# ls -l /etc/rc.d/rc?.d/*crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc0.d/K60crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc1.d/K60crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc2.d/S90crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc3.d/S90crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc4.d/S90crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc5.d/S90crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15  9 sept. 11:39 /etc/rc.d/rc6.d/K60crond -> ../init.d/crond
```

La commande service permet d'arrêter, de démarrer, de redémarrer ou de recharger la configuration d'un service.

Afficher le statut d'un service

```
# service crond status
```

Arrêter un service.

```
# service crond stop
```

Démarrer un service.

```
# service crond start
```

Recharger un service.

```
# service crond reload
```

La commande '*chkconfig*' permet de gérer les services SysInit en créant automatiquement les liens symboliques vers les scripts présents dans le répertoire /etc/init.d.

Ce mécanisme a été remplacé à partir de la version 7 de RedHat (systemd).

La commande '*chkconfig*' permet de paramétrer les niveaux pour lesquels le service démarre. Cet utilitaire recréé les liens symboliques dans les répertoires /etc/rc.d/rc?.d.

```
# chkconfig --list crond
crond           0:arrêt 1:arrêt 2:marche        3:marche        4:marche        5:marche
6:arrêt
# chkconfig --level 24 crond off
# chkconfig --list crond
crond           0:arrêt 1:arrêt 2:arrêt 3:marche        4:arrêt 5:marche        6:arrêt
# ls -l /etc/rc.d/rc?.d/*crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc0.d/K60crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc1.d/K60crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc2.d/K60crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc3.d/S90crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc4.d/K60crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc5.d/S90crond -> ../init.d/crond
lrwxrwxrwx. 1 root root 15 26 janv. 11:47 /etc/rc.d/rc6.d/K60crond -> ../init.d/crond
```

Les niveaux de démarrage et d'arrêt des services proviennent du script présent dans /etc/init.d.

```
# head /etc/init.d/crond
#!/bin/sh
#
# crond          Start/Stop the cron clock daemon.
#
# chkconfig: 2345 90 60
# description: cron is a standard UNIX program that runs user-specified \
#              programs at periodic scheduled times. vixie cron adds a \
#              number of features to the basic UNIX cron, including better \
#              security and more powerful configuration options.
```

La ligne contenant 'chkconfig' indique qu'il faut créer des scripts de démarrage pour les niveaux 2, 3 , 4 et 5. Les scripts de démarrage s'appelleront S90crond et les scripts d'arrêt K60crond.

L'utilitaire 'chkconfig' permet de configurer le niveau de démarrage des services. Ci-dessous, un exemple pour un démarrage du service 'crond' au niveau 2.

```
# chkconfig --level 2 crond on
# chkconfig --list crond
crond           0:arrêt 1:arrêt 2:marche        3:marche        4:arrêt 5:marche
6:arrêt
```

Le démarrage du système et des services

Tableau comparatif sysVinit et systemd

Commande sysVinit	Équivalence systemd
`chkconfig crond on`	`systemctl enable crond.service`
`chkconfig crond off`	`systemctl disable crond.service`
`chkconfig crond --list`	`systemctl is-enabled crond.service`
`service crond status`	`systemctl status crond.service` `service crond status`
`service crond start`	`systemctl start crond.service` `service crond start`
`service crond stop`	`systemctl stop crond.service` `service crond stop`
`service crond reload`	`systemctl reload crond.service` `service crond reload`

Tableau comparatif des commandes sysVinit et systemd

Tableau de correspondance entre les commandes de sysinit et de systemd :

Commande sysVinit	Équivalence systemd
`chkconfig crond on`	`systemctl enable crond.service`
`chkconfig crond off`	`systemctl disable crond.service`
`chkconfig crond --list`	`systemctl is-enabled crond.service`
`service crond status`	`systemctl status crond.service` `service crond status`
`service crond start`	`systemctl start crond.service` `service crond start`
`service crond stop`	`systemctl stop crond.service` `service crond stop`
`service crond reload`	`systemctl reload crond.service` `service crond reload`

Notes

Le noyau et les modules

Dans ce chapitre, nous allons étudier les périphériques et les drivers, ainsi que la compilation du noyau d'un serveur Linux.

Table des matières

Le noyau et les modules

Le noyau modulaire et le noyau monolithique

- Noyau modulaire : modules chargés selon les besoin
- Noyau monolithique: tout dans le noyau

Le noyau modulaire et le noyau monolithique

Noyau modulaire :

La plupart des noyaux actuels sont des noyaux modulaires. Il n'y a qu'une partie du noyau qui est statique, le reste des modules sont chargés au fur à mesure des besoins.

Le driver du lecteur DVD n'est pas chargé au démarrage en mémoire. Il ne sera chargé que lorsqu'il aura besoin d'accéder au périphérique (insertion d'un dvd dans le lecteur). Le module restera par la suite chargé en mémoire sauf si on le décharge manuellement.

Cette conception du noyau évite d'avoir un noyau trop important chargé en mémoire.

Noyau monolithique :

Les noyaux monolithiques (ou statiques) contiennent l'ensemble des modules nécessaire au fonctionnement. Ce type de noyau peut se construire pour des raisons de sécurité (pas de modules usb par exemple) et contrôler les périphériques accessibles par la machine.

Le noyau et les modules

Les périphériques

- Le numéro de majeur d'un périphérique
- Le numéro de mineur d'un périphérique
- Création de fichiers spéciaux avec mknod
- Présentation de udev

Les périphériques

Le fichiers spéciaux sont des fichiers qui représentent des périphériques. Sur un système Linux, le terminal ou le disque dur sont vus comme des fichiers qu'on appelle fichiers spéciaux. A la place de la taille du fichier, deux chiffres indiquent le numéro de majeur et le numéro de mineur du périphérique.

Le numéro de majeur est utilisé par le noyau pour déterminer quel driver il doit utiliser pour le piloter. Le numéro de mineur d'un périphérique représente l'instance particulière du périphérique. Une partition par exemple pour un périphérique de type disque dur.

Le terminal /dev/pts/0 utilisé pour l'affichage a un numéro de majeur 136. Le noyau utilise donc le driver 'pts'. Le noyau sait sur quel terminal on se trouve grâce au numéro de mineur qui différencie les terminaux. Le 'c' pour le type de fichier indique que le terminal fonctionne en mode caractère.

```
# tty
/dev/pts/0
# ls -l /dev/pts/0
crw--w---- 1 root tty 136, 0 30 oct.  11:58 /dev/pts/0
```

Les disques durs utilisent un driver de type 'sd'. Chaque disque dur pouvant contenir jusqu'à 15 partitions, le premier disque verra les numéros de mineur 1 à 15 affectés à ces partitions (le 0 est réservé pour le disque entier). Le numéro de mineur 16 représente le deuxième disque et les numéros 17 à 31 seront utilisés pour les partitions. Le 'b' pour le type de fichier indique que le périphérique fonctionne en mode bloc.

```
# ls -l /dev/sd*
brw-rw---- 1 root disk 8,  0 30 oct.  10:12 sda
brw-rw---- 1 root disk 8,  1 30 oct.  10:12 sda1
brw-rw---- 1 root disk 8,  2 30 oct.  10:12 sda2
brw-rw---- 1 root disk 8,  3 30 oct.  10:12 sda3
brw-rw---- 1 root disk 8,  4 30 oct.  10:12 sda4
brw-rw---- 1 root disk 8,  5 30 oct.  10:12 sda5
brw-rw---- 1 root disk 8,  6 30 oct.  10:12 sda6
brw-rw---- 1 root disk 8,  7 30 oct.  10:12 sda7
brw-rw---- 1 root disk 8,  8 30 oct.  10:12 sda8
brw-rw---- 1 root disk 8, 16 30 oct.  10:12 sdb
brw-rw---- 1 root disk 8, 32 30 oct.  10:12 sdc
brw-rw---- 1 root disk 8, 48 30 oct.  10:12 sdd
brw-rw---- 1 root disk 8, 64 30 oct.  10:12 sde
brw-rw---- 1 root disk 8, 80 30 oct.  10:12 sdf
brw-rw---- 1 root disk 8, 96 30 oct.  10:12 sdg
```

Le fichier /proc/devices contient la correspondance entre le numéro de majeur et le driver.

```
# more /proc/devices
Character devices:
  1 mem
  4 /dev/vc/0
  4 tty
...

Block devices:
259 blkext
  8 sd
  9 md
 11 sr
..
```

Exemple de création d'un périphérique spécial :

```
# mknod /dev/sdh b 8 112

# ls -l /dev/sd*
brw-rw---- 1 root disk 8,   0 30 oct.  10:12 /dev/sda
brw-rw---- 1 root disk 8,   1 30 oct.  10:12 /dev/sda1
brw-rw---- 1 root disk 8,   2 30 oct.  10:12 /dev/sda2
brw-rw---- 1 root disk 8,   3 30 oct.  10:12 /dev/sda3
brw-rw---- 1 root disk 8,   4 30 oct.  10:12 /dev/sda4
brw-rw---- 1 root disk 8,   5 30 oct.  10:12 /dev/sda5
brw-rw---- 1 root disk 8,   6 30 oct.  10:12 /dev/sda6
brw-rw---- 1 root disk 8,   7 30 oct.  10:12 /dev/sda7
brw-rw---- 1 root disk 8,   8 30 oct.  10:12 /dev/sda8
brw-rw---- 1 root disk 8,  16 30 oct.  10:12 /dev/sdb
brw-rw---- 1 root disk 8,  32 30 oct.  10:12 /dev/sdc
brw-rw---- 1 root disk 8,  48 30 oct.  10:12 /dev/sdd
brw-rw---- 1 root disk 8,  64 30 oct.  10:12 /dev/sde
brw-rw---- 1 root disk 8,  80 30 oct.  10:12 /dev/sdf
brw-rw---- 1 root disk 8,  96 30 oct.  10:12 /dev/sdg
brw-r--r-- 1 root root 8, 112 30 oct.  12:22 /dev/sdh
```

Présentation de udev :

Udev permet d'affecter un nom de périphérique de manière dynamique (insertion d'une clef usb) à partir des propriétés de celui-ci (identifiant du vendeur, du périphérique).
Avec udev vous pouvez créer vos règles spécifiques pour qu'un périphérique soit toujours détecté sous le même nom. Cela peut-être utile si des scripts s'appuient sur le nom d'un périphérique.
Udev remplace devfs depuis les noyaux 2.6.

C'est le démon udevd qui a en charge de détecter les nouveaux périphériques qui sont branchés à chaud.
Le fichier de configuration principal de udevd est le fichier /etc/udev/udev.conf. Ce fichier est complété par des règles qui sont présentes dans le répertoire /etc/udev/rules.d. Les fichiers sont analysés dans l'ordre alpha-numérique. Pour que la modification d'un de ses fichiers soit prise en compte, il faut redémarrer le démon (ou utiliser la commande udevadm).

```
# more /etc/udev/udev.conf
# The initial syslog(3) priority: "err", "info", "debug" or its
# numerical equivalent. For runtime debugging, the daemons internal
# state can be changed with: "udevadm control --log-priority=<value>".
udev_log="err"
```

```
# ls /etc/udev/rules.d/
60-fprint-autosuspend.rules  70-persistent-net.rules  97-bluetooth-serial.rules
60-pcmcia.rules              80-kvm.rules             98-kexec.rules
60-raw.rules                 90-alsa.rules            99-fuse.rules
70-persistent-cd.rules       90-hal.rules
```

```
# more /etc/udev/rules.d/70-persistent-cd.rules
# This file was automatically generated by the /lib/udev/write_cd_rules
# program, run by the cd-aliases-generator.rules rules file.
#
# You can modify it, as long as you keep each rule on a single
# line, and set the $GENERATED variable.

# CD-ROM (pci-0000:00:01.1-scsi-1:0:0:0)
SUBSYSTEM=="block", ENV{ID_CDROM}=="?*", ENV{ID_PATH}=="pci-0000:00:01.1-scsi-1:
0:0:0", SYMLINK+="cdrom", ENV{GENERATED}="1"
SUBSYSTEM=="block", ENV{ID_CDROM}=="?*", ENV{ID_PATH}=="pci-0000:00:01.1-scsi-1:
0:0:0", SYMLINK+="dvd", ENV{GENERATED}="1"
```

Le noyau et les modules

Les commandes de gestion des modules

- Liste des modules chargés en mémoire : lsmod
- Information sur les modules : modinfo
- Décharger un module en mémoire : rmmod ou modprobe
- Charger un module en mémoire : insmod ou modprobe

Les commandes de gestion des modules

Lister les modules chargés en mémoire : lsmod

```
# lsmod | more
Module                  Size  Used by
ip6t_rpfilter          12546  1
ip6t_REJECT            12939  2
ipt_REJECT             12541  2
xt_conntrack           12760  7
ebtable_nat            12807  0
ebtable_broute         12731  0
bridge                115385  1 ebtable_broute
stp                    12976  1 bridge
llc                    14552  2 stp,bridge
ebtable_filter         12827  0
ebtables               30913  3 ebtable_broute,ebtable_nat,ebtable_filter
ip6table_nat           12864  1
nf_conntrack_ipv6      18738  5
```

Informations sur un module :

```
# modinfo cdrom
filename:       /lib/modules/3.10.0-229.14.1.el7.x86_64/kernel/drivers/cdrom/cdrom.ko
license:        GPL
rhelversion:    7.1
srcversion:     EB46A7E87598E0DD56A115E
depends:
intree:         Y
vermagic:       3.10.0-229.14.1.el7.x86_64 SMP mod_unload modversions
signer:         CentOS Linux kernel signing key
sig_key:        E9:9F:C4:37:BD:9C:BF:B4:F1:B1:DA:87:C1:57:FF:66:56:9B:EE:66
sig_hashalgo:   sha256
parm:           debug:bool
parm:           autoclose:bool
parm:           autoeject:bool
parm:           lockdoor:bool
parm:           check_media_type:bool
parm:           mrw_format_restart:bool
```

Pour décharger un module : il ne faut pas qu'il soit utilisé par le système.

```
# rmmod cdrom
rmmod: ERROR: Module cdrom is in use by: sr_mod
```

On constate que le module est utilisé par un autre module. Affichons les informations du module :

```
# modinfo sr_mod
filename:       /lib/modules/3.10.0-229.14.1.el7.x86_64/kernel/drivers/scsi/sr_mod.ko
license:        GPL
alias:          scsi:t-0x04*
alias:          scsi:t-0x05*
alias:          block-major-11-*
license:        GPL
description:    SCSI cdrom (sr) driver
rhelversion:    7.1
srcversion:     8E5DF8BADB8A38AF97727B3
depends:        cdrom
intree:         Y
vermagic:       3.10.0-229.14.1.el7.x86_64 SMP mod_unload modversions
signer:         CentOS Linux kernel signing key
sig_key:        E9:9F:C4:37:BD:9C:BF:B4:F1:B1:DA:87:C1:57:FF:66:56:9B:EE:66
sig_hashalgo:   sha256
parm:           xa_test:int
```

Supprimons d'abord ce module :

```
# rmmod sr_mod
rmmod: ERROR: Module sr_mod is in use
```

L'opération échoue car le cdrom est monté.

```
# df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/sda7          969M    708M  195M  79% /
devtmpfs           912M       0  912M   0% /dev
tmpfs              921M     84K  921M   1% /dev/shm
tmpfs              921M    8,8M  912M   1% /run
tmpfs              921M       0  921M   0% /sys/fs/cgroup
/dev/sda2          7,6G    4,7G  2,6G  65% /usr
/dev/sda6          1,9G    622M  1,2G  35% /home
/dev/sda1          969M    116M  787M  13% /boot
/dev/sda3          3,8G    513M  3,1G  15% /var
/dev/sr0           3,9G    3,9G     0 100% /run/media/root/CentOS 7 x86_64
```

Après le démontage du cdrom, les modules peuvent être déchargés de la mémoire :

```
# umount /dev/sr0
# rmmod sr_mod
# rmmod cdrom
# lsmod | egrep 'cdrom|sr_mod'
```

Pour charger un module en mémoire, il faut utiliser de manière préférentielle la commande modprobe car elle résout les dépendances :

```
# modprobe sr_mod

# lsmod | egrep 'cdrom|sr_mod'
sr_mod                 22416  0
cdrom                  42556  1 sr_mod
```

Le noyau

La configuation et le paramétrage du noyau

- Le répertoire /usr/lib/sysctl.d/ (depuis CentOS 7)
- Passer un paramètre au noyau lors du démarrage
- La commande sysctl

La configuration et le paramétrage du noyau

Lorsque le système démarre, vous pouvez éditer grub pour passer un paramètre au noyau.

Vous pouvez aussi agir à chaud sur le noyau en modifiant directement des valeurs dans le répertoire /proc (non persistent au reboot).

Pour passer un paramètre au noyau, il faut modifier son fichier de configuration. Puis pour que cela soit pris en compte, il faut recharger le noyau en mémoire (reboot ou autre méthode moins contraignante). Les paramètres du fichier de configuration du noyau ont une valeur égale à 0 (désactivé) ou une valeur égale à 1 (activé).

Le paramètre ip_forward permet à la machine de jouer le rôle d'un routeur.

Pour connaître la valeur actuelle du paramètre, il faut consulter la valeur dans le répertoire /proc.

```
# more /proc/sys/net/ipv4/ip_forward
0
```

Visualiser le fichier de configuration du noyau. Les fichiers depuis Cent0S 7 sont situés dans /usr/lib/sysctl.d

```
# more /usr/lib/sysctl.d/00-system.conf
# Kernel sysctl configuration file
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Disable netfilter on bridges.
net.bridge.bridge-nf-call-ip6tables = 0
net.bridge.bridge-nf-call-iptables = 0
net.bridge.bridge-nf-call-arptables = 0

# Controls the maximum shared segment size, in bytes
kernel.shmmax = 4294967295

# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 268435456
```

```
# more /usr/lib/sysctl.d/50-default.conf
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

# See sysctl.d(5) and core(5) for for details.

# System Request functionality of the kernel (SYNC)
kernel.sysrq = 16

# Append the PID to the core filename
kernel.core_uses_pid = 1

# Source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Enable hard and soft link protection
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
```

Modifier le fichier 50-default.conf pour activer la fonctionnalité de routage au démarrage de la machine.

```
# tail -2 50-default.conf
# Activation du routage
net.ipv4.ip_forward = 1
```

Cette modification sera prise en compte lors du prochain reboot. Actuellement le noyau détecte toujours le paramètre ip_forward à 0.

```
# more /proc/sys/net/ipv4/ip_forward
0
```

L'option -p de la commande 'sysctl' peut prendre un argument un fichier de configuration du noyau pour appliquer les paramètres s'y trouvant.

```
# sysctl -p /usr/lib/sysctl.d/50-default.conf
kernel.sysrq = 16
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
net.ipv4.ip_forward = 1
```

```
# more /proc/sys/net/ipv4/ip_forward
1
```

L'option -a de 'sysctl' liste tous les paramètres du noyau :

```
# sysctl -a | wc -l
769
```

```
# sysctl -a
abi.vsyscall32 = 1
crypto.fips_enabled = 0
debug.exception-trace = 1
debug.kprobes-optimization = 1
dev.cdrom.autoclose = 1
dev.cdrom.autoeject = 0
dev.cdrom.check_media = 0
dev.cdrom.debug = 0
dev.cdrom.info = CD-ROM information, Id: cdrom.c 3.20 2003/12/17
dev.cdrom.info =
dev.cdrom.info = drive name:            sr0
```

Le noyau et les modules

Les versions du noyau

- Les révisions stables
- Les révisions en cours de développement
- Les patchs d'un noyau

Les versions du noyau

Pour les versions inférieures au noyau 3.0, toutes les versions impaires étaient des versions en cours de développement (2.3, 2.5, …). Les versions stables étaient les versions paires (2.4,2.6,...).

Depuis la version 3.X du noyau cette distinction n'existe plus. Le site www.kernel.org met à disposition les derniers noyaux. Pour une machine en production, installez toujours une révision stable du noyau.

Pour mettre à jour le noyau, il n'est pas nécessaire de le compiler entièrement. La mise à jour peut se faire en appliquant un patch noyau.

Les patchs sont téléchargeables depuis le site www.kernel.org. Lisez attentivement le fichier README pour avoir la procédure pour patcher le noyau.

Le noyau et les modules

Procédure de compilation du noyau

- Récupération du noyau sur http://www.kernel.org
- Choisir les options du noyau
- Les étapes de la compilation
- make ; make modules ; make modules_install ; make install

Procédure de compilation du noyau

La compilation d'un noyau est toujours une procédure délicate. Lorsque vous désirez l'upgrader vers une version trop récente, vous pouvez rencontrer des problèmes (changement de version de udev par exemple).

Procédure pour compiler un noyau 4.4 récupéré sur le site kernel.org.

Version actuelle du système :

```
# cat /etc/redhat-release
CentOS Linux release 7.0.1406 (Core)
```

```
# uname -r
3.10.0-123.el7.x86_64
```

Copie du noyau compressé dans le répertoire /usr/src :

```
# cp linux-4.4.tar.xz /usr/src
```

Décompression des sources du noyau :

```
# cd /usr/src
# unxz linux-4.4.tar.xz
# tar xf linux-4.4.tar
```

Création d'un lien symbolique pour travailler dans le répertoire /usr/src/linux :

```
# ln -s linux-4.4 linux
# ls -l
total 633164
drwxr-xr-x.  2 root root         6 10 juin   2014 debug
drwxr-xr-x.  2 root root         6 10 juin   2014 kernels
lrwxrwxrwx.  1 root root         9 28 janv. 12:39 linux -> linux-4.4
drwxrwxr-x. 24 root root      4096 11 janv. 00:01 linux-4.4
-rw-r--r--.  1 root root 648355840 28 janv. 12:31 linux-4.4.tar
```

Il faut se positionner dans le répertoire contenant les sources à compiler :

```
# cd linux
# ls -a
.     block    CREDITS        drivers   .get_maintainer.ignore  init    Kconfig  .mailmap
mm      REPORTING-BUGS  security  usr
..    certs    crypto         firmware  .gitignore              ipc     kernel
MAINTAINERS  net     samples        sound     virt
arch  COPYING  Documentation  fs        include                 Kbuild  lib      Makefile
README  scripts         tools
```

Il faut installer les outils de compilation si ce n'est pas déjà fait :

```
# yum install -y gcc
```

La commande make peut prendre des arguments pour effectuer un certain nombre d'opérations.

Suppression des traces des compilations antérieures :

```
# make mrproper
```

Le fichier /boot/config-<version_noyau> contient les options de compilation du noyau actuel. Pour ne pas avoir à choisir toutes les options, on génère un fichier .config à partir de la configuration actuelle du noyau. Il faudra répondre à un certain nombre de questions :

```
# make oldconfig
  HOSTCC  scripts/basic/fixdep
  HOSTCC  scripts/kconfig/conf.o
  SHIPPED scripts/kconfig/zconf.tab.c
  SHIPPED scripts/kconfig/zconf.lex.c
  SHIPPED scripts/kconfig/zconf.hash.c
  HOSTCC  scripts/kconfig/zconf.tab.o
  HOSTLD  scripts/kconfig/conf
scripts/kconfig/conf  --oldconfig Kconfig
#
# using defaults found in /boot/config-3.10.0-123.el7.x86_64
#
*
* Restart config...
*
*
* General setup
*
```

```
Cross-compiler tool prefix (CROSS_COMPILE) []
Compile also drivers which will not load (COMPILE_TEST) [N/y/?] (NEW)ENTREE
Local version - append to kernel release (LOCALVERSION) []
Automatically append version information to the version string (LOCALVERSION_AUTO)
[N/y/?] n
Kernel compression mode
> 1. Gzip (KERNEL_GZIP)
  2. Bzip2 (KERNEL_BZIP2)
  3. LZMA (KERNEL_LZMA)
  4. XZ (KERNEL_XZ)
  5. LZO (KERNEL_LZO)
  6. LZ4 (KERNEL_LZ4) (NEW)
choice[1-6?]:ENTREE
...
...
Select compiled-in fonts (FONTS) [N/y/?] n
#
# configuration written to .config
```

```
# more .config
#
# Automatically generated file; DO NOT EDIT.
# Linux/x86 4.4.0 Kernel Configuration
#
CONFIG_64BIT=y
CONFIG_X86_64=y
CONFIG_X86=y
CONFIG_INSTRUCTION_DECODER=y
CONFIG_PERF_EVENTS_INTEL_UNCORE=y
CONFIG_OUTPUT_FORMAT="elf64-x86-64"
CONFIG_ARCH_DEFCONFIG="arch/x86/configs/x86_64_defconfig"
CONFIG_LOCKDEP_SUPPORT=y
CONFIG_STACKTRACE_SUPPORT=y
CONFIG_HAVE_LATENCYTOP_SUPPORT=y
CONFIG_MMU=y
CONFIG_NEED_DMA_MAP_STATE=y
CONFIG_NEED_SG_DMA_LENGTH=y
CONFIG_GENERIC_ISA_DMA=y
CONFIG_GENERIC_BUG=y
CONFIG_GENERIC_BUG_RELATIVE_POINTERS=y
CONFIG_GENERIC_HWEIGHT=y
CONFIG_ARCH_MAY_HAVE_PC_FDC=y
CONFIG_RWSEM_XCHGADD_ALGORITHM=y
CONFIG_GENERIC_CALIBRATE_DELAY=y
CONFIG_ARCH_HAS_CPU_RELAX=y
CONFIG_ARCH_HAS_CACHE_LINE_SIZE=y
CONFIG_HAVE_SETUP_PER_CPU_AREA=y
...
```

Choisir maintenant les options de compilation :

Il faut installer les packages ncurses-devel pour pouvoir exécuter la commande :

```
# yum install -y ncurses-devel
```

make menuconfig va permettre de choisir ce qu'il faut inclure ou non dans notre noyau. Vous avez la possibilité de choisir d'intégrer des fonctionnalités de manière modulaire ou statique. La barre d'espace sert à faire défiler les choix :

```
# make menuconfig
  HOSTCC  scripts/kconfig/mconf.o
  HOSTCC  scripts/kconfig/zconf.tab.o
  HOSTCC  scripts/kconfig/lxdialog/checklist.o
  HOSTCC  scripts/kconfig/lxdialog/util.o
  HOSTCC  scripts/kconfig/lxdialog/inputbox.o
  HOSTCC  scripts/kconfig/lxdialog/textbox.o
  HOSTCC  scripts/kconfig/lxdialog/yesno.o
  HOSTCC  scripts/kconfig/lxdialog/menubox.o
  HOSTLD  scripts/kconfig/mconf
scripts/kconfig/mconf  Kconfig
configuration written to .config

*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.
```

Naviguer dans les menus et sélectionner ce que vous voulez ajouter ou supprimer du noyau. La configuration va être écrite dans le fichier .config du répertoire courant. La commande make s'appuie sur ce fichier pour compiler tout ce qui est statique dans le noyau :

```
# make
```

Remarque : la commande make prend un certain temps en fonction de l'architecture de votre machine et de la puissance de votre CPU (c'est essentiellement lui qui travaille lors de la compilation).

Si SSL n'est pas installé, une erreur est générée :

```
# make
  CHK     include/config/kernel.release
  CHK     include/generated/uapi/linux/version.h
  CHK     include/generated/utsrelease.h
  CHK     include/generated/bounds.h
  CHK     include/generated/timeconst.h
  CHK     include/generated/asm-offsets.h
  CALL    scripts/checksyscalls.sh
  HOSTCC  scripts/sign-file
scripts/sign-file.c:23:30: erreur fatale: openssl/opensslv.h : Aucun fichier ou dossier
de ce type
 #include <openssl/opensslv.h>
                              ^
compilation terminée.
make[1]: *** [scripts/sign-file] Erreur 1
make: *** [scripts] Erreur 2
# make menuconfig
scripts/kconfig/mconf  Kconfig


*** End of the configuration.
*** Execute 'make' to start the build or try 'make help'.
```

```
# yum install -y openssl-devel
```

Compilation de tout ce qui est modulaire dans le noyau, la commande 'make modules' permet de l'effectuer :

```
# make modules
  CHK     include/config/kernel.release
  CHK     include/generated/uapi/linux/version.h
  CHK     include/generated/utsrelease.h
  CHK     include/generated/bounds.h
  CHK     include/generated/timeconst.h
  CHK     include/generated/asm-offsets.h
  CALL    scripts/checksyscalls.sh
  Building modules, stage 2.
  MODPOST 2168 modules
```

Il reste à installer tout ce qui est modulaire :

```
# make modules_install
  CHK     include/config/kernel.release
  CHK     include/generated/uapi/linux/version.h
  CHK     include/generated/utsrelease.h
  CHK     include/generated/bounds.h
  CHK     include/generated/timeconst.h
  CHK     include/generated/asm-offsets.h
  CALL    scripts/checksyscalls.sh
  CHK     include/generated/compile.h
  CHK     include/generated/uapi/linux/version.h
  Building modules, stage 2.
  MODPOST 2169 modules
sh ./arch/x86/boot/install.sh 4.4.0 arch/x86/boot/bzImage \
        System.map "/boot"
```

La commande 'make install' permet de mettre à jour le fichier de configuration de grub pour insérer le nouveau noyau sur lequel on souhaite booter :

```
# make install
sh ./arch/x86/boot/install.sh 4.4.0 arch/x86/boot/bzImage \
        System.map "/boot"
```

Avec Grub 2, le système démarre sur le nouveau noyau contrairement à Grub legacy qui boote sur l'ancien noyau.

Notes

Administration des utilisateurs

Dans ce chapitre, nous allons étudier l'administration des comptes utilisateurs et des groupes, de la gestion de leur sécurité et la personnalisation de leur environnement de travail.

Table des matières

Administration des utilisateurs

Caractéristiques des comptes utilisateurs

Le compte root

Un compte système

Un compte utilisateur

Caractéristiques des comptes utilisateurs

Tout accès ou toute action sur un système d'exploitation est faite avec un compte ou un identifiant (UID et GID).

L'exécution d'une commande appartient à un compte. Par la commande « ps -ef » on liste l'ensemble des processus et il est précisé le propriétaire par les champs UID et GID.

Il existe trois catégories de comptes :

- le compte « root » : ce compte est le compte d'administration du serveur. Cet utilisateur a tous les droits sur la machine et le système. Son prompt est spécifique le « # » afin de l'identifier immédiatement. Le compte d'administration correspond au UID=0 et GID=0, soit le login root et le nom de groupe root.

- les comptes systèmes : ces comptes systèmes ou applicatifs sont dédiés et utilisés par des services du système d'exploitation ou par des applications. Ils fournissent surtout un UID, GID, exceptionnellement un répertoire de travail à une application ou service spécifique. Ces comptes n'ayant pas de shell de défini, ni de mot de passe exploitable, il est impossible d'utiliser ces comptes pour se connecter au système en tant qu'utilisateur. Les UID 1 à 99 sont réservés pour des comptes systèmes.

- les comptes utilisateurs : ces comptes ont des UID supérieur à 99, ils sont utilisés pour identifier une personne en particulier. Un utilisateur va pouvoir se connecter au système via un de ces comptes. Il est donc nécessaire que les champs soit correctement informés, tels que le login, mot de passe, shell et répertoire de connexion.

Administration des utilisateurs

Les fichiers /etc/passwd

Utilisateur et Groupe utilisateur

Login	UID
Groupe	GID
Mot de passe	Répertoire de connexion
Shell de connexion	

… autres contraintes (mot de passe, groupe, ...)

Le fichier /etc/passwd

Le fichier /etc/passwd contient la définition des comptes de tous les utilisateurs du système. Il s'agit aussi bien des utilisateurs administratifs (comme adm, bin, …) que d'utilisateurs réels (root, user1, user2,...).

Le fichier est composé des champs suivants :

login:x:UID:GID:GECOS:Répertoire de connexion:Processus à exécuter

Nom du champ	Description
login	nom de l'utilisateur
x	indique que le mot de passe est stocké dans /etc/shadow.
UID : User Identifiant	un numéro unique identifiant l'utilisateur (root est l'administrateur car son UID est égal à 0).
GID : Group IDentifiant	groupe primaire de l'utilisateur. Un utilisateur appartient à un groupe primaire et peut appartenir jusqu'à 15 groupes secondaires.
GECOS	Un commentaire qui est souvent omis.
répertoire de connexion	le home directory de l'utilisateur.
processus à exécuter	pour un utilisateur classique le processus sera un shell.

Administration des utilisateurs

Le fichier /etc/shadow

- Le fichier /etc/shadow

login: mot de passe crypté: LAST: MIN:MAX: WARN:INACTIVE:EXPIRE:RESERVE

Le fichier /etc/shadow

Le fichier /etc/shadow vient suppléer le fichier /etc/passwd pour l'authentification locale des utilisateurs.

Les deux fichiers doivent donc être cohérents au niveau des logins. Il existe des commandes pour reconstruire /etc/shadow à partir du fichier /etc/passwd (pwconv) et inversement.

Les différents champs du fichier /etc/shadow sont :

login: mot de passe crypté: LAST: MIN:MAX: WARN:INACTIVE:EXPIRE:RESERVE

Nom du champ	Description
login	le nom de l'utilisateur
mot de passe crypté	mot de passe de l'utilisateur. Si le champ est vide, l'utilisateur se connecte sans mot de passe.
LAST	nombre de jours entre le dernier changement de mot de passe et le 01/01/1970. Si ce champ a une valeur de 0, cela oblige l'utilisateur à modifier son mot de passe à la prochaine connexion.
MIN	durée minimum en jours avant de pouvoir modifier son mot de passe.
MAX	durée maximum en jours avant que l'utilisateur soit invité à modifier son mot de passe.
WARN	nombre de jours avant MAX durant lesquels l'utilisateur est invité à modifier son mot de passe
INACTIVE	nombre de jours après MAX durant lequel le mot de passe sera accepté.
EXPIRE	date d'expiration du compté calculé en nombre de jours depuis le 01/01/1970.
RESERVE	champ réservé pour une utilisation future.

Les caractères !! apparaissent pour un utilisateur n'ayant jamais eu de mot passe.

```
# grep user2 /etc/shadow
user2:!!:16736:0:99999:7:::
```

```
# passwd user2
Changement de mot de passe pour l'utilisateur user2.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 7 caractères
Retapez le nouveau mot de passe :
passwd : mise à jour réussie de tous les jetons d'authentification.
```

```
# grep user2 /etc/shadow
user2:$6$UsRpUq56$x0zQmVAf3CZR7DeC.0GBGWayYxzp3CGAKBh00KGpRm8W5Y5.qK1/e.uy5IDnFl/uDuryIPB
8jy/sz7j1Oh.1x/:16736:0:99999:7:::
```

Administration des utilisateurs

Le fichier /etc/group

- Le fichier /etc/group

  login : x GID: liste utilisateur

Le fichier /etc/group

Le fichier /etc/group contient la liste de tous les groupes du système.

Le fichier est composé des champs suivants :

nom_du_groupe:mot_de_passe: GID:liste_utilisateurs

Nom du champ	Description
nom_du_goupe	le nom affecté au groupe
mot_de_passe	mot de passe chiffré du groupe. En général il n'est pas utilisé, il contient un x
GID : Group IDentifiant	Group Identifiant, numéro unique identifiant le groupe
liste_utilisateurs	liste des utilisateurs qui appartiennent au groupe

Administration des utilisateurs

La gestion des groupes

- groupadd
- groupmod
- groupdel

La gestion des groupes : groupadd, groupmod, groupdel

La commande groupadd permet de créer un groupe. La commande groupmod permet de modifier le nom ou le gid du groupe. La commande groupdel supprime le groupe si aucun utilisateur en fait partie.

```
# groupadd -g 600 pub
# grep pub /etc/group
pub:x:600:
```

```
# groupmod -g 700 pub
# grep pub /etc/group
pub:x:700:
```

```
# groupmod -n publicite pub
# grep pub /etc/group
publicite:x:700:
```

```
# groupdel publicite
# grep pub /etc/group
```

Pour affecter des groupes secondaires aux utilisateurs, il faut utiliser la commande usermod.

```
# usermod -G "finance,100,compta" user1
# grep user1 /etc/group
users:x:100:user1
compta:x:400:theo,user1
user1:x:1001:
finance:x:500:user1
```

Administration des utilisateurs

La gestion des utilisateurs

- useradd
- usermod
- userdel [-r]
- passwd

La gestion des utilisateurs : useradd, usermod, userdel, passwd

La commande useradd permet de créer un utilisateur. Si tous les champs ne sont pas renseignés, la commande va prendre les valeurs par défaut stockées dans certains fichiers. Si aucun groupe n'est spécifié sur la ligne de commande, un groupe portant le nom de l'utilisateur sera créé et affecté comme groupe primaire par défaut (la variable USERGROUPS_ENAB est à YES dans /etc/login.defs).

Création d'un utilisateur avec toutes les options nécessaires :

```
# useradd -u 1010 -g 100 -d /home/user10 -m -s /bin/bash -c "compte utilisateur" user10
# grep user10 /etc/passwd
user10:x:1010:100:compte utilisateur:/home/user10:/bin/bash
```

Les options utilisées :

Option useradd	Description
-u	UID de l'utilisateur
-g	GID de l'utilisateur (groupe primaire)
-d	Directory : répertoire de connexion de l'utilisateur
-m	make : créer le répertoire de connexion
-s	shell : shell de connexion de l'utilisateur
-c	commentaire

Création d'un utilisateur sans option :

```
# useradd user20
# grep user20 /etc/passwd
user20:x:1011:1011::/home/user20:/bin/bash
```

Le dernier UID du fichier /etc/passwd a été incrémenté de 1, le système a créé un groupe appelé user20 avec un GID de 1011. Le répertoire de connexion a été créé par défaut (ce n'est pas le comportement de tous les systèmes) et un shell par défaut a été positionné.

Les valeurs par défaut de la commande useradd peuvent être affiché grâce à l'option -D.

```
# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Tout le paramétrage par défaut n'est pas appliqué (le nom de groupe par exemple) car cela est en contradiction avec le fichier /etc/login.defs.

Ces valeurs proviennent du fichier /etc/default/useradd.

```
# more /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Quelques variables du fichier /etc/login.defs

```
# egrep 'UID|GID|ENAB|CREATE' /etc/login.defs
UID_MIN                  1000
UID_MAX                 60000
SYS_UID_MIN               201
SYS_UID_MAX               999
GID_MIN                  1000
GID_MAX                 60000
SYS_GID_MIN               201
SYS_GID_MAX               999
CREATE_HOME     yes
USERGROUPS_ENAB yes
```

On constate que ce fichier est utilisé pour déterminer les UID/GID min et max. Le répertoire de connexion est créé automatiquement grâce à la variable CREATE_HOME positionné sur YES.

Par défaut la duplication d'un UID est refusée.

```
# useradd -u 0 -g 0 -s /bin/ksh kroot
useradd : l'identifiant d'utilisateur (UID) 0 n'est pas unique
```

Il faut le forcer avec l'option -o.

```
# useradd -o -u 0 -g 0 -s /bin/ksh kroot
# grep kroot /etc/passwd
kroot:x:0:0::/home/kroot:/bin/ksh
```

La commande usermod permet de modifier les caractéristiques d'un utilisateur. Pour modifier certains paramètres des commandes spécifiques existent (chsh pour modifier le shell de connexion, ...).

```
# usermod -s /bin/ksh user10
# chsh -s /bin/ksh user20
Modification d'interpréteur pour user20.
L'interpréteur a été modifié.
```

```
# grep 'user[12]0' /etc/passwd
user10:x:1010:100:compte utilisateur:/home/user10:/bin/ksh
user20:x:1011:1011::/home/user20:/bin/ksh
```

La commande userdel permet de supprimer un utilisateur. Par défaut le répertoire de connexion de l'utilisateur n'est pas supprimé. L'option -r de userdel permet de supprimer en même temps le répertoire de connexion.

```
# userdel user10
# userdel -r user20
# ls /home | egrep 'user10|user20'
user10
```

Verrouiller un compte utilisateur : option -l (lock)

```
# passwd -l user2
Verrouillage du mot de passe pour l'utilisateur user2.
passwd: Succès
```

```
# grep user2 /etc/shadow
user2:!!$6$UsRpUq56$x0zQmVAf3CZR7DeC.0GBGWayYxzp3CGAKBh00KGpRm8W5Y5.qK1/e.uy5IDnFl/uDur
yIPB8jy/sz7j1Oh.1x/:16736:0:99999:7:::
```

Déverrouiller un compte utilisateur : option -u (unlock)

```
# passwd -u user2
Déverrouillage du mot de passe pour l'utilisateur user2.
passwd: Succès
```

Supprimer un mot de passe : option -d (delete)

```
# passwd -d user2
Suppression du mot de passe pour l'utilisateur user2.
passwd: Succès
```

```
# grep user2 /etc/shadow
user2::16736:0:99999:7:::
```

Positionner les règles de vieillissement du mot de passe : option -x pour MAX, -n pour MIN, -w pour WARN, -i pour INACTIVE

```
# passwd -x 60 -n 55 -w 5 -i 10 user1
Ajustement des données d'expiration pour l'utilisateur user1.
passwd: Succès
```

```
# grep user1 /etc/shadow
user1:$6$bNP7iX14$07lJU4xh9mYj9Y41PnTVTwKcK9a12xHkyKY9lQW1iHyp/4KRCY2P9WhG5DzyBmONOGeXrum
88qQpD4VWwPy0R.:16736:55:60:5:10::
```

Obliger un utilisateur à modifier son mot de passe à la prochaine connexion :

```
# chage -d 0 user1
# grep user1 /etc/shadow
user1:$6$bNP7iX14$07lJU4xh9mYj9Y41PnTVTwKcK9a12xHkyKY9lQW1iHyp/4KRCY2P9WhG5DzyBmONOGeXrum
88qQpD4VWwPy0R.:0:55:60:5:10::
```

```
[user2@formateur ~]$ su - user1
Mot de passe :
Vous devez changer votre mot de passe immédiatement (imposé par root)
Changement du mot de passe pour user1.
Mot de passe UNIX (actuel) :
Nouveau mot de passe :
Retapez le nouveau mot de passe :
```

Paramétrer la date d'expiration du compte :

```
# usermod -e 2015-31-12 user1
# grep user1 /etc/shadow
user1:$6$VbNH8Mjz$puSHdo6.GGaEgdlu8flNfVCxetSFZHL7PmWPqoJ0JczLrklsiXgb//Y0dXYItqgHg6bs0eU
c20V2iBaJ0vaCo/:16736:55:60:5:10:17359:
```

Avoir des informations sur un compte : option -S

```
# passwd -S user1
user1 PS 2015-10-28 55 60 5 10 (Mot de passe défini, chiffrement SHA512.)
```

```
# passwd -S user2
user2 NP 2015-10-28 0 99999 7 -1 (Mot de passe vide.)
```

```
# passwd -S user3
user3 LK 2015-10-28 0 99999 7 -1 (Mot de passe verrouillé.)
```

```
# passwd -S user4
user4 PS 1970-01-01 0 99999 7 -1 (Mot de passe défini, chiffrement SHA512.)
```

La date du 01/01/1970 pour user4 indique qu'il faudra qu'il modifie son mot de passe à la prochaine connexion.

Administration des utilisateurs

Les commandes chgrp et chown

- La commande chgrp
- La commande chown

Les commandes chgrp et chown

La commande chgrp permet de modifier le groupe propriétaire d'un fichier. Un simple utilisateur peut modifier le groupe propriétaire d'un de ses fichiers pour l'affecter à un autre groupe auquel il appartient.

```
[theo@formateur ~]$ touch fic1
[theo@formateur ~]$ ls -l fic1
-rw-r--r-- 1 theo formation 0 28 oct.  12:12 fic1

[theo@formateur ~]$ chgrp compta fic1

[theo@formateur ~]$ ls -l fic1
-rw-r--r-- 1 theo compta 0 28 oct.  12:12 fic1
```

Le groupe finance ne fait pas partie de mes groupes donc l'opération échoue.

```
[theo@formateur ~]$ chgrp finance fic1
chgrp: modification du groupe de « fic1 »: Opération non permise

[theo@formateur ~]$ id
uid=1000(theo) gid=300(formation) groupes=300(formation),10(wheel),400(compta)
```

La commande chown permet de modifier le propriétaire d'un fichier, le groupe propriétaire d'un fichier (comme chgrp) ou les deux à la fois.

```
# touch fic
# ls -l fic
-rw-r--r-- 1 root root 0 28 oct.  12:17 fic
```

```
# chown theo fic
# ls -l fic
-rw-r--r-- 1 theo root 0 28 oct.  12:17 fic
```

```
# chown :finance fic
# ls -l fic
-rw-r--r-- 1 theo finance 0 28 oct.  12:17 fic
```

```
# chown user1:compta fic
# ls -l fic
-rw-r--r-- 1 user1 compta 0 28 oct.  12:17 fic
```

Gestion des comptes utilisateurs

La configuration de l'environnement utilisateur

- Les fichiers de configurations intervenant à l'initialisation du système
- Les fichiers modèles contenu dans /etc/skel
- Paramétrer son environnement de travail

La configuration de l'environnement utilisateur

A l'initialisation du système, des fichiers de configurations viennent paramétrer l'environnement. Ces fichiers de configurations système ne sont modifiables que par root. Le nom des fichiers sollicités dépend du type de système et du shell utilisé.

Deux fichiers principaux interviennent :

/etc/profile : configure notamment certaines variables d'environnement, des alias et le umask.

/etc/bashrc : configuration plus spécifique au bash.

Remarque : le module pam.env.so est souvent exécuté. Il lit le contenu du fichier /etc/environment (vide par défaut) pour positionner certaines variables. C'est un autre moyen de configurer des variables systèmes.

Lors de la création d'un compte utilisateur, le contenu du fichier /etc/skel est recopié dans le répertoire de connexion de l'utilisateur. Le contenu de ce répertoire peut varier en fonction des shells installés sur la machine.

Exemple sans ksh :

```
# ls -a /etc/skel
.  ..  .bash_logout  .bash_profile  .bashrc  .mozilla
```

Exemple avec ksh :

```
# ls -a /etc/skel
.  ..  .bash_logout  .bash_profile  .bashrc  .kshrc  .mozilla
```

Le fichier .bash_logout est exécuté lors de la déconnexion d'un utilisateur. Il est souvent vide ou exécute la commande 'clear' qui permet d'effacer l'écran.

Le fichier .bash_profile est lu une fois au moment de la connexion de l'utilisateur. Il teste la présence du fichier $HOME/.bashrc et l'exécute s'il existe. Certaines variables peuvent être définies dans ce fichier.

```
# more .bash_profile
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/.local/bin:$HOME/bin

export PATH
```

Le fichier .bashrc est lu à chaque fois qu'un shell bash est lancé. Il teste la présence du fichier /etc/bashrc et l'exécute s'il est présent. C'est usuellement dans ce fichier qu'on positionne nos propres alias de commandes et variables.

```
# more .bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
```

Exemple de modification d'un fichier de configuration utilisateur :

```
[theo@formateur ~]$ more .bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
alias h=history
alias r='fc -s'
alias D='date +%D'
alias c=clear
alias cx='chmod +x'

prenom=theo
export VILLE=Paris
```

Pour que les modifications soient prises en compte, il faut faire relire le fichier par le shell.

```
[theo@formateur ~]$ . ./.bashrc
[theo@formateur ~]$ echo $VILLE
Paris
[theo@formateur ~]$ D
10/30/15
```

Gestion des comptes utilisateurs

Les permissions

- Rappel sur les permissions de base : notation symbolique et octale
- Les permissions spéciales : setuid, setgid, stickybit
- La commande chmod

Les permissions

Droit	Fichier	Répertoire
r	Droit de lire le contenu du fichier. cat, more, tail ,head, vi, gedit, …	Droit de lire le contenu du répertoire. ls, ls -i, ...
w	Droit de modifier le contenu du fichier. vi(+r), cat >> fic	Droit de modifier le contenu du répertoire. touch, mkdir, rm
x	Droit d'exécuter le fichier comme une commande. ./fic	Droit de se déplacer/traverser le répertoire. cd rep

```
[theo@formateur ~]$ ls -l fic
-rw-r--r--. 1 theo formation 0 28 oct.  10:53 fic
```

Le 1er bit indique le type de fichier (- pour un fichier ordinaire, d pour un répertoire).

Les 3 triplets de permissions qui suivent indiquent les permissions pour le propriétaire du fichier (symbolisé par la lettre u), le groupe propriétaire du fichier (symbolisé par la lettre g) et tous les autres utilisateurs (symbolisé par la lettre o).

L'ensemble des permissions affecté au fichier est le mode du fichier. Pour modifier le mode du fichier, il faut utiliser la commande chmod. Cette commande accepte une notation symbolique ou une notation octale.

Modifier les droits en notation symbolique :

```
[theo@formateur ~]$ chmod a=rwx fic
[theo@formateur ~]$ ls -l fic
-rwxrwxrwx. 1 theo formation 0 28 oct.  10:53 fic
```

```
[theo@formateur ~]$ chmod ug-x,o-wx fic
[theo@formateur ~]$ ls -l fic
-rw-rw-r--. 1 theo formation 0 28 oct.  10:53 fic
```

```
[theo@formateur ~]$ chmod u+x,go=r fic
[theo@formateur ~]$ ls -l fic
-rwxr--r--. 1 theo formation 0 28 oct.  10:53 fic
```

Notation octale :

En octal, chaque droit possède une valeur :

le droit 'r' a une valeur octale de : 4
le droit 'w' a une valeur octale de : 2
le droit 'x' a une valeur octale de : 1

L'ensemble des droits rwx donne une valeur octale de 7. Le chiffre des centaines représente le droits pour le propriétaire, celui des dizaines pour le groupe et celui des unités pour tous les autres.

Modification des droits en notation octale :

```
[theo@formateur ~]$ chmod 700 fic
[theo@formateur ~]$ ls -l fic
-rwx------. 1 theo formation 0 28 oct.  10:53 fic
```

```
[theo@formateur ~]$ chmod 664 fic
[theo@formateur ~]$ ls -l fic
-rw-rw-r--. 1 theo formation 0 28 oct.  10:53 fic
```

Les permissions spéciales :

Le setuid est une permission qui permet de prendre l'identité du propriétaire de la commande durant son exécution. Il se positionne au-dessus du droit x pour le propriétaire du fichier.

```
# ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 27832 10 juin   2014 /usr/bin/passwd
```

La commande passwd possède un setuid. Cela permet aux utilisateurs de modifier leur mot de passe. En effet le processus qui va écrire dans le fichier /etc/shadow appartient à l'utilisateur root et non à l'uid de l'utilisateur qui exécute la commande. Ceci grâce au setuid de la commande.

Le setgid fonctionne comme le setuid mais il s'applique au groupe propriétaire.

```
# ls -l /usr/bin/write
-rwxr-sr-x. 1 root tty 19536  6 août  02:24 /usr/bin/write
```

La commande write possède un setgid. Ainsi le processus qui va écrire appartiendra au groupe tty et non au groupe primaire de l'utilisateur exécutant la commande.

Si le droit x n'est pas positionné sous le setuid ou le setgid, un S apparaît indiquant une mauvaise administration des droits.

Le setgid positionné sur un répertoire indique que tous les fichiers créés à l'intérieur du répertoire appartiendront au groupe propriétaire du répertoire et non au groupe primaire de l'utilisateur qui a créé le fichier.

```
[theo@formateur ~]$ ls -ld /comptes/
drwxrwsr-x. 2 root compta 4096 28 oct.  11:44 /comptes/
```

```
[theo@formateur ~]$ id
uid=1000(theo) gid=300(formation) groupes=300(formation),400(compta)
contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
[theo@formateur ~]$ touch /comptes/fic1
[theo@formateur ~]$ ls -l /comptes/
total 0
-rw-r--r--. 1 theo compta 0 28 oct.  11:45 fic1
```

Le sticky bit se positionne sur les répertoires. Il est symbolisé par la lettre t au dessus du droit x pour les autres utilisateurs. Il indique que seul le propriétaire d'un fichier au sein de ce répertoire pourra supprimer le fichier. Le sticky bit est donc pratique pour créer des répertoires partagés entre utilisateurs.

```
[theo@formateur ~]$ ls -ld /tmp
drwxrwxrwt. 24 root root 4096 28 oct.  11:46 /tmp
```

```
[theo@formateur ~]$ touch /tmp/fic1
[theo@formateur ~]$ ls -l /tmp/fic1
-rw-r--r--. 1 theo formation 0 28 oct.  11:50 /tmp/fic1
```

```
[theo@formateur ~]$ su - user1
Mot de passe :
```

```
[user1@formateur ~]$ rm /tmp/fic1
rm : supprimer fichier vide (protégé en écriture) « /tmp/fic1 » ? y
rm: impossible de supprimer « /tmp/fic1 »: Opération non permise
```

Pour positionner les droits spéciaux il faut utiliser la commande chmod en notation symbolique (u+s pour le setuid, g+s pour le setgid , o+t pour le stickybit) ou la notation octale (setuid=4, setgid=2 , stickybit=1).

Notes

Sauvegarde et restauration

Dans ce chapitre, nous allons étudier différents mécanismes des sauvegardes et des restaurations.

Table des matières

Sauvegarde et restauration

Présentation

- Sauvegardes des données - Restauration
- Importance - Rétention - Fréquence - Lieu
- Des Processus régulièrement testés
- Des outils Time Navigator Baccula

Présentation

La sauvegarde consiste à récupérer les données de l'utilisateur, d'un projet ou du système d'exploitation et de les stocker dans un lieu sûr. Il est fondamental d'avoir un processus de sauvegarde de ses données, ainsi qu'un processus de restauration.

Il est également à prévoir un niveau de rétention. C'est à dire fixer le nombre d'historique d'une sauvegarde, par exemple : sauvegarde de début du mois (n-1), sauvegarde de début du mois (n), sauvegarde de début de semaine et une sauvegarde de la veille.
Il faut déterminer la fréquence des sauvegardes, par exemple : sauvegardes journalières ou mensuelles, ...
Il faut prévoir la localisation où sont stockées les sauvegardes en prenant en compte les avantages et inconvénients, par exemple :
un jeu de sauvegardes sur son poste : facilement accessible mais indisponible si le poste est défectueux. Il est donc plus pratique que se soit sur un serveur accessible via le réseau.
Un jeu de sauvegardes sur un site distant : peut-être moins facilement accessible mais préserve les données en cas de problème sur le site sur lequel vous vous trouvez.

Les sauvegardes et les restaurations doivent avoir un processus de mise en œuvre détaillé, qui est régulièrement testé et validé.

Les sauvegardes systèmes sont à la charge de l'administrateur, ainsi que celles des données des utilisateurs. Mais pour des besoins ponctuels, l'utilisateur peut s'occuper de ses propres sauvegardes.
En plus des commandes, il existe des outils tels que Time Navigator (tina) ou Baccula.

Sauvegarde et restauration

Les utilitaires de compression : gzip, bzip2, xz, zip

- Compresser un fichier
- Lire un fichier compressé
- Décompresser un fichier

Les utilitaires de compression : gzip, bzip2, xz, zip

Plusieurs outils de compression existent sous Linux. Certains sont plus performants que d'autres selon le type de fichiers à compresser. Lors de la compression, les fichiers sont renommés avec l'extension de l'utilitaire de compression.

Exemple avec gzip :

```
# ls -l passwd
-rw-r--r-- 1 root root 2394 30 oct.  13:55 passwd
# gzip passwd
# ls -l
total 4
-rw-r--r-- 1 root root 928 30 oct.  13:55 passwd.gz
```

La lecture d'un fichier compressé peut s'effectuer avec la commande adéquate (zcat pour lire un fichier au format .gz) :

```
# file passwd.gz
passwd.gz: gzip compressed data, was "passwd", from Unix, last modified: Fri Oct 30
13:55:19 2015
# zcat passwd.gz | head -5
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

La commande gunzip décompresse (dézippe) un fichier au format .gz :

```
# gunzip passwd.gz
# ls -l
total 4
-rw-r--r-- 1 root root 2394 30 oct.  13:55 passwd
```

Exemple avec bzip2 :

```
# bzip2 passwd
# ls -l
total 4
-rw-r--r-- 1 root root 960 30 oct.  13:55 passwd.bz2
```

```
# bzcat passwd.bz2 | head -5
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

```
# bunzip2 passwd.bz2
# ls -l
total 4
-rw-r--r-- 1 root root 2394 30 oct.  13:55 passwd
```

Exemple avec xz :

xz possède quelques commandes permettant d'effectuer directement des opérations sur les fichiers compressés comme xzmore, xzcmp ; xzdiff ; xzgrep ...

```
# xz passwd
# ls -l
total 4
-rw-r--r-- 1 root root 984 30 oct.  13:55 passwd.xz
```

```
# xzcat passwd.xz | head -5
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

```
# xzgrep root passwd.xz
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
kroot:x:0:0::/home/kroot:/bin/ksh
```

```
# unxz passwd.xz
# ls -l
total 4
-rw-r--r-- 1 root root 2394 30 oct.  13:55 passwd
```

L'utilitaire zip crée un fichier zip et peut y ajouter au fur à mesure des fichiers :

```
# zip fic.zip passwd /etc/hosts
  adding: passwd (deflated 62%)
  adding: etc/hosts (deflated 65%)
```

Consulter le contenu d'une archive zip :

```
# unzip -l fic.zip
Archive:  fic.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
     2394  10-30-2015 13:55   passwd
      158  06-07-2013 16:31   etc/hosts
---------                     -------
     2552                     2 files
```

```
# unzip -v fic.zip
Archive:  fic.zip
 Length   Method    Size  Cmpr    Date    Time   CRC-32   Name
--------  ------  ------- ---- ---------- ----- --------  ----
    2394  Defl:N      903  62% 10-30-2015 13:55 0a33125a  passwd
     158  Defl:N       56  65% 06-07-2013 16:31 6ab3fd78  etc/hosts
--------          -------  ---                            -------
    2552              959  62%                            2 files
```

Ajouter un fichier à une archive zip :

```
# zip fic.zip /etc/securetty
  adding: etc/securetty (deflated 52%)
```

```
# unzip -l fic.zip
Archive:  fic.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
     2394  10-30-2015 13:55   passwd
      158  06-07-2013 16:31   etc/hosts
      221  10-29-2014 10:47   etc/securetty
---------                     -------
     2773                     3 files
```

Extraction de fichiers. L'exemple montre l'extraction de tous les fichiers sauf le fichier passwd dans le répertoire /var/tmp.

```
# unzip fic.zip -x passwd -d /var/tmp
Archive:  fic.zip
  inflating: /var/tmp/etc/hosts
  inflating: /var/tmp/etc/securetty
```

Sauvegarde et restauration

Les commandes tar, cpio, dd

- La commande tar
- La commande cpio
- La commande dd

Les commandes tar, cpio, dd

La commande tar (tape archive recorder) est initialement prévue pour créer des archives au format tar sur un lecteur de bande.

Les options usuelles de la commande tar sont :

Option	Description
c	créer l'archive
t	table of contents : consulter le contenu de l'archive
x	extraire l'archive
C	répertoire de destination pour l'extraction
z	appel à gzip pour compresser l'archive
j	appel à bzip2 pour compresser l'archive
v	mode verbeux
h	suivre les liens symboliques
P	sauvegarder en absolu, ne pas enlever le / au début des noms de fichiers

Par défaut la commande tar de GNU effectue une sauvegarde en relatif. Cela signifie que vous pouvez restaurer l'archive à l'endroit que vous voulez. Si on force la sauvegarde en absolu, on ne pourra restaurer qu'à l'endroit indiqué dans le nom du fichier (chemin absolu).

Création d'une archive tar :

```
# tar cf backup.tar /etc
tar: Suppression de « / » au début des noms des membres
```

Consulter le contenu de l'archive :

```
# tar tf backup.tar | tail -5
etc/gtk-2.0/gtkrc
etc/rsyslog.d/
etc/rsyslog.d/gluster.conf.example
etc/rsyslog.d/listen.conf
etc/enscript.cfg
```

Extraction de toute l'archive dans le répertoire /var/tmp :

```
# tar xf backup.tar -C /var/tmp
```

Extraction du fichier passwd dans le répertoire /tmp :

```
# tar xf backup.tar -C /tmp etc/passwd
```

Les archives tar sont la plupart du temps compressées. Cette compression peut se faire après la création de l'archive ou en faisant appel à l'option de compression.

Création d'une archive tar compressée :

Au format gzip :

```
# tar zcf backup1.tar.gz /etc
tar: Suppression de « / » au début des noms des membres
```

Au format bzip2 :

```
# tar jcf backup2.tar.bz2 /etc
tar: Suppression de « / » au début des noms des membres
```

La commande cpio (copy input output) s'utilise derrière un pipe ou avec une redirection d'entrées/sorties.

Les options les plus courantes sont :

Option	Signification
o	output
i	input
t	table of contents
B	effectuer une copie par blocks de 5120 octets au lieu de 512 (par défaut)
d	créer le répertoires lors de la restauration s'ils n'existent pas.
v	mode verbeux

Sauvegarde du répertoire /home avec cpio :

```
# cd /home
# find . | cpio -oB > /tmp/home.cpio
125750 blocs
```

```
# file /tmp/home.cpio
/tmp/home.cpio: cpio archive
```

Consulter le contenu de l'archive :

```
# cpio -it < /tmp/home.cpio  | head
.
user1
user1/.bash_history
user1/.mozilla
user1/.mozilla/extensions
user1/.mozilla/plugins
user1/.bash_logout
user1/fic1
user1/.cache
user1/.cache/abrt
```

Extraction de l'archive dans le répertoire /var/tmp/users :

```
# mkdir /var/tmp/users
# cd /var/tmp/users/
# cpio -iB < /tmp/home.cpio
125750 blocs
# ls
kroot  lost+found  theo  user1  user10  user100  user2  user3  user4  user5
```

La commande dd réalise des sauvegardes de bas niveau. Cette commande va copier directement octet par octet vers le périphérique de destination. Par défaut, la commande dd commence toujours au début du périphérique.

Les options usuelles de la commande dd sont :

Option	Signification
if	input file : fichier d'entrée
of	output file : fichier de sortie
bs	block size la taille des blocs (512 octets par défaut)
skip	le nombre de blocs à ignorer (à sauter).
count	le nombre de blocs à sauvegarder

Exemple : Sauvegarde de la MBR.

La MBR est stockée sur le premier secteur du disque :

```
# dd if=/dev/sda of=/tmp/ma_mbr bs=512 count=1
1+0 enregistrements lus
1+0 enregistrements écrits
512 octets (512 B) copiés, 0,0177903 s, 28,8 kB/s
```

La commande file permet de visualiser le type de fichier :

```
# file /tmp/ma_mbr
/tmp/ma_mbr: x86 boot sector; partition 1: ID=0x83, active, starthead 32, startsector
2048, 2048000 sectors; partition 2: ID=0x83, starthead 155, startsector 2050048, 16384000
sectors; partition 3: ID=0x83, starthead 254, startsector 18434048, 8192000 sectors;
partition 4: ID=0x5, starthead 254, startsector 26626048, 15316992 sectors, code offset
0x63
```

Ce type de fichier peut se lire avec la commande hexdump ou od. La commande strings affiche les caractères ASCII du fichier.

```
# hexdump /tmp/ma_mbr
0000000 63eb 1090 d08e 00bc b8b0 0000 d88e c08e
0000010 befb 7c00 00bf b906 0200 a4f3 21ea 0006
0000020 be00 07be 0438 0b75 c683 8110 fefe 7507
0000030 ebf3 b416 b002 bb01 7c00 80b2 748a 8b01
0000040 024c 13cd 00ea 007c eb00 00fe 0000 0000
0000050 0000 0000 0000 0000 0000 8000 0001 0000
0000060 0000 0000 faff 9090 c2f6 7480 f605 70c2
0000070 0274 80b2 79ea 007c 3100 8ec0 8ed8 bcd0
0000080 2000 a0fb 7c64 ff3c 0274 c288 be52 7c05
0000090 41b4 aabb cd55 5a13 7252 813d 55fb 75aa
00000a0 8337 01e1 3274 c031 4489 4004 4488 89ff
00000b0 0244 04c7 0010 8b66 5c1e 667c 5c89 6608
00000c0 1e8b 7c60 8966 0c5c 44c7 0006 b470 cd42
00000d0 7213 bb05 7000 76eb 08b4 13cd 0d73 845a
00000e0 0fd2 de83 be00 7d85 82e9 6600 b60f 88c6
```

```
00000f0 ff64 6640 4489 0f04 d1b6 e2c1 8802 88e8
0000100 40f4 4489 0f08 c2b6 e8c0 6602 0489 a166
0000110 7c60 0966 75c0 664e 5ca1 667c d231 f766
0000120 8834 31d1 66d2 74f7 3b04 0844 377d c1fe
0000130 c588 c030 e8c1 0802 88c1 5ad0 c688 00bb
0000140 8e70 31c3 b8db 0201 13cd 1e72 c38c 1e60
0000150 00b9 8e01 31db bff6 8000 c68e f3fc 1fa5
0000160 ff61 5a26 be7c 7d80 03eb 8fbe e87d 0034
0000170 94be e87d 002e 18cd feeb 5247 4255 0020
0000180 6547 6d6f 4800 7261 2064 6944 6b73 5200
0000190 6165 0064 4520 7272 726f 0a0d bb00 0001
00001a0 0eb4 10cd 3cac 7500 c3f4 0000 0000 0000
00001b0 0000 0000 0000 0000 b584 000a 0000 2080
00001c0 0021 9b83 7f1c 0800 0000 4000 001f 9b00
00001d0 7f1d fe83 ffff 4800 001f 0000 00fa fe00
00001e0 ffff fe83 ffff 4800 0119 0000 007d fe00
00001f0 ffff fe05 ffff 4800 0196 b800 00e9 aa55
0000200
```

Exemple : Sauvegarde de la table de partitionnement.

La table de partitionnement est stockée sur les secteurs 446 à 510 du disque de démarrage.

Sauvegarde de la table de partitionnement:

```
# dd if=/dev/sda of=/tmp/partition_table bs=1 skip=446 count=64
64+0 enregistrements lus
64+0 enregistrements écrits
64 octets (64 B) copiés, 0,00024363 s, 263 kB/s
```

```
# file /tmp/partition_table
/tmp/partition_table: 8086 relocatable (Microsoft)
```

Sauvegarde d'une partition entière :

Sauvegarder la partition contenant /home sur un autre disque.

```
# df -h /home
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/sda6          1,9G    622M  1,2G  35% /home
```

Créer d'abord une partition d'au moins la taille de la partition à recopier. Dans cet exemple, une partition de 2Go sur /dev/sdb1 avec l'utilitaire fdisk.

Avant partitionnement :

```
# fdisk -l /dev/sdb

Disque /dev/sdb : 8589 Mo, 8589934592 octets, 16777216 secteurs
Unités = secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
```

Après partitionnement :

```
# fdisk -l /dev/sdb

Disque /dev/sdb : 8589 Mo, 8589934592 octets, 16777216 secteurs
Unités = secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0xe9a6fcde

Périphérique Amorçage  Début         Fin      Blocs    Id. Système
/dev/sdb1            2048     4196351     2097152   83  Linux
```

Il ne reste plus qu'à effectuer la copie avec dd de la partition 6 du disque sda vers la partition 1 du disque sdb. Attention à ne pas se tromper, la commande dd est destructrice et ne demande aucune confirmation.

```
# dd if=/dev/sda6 of=/dev/sdb1 bs=1024
2048000+0 enregistrements lus
2048000+0 enregistrements écrits
2097152000 octets (2,1 GB) copiés, 97,8644 s, 21,4 MB/s
```

La commande dd a tout copié, même l'UUID du périphérique. Il risque d'y avoir un conflit dans le futur si on ne le modifie pas.

```
# uuidgen -r
833f875f-82a1-4a5e-a46c-1afb3d5bd958
```

```
#  tune2fs -U 833f875f-82a1-4a5e-a46c-1afb3d5bd958 /dev/sdb1
tune2fs 1.42.9 (28-Dec-2013)
```

Vérification en montant /dev/sdb1 sur un répertoire. On retrouve bien le contenu de /home.

```
# mkdir /users
# mount /dev/sdb1 /users
# ls /users
kroot  lost+found  theo  user1  user10  user100  user2  user3  user4  user5
```

Exemple : Recopier un disque.

La commande dd est pratique pour copier à l'identique deux disques :

```
# dd if=/dev/sda of=/dev/sdb
```

Sauvegarde et restauration

La commande rsync

- Présentation de rsync
- Le fichier /etc/xinetd.d/rsync
- Synchronisation d'un répertoire local avec un répertoire distant

La commande rsync

La commande rsync permet de synchroniser un répertoire local avec un répertoire distant ou inversement. La source ou la destination doit obligatoirement être locale.

L'avantage de rsync est d'envoyer que le différentiel entre la source et la destination, évitant ainsi de surcharger le réseau. Les rsync récents utilisent ssh pour le transfert des fichiers. Si des clefs dsa ou rsa ont été échangées, elles seront utilisées pour l'authentification.

rsync peut fonctionner en mode daemon (sans ssh). Dans ce cas, il est sous le contrôle de xinetd, utilise le port TCP 873 et le fichier de configuration /etc/xinetd.d/rsync. La valeur disable doit être positionnée à no pour activer le service. Enfin, il faut recharger xinetd. La syntaxe des commandes est identique dans les deux modes.

Transférer le répertoire /etc de la machine locale dans le répertoire /var/tmp de la machine distante dont l'adresse IP est 192.168.1.4 :

```
# rsync -a /etc 192.168.1.4:/var/tmp
root@192.168.1.4's password: MDP
```

Transférer le **contenu** du répertoire /etc de la machine locale dans le répertoire /var/tmp de la machine distante dont l'adresse IP est 192.168.1.4 :

```
# rsync -a /etc/ 192.168.1.4:/var/tmp
root@192.168.1.4's password: MDP
```

Pour transférer le contenu d'un répertoire, il faut ajouter le slash (/) derrière le nom du répertoire à transférer.

Dans la ligne de commande, il est possible d'exclure des fichiers du transfert :

```
# rsync -avz --exclude="/etc/passwd" --exclude="/etc/shadow" /etc
192.168.1.4:/var/tmp
root@192.168.1.4's password:MDP
sending incremental file list

sent 72555 bytes  received 283 bytes  3735.28 bytes/sec
total size is 33838415  speedup is 464.57
```

La liste d'exclusion peut aussi provenir d'un fichier :

```
# more /root/exclu
etc
 hosts
 passwd
 shadow
```

```
# rsync -avz --exclude-from=/root/exclu /etc 192.168.1.4:/var/tmp/
root@192.168.1.4's password:MDP
sending incremental file list

sent 10 bytes  received 12 bytes  8.80 bytes/sec
total size is 0  speedup is 0.00
```

Sauvegarde et restauration

Types de sauvegardes : totale, incrémentale ou différentielle

- Sauvegarde totale
- Sauvegarde incrémentale
- Sauvegarde différentielle

Types de sauvegarde : totale, incrémentale ou différentielle

La commande dump permet d'effectuer des sauvegardes totales, incrémentales ou différentielles de systèmes de fichiers.

Sauvegarde totale : sauvegarder le système de fichiers en totalité.

Sauvegarde incrémentale : sauvegarder tous les fichiers modifiés par rapport à la dernière sauvegarde de niveau inférieur.

Sauvegarde différentielle : sauvegarder tous les fichiers modifiés par rapport à la dernière sauvegarde totale.

Les niveaux de sauvegardes sont représentés par des chiffres allant de 0 à 9. Le niveau 0 représente une sauvegarde totale. Les niveau 1 à 9 servent à implémenter la stratégie de sauvegarde incrémentale ou différentielle.

Exemple de stratégie de sauvegarde :

Samedi	Lundi	Mardi	Mercredi	Jeudi	Vendredi
0	3	4	5	6	2
	3	4	5	6	2

Une sauvegarde totale est réalisée le samedi.

Le lundi : une sauvegarde de niveau 3. C'est à dire une sauvegarde de tous les fichiers qui ont été modifiés par rapport à la dernière sauvegarde de niveau inférieur qui est celle du samedi.

Le mardi : une sauvegarde de niveau 4. Soit une sauvegarde de tous les fichiers modifiés depuis la dernière sauvegarde de niveau inférieur qui est celle du lundi (niveau 3).

Même logique pour le mercredi et le jeudi. Il s'agit de sauvegardes incrémentales par rapport à la veille.

Le vendredi : une sauvegarde de niveau 2. Soit une sauvegarde de tous les fichiers modifiés depuis la dernière sauvegarde de niveau inférieur qui est celle du samedi (0). On sauvegarde donc tous les fichiers modifiés durant la semaine.

Le deuxième vendredi, on sauvegarde tous les fichiers modifiés depuis 2 semaines étant donné que c'est par rapport au niveau strictement inférieur.

Exemple d'un stratégie différentielle :

Samedi	Lundi	Mardi	Mercredi	Jeudi	Vendredi
0	8	7	6	5	4

Dans cette stratégie, toutes les sauvegardes sont faites par rapport à la sauvegarde de samedi de niveau 0.

Sauvegarde et restauration

Les commandes xfsdump et xfsrestore

- Sauvegarde d'un système de fichiers avec xfsdump

```
# xfsdump [-l niveau_de_dump]
          -f dest_sauvegarde
          point_montage_du_FS_ à_sauvegarder
```

- Restauration d'un système de fichiers avec xfsrestore

```
# xfsrestore -f /dev/st0 /home          Restauration complète du contenu de la bande.
# xfsrestore -tf /dev/st0               Liste le contenu de la sauvegarde.
# xfsrestore -I /dev/st0                Liste l'inventaire (i majuscule).
# xfsrestore -if /dev/st0 /home         Restauration interactive.
# xfsrestore -f /dev/st0 -X element /home   Exclure des éléments de la restauration.
# xfsrestore -f /dev/st0 -s element /home   Restaurer que les éléments spécifiés.
```

Les commandes xfsdump et xfsrestore

Sauvegarde : xfsdump

```
# xfsdump [-l niveau_de_dump] -f dest_sauvegarde point_montage_du_FS_ à_sauvegarder
```

avec : niveau_de_dump valeur comprise entre 0 et 9.
dest_sauvegarde identification de la sauvegarde. Un lecteur de nade ou un fichier.
point_montage_du_FS_ à_sauvegarder
Le système de fichiers à sauvegarder doit être monté sur ce point de montage.

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

Sauvegarde totale sur une bande du système de fichiers monté sur /home.

```
# xfsdump -l 8 -f /tmp/sauve.dump /home
```

sauvegarde incrémentale de niveau 8. Il y aura donc une sauvegarde du delta par rapport à une sauvegarde de niveau strictement inférieure en remontant dans le temps. La sauvegarde est un fichier /tmp/sauve.dump.

L'historique des sauvegardes avec la date, le niveau de dump, le système de fichiers, etc... est localisé au sein du répertoire /var/lib/xfsdump/inventory.

Restauration : xfsrestore

xfsrestore -f dest_sauvegarde point_de_montage_pour_la_restauration

xfsrestore -f /dev/st0 /home restauration complète du contenu de la bande.

xfsrestore -tf /dev/st0 liste le contenu de la sauvegarde.

xfsrestore -I /dev/st0 liste l'inventaire (i majuscule).

xfsrestore -if /dev/st0 /home restauration interactive.

xfsrestore -f /dev/st0 -X element /home Exclure des éléments de la restauration.

xfsrestore -f /dev/st0 -s element /home Restaurer que les éléments spécifiés.

Mise en œuvre

Sauvegarder le répertoire /users.

```
# df -h /users
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/sdc2          1,9G    622M  1,2G  35% /users
```

Réalisation d'une sauvegarde de niveau 0 du système de fichiers :

```
# xfsdump -f /var/tmp/users0.dump /users
xfsdump: using file dump (drive_simple) strategy
xfsdump: version 3.1.4 (dump format 3.0) - type ^C for status and control

 ============================ dump label dialog ==============================

please enter label for this dump session (timeout in 300 sec)
 ->
session label entered: ""

 -------------------------------- end dialog --------------------------------

xfsdump: WARNING: no session label specified
xfsdump: level 0 dump of cent1708:/users
xfsdump: dump date: Fri Feb 16 09:33:22 2018
xfsdump: session id: ec46fac6-a1db-4fc9-bd23-6eec9a0f5606
xfsdump: session label: ""
xfsdump: ino map phase 1: constructing initial dump list
xfsdump: ino map phase 2: skipping (no pruning necessary)
xfsdump: ino map phase 3: skipping (only one dump stream)
xfsdump: ino map construction complete
xfsdump: estimated dump size: 64384 bytes
xfsdump: /var/lib/xfsdump/inventory created

 ============================ media label dialog ==============================

please enter label for media in drive 0 (timeout in 300 sec)
 ->
media label entered: ""

 -------------------------------- end dialog --------------------------------

xfsdump: WARNING: no media label specified
xfsdump: creating dump session media file 0 (media 0, file 0)
xfsdump: dumping ino map
xfsdump: dumping directories
xfsdump: dumping non-directory files
xfsdump: ending media file
xfsdump: media file size 39424 bytes
xfsdump: dump size (non-dir files) : 4896 bytes
xfsdump: dump complete: 20 seconds elapsed
xfsdump: Dump Summary:
xfsdump:   stream 0 /var/tmp/users0.dump OK (success)
xfsdump: Dump Status: SUCCESS
```

Modification de /users et sauvegarde incrémentale de niveau 4 :

```
# mkdir /users/usertest
# … etc …
```

```
# xfsdump -l 4 -f /var/tmp/users4.dump /users
xfsdump: using file dump (drive_simple) strategy
xfsdump: version 3.1.4 (dump format 3.0) - type ^C for status and control

 ============================ dump label dialog ==============================

please enter label for this dump session (timeout in 300 sec)
 ->
session label entered: ""

 -------------------------------- end dialog --------------------------------

xfsdump: WARNING: no session label specified
xfsdump: level 4 incremental dump of cent1708:/users based on level 0 dump begun Fri Feb
16 09:33:22 2018
xfsdump: dump date: Fri Feb 16 09:41:08 2018
xfsdump: session id: f756f880-7af7-43b1-b23a-8d4e3bef36f5
xfsdump: session label: ""
xfsdump: ino map phase 1: constructing initial dump list
xfsdump: ino map phase 2: pruning unneeded subtrees
xfsdump: ino map phase 3: skipping (only one dump stream)
xfsdump: ino map construction complete
xfsdump: estimated dump size: 35328 bytes

 ============================ media label dialog ============================

please enter label for media in drive 0 (timeout in 300 sec)
 ->
media label entered: ""

 -------------------------------- end dialog --------------------------------

xfsdump: WARNING: no media label specified
xfsdump: creating dump session media file 0 (media 0, file 0)
xfsdump: dumping ino map
xfsdump: dumping directories
xfsdump: dumping non-directory files
xfsdump: ending media file
xfsdump: media file size 27248 bytes
xfsdump: dump size (non-dir files) : 1632 bytes
xfsdump: dump complete: 4 seconds elapsed
xfsdump: Dump Summary:
xfsdump:   stream 0 /var/tmp/user4.dump OK (success)
xfsdump: Dump Status: SUCCESS
```

Restauration des sauvegardes :

Création d'un nouveau système de fichiers

```
# mkfs.xfs -f /dev/sdc2
```

Mise à jour de l'UUID par rapport à l'information dans /etc/fstab. Cette modification se fait obligatoirement sur un système de fichiers démonté.

```
# grep users /etc/fstab
UUID=4d750625-f2cd-4f32-9dfd-0c705af7f40a     /users     xfs     defaults    0   0

# xfs_admin -U 4d750625-f2cd-4f32-9dfd-0c705af7f40a /dev/sda6
tune2fs 1.42.9 (28-Dec-2013)
```

Montage du système de fichiers.

```
# mount /users
# df -h /users
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/sdc2          1,9G    5,9M  1,8G   1% /users
```

Restauration de la sauvegarde de niveau 0.

```
# xfsrestore -f /var/tmp/users0.dump /users
xfsrestore: using file dump (drive_simple) strategy
xfsrestore: version 3.1.4 (dump format 3.0) - type ^C for status and control
xfsrestore: searching media for dump
xfsrestore: examining media file 0
xfsrestore: dump description:
xfsrestore: hostname: cent1708
xfsrestore: mount point: /users
xfsrestore: volume: /dev/sdc2
xfsrestore: session time: Fri Feb 16 09:33:22 2018
xfsrestore: level: 0
xfsrestore: session label: ""
xfsrestore: media label: ""
xfsrestore: file system id: dfed9332-418f-4a18-a3a2-e6ba0b3ba900
xfsrestore: session id: ec46fac6-a1db-4fc9-bd23-6eec9a0f5606
xfsrestore: media id: 71160733-161f-4d7a-8cfc-ddae42a6f447
xfsrestore: using online session inventory
xfsrestore: searching media for directory dump
xfsrestore: reading directories
xfsrestore: 13 directories and 21 entries processed
xfsrestore: directory post-processing
xfsrestore: restoring non-directory files
xfsrestore: restore complete: 0 seconds elapsed
xfsrestore: Restore Summary:
xfsrestore:   stream 0 /var/tmp/users0.dump OK (success)
xfsrestore: Restore Status: SUCCESS

# ls
user1   user100  user3  user5  ...
```

Restauration de la sauvegarde de niveau 4.

```
# xfsrestore -f /var/tmp/users4.dump /users

# ls
user1   user100  user3  user5  ...  usertest
```

La commande xfsrestore en mode interactif

Les sous-commandes 'add' et 'delete' permettent de sélectionner ce que vous voulez restaurer. Une fois la sélection effectuée, il ne reste plus qu'à extraire le contenu via 'extract'.

Restauration de quelques fichiers au sein de /tmp.

```
# xfsrestore -if /var/tmp/users0.dump /tmp
xfsrestore: using file dump (drive_simple) strategy
xfsrestore: version 3.1.4 (dump format 3.0) - type ^C for status and control
xfsrestore: searching media for dump
xfsrestore: examining media file 0
xfsrestore: dump description:
xfsrestore: hostname: cent1708
xfsrestore: mount point: /users
xfsrestore: volume: /dev/sdc2
xfsrestore: session time: Fri Feb 16 09:33:22 2018
xfsrestore: level: 0
xfsrestore: session label: ""
xfsrestore: media label: ""
xfsrestore: file system id: dfed9332-418f-4a18-a3a2-e6ba0b3ba900
xfsrestore: session id: ec46fac6-a1db-4fc9-bd23-6eec9a0f5606
xfsrestore: media id: 71160733-161f-4d7a-8cfc-ddae42a6f447
xfsrestore: using online session inventory
xfsrestore: searching media for directory dump
xfsrestore: reading directories
xfsrestore: 13 directories and 21 entries processed
xfsrestore: directory post-processing

 ========================= subtree selection dialog ==========================

the following commands are available:
        pwd
        ls [ <path> ]
        cd [ <path> ]
        add [ <path> ]
        delete [ <path> ]
        extract
        quit
        help

 -> ls
              75 user12/
              71 user11/
              67 user10/

 -> add user10

 -> cd user10

 -> ls
    *         70 .bashrc
    *         69 .bash_profile
    *         68 .bash_logout
    *     524352 .mozilla/

 -> delete .bashrc

 -> ls
              70 .bashrc
    *         69 .bash_profile
    *         68 .bash_logout
    *     524352 .mozilla/

 -> extract

 -------------------------------- end dialog ---------------------------------
```

```
xfsrestore: restoring non-directory files
xfsrestore: restore complete: 59 seconds elapsed
xfsrestore: Restore Summary:
xfsrestore:   stream 0 /var/tmp/users0.dump OK (success)
xfsrestore: Restore Status: SUCCESS
```

Vérification :

```
# ls
user10
# ls –a user10
.    ..    .bash_logout    .mozilla    .bash_profile
```

Lister le contenu de l'inventaire

```
# xfsrestore -I
file system 0:
        fs id:          dfed9332-418f-4a18-a3a2-e6ba0b3ba900
        session 0:
                mount point:    cent1708:/users
                device:         cent1708:/dev/sdc2
                time:           Fri Feb 16 09:33:22 2018
                session label:  ""
                session id:     ec46fac6-a1db-4fc9-bd23-6eec9a0f5606
                level:          0
                resumed:        NO
                subtree:        NO
                streams:        1
                stream 0:
                        pathname:       /var/tmp/users0.dump
                        start:          ino 68 offset 0
                        end:            ino 79 offset 0
                        interrupted:    NO
                        media files:    1
                        media file 0:
                                mfile index:    0
                                mfile type:     data
                                mfile size:     39424
                                mfile start:    ino 68 offset 0
                                mfile end:      ino 79 offset 0
                                media label:    ""
                                media id:       71160733-161f-4d7a-8cfc-ddae42a6f447
        session 1:
                mount point:    cent1708:/users
                device:         cent1708:/dev/sdc2
                time:           Fri Feb 16 09:41:08 2018
                session label:  ""
                session id:     f756f880-7af7-43b1-b23a-8d4e3bef36f5
                level:          4
                resumed:        NO
                subtree:        NO
                streams:        1
                stream 0:
                        pathname:       /var/tmp/user4.dump
                        start:          ino 80 offset 0
                        end:            ino 83 offset 0
                        interrupted:    NO
                        media files:    1
                        media file 0:
                                mfile index:    0
                                mfile type:     data
                                mfile size:     27248
                                mfile start:    ino 80 offset 0
                                mfile end:      ino 83 offset 0
                                media label:    ""
                                media id:       6df0d684-b070-4373-b7a0-3cafd91675fa
file system 1:
 ...
```

Afficher le contenu d'une sauvegarde

```
# xfsrestore -tf /var/tmp/users0.dump
xfsrestore: using file dump (drive_simple) strategy
xfsrestore: version 3.1.4 (dump format 3.0) - type ^C for status and control
xfsrestore: searching media for dump
xfsrestore: examining media file 0
xfsrestore: dump description:
xfsrestore: hostname: cent1708
xfsrestore: mount point: /users
xfsrestore: volume: /dev/sdc2
xfsrestore: session time: Fri Feb 16 09:33:22 2018
xfsrestore: level: 0
xfsrestore: session label: ""
xfsrestore: media label: ""
xfsrestore: file system id: dfed9332-418f-4a18-a3a2-e6ba0b3ba900
xfsrestore: session id: ec46fac6-a1db-4fc9-bd23-6eec9a0f5606
xfsrestore: media id: 71160733-161f-4d7a-8cfc-ddae42a6f447
xfsrestore: using online session inventory
xfsrestore: searching media for directory dump
xfsrestore: reading directories
xfsrestore: 13 directories and 21 entries processed
xfsrestore: directory post-processing
xfsrestore: reading non-directory files
user10/.bash_logout
user10/.bash_profile
user10/.bashrc
user11/.bash_logout
user11/.bash_profile
user11/.bashrc
user12/.bash_logout
user12/.bash_profile
user12/.bashrc
xfsrestore: table of contents display complete: 0 seconds elapsed
xfsrestore: Restore Summary:
xfsrestore:   stream 0 /var/tmp/users0.dump OK (success)
xfsrestore: Restore Status: SUCCESS
```

Exclure des éléments d'une restauration

Exclure le répertoire user10 d'une restauration.

```
# xfsrestore -f /var/tmp/users0.dump -X user10 /tmp/restore
```

Exclure un fichier d'une restauration.

```
# xfsrestore -f /var/tmp/users0.dump -X user10/.bashrc /tmp/restore
```

Restauration que de quelques éléments

Restaurer que le répertoire user11.

```
# xfsrestore -f /var/tmp/users0.dump -s user11 /tmp/restore
```

Restaurer qu'un fichier.

```
# xfsrestore -f /var/tmp/users0.dump -s user11/.bashrc /tmp/restore
```

Sauvegarde et restauration

La procédure pour restorer la racine

- Sauvegarde du slash
- Booter sur le cdrom en mode secours
- Restauration du slash
- Paramétrage du slash

La procédure pour restaurer la racine

La sauvegarde su slash.

```
# xfsdump -l 0 -f /backup/slash0.dump /
xfsdump: using file dump (drive_simple) strategy
xfsdump: version 3.1.4 (dump format 3.0) - type ^C for status and control

 ============================ dump label dialog ==============================

please enter label for this dump session (timeout in 300 sec)
 -> slash_dump
session label entered: "slash_dump"

 -------------------------------- end dialog ---------------------------------

xfsdump: WARNING: most recent level 0 dump was interrupted, but not resuming that dump
since resume (-R) option not specified
xfsdump: level 0 dump of poste-centos7:/
xfsdump: dump date: Tue Mar  7 15:13:14 2017
xfsdump: session id: cc6a5f37-bf4d-43eb-b2dc-3824714ef023
xfsdump: session label: "slash_dump"
xfsdump: ino map phase 1: constructing initial dump list
xfsdump: ino map phase 2: skipping (no pruning necessary)
xfsdump: ino map phase 3: skipping (only one dump stream)
xfsdump: ino map construction complete
xfsdump: estimated dump size: 4334218048 bytes

 ============================ media label dialog ==============================

please enter label for media in drive 0 (timeout in 300 sec)
 -> rep_backup
media label entered: "rep_backup"

 -------------------------------- end dialog ---------------------------------
```

```
xfsdump: creating dump session media file 0 (media 0, file 0)
xfsdump: dumping ino map
xfsdump: dumping directories
xfsdump: dumping non-directory files
xfsdump: ending media file
xfsdump: media file size 4170583344 bytes
xfsdump: dump size (non-dir files) : 4086303488 bytes
xfsdump: dump complete: 373 seconds elapsed
xfsdump: Dump Summary:
xfsdump:   stream 0 /backup/slash0.dump OK (success)
xfsdump: Dump Status: SUCCESS
```

```
# file /backup/slash0.dump
/backup/slash0.dump: xfsdump archive (version 3)
```

Suppression de répertoires indispensables. (Ne pas faire en production !!!).

```
# rm -rf /etc /dev
rm: impossible de supprimer « /dev/mqueue »: Périphérique ou ressource occupé
rm: impossible de supprimer « /dev/hugepages »: Périphérique ou ressource occupé
rm: impossible de supprimer « /dev/pts/2 »: Opération non permise
rm: impossible de supprimer « /dev/pts/ptmx »: Opération non permise
rm: impossible de supprimer « /dev/shm »: Périphérique ou ressource occupé
```

Le système ne redémarre pas.
Pour restaurer la racine, il faut booter sur le cdrom en mode secours (***Troubleshooting*** sur un DVD CentOS 7, puis ***Rescue a CentOS Linux system***).

Le système va alors chercher la partition qui contient la racine et la monter sur le répertoire ***/mnt/sysimage***.

Le choix 1 du menu permet de continuer et d'effectuer le montage. Le slash a été tellement cassé que le système n'arrive pas à faire le montage. IL faut donc appuyer sur enter pour avoir un shell et pour effectuer le montage à la main.

Remarque : le clavier est en qwerty. Pour charger un clavier français tapez la commande ***loadkeys fr***.

Étant donné que notre slash est entièrement corrompu, on va créer une nouveau système de fichiers sur le volume logique contenant la racine.

Afficher les groupes de volume.

```
# lvm vgscan -v
```

Activer les volumes logiques.

```
# lvm vgchange -a y
```

Lister les volumes logiques.

```
# lvm lvs  --all
```

Création d'un nouveau système de fichiers.

```
# mkfs.xfs -f /dev/cl_poste-centos7/root
```

Montage de la partition sur un point de montage.

```
# mkdir /resto
# mount /dev/cl_poste-centos7/root /resto
```

Montage de la partition contenant la sauvegarde xfs.

```
# mkdir /backup
# mount /dev/sdb1 /backup
```

Restauration des données.

```
# xfsrestore -f /backup/slash0.dump /resto
…
…
xfsrestore : Restore Status : SUCCESS
```

La commande ***exit*** permet de sortir du shell de secours et la machine redémarre.

Sauvegarde de la table GPT :

```
# sfdisk -d /dev/sda > /tmp/table_gpt_sda
```

Il faut copier le fichier /tmp/table_gpt_sda sur un partage NFS ou un disque dur externe.

Pour restaurer la table GPT :

```
# sfdisk -d /dev/sda < /tmp/table_gpt_sda
```

Procédure de Sauvegarde / Restauration de la table GPT et du slash.

Partitionnement actuel :

```
# df -h
Sys. de fichiers    Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/cl-root    17G    5,6G   12G  34% /
devtmpfs              905M       0  905M   0% /dev
tmpfs                 920M     96K  920M   1% /dev/shm
tmpfs                 920M    8,8M  911M   1% /run
tmpfs                 920M       0  920M   0% /sys/fs/cgroup
/dev/sda2            1014M    257M  758M  26% /boot
/dev/sda1             200M    9,5M  191M   5% /boot/efi
tmpfs                 184M    8,0K  184M   1% /run/user/1000
tmpfs                 184M       0  184M   0% /run/user/0
/dev/sdb1              30G     33M   30G   1% /data
```

Sauvegarde de la table GPT :

```
# sfdisk -d /dev/sda > /data/table_gpt_sda
```

Sauvegarde de /boot/efi :

```
# dd if=/dev/sda1 of=/data/partition_efi
```

Sauvegarde du slash

```
# xfsdump -l 0 -f /data/slash_sda.dump /
```

Remarque : Le système de fichiers /boot peut aussi être sauvegardé avec xfsdump.

```
# file /data/*
/data/partition_efi:  x86 boot sector, mkdosfs boot message display, code offset 0x3c,
OEM-ID "mkfs.fat", sectors/cluster 8, root entries 512, Media descriptor 0xf8,
sectors/FAT 200, heads 255, sectors 409600 (volumes > 32 MB) , reserved 0x1, serial
number 0x4a187e1e, unlabeled, FAT (16 bit)
/data/slash_sda.dump: xfsdump archive (version 3)
/data/table_gpt_sda:  ASCII text
```

Suppression de certains fichiers indispensables pour le système :

```
# rm -rf /etc /dev
```

→ Le système ne reboot plus. Il faut donc utiliser la procédure décrite auparavant et booter sur le cdrom en mode troubleshooting.

Restauration du système.

En bootant sur le CDROM en mode troubleshooting, le système n'arrive pas à monter la partition linux sur /mnt/sysimage. Il faut donc effectuer le montage à la main.

Lister les volumes logiques :

```
# lvm lvs--all
```

Accès à mes sauvegardes qui sont stockés sur /dev/sdb1

```
# mkdir /sauve
# mount /dev/sdb1 /sauve
```

Restauration de la table GPT

```
# sfdisk /dev/sda < /sauve/table_gpt_sda
```

Restauration de /boot

```
# dd if=/sauve/partition_efi of=/dev/sda1
```

Restauration du /

```
# mkfs.xfs -f /dev/cl/root
# mkdir /resto
# mount /dev/cl/root /resto
# xfsrestore -f /sauve/slash_sda.dump /resto
# exit
```

Sauvegarde et restauration

Les systèmes de fichiers ext : dump et restore

- Sauvegarde d'un système de fichiers avec dump

```
#  dump  {01...9}uf  /dev/st0  /home
#  dump  {01...9}uf  /dev/st0  /dev/sda6
```

- Restauration d'un système de fichiers avec restore

```
#  restore  rf   /dev/st0
#  restore  xf   /dev/st0  fic1  fic2
#  restore  ivf  /dev/st0
#  restore  tvf  /dev/st0
```

Supprimer restoresymtable

Les systèmes de fichiers ext : dump et restore

Sauvegarde : dump

```
# dump  options  <système de fichier à sauvegarder>
```

```
# dump  0f  /dev/st0  /home
```

Sauvegarde totale sur une bande. Il n'est pas prévu de sauvegardes incrémentales.

```
# dump  0uf  /dev/st0  /home
```

Sauvegarde totale sur une bande.
L'option « u » met à jour le fichier /etc/dumpdates, ce qui nous permettra d'exploiter des sauvegardes incrémentales.

```
# dump  8uf  /dev/st0  /home
```

sauvegarde incrémentale de niveau 8. Il y aura donc une sauvegarde du delta par rapport à une sauvegarde de niveau strictement inférieure en remontant dans le temps. C'est le fichier /etc/dumpdates qui est utilisé.

Restauration : restore

La restauration se fait en chemin relatif.

# restore rf /dev/st0 (récursive)	restauration complète du contenu de la bande
# restore xf /dev/st0 fic1 fic2	restauration des fichiers fic1 et fic2 à partir de la bande.
# restore ivf /dev/st0	restauration interactive.
# restore tvf /dev/st0	liste le contenu de la sauvegarde.

La commande restore créé un fichier restoresymtable qu'il faut supprimer à la fin du processus de restauration.

Notes

Gestion des journaux système

Dans ce chapitre, nous allons étudier la configuration de syslogd pour renseigner les fichiers de logs.

Table des matières

Gestion des journaux système

Les fichiers journaux

/var/log/messages

/var/log/lastlog

/var/log/cron

/var/log/maillog

/var/log/secure

/var/log/dmesg

/var/log/boot.log

Les fichiers journaux

La journalisation est fondamentale pour les opérations de suivi et de sécurité :

- Suivi de l'activité du système d'exploitation, de services et d'applications.
- Sécurité, pour pouvoir retracer se qui s'est passé et par qui sur le système, un service ou une application.

Quelques fichiers de log à surveiller et à purger :

/var/log/messages : fichier de journalisation du système, également alimenté par le mécanisme syslog. Il est utile de s'intéresser aux lignes 'NOTICE', 'WARNING' et 'ERROR'.

/var/log/lastlog : fichier contenant la liste des dernières connexions de chaque utilisateur. Il est utilisé par la commande finger.

/var/log/cron : fichier de journalisation du mécanisme cron.

/var/log/maillog : fichier de journalisation du service mail.

/var/log/secure : fichier de journalisation des services d'authentification.

/var/log/dmesg : fichier de journalisation associé au noyau.

/var/log/boot.log : fichier de journalisation de la séquence de boot et du démarrage des services.

Gestion des journaux système

Présentation de rsyslogs

- Présentation de rsyslogd
- Le fichier /etc/rsyslog.conf

Présentation de rsyslogd

La fonction rsyslog envoie des messages produits par les programmes du kernel et les services utilitaires système au démon rsyslogd. Avec la fonction rsyslog, vous pouvez contrôler la journalisation des messages en fonction de la configuration du fichier /etc/rsyslog.conf. Le démon peut :

- Écrire des messages à un journal système,
- Transmettre des messages à un loghost centralisé,
- Transmettre des messages à une liste d'utilisateurs,
- Écrire des messages sur la console système.

Le champ sélecteur comprend deux composants, un service et un niveau exprimé sous la forme service.niveau. Les services représentent des catégories de processus du système qui peuvent produire des messages. Les niveaux représentent la gravité ou l'importance du message.

Syntaxe d'une ligne du fichier /etc/rsyslog.conf :

service1.niveau1; service2.niveau2 Action

Les différents services sont :

Nom service	Description
kern	Messages générés par le kernel.
user	Messages générés par un processus utilisateur.
mail	Messages générés par le mécanisme de mail.
daemon	Messages générés par un processus démon (ex: in.ftpd, telnetd).
auth	Messages générés par demande d'autorisation système (ex: login, su).
authpriv	Messages générés par certains services d'authentification.
lpr	Messages générés par le système d'impression.
news	pour le mécanisme USENET (network news system).
uucp	pour le mécanisme UNIX-to-UNIX copy (UUCP).
cron	pour le mécanisme cron et at (crontab, at, et cron).
audit	les messages d'audit.
local0-7	un champ réservé pour un usage local.
mark	intègre une référence de la date au sein du mécanisme syslogd.
*	Tout le monde, à l'exception de 'mark'.

Liste des niveaux (dans l'ordre décroissant de gravité) :

Niveau d'alerte	Description
emerg	conditions de panique qui sont envoyées par broadcast à tous les utilisateurs connectés sur le système.
alert	erreurs qui doivent être corrigées immédiatement, comme une base de données système corrompue.
crit	alertes sur des conditions critiques, comme des erreurs hardware.
err	autres erreurs.
warning	messages d'alertes.
notice	conditions qui ne sont pas des conditions d'erreurs, mais qui demandent une attention particulière.
info	messages d'informations.
debug	messages qui sont normalement utilisés seulement pour débugger un programme.
none	pour exclure un service spécifique lors de l'utilisation du caractère *.

Type des actions :

Valeur	Description
/fichier	lorsqu'une action débute par un slash (/), il s'agit d'un fichier.
@host	lorsqu'une action débute par un arobas (@), il s'agit d'une redirection vers le démon syslogd d'une machine distante.
user1,user2	envoie du message à user1 et user2 s'ils sont connectés.
*	il s'agit de l'envoi d'un message à l'ensemble des utilisateurs connectés.

Le fichier de configuration /etc/rsyslogd.conf comporte trois sections :

- la section MODULES qui permet de charger un certain nombre de modules. C'est dans cette section qu'il faut décommenter des variables pour autoriser la réception de rsyslogd distants.

- la section GLOBAL DIRECTIVES qui contient une configuration globale de rsyslogd.

- la section RULES qui contient les règles rsyslogd.

Extrait du fichier de configuration de rsyslogd :

```
# cat /etc/rsyslog.conf | tail -n +45 | head -30 | nl

     1  #### RULES ####

     2  # Log all kernel messages to the console.
     3  # Logging much else clutters up the screen.
     4  #kern.*                                                 /dev/console

     5  # Log anything (except mail) of level info or higher.
     6  # Don't log private authentication messages!
     7  *.info;mail.none;authpriv.none;cron.none                /var/log/messages

     8  # The authpriv file has restricted access.
     9  authpriv.*                                              /var/log/secure

    10  # Log all the mail messages in one place.
    11  mail.*                                                  -/var/log/maillog


    12  # Log cron stuff
    13  cron.*                                                  /var/log/cron

    14  # Everybody gets emergency messages
    15  *.emerg                                                 :omusrmsg:*

    16  # Save news errors of level crit and higher in a special file.
    17  uucp,news.crit                                          /var/log/spooler

    18  # Save boot messages also to boot.log
    19  local7.*                                                /var/log/boot.log
```

Ligne 7 :
Les logs de tous les services de niveau info (*.info) sauf pour les services mail (mail.none), authpriv (authpriv.none) et cron (cron.none) sont stockés dans le fichier /var/log/messages.

Ligne 9 :
Les logs du service authpriv pour tous les niveaux (authpriv.*) sont stockés dans le fichier /var/log/secure.

Ligne 11 :
Les logs du service mail pour tous les niveaux (mail.*) sont stockés dans le fichier /var/log/maillog. Le signe – indique d'effectuer l'écriture de manière asynchrone.

Ligne 13 :
Les logs du service cron pour tous les niveaux (cron.*) sont stockés dans le fichier /var/log/cron.

Ligne 15 :
Les logs de tous les services de niveau emerg (*.emerg) sont envoyés à tous les terminaux de tous les utilisateurs connectés (:omusrmsg :*).

ligne 17 :
Les logs des services uucp et news de niveau crit (uucp,news.crit) sont stockés dans le fichier /var/log/spooler. A noter que cette écriture est identique à uucp.crit;news.crit.

Ligne 19 :
Les logs du service local7 de niveau info sont stockés dans le fichier /var/log/boot. Les messages générés lors du boot sont attachés à local7.

Le comportement par défaut du service rsyslogd est de logger (journaliser) pour le service et le niveau ainsi que les niveaux supérieurs.

Le signe '=' permet de logger exactement pour le niveau spécifié.

Ainsi pour auth.info, il sera loggé tous les messages venant du service authentification des niveaux info à emerg.
Alors qu'avec auth.=info, il sera loggé tous les messages du service d'authentification de niveau info.

Gestion des journaux système

La commande logwatch

- Présentation de logwatch
- Les fichiers de configuration
- Les rapports

La commande logwatch

Logwatch est un mécanisme de récupération de logs d'un système. On peut utiliser des filtres pour trier les informations. Logwatch peut aussi envoyer un mail à l'administrateur du système. Logwatch est écrit en perl, il faut l'installer sur le système.

```
# yum install –y logwatch
```

Le mécanisme logwatch est exécuté quotidiennement par crond grâce au fichier /etc/cron.daily/0logwatch.

Le fichier de configuration se trouve dans /usr/share/logwatch/default.conf et s'appelle logwatch.conf.

Le fichier est très bien commenté, il est donc assez aisé de le comprendre.

MailTo = nom@mail indique le mail de la personne recevant le rapport.

Print= No indique à logwatch de ne pas afficher directement le résultat.

DailyReport = No indique qu'il ne faut pas envoyer de rapport quotidien (commenté par défaut).

Save= /rep/fic indique un fichier local dans lequel sauvegarder le rapport.

Extrait du fichier de configuration de logwatch :

```
# more /usr/share/logwatch/default.conf/logwatch.conf
########################################################
# This was written and is maintained by:
#    Kirk Bauer <kirk@kaybee.org>
#
# Please send all comments, suggestions, bug reports,
#    etc, to kirk@kaybee.org.
#
########################################################

# NOTE:
#   All these options are the defaults if you run logwatch with no
#   command-line arguments.  You can override all of these on the
#   command-line.

# You can put comments anywhere you want to.  They are effective for the
# rest of the line.

# this is in the format of <name> = <value>.  Whitespace at the beginning
# and end of the lines is removed.  Whitespace before and after the = sign
# is removed.  Everything is case *insensitive*.

# Yes = True  = On  = 1
# No  = False = Off = 0

# Default Log Directory
# All log-files are assumed to be given relative to this directory.
LogDir = /var/log

# You can override the default temp directory (/tmp) here
TmpDir = /var/cache/logwatch

# Default person to mail reports to.  Can be a local account or a
# complete email address.  Variable Print should be set to No to
# enable mail feature.
MailTo = root
# WHen using option --multiemail, it is possible to specify a different
# email recipient per host processed.  For example, to send the report
# for hostname host1 to user@example.com, use:
#Mailto_host1 = user@example.com
# Multiple recipients can be specified by separating them with a space.

# Default person to mail reports from.  Can be a local account or a
# complete email address.
MailFrom = Logwatch

# If set to 'Yes', the report will be sent to stdout instead of being
# mailed to above person.
Print =

# if set, the results will be saved in <filename> instead of mailed
# or displayed.
#Save = /tmp/logwatch

# Use archives?  If set to 'Yes', the archives of logfiles
# (i.e. /var/log/messages.1 or /var/log/messages.1.gz) will
# be searched in addition to the /var/log/messages file.
# This usually will not do much if your range is set to just
# 'Yesterday' or 'Today'... it is probably best used with
# By default this is now set to Yes. To turn off Archives uncomment this.
```

Les services à surveiller sont indiqués dans le fichier de conf de logwatch. Par défaut, presque tous les services sont surveillés (ligne Service = All dans le fichier de configuration). Pour surveiller seulement certains services, il faut faire suivre le mot clef service par le nom du service. Par exemple pour surveiller httpd et dhcpd :

```
Service = http
Service = dhcp
```

Pour surveiller tous les services sauf http et dhcp, la syntaxe suivante sera utilisée (le – pour exclure).

```
Service = All
Service = ''-http''
Service = ''-dhcp''
```

Pour vérifier quels services sont surveillés sur notre système :

```
# grep -i service logwatch.conf | grep -v '^#'
Service = All
Service = "-zz-network"      # Prevents execution of zz-network service, which
Service = "-zz-sys"          # Prevents execution of zz-sys service, which
Service = "-eximstats"       # Prevents execution of eximstats service, which
```

Pour lancer manuellement logwatch, on peut exécuter directement la commande :

```
# logwatch
```

Pour forcer l'impression d'un rapport à l'écran, ajouter l'option –print :

```
# logwatch --print

 ################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Fri Jan 29 16:03:34 2016
        Date Range Processed: yesterday
                              ( 2016-Jan-28 )
                              Period is day.
      Detail Level of Output: 0
             Type of Output: unformatted
          Logfiles for Host: formateur
  ################################################################

 ---------------------- Automount Begin ------------------------

 **Unmatched Entries**
 lookup_read_master: lookup(nisplus): couldn't locate nis+ table auto.master: 1 Time(s)

 ----------------------- Automount End -------------------------


 ---------------------- Cron Begin ------------------------


 **Unmatched Entries**
 INFO (RANDOM_DELAY will be scaled with factor 24% if used.)
```

```
 ---------------------- Cron End -------------------------


 --------------------- pam_unix Begin ------------------------

 gdm-password:
    Unknown Entries:
       authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=  user=theo: 1
Time(s)
       session opened for user theo by (uid=0): 1 Time(s)


 ---------------------- pam_unix End -------------------------


 --------------------- Postfix Begin ------------------------

        1   Postfix start


 ---------------------- Postfix End -------------------------


 --------------------- Connections (secure-log) Begin ------------------------


 **Unmatched Entries**
    polkitd(authority=local): Registered Authentication Agent for session
/org/freedesktop/ConsoleKit/Session1 (system bus name :1.31 [/usr/libexec/polkit-gnome-
authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, locale
fr_FR.UTF-8): 1 Time(s)
    polkitd(authority=local): Registered Authentication Agent for session
/org/freedesktop/ConsoleKit/Session2 (system bus name :1.51 [/usr/libexec/polkit-gnome-
authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, locale
fr_FR.UTF-8): 1 Time(s)
    polkitd(authority=local): Unregistered Authentication Agent for session
/org/freedesktop/ConsoleKit/Session1 (system bus name :1.31, object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale fr_FR.UTF-8) (disconnected from bus): 1
Time(s)

 ---------------------- Connections (secure-log) End -------------------------


 --------------------- SSHD Begin ------------------------


 SSHD Started: 2 Time(s)

 Users logging in through sshd:
    root:
       192.168.1.1 (PosteSpherius.home): 1 time

 ---------------------- SSHD End -------------------------


 --------------------- Disk Space Begin ------------------------

 Filesystem                      Size  Used Avail Use% Mounted on
 /dev/mapper/vg_formateur-lv_root   18G   12G  4.8G  71% /
 /dev/sda1                      485M   39M  421M   9% /boot
 /dev/sdb1                       20G  2.3G   17G  13% /iso
 /dev/sdb2                       30G  172M   28G   1% /vm


 ---------------------- Disk Space End -------------------------


 ######################## Logwatch End #########################
```

Gestion des journaux système

La rotation des logs avec logrotate

- Présentation de logrotate
- Le fichier /etc/logrotate.conf
- Les répertoire /etc/logrotate.d

La rotation des logs avec logrotate

Pour éviter quel les fichiers de journalisation aient une taille trop importante une rotation automatique des logs est effectué. Ainsi le fichier /var/log/messages va etre renommé en /var/log/messages_1 (ou avec un extension de date selon le paramétrage), et un nouveau fichier vide sera créer pour les logs futurs.

Le fichier de configuration pour tous les services est /etc/logrotate.conf. Dans le répertoire /etc/logrotate.d une rotation spécifique pour chaque service peut être indiquée.

Extrait du fichier /etc/logrotate.conf

```
# head -18 /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

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

# use date as a suffix of the rotated file
dateext

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

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

La configuration générale indique:

La rotation se fait de manière hebdomadaire (***weekly***).

On garde 4 fichiers après les rotations (par exemple: messages, messages-1, messages-2, messages-3, messages-4). Pour la prochaine rotation messages-4 sera supprimé. message-3 sera renommé en message-4, message-2 en message-3, etc...). (***rotate 4***).

Après la rotation , on créé un nouveau fichier (***create***).

J'utilise une extension de date pour renommer mes fichiers (***dateext***).

Les fichiers ne sont pas compressés après la rotation (***compress*** est commenté).

Pour des services spécifiques la définition de la rotation des logs est dans le répertoire /etc/logrotate.d (***include /etc/logrotate.d***).

Gestion des journaux système

Les logs avec journald

- Présentation de journald
- journalctl
- Filtrage des messages

Les logs avec journald

Les fichiers journaux sont une composante de systemd qui est responsable de maintenir les fichiers de log. Journald peut-etre utilisé à la place ou en parralèle de rsyslogd. Journald crée et maintient des fichiers binaires concernant les informations reçus part le noyau, les processus utilisateurs, et les messages d'erreurs applicatives. Les fichiers journaux sont indexés et structurés ce qui permet une recherche rapide. Les fichiers journaux actuels sont sécurisés et ne peuvent donc pas être édités manuellement. Journald stocke les messages uniquement en mémoire ou dans un petit tampon dans le répertoire /run/log/journal. Pour stocker les fichiers de manière permanente (comme rsyslogd) il faudra créer le fichier /var/log/journal qui sera persistent au reboot.

La commande journalctl permet d'afficher les logs.

```
# journalctl
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:30:01
oct. 26 14:25:43 centos-uefi systemd-journal[94]: Runtime journal is using 8.0M
oct. 26 14:25:43 centos-uefi kernel: Initializing cgroup subsys cpuset
…
```

L'option -n permet de voir les n derniers messages

```
# journalctl -n 3
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:30:01
oct. 26 15:30:01 newname systemd[1]: Started Session 10 of user root.
oct. 26 15:30:01 newname systemd[1]: Starting Session 10 of user root.
oct. 26 15:30:01 newname CROND[3418]: (root) CMD (/usr/lib64/sa/sa1 1 1)
```

L'option -o permet de prendre en argument un certains nombre d'arguments. L'argument verbose permet un affichage très détaillé

```
# journalctl -o verbose | more
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:30:01
CEST. --
jeu. 2017-10-26 14:25:43.646714 CEST [s=0afd3e0aafe947cf988ca6068653bbc3;i=1;b=0
907056d1de14b3bad3a3cebd7dfa68a;m=cc6b2;t=55c7245623dfa;x=e5415c4dd6e9037e]
    PRIORITY=6
    _TRANSPORT=driver
    MESSAGE=Runtime journal is using 8.0M (max allowed 91.9M, trying to leave 13
7.9M free of 911.3M available → current limit 91.9M).
    MESSAGE_ID=ec387f577b844b8fa948f33cad9a75e6
    _PID=94
    _UID=0
    _GID=0
    _COMM=systemd-journal
    _EXE=/usr/lib/systemd/systemd-journald
    _CMDLINE=/usr/lib/systemd/systemd-journald
...
```

L'option -f permet d'afficher les messages en temps réel (comme l'option -f de grep il afficher les 10 dernières lignes).

```
# journalctl -f
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST. --
oct. 26 15:18:13 newname dbus-daemon[712]: dbus[712]: [system] Activating service
name='org.freedesktop.problems' (using servicehelper)
```

L'option -p permet de filtrer la sortie avec une priorité spécifique

```
# journalctl -p info
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:40:01 CEST. --
oct. 26 14:25:43 centos-uefi systemd-journal[94]: Runtime journal is using 8.0M (max
allowed 91.9M, trying to leave 137.9M free of 911.3M available → current
oct. 26 14:25:43 centos-uefi kernel: Initializing cgroup subsys cpuset
...
# journalctl -p err
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:40:01 CEST. --
oct. 26 14:25:45 centos-uefi kernel: sd 2:0:1:0: [sdb] Incomplete mode parameter data
oct. 26 14:25:45 centos-uefi kernel: sd 2:0:1:0: [sdb] Assuming drive cache: write
through
```

Filter en fonction de la date du message

```
# journalctl --since="2017-10-26 14:25:00"
```

```
# journalctl --until="2017-10-26 14:26:00"
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:50:01 CEST. --
oct. 26 14:25:43 centos-uefi systemd-journal[94]: Runtime journal is using 8.0M (max
allowed 91.9M, trying to leave 137.9M free of 911.3M a
oct. 26 14:25:43 centos-uefi kernel: Initializing cgroup subsys cpuset
# journalctl -p err --since="2017-10-26 14:30:00" -n 2
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 15:50:01 CEST. --
oct. 26 14:46:59 newname gnome-session-binary[1734]: GLib-GObject-CRITICAL:
g_object_unref: assertion 'G_IS_OBJECT (object)' failed
oct. 26 14:46:59 newname gnome-session-binary[1734]: GLib-GObject-CRITICAL:
g_object_unref: assertion 'G_IS_OBJECT (object)' failed
```

Il existe des options avancées de filtrage. En apuyant 2 fois sur TAB après la commande journalctl les valeurs sur lesquels vous pouvez filtrer s'affichent.

```
# journalctl TAB TAB
_AUDIT_LOGINUID=              ERRNO=                        _PID=
_SYSTEMD_SESSION=
_AUDIT_SESSION=               _EXE=                         PRIORITY=
_SYSTEMD_UNIT=
_BOOT_ID=                     _GID=                         __REALTIME_TIMESTAMP=
_TRANSPORT=
_CMDLINE=                     _HOSTNAME=                    _SELINUX_CONTEXT=
_UDEV_DEVLINK=
CODE_FILE=                    _KERNEL_DEVICE=               _SOURCE_REALTIME_TIMESTAMP=
_UDEV_DEVNODE=
CODE_FUNC=                    _KERNEL_SUBSYSTEM=            SYSLOG_FACILITY=
_UDEV_SYSNAME=
CODE_LINE=                    _MACHINE_ID=                  SYSLOG_IDENTIFIER=
_UID=
_COMM=                        MESSAGE=                      SYSLOG_PID=
COREDUMP_EXE=                 MESSAGE_ID=                   _SYSTEMD_CGROUP=
__CURSOR=                     __MONOTONIC_TIMESTAMP=        _SYSTEMD_OWNER_UID=
```

Filtrer par rapport à un PID

```
# journalctl _UID=1000 -n 3
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 16:01:01 CEST. --
oct. 26 14:52:01 newname gnome-software-service.desktop[2650]: 12:52:01:0813 Gs  no app
for changed alternate-tab@gnome-shell-extensions.g
oct. 26 14:52:01 newname gnome-software-service.desktop[2650]: 12:52:01:0818 Gs  no app
for changed apps-menu@gnome-shell-extensions.gcamp
oct. 26 14:52:01 newname gnome-software-service.desktop[2650]: 12:52:01:0821 Gs  no app
for changed window-list@gnome-shell-extensions.gca
```

Filtrer par rapport à une unité systemd.

```
# journalctl _SYSTEMD_UNIT=crond.service
-- Logs begin at jeu. 2017-10-26 14:25:43 CEST, end at jeu. 2017-10-26 16:01:01 CEST. --
oct. 26 14:26:11 newname crond[1324]: (CRON) INFO (RANDOM_DELAY will be scaled with
factor 90% if used.)
oct. 26 14:26:12 newname crond[1324]: (CRON) INFO (running with inotify support)
```

Notes

La gestion des processus

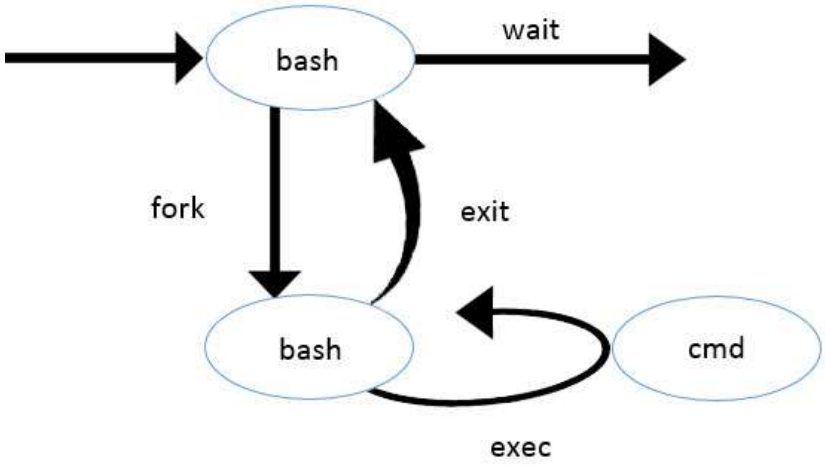
Dans ce chapitre nous allons traiter le mécanisme de fonctionnement et de gestion des processus ainsi que du traitement différé de commandes.

Table des matières

La gestion des processus

Définition

- PID PPID UID
- Multitâche
- Scheduler



- Appels systèmes fork() exec() wait() exit()

Définition

Un processus est toute tâche exécutée par le système d'exploitation.
Un **thread** est un traitement spécifique au sein d'un processus.

Attributs des processus

Il existe plusieurs attributs pour identifier un processus :

PID	:	c'est un numéro unique permettant d'identifier le processus.
PPID	:	c'est le numéro du processus parent.
UID	:	c'est le numéro correspondant au propriétaire du processus.

Multitâche

On parle d'un système d'exploitation multitâche lorsque celui-ci peut exécuter plusieurs programmes de façon simultané.
C'est un partage équitable du temps unité centrale entre les différents processus, appelé «**time sharing**».

Scheduler

Le «**scheduler**» est un processus du noyau. Il permet de distribuer du temps CPU aux processus actifs du système d'exploitation.
Si un processus est inactif, le «**scheduler**» est averti et passe ce processus en état «**dormant**».

Appels systèmes

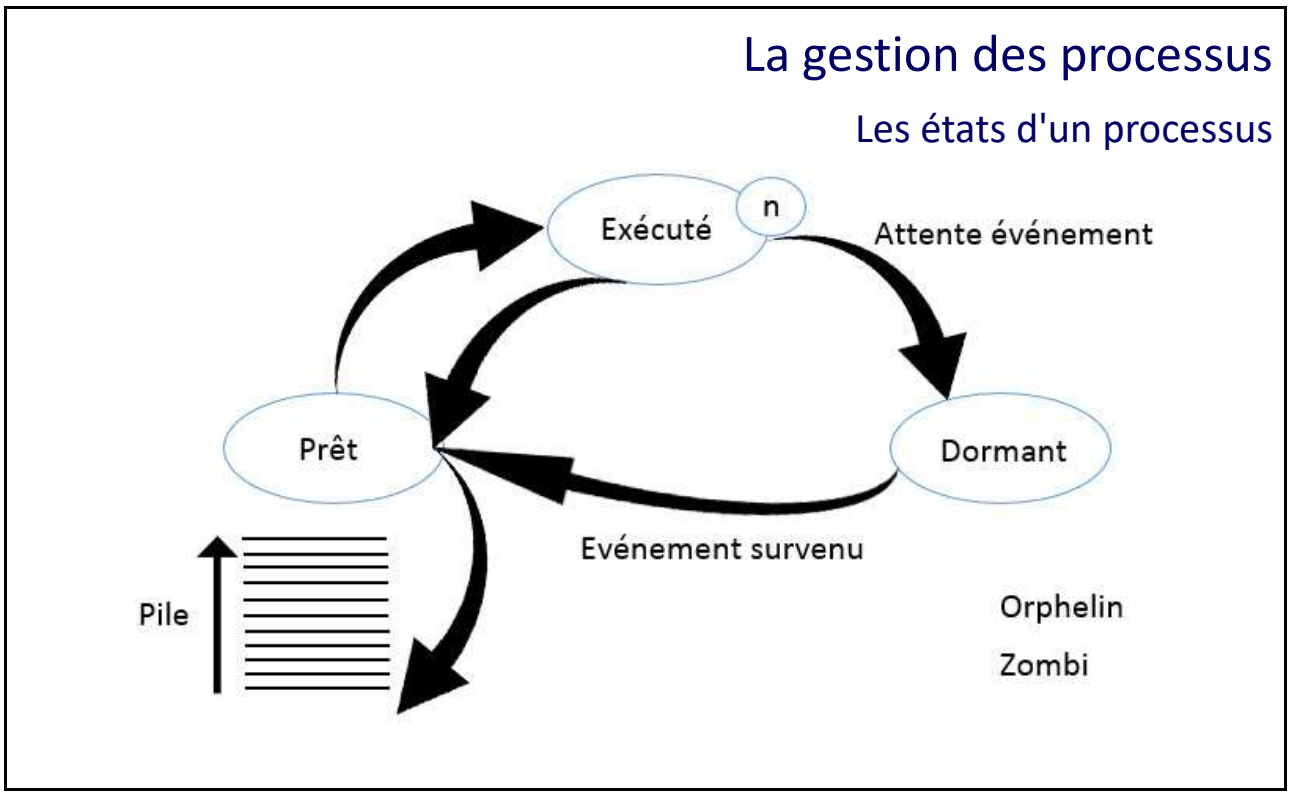
La gestion des processus est réalisée par le noyau via les appels systèmes :

- «**fork()**» : sert à créer un processus fils, identique au père, pour l'exécution et le traitement spécifique du processus dans son propre environnement. Le code de retour de cet appel système est exploité par le processus père à la fin (la mort) du processus fils.

- «**exec()**» : sert à récupérer le code du processus et à l'exécuter.

- «**wait()**» : sert au processus père à attendre la fin du processus fils.

- «**exit()**» : sert à terminer le processus (libère les ressources, le **PID** de la table des processus, etc), renvoie le code de retour du processus fils au processus père, et permet ainsi le déblocage de l'appel système **wait** du processus père.



Les états d'un processus

Les différents états d'un processus

- «**exécuté**» : le processus est en train de s'exécuter sur un cœur d'un processeur.
- «**prêt**» ou «**runnable**» : le processus est dans une pile, en attente d'exécution sur un cœur d'un processeur.
- «**dormant**» ou «**sleeping**» ou «**not runnable**» : le processus est hors de la pile «**runnable**» car il est en attente d'un événement.
- «**orphelin**» : le processus a son processus père qui est «**mort**». Il ne peut donc pas lui retourner son code de retour lors de sa propre fin d'exécution. Ainsi pour cette situation qui reste exceptionnelle, le processus est automatiquement rattaché au processus père de pid 1 (init).
- «**zombi**» : le processus est «**mort**» mais le processus père n'en a pas été informé. Le problème d'un tel état de processus est, en autres, que le numéro de **PID** n'a pas été libéré.

La gestion des processus

Les commandes «ps» et «pgrep»

- Commande «ps»
  - Options : -l -ef -aux
- Commande «pgrep»
  - Options : -t -u -l

Les commandes «ps» et «pgrep»

La commande «ps»

Cette commande permet d'afficher tout les processus en cours d'exécution.

Les options de «**ps**» :

-l : permet un affichage long et détaillé des processus.
-e : permet d'afficher tout les processus.
-f : permet d'afficher toutes les informations disponibles.
-aux : -a : liste l'ensemble des processus.
-u : affiche l'utilisateur du processus.
-x : affiche les processus sans terminal.

Exemples :

```
$ ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 13:26 ?        00:00:01 /usr/lib/systemd/systemd --switc
root         2     0  0 13:26 ?        00:00:00 [kthreadd]
root       688     1  0 13:27 ?        00:00:00 /usr/sbin/crond -n
root       689     1  0 13:27 ?        00:00:00 /usr/sbin/atd -f
user1     2892  2621  2 13:29 ?        00:00:21 /usr/bin/gnome-shell
root      2897     1  0 13:29 ?        00:00:00 /usr/sbin/cupsd -f
user1     3294  3277  0 13:30 pts/0    00:00:00 /bin/bash
user1     3605  3362  0 13:45 pts/1    00:00:00 ps -ef
```

```
$  ps  -aux
USER     PID %CPU  %MEM     VSZ      RSS   TTY   STAT  START  TIME     COMMAND
root       1  0.1   0.4    53668     7596   ?      Ss   13:26  0:01     *
                  */usr/lib/systemd/systemd--switched-root --system --deserialize 24
root       2  0.0   0.0        0        0   ?      S    13:26  0:00     [kthreadd]
root     688  0.0   0.0   126292     1700   ?      Ss   13:27  0:00     /usr/sbin/crond -n
root     689  0.0   0.0    25928      968   ?      Ss   13:27  0:00     /usr/sbin/atd -f
user1   2892  1.8  11.7  1560600   222400   ?      Sl   13:29  0:21     /usr/bin/gnome-shell
root    2897  0.0   0.2   178032     3864   ?      Ss   13:29  0:00     /usr/sbin/cupsd -f
user1   3294  0.0   0.1   116264     2876  pts/0   Ss+  13:30  0:00     /bin/bash
user1   3631  0.0   0.0   125440     1420  pts/1   R+   13:48  0:00     ps -aux
```

La commande «pgrep»

Cette commande permet de rechercher les processus en cours d'exécution selon un critère de recherche.

Les options de «**pgrep**» :

-t : permet de sélectionner les processus dont le terminal est listé.
-u : permet de sélectionner les processus dont l'**UID** est listé.
-l : permet de lister le nom du processus avec son identifiant.
-x : permet de sélectionner les processus exact au nom du motif.

Exemples :

```
$ pgrep    -l    bash
3892 bash
3946 bash
7836 bash

$ pgrep    -l    -t pts/1   bash
3946 bash

$ pgrep    -l    -u user1   bash
3892 bash
3946 bash
$ pgrep    -l    -u root    bash
7836 bash

$ pgrep    -l    -x    bash
3892 bash
3946 bash
7836 bash
$ pgrep    -l    -x    ba
$
```

La gestion des processus

Les commandes «kill» et «pkill»

- kill PID_du_programme
- Les signaux
  kill -15 PID_du_programme
  kill -9 PID_du_programme
- Commande «pkill»
  pkill nom_du_programme
  pkill -9 -x mail

Les commandes «kill» et «pkill»

Cette commande permet de communiquer avec un processus. Il faut être le propriétaire du processus pour communiquer avec, ou être 'root'.
Par défaut cela permet de tuer un ou plusieurs processus actifs. Il est nécessaire de connaître le **PID** du processus pour pouvoir le terminer avec cette commande.

Syntaxe : kill pid1
kill pid1 pid2 pid3

Les signaux

Un signal correspond à l'action à entreprendre sur un processus.
La commande «**kill -l**» permet de lister les signaux.
Pour avoir accès au manuel des signaux, il faut utiliser la commande «**man -s7 signal**».

Exemple :

```
$ kill -l
1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL      10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
Etc…
```

Exemple :

```
$ man -s7 signal

SIGNAL(7)                Manuel du programmeur Linux                SIGNAL(7)
…
  Signal      Valeur      Action      Commentaire
──────────────────────────────────────────────────────────────────────
 SIGHUP       1           Term        Déconnexion détectée sur le terminal
                                      de contrôle ou mort du processus de
                                      contrôle.
 SIGINT       2           Term        Interruption depuis le clavier.
 SIGQUIT      3           Core        Demande « Quitter » depuis le clavier.
 SIGILL       4           Core        Instruction illégale.
 SIGABRT      6           Core        Signal d'arrêt depuis abort(3).
 SIGFPE       8           Core        Erreur mathématique virgule flottante.
 SIGKILL      9           Term        Signal « KILL ».
 SIGSEGV      11           Core       Référence mémoire invalide.
 SIGPIPE      13          Term        Écriture dans un tube sans lecteur.
 SIGALRM      14          Term        Temporisation alarm(2) écoulée.
 SIGTERM      15          Term        Signal de fin.
 SIGUSR1      30,10,16    Term        Signal utilisateur 1.
 SIGUSR2      31,12,17    Term        Signal utilisateur 2.
 SIGCHLD      20,17,18    Ign         Fils arrêté ou terminé.
 SIGCONT      19,18,25    Cont        Continuer si arrêté.
 SIGSTOP      17,19,23    Stop        Arrêt du processus.
 SIGTSTP      18,20,24    Stop        Stop invoqué depuis le terminal.
 SIGTTIN      21,21,26    Stop        Lecture sur le terminal en arrière-plan.
 SIGTTOU      22,22,27    Stop        Écriture dans le terminal en arrière-plan.
Etc…
```

Les signaux les plus couramment utilisés sont :

Le signal **TERM** (15) est un signal de terminaison classique. Il peut être ignoré par le processus.

Syntaxe : kill -15 PID_du_programme

Le signal **KILL** (9) qui correspond à l'arrêt immédiat du processus. Utilisé lorsque le signal **TERM** échoue.

Syntaxe : kill -9 PID_du_programme

La commande «pkill»

Cette commande a le même effet que «**kill**», mais simplifiée car il n'exige pas de connaître le **PID** du processus. La plupart des options de «**pgrep**» sont également disponible pour cette commande.

Syntaxe : pkill nom_du_programme
pkill -Signal nom_du_programme

Exemples : pkill mail

Dans l'exemple ci -dessus, «**pkill**» envoie le signal 15 à tous les processus qui contiennent «**mail**» dans leur nom.

```
pkill -9 -x mail
```

Dans l'exemple ci-dessus, «**pkill**» envoie le signal 9 à tous les processus qui s'appellent exactement «**mail**».

La gestion des processus

Les commandes pstree, uptime et top

- pstree
- top
- uptime

Les commandes pstree, uptime et top

La commande «pstree»

Permet d'afficher l'arborescence des processus. Cette commande est pratique pour connaître de quel processus dépend un **PID**.

Exemple :

```
$ pstree
systemd─┬─ModemManager───2*[{ModemManager}]
        ├─NetworkManager─┬─dhclient
        │                └─3*[{NetworkManager}]
        ├─2*[abrt-watch-log]
        ├─abrtd
        ├─accounts-daemon───2*[{accounts-daemon}]
        ├─alsactl
        ├─at-spi-bus-laun─┬─dbus-daemon───{dbus-daemon}
        │                 └─3*[{at-spi-bus-laun}]
...etc
```

La commande «top»

Permet d'afficher les processus sur une page. Par défaut, ils sont triés dans l'ordre décroissant du taux d'utilisation CPU. L'affichage se rafraîchi régulièrement.

Quelques options :

-q : permet de quitter la commande «**top**».
-h : affiche l'aide.
-f : ajoute ou supprime des colonnes.
-u : filtre en fonction de l'utilisateur.
-k : tue un processus.
-s : change l'intervalle de temps de rafraîchissement de la liste (3 secondes par défaut).

Exemple :

```
$ top
top - 15:19:43 up  6:11,  3 users,  load average: 0,00, 0,01, 0,05
Tasks: 154 total,   3 running, 151 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,0 us,  0,0 sy,  0,0 ni,100,0 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
KiB Mem:   1885264 total,  1778880 used,   106384 free,      148 buffers
KiB Swap:  2113532 total,        0 used,  2113532 free.  1175304 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
    1 root      20   0   53672   7616   2520 S  0,0  0,4   0:01.60 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.01 kthreadd
    3 root      20   0       0      0      0 S  0,0  0,0   0:00.20 ksoftirqd/0
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/u2:0
    7 root      rt   0       0      0      0 S  0,0  0,0   0:00.00 migration/0
    8 root      20   0       0      0      0 S  0,0  0,0   0:00.00 rcu_bh
```

La commande «uptime»

Permet d'indiquer des informations sur le système, l'heure actuelle, depuis combien de temps le système est en marche, le nombre d'utilisateurs connectés et la charge du système.
La charge du système (load average) nous informe sur le nombre de processus en attente de ressources pour les 1, 5 et 15 dernière minutes.

```
$ uptime
11:11:17 up       1:32,      3 users,      load average:   0,00,    0,01,    0,05
```

La commande «time»

Permet de mesurer le temps d'exécution d'une commande. Trois résultats sont affichés :

real : affiche le temps total.
user : affiche le temps nécessaire au processeur pour exécuter les directives du programme.
sys : affiche le temps nécessaire au processeur pour traiter les directives du système.

```
$ time     sleep 5
real        0m5.004s
user        0m0.001s
sys         0m0.002s
```

Les processus

Présentation du «&» et du «;»

- & Arrière plan

  cp vidéo1 copie_vidéo1 **&**

- ; Exécution séquentielle

  cp video1 videoA **;** cp video2 videoB **;** cp son sonA

Présentation du «&» et du «;»

Arrière plan

Pour des raisons pratiques, il est possible de lancer des processus en arrière plan. Pour cela nous utiliserons le symbole «**&**» (et commercial).

Dans l'exemple ci-dessous, je souhaite lancer une copie d'un fichier (une vidéo) en arrière plan.

```
$ cp vidéo1 copie_vidéo1 &
[1] 16504
```

Nous pouvons voir l'apparition d'une ligne d'informations.
Le **[1]** nous indique que c'est le premier processus que nous envoyons en arrière plan (numéro de jobs). Le nombre **16504** est le **PID** de ce processus.

Exécution séquentielle

Le caractère «**;**» réalise des exécutions séquentielles de commandes.

```
$ cp video1 videoA ; cp video2 videoB ; cp son sonA
```

Dans l'exemple ci-dessus, une seule ligne de commande nous permet de copier plusieurs fichiers.

Les processus

Les jobs

- Commande «fg»
- Commande «bg»
- Le «Ctrl + Z»
- Le «Ctrl + C»

Les jobs

La commande «**jobs**» permet de connaître les processus qui sont exécutés en arrière plan.

```
$ jobs
[1]+      Fini            cp   fic1   copiefic1
```

Dans l'exemple ci-dessus, «**jobs**» nous indique que le fichier à été copié et nous informe sur la ligne de commande entrée pour cette copie.

```
$ sleep 1001&
[1] 3418
$ sleep 1002&
[2] 3419
$ sleep 1003&
[3] 3420

$ jobs
[1]   En cours d'exécution   sleep 1001 &
[2]-  En cours d'exécution   sleep 1002 &
[3]+  En cours d'exécution   sleep 1003 &
```

Tous ces jobs sont en cours d'exécution. Le caractère «**+**» indique le dernier processus lancé, et le caractère «**-**» l'avant dernier.

La commande «fg»

Permet de passer le processus en premier plan.
Si vous avez lancé une commande en arrière plan et que vous voulez la passer en premier plan, vous devrez utiliser la commande «**fg**» suivi du numéro du **jobs** à traiter.

```
$ sleep 1001&
[1] 3813

$ jobs
[1]+  En cours d'exécution   sleep 1001 &

$ fg %1
sleep 1001
```

Dans l'exemple ci-dessus, nous n'avons plus le prompt car la commande 'sleep', le job 1, est passée en premier plan.

La commande «bg»

Permet de passer le processus en arrière plan.
Si vous avez lancé une commande en premier plan et que vous voulez la passer en arrière plan, vous devrez la mettre en pause et récupérer l'invite de commande grâce à «**Ctrl + z**».
Puis exécuter «**bg**» pour que le processus soit relancée en arrière plan.

```
$ jobs                                      liste les jobs.
[1]+  En cours d'exécution   sleep 1001 &

$ fg  %1                                    bascule le job 1 en premier plan.
Sleep 1001
^z                                          freeze la commande en premier plan.
[1]+  Stoppé                 sleep 1001

$                                           on a «repris la main» sur le prompt.

$ jobs
[1]+  Stoppé                 sleep 1001

$ bg  %1                                    bascule le job 1 en arrière plan.
[1]+ sleep 1001 &

$ jobs
[1]+  En cours d'exécution   sleep 1001 &
```

Le «Ctrl + Z»

Matérialisé dans le terminal avec les caractères «**^Z**».
Cette commande permet de mettre en pause l'exécution du programme qui est en premier plan et de le basculer en arrière plan.
Cette commande est utile lorsque l'on veut passer un programme de premier plan en arrière plan.

```
$ programme
^Z
[1]+   Stoppé        programme
$
```

Après le «**Ctrl + Z**», nous avons récupéré le prompt car le programme est suspendu en arrière plan.

Le «Ctrl + C»

Matérialisé dans le terminal avec les caractère «**^C**».
Cette commande permet d'arrêter le programme en cours d'exécution en premier plan.

```
$ programme
^C
$
```

Après le «**Ctrl + C**», nous avons récupéré le prompt car le programme ne fonctionne plus.

Gestion des comptes utilisateurs

L'exécution ponctuelle en différée : la commande at

- Exécution d'un tâche ponctuelle
- Les commandes at, atq, atrm
- La sécurité de at

L'exécution ponctuelle en différée : la commande at

La commande 'at' permet d'exécuter une commande de manière ponctuelle à un moment différé. Elle est usuellement suivie de l'heure à laquelle la tâche doit être programmée. Si l'heure est passée vous programmez la tâche pour le lendemain. Il est possible de spécifier une date en plus de l'heure.

```
[user1@formateur ~]$ at 18:30
at> echo bonsoir > /dev/pts/1
at> <EOT>
job 4 at Wed Oct 28 18:30:00 2015
```

```
[user1@formateur ~]$ at teatime
at> echo bonjour > /dev/pts/1
at> <EOT>
job 5 at Thu Oct 29 16:00:00 2015
```

```
[user1@formateur ~]$ at now +5days
at> echo coucou
at> <EOT>
job 6 at Mon Nov  2 16:08:00 2015
```

```
[user1@formateur ~]$ at 5am tomorrow
at> echo hello
at> <EOT>
job 7 at Thu Oct 29 05:00:00 2015
```

```
[user1@formateur ~]$ at 16:30 122415
at> echo joyeux noel
at> <EOT>
job 8 at Thu Dec 24 16:30:00 2015
```

La commande 'atq' ou 'at -l' permet de lister les tâches 'at' en attente d'exécution.

```
[user1@formateur ~]$ atq
6       Mon Nov  2 16:08:00 2015 a user1
4       Wed Oct 28 18:30:00 2015 a user1
5       Thu Oct 29 16:00:00 2015 a user1
8       Thu Dec 24 16:30:00 2015 a user1
7       Thu Oct 29 05:00:00 2015 a user1
```

```
[user1@formateur ~]$ at -l
6       Mon Nov  2 16:08:00 2015 a user1
4       Wed Oct 28 18:30:00 2015 a user1
5       Thu Oct 29 16:00:00 2015 a user1
8       Thu Dec 24 16:30:00 2015 a user1
7       Thu Oct 29 05:00:00 2015 a user1
```

La commande 'atrm' ou 'at -d' permet de supprimer une tâche.

```
[user1@formateur ~]$ atrm 4
[user1@formateur ~]$ atrm 6
[user1@formateur ~]$ atq
5       Thu Oct 29 16:00:00 2015 a user1
8       Thu Dec 24 16:30:00 2015 a user1
7       Thu Oct 29 05:00:00 2015 a user1
```

Les tâches 'at' en attente d'exécution sont stockées dans le répertoire /var/spool/at.

```
# ls /var/spool/at
a00003016fbffc  a00005016fc524  a00007016fc290  a0000801710042  spool
```

```
# more /var/spool/at/a00003016fbffc
#!/bin/sh
# atrun uid=1000 gid=300
# mail theo 0
umask 22
XDG_SESSION_ID=22; export XDG_SESSION_ID
HOSTNAME=formateur; export HOSTNAME
SHELL=/bin/bash; export SHELL
HISTSIZE=1000; export HISTSIZE
QTDIR=/usr/lib64/qt-3.3; export QTDIR
QTINC=/usr/lib64/qt-3.3/include; export QTINC
QT_GRAPHICSSYSTEM_CHECKED=1; export QT_GRAPHICSSYSTEM_CHECKED
USER=theo; export USER
LS_COLORS=rs=0:di=01\;34:ln=01\;36:mh=00:pi=40\;33:so=01\;35:do=01\;35:bd=40\;33\;01:cd=4
...
SHLVL=1; export SHLVL
HOME=/home/theo; export HOME
LOGNAME=theo; export LOGNAME
QTLIB=/usr/lib64/qt-3.3/lib; export QTLIB
LESSOPEN=\|\|/usr/bin/lesspipe.sh\ %s; export LESSOPEN
XDG_RUNTIME_DIR=/run/user/1000; export XDG_RUNTIME_DIR
QT_PLUGIN_PATH=/usr/lib64/kde4/plugins:/usr/lib/kde4/plugins; export QT_PLUGIN_PATH
cd /home/theo || {
         echo 'Execution directory inaccessible' >&2
         exit 1
}
${SHELL:-/bin/sh} << 'marcinDELIMITER75e8e479'
echo bonjour > /dev/pts/1

marcinDELIMITER75e8e479
```

Par défaut, tous les utilisateurs ont le droit d'utiliser la commande 'at' à l'exception de ceux qui sont listés dans le fichier /etc/at.deny (vide par défaut).

```
# more /etc/at.deny
user3
user1
```

```
[user3@formateur ~]$ at 15:30
You do not have permission to use at.
```

Vous pouvez modifier le comportement de la sécurité en créant le fichier /etc/at.allow. Dans ce cas, seuls les utilisateurs listés dans le fichier auront le droit d'utiliser la commande at.

```
# more /etc/at.allow
user3
```

```
[user3@formateur ~]$ at 13:40
at> echo coucou
at> <EOT>
job 9 at Thu Oct 29 13:40:00 2015
```

```
[user5@formateur ~]$ at 15:20
You do not have permission to use at.
```

Il n'y a que root qui a le droit d'utiliser la commande at si aucun des deux fichiers n'existent (at.deny et at.allow).

Gestion des comptes utilisateurs

L'exécution récurrente en différée: la crontab

- Exécution d'un tâche récurrente
- Le format d'un fichier crontab
- La commande crontab et ses options
- La sécurité de crontab

L'exécution récurrente en différée : la crontab

Une crontab permet d'exécuter des tâches de manière récurrente. Chaque utilisateur peut posséder une crontab.

Chaque fichier crontab possède 5 champs pour définir à quel moment la tâche doit être lancée.

Exemple d'un fichier crontab

```
[theo@formateur ~]$ crontab -l
20 10 * * * /scripts/script1.bash
10 00 1 * * /scripts/script_sauve.bash
*/10 * * * 0 /scripts/script2.bash
20,40 10,20 * * * /scripts/script3.bash
15,45 14-16 * * 1-5 /scripts/script4.bash
```

Le premier champ représente le champ **minutes**. Il peut prendre les valeurs de **0 à 59.**
Le deuxième champ représente le champ **heures**. Il peut prendre les valeurs de **0 à 23**.
Le troisième champ représente le champ **jour du mois**. Il peut prendre les valeurs **1 à 31.**
Le quatrième champ représente le champ **mois**. Il peut prendre les valeurs **1 à 12.**
Le cinquième champ représente le champ **jour de la semaine**. Il peut prendre les valeurs **0 à 7.** 0 étant le dimanche, 1 le lundi, …

script1.bash est exécuté tous les jours à 10h20
script_sauve.bash est exécuté tous les 1er du mois à 00h10
script2.bash est exécuté toutes les 10 minutes tous les dimanches.
script3.bash est exécuté tous les jours à 10h20, 10h40, 20h20, 20h40
script4.bash est exécuté tous les lundi à vendredi à 14h15,14h45,15h15,15h45,16h15,16h45

Pour éditer sa crontab, il faut exécuter 'crontab -e'. La crontab est éditée avec l'utilitaire 'vi' par défaut.
Pour paramétrer un autre utilitaire, il faut configurer la variable EDITOR.

```
[theo@formateur ~]$ export EDITOR=/usr/bin/nano
```

En tant que root vous pouvez éditer, modifier, ou supprimer les crontabs des utilisateurs.

```
# crontab -l -u theo
20 10 * * * /scripts/script1.bash
10 00 1 * * /scripts/script_sauve.bash
*/10 * * * 0 /scripts/script2.bash
20,40 10,20 * * * /scripts/script3.bash
15,45 14-16 * * 1-5 /scripts/script4.bash
```

Sauvegarde de la crontab de theo dans le fichier /tmp/crontab.txt :

```
# crontab -l -u theo > /tmp/crontab.txt
# more /tmp/crontab.txt
20 10 * * * /scripts/script1.bash
10 00 1 * * /scripts/script_sauve.bash
*/10 * * * 0 /scripts/script2.bash
20,40 10,20 * * * /scripts/script3.bash
15,45 14-16 * * 1-5 /scripts/script4.bash
```

Suppression d'une crontab :

```
# crontab -r -u theo
# crontab -l -u theo
no crontab for theo
```

Restauration d'une crontab :

```
# crontab -u theo /tmp/crontab.txt
# crontab -l -u theo
20 10 * * * /scripts/script1.bash
10 00 1 * * /scripts/script_sauve.bash
*/10 * * * 0 /scripts/script2.bash
20,40 10,20 * * * /scripts/script3.bash
15,45 14-16 * * 1-5 /scripts/script4.bash
```

```
# crontab -u user5 /tmp/crontab.txt
# crontab -l -u user5
20 10 * * * /scripts/script1.bash
10 00 1 * * /scripts/script_sauve.bash
*/10 * * * 0 /scripts/script2.bash
20,40 10,20 * * * /scripts/script3.bash
15,45 14-16 * * 1-5 /scripts/script4.bash
```

Les crontabs sont stockées dans le répertoire /var/spool/cron. Un fichier portant le nom de l'utilisateur possédant une crontab est présent.

```
# ls /var/spool/cron
theo  user5
```

```
# more /var/spool/cron/user5
20 10 * * * /scripts/script1.bash
10 00 1 * * /scripts/script_sauve.bash
*/10 * * * 0 /scripts/script2.bash
20,40 10,20 * * * /scripts/script3.bash
15,45 14-18 * * 1-5 /scripts/script4.bash
```

Tous les utilisateurs ont le droit d'utiliser la crontab à l'exception de ceux spécifiés dans /etc/cron.deny (vide par défaut).

```
# more /etc/cron.deny
user1
user2
user3
```

```
[user3@formateur ~]$ crontab -e
You (user3) are not allowed to use this program (crontab)
See crontab(1) for more information
```

Le comportement peut être inversé en créant le fichier /etc/cron.allow. Alors, il n'y aura que les utilisateurs présents dans ce fichier qui pourront utiliser la commande crontab.

```
# more /etc/cron.allow
user2
user3
```

```
[user3@formateur ~]$ crontab -l
*/5 * * * * echo bonjour
```

```
[user1@formateur ~]$ crontab -l
You (user1) are not allowed to use this program (crontab)
See crontab(1) for more information
```

Si aucun des deux fichiers existe (/etc/cron.deny et /etc/cron.allow), seul root peut utiliser la commande crontab.

Le système possède une crontab qui est /etc/crontab. Il est actuellement vide. A l'origine, il était utilisé pour exécuter les commandes situés dans les répertoires /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly, /etc/cron.monthly et /etc/cron.yearly (n'existent plus).

C'est 'anacron' qui exécute le contenu de certains de ces répertoires comme on peut le constater dans le fichier /etc/anacrontab.

Notes

Surveillance système

Dans ce chapitre, nous allons étudier les commandes et utilitaires permettant l'analyse des performances et la gestion des logs d'un serveur Linux.

Table des matières

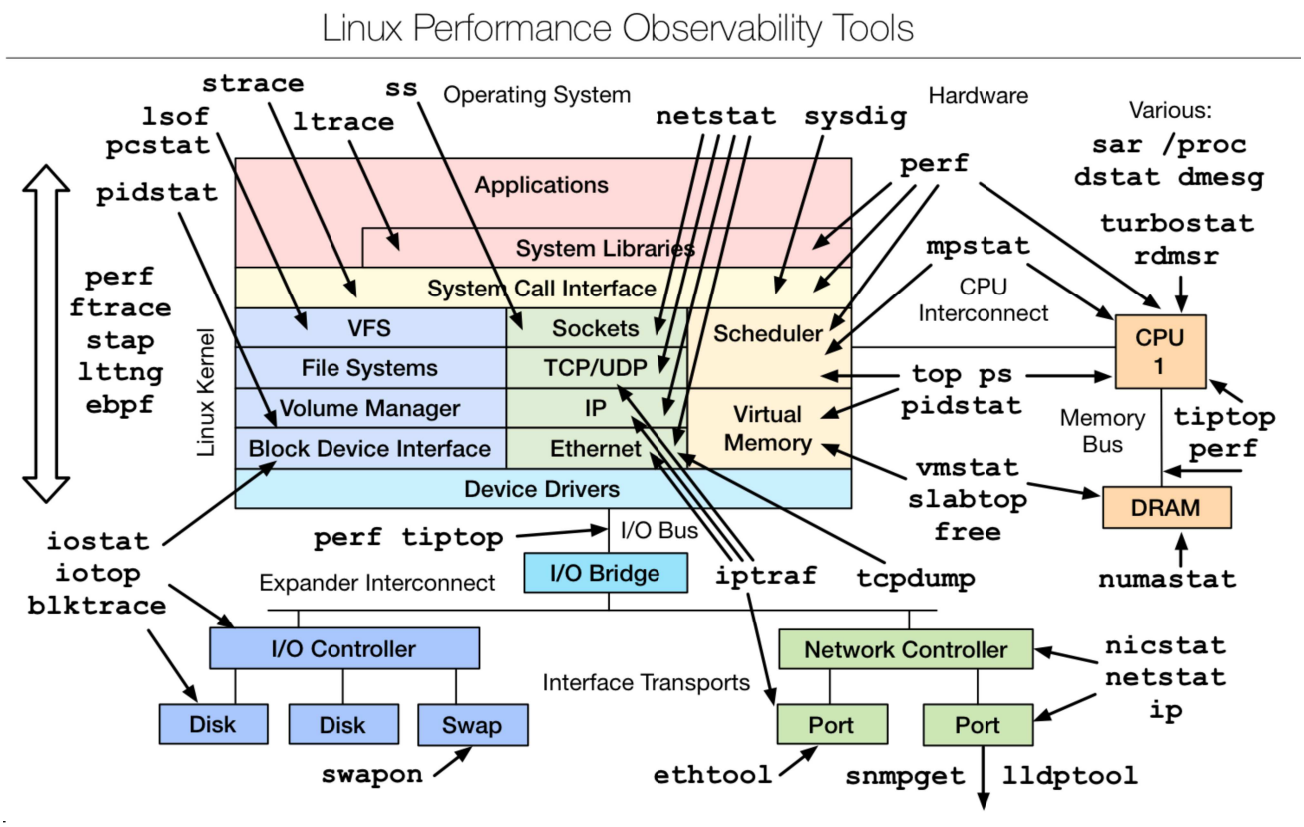
Surveillance système

La surveillance des sous-système: ram, cpu, io, reseau

- La mémoire vive
- Le processeur
- Les disques durs
- Les interfaces réseaux.

La surveillance des sous-systèmes : ram, cpu, io, réseau

Les 4 sous-systèmes à surveiller sont la RAM, la CPU, le réseau et les entrées/sorties disques. Pour chaque sous système à surveiller des commandes spécifiques existent. RedHat recommande d'utiliser sar (system activity report) pour la surveillance des performances.
Source de l'image :http://www.brendangregg.com/Perf/linux_observability_tools.png



Surveillance système

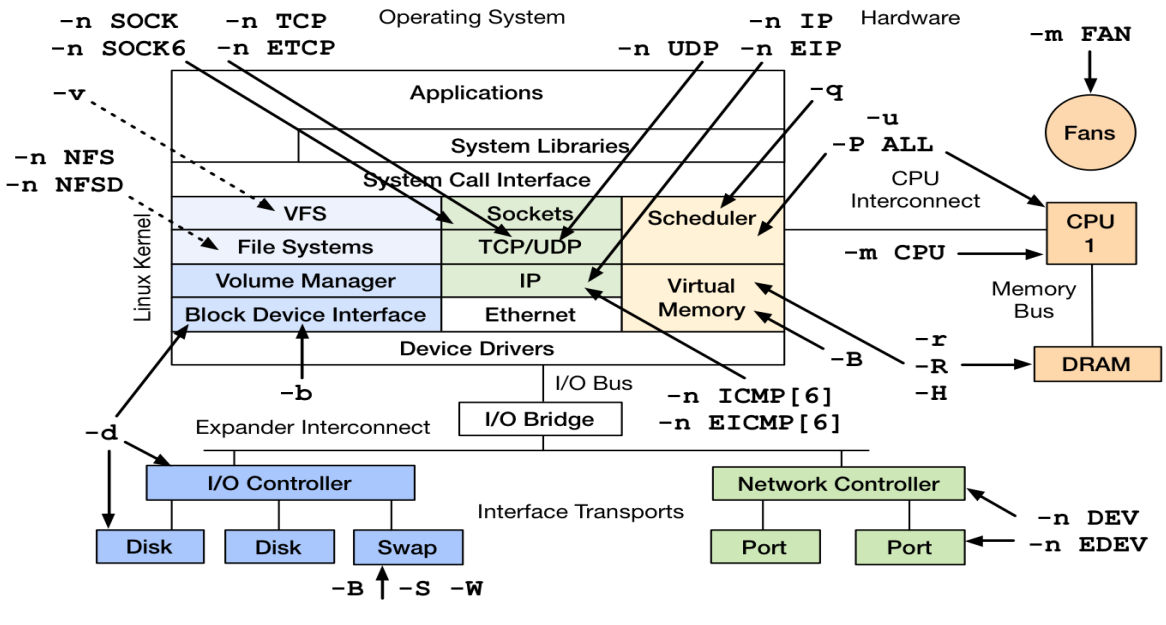
La commande sar

- /etc/cron.d/sysstat
- sar -r sar -W sar -b sar -d
- sar 1 10

La commande sar

La commande sar (system activity report) permet de récupérer des informations sur l'activité système. La commande appartient au package sysstat.

Linux Performance Observability: sar



Source de l'image: http://www.brendangregg.com/Perf/linux_observability_sar.png

La crontab de systat (le fichier /etc/cron.d/sysstat) contient les lignes pour effectuer une collecte d'informations toutes les 10 minutes.

De plus, un rapport journalier est généré tous les jours à 23h53. Si vous désirez augmenter la fréquence de collecte, modifier le fichier ci-dessous :

```
# more /etc/cron.d/sysstat
# Run system activity accounting tool every 10 minutes
*/10 * * * * root /usr/lib64/sa/sa1 1 1
# 0 * * * * root /usr/lib64/sa/sa1 600 6 &
# Generate a daily summary of process accounting at 23:53
53 23 * * * root /usr/lib64/sa/sa2 -A
```

Pour démarrer la collecte, il faut démarrer le service sysstat :

```
# service sysstat start
Calling the system activity data collector (sadc)...
```

Résultat de la commande sar sans options :

```
# sar
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

09:17:48          LINUX RESTART

09:20:02        CPU     %user     %nice   %system   %iowait    %steal     %idle
09:30:01        all      0,84      0,00      0,78      1,07      0,00     97,30
09:40:01        all      0,24      0,00      0,37      0,71      0,00     98,68
09:50:01        all      0,99      0,00      0,86      0,70      0,00     97,46
10:00:01        all      0,48      0,00      0,54      0,55      0,00     98,42
10:10:01        all      1,99      0,00      1,02      0,65      0,00     96,34
10:20:01        all      3,60      0,00      1,02      2,45      0,00     92,93
Moyenne :       all      1,35      0,00      0,77      1,02      0,00     96,86

10:29:07          LINUX RESTART

10:30:01        CPU     %user     %nice   %system   %iowait    %steal     %idle
10:40:01        all      1,38      0,00      1,03      2,10      0,00     95,50
Moyenne :       all      1,38      0,00      1,03      2,10      0,00     95,50

10:43:07          LINUX RESTART
```

Pour obtenir les statistiques sur l'utilisation de la mémoire :

```
# sar -r
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

09:17:48          LINUX RESTART

09:20:02    kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit
09:30:01      1709596    420944     19,76     54780    142300    460776     10,45
09:40:01      1705852    424688     19,93     55528    144972    460964     10,46
09:50:01      1700944    429596     20,16     55816    147344    473884     10,75
10:00:01      1681820    448720     21,06     55948    151352    485372     11,01
10:10:01      1683084    447456     21,00     55956    151392    484104     10,98
10:20:01      1427836    702704     32,98     60392    394268    496868     11,27
Moyenne :     1651522    479018     22,48     56403    188605    476995     10,82

10:29:07          LINUX RESTART

10:30:01    kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit
10:40:01      1643324    487216     22,87     27036    237568    451956     10,25
Moyenne :     1643324    487216     22,87     27036    237568    451956     10,25

10:43:07          LINUX RESTART
```

Pour obtenir les statistique sur l'utilisation de la swap :

```
# sar -W
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

09:17:48          LINUX RESTART

09:20:02     pswpin/s pswpout/s
09:30:01         0,00      0,00
09:40:01         0,00      0,00
09:50:01         0,00      0,00
10:00:01         0,00      0,00
10:10:01         0,00      0,00
10:20:01         0,00      0,00
Moyenne :        0,00      0,00

10:29:07          LINUX RESTART

10:30:01     pswpin/s pswpout/s
10:40:01         0,00      0,00
Moyenne :        0,00      0,00

10:43:07          LINUX RESTART
```

Pour obtenir les statistiques sur les I/O disques :

```
# sar -b
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

09:17:48          LINUX RESTART

09:20:02          tps      rtps      wtps   bread/s   bwrtn/s
09:30:01         6,41      4,13      2,28    199,11     24,60
09:40:01         3,29      0,74      2,55     19,74     31,86
09:50:01         2,09      0,62      1,46     14,85     14,80
10:00:01         2,15      0,17      1,98     25,11     19,60
10:10:01         2,14      0,02      2,11      0,21     20,55
10:20:01        58,21     14,09     44,12   1726,10    670,77
Moyenne :       12,35      3,29      9,06    329,80    129,95

10:29:07          LINUX RESTART

10:30:01          tps      rtps      wtps   bread/s   bwrtn/s
10:40:01        16,19     12,45      3,74    852,08     42,19
Moyenne :       16,19     12,45      3,74    852,08     42,19

10:43:07          LINUX RESTART
```

Afficher 5 sorties à une fréquence d'une seconde.

```
# sar -b 1 5
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

11:07:52          tps      rtps      wtps   bread/s   bwrtn/s
11:07:53         0,00      0,00      0,00      0,00      0,00
11:07:54         0,00      0,00      0,00      0,00      0,00
11:07:55         0,00      0,00      0,00      0,00      0,00
11:07:56         0,00      0,00      0,00      0,00      0,00
11:07:57         2,02      0,00      2,02      0,00     16,16
Moyenne :        0,40      0,00      0,40      0,00      3,21
```

Pour visualiser l'activité des buffers

```
# sar -B 1 5
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

11:07:25     pgpgin/s pgpgout/s   fault/s  majflt/s  pgfree/s pgscank/s pgscand/s pgsteal/s    %vmeff
11:07:26         0,00      0,00     35,00      0,00     75,00      0,00      0,00      0,00      0,00
11:07:27         0,00      0,00     38,00      0,00     77,00      0,00      0,00      0,00      0,00
11:07:28         0,00     28,28     31,31      0,00     76,77      0,00      0,00      0,00      0,00
11:07:29         0,00      0,00     31,31      0,00     73,74      0,00      0,00      0,00      0,00
11:07:30         0,00      0,00     31,00      0,00     75,00      0,00      0,00      0,00      0,00
Moyenne :        0,00      5,62     33,33      0,00     75,50      0,00      0,00      0,00      0,00
```

Pour obtenir les informations sur les I/O par disque. Les dernières lignes contiennent la moyenne depuis le dernier boot de la machine :

```
# sar -d
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

09:17:48          LINUX RESTART

09:20:02          DEV       tps  rd_sec/s  wr_sec/s  avgrq-sz  avgqu-sz     await     svctm     %util
09:30:01      dev11-0      0,02      0,07      0,00      4,00      0,00     11,18     11,09      0,02
09:30:01       dev8-0      2,48     99,52     12,30     45,04      0,03     13,75      7,73      1,92
09:30:01      dev8-16      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
```

L'option -p permet de visualiser l'activité au niveau des partitions.

```
# sar -d -p
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

09:17:48          LINUX RESTART

09:20:02          DEV       tps  rd_sec/s  wr_sec/s  avgrq-sz  avgqu-sz     await     svctm     %util
09:30:01          sr0      0,02      0,07      0,00      4,00      0,00     11,18     11,09      0,02
09:30:01          sda      2,48     99,52     12,30     45,04      0,03     13,75      7,73      1,92
09:30:01          sdb      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
```

Pour 2 affichages à une fréquence de 1 seconde.

```
# sar -d -p  1 2
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

10:59:33          DEV       tps  rd_sec/s  wr_sec/s  avgrq-sz  avgqu-sz     await     svctm     %util
10:59:34          sr0      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
10:59:34          sda      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
```

Pour obtenir des informations sur l'activité CPU :

```
# sar -u 1 10
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

11:02:14        CPU     %user     %nice   %system   %iowait    %steal     %idle
11:02:15        all      0,00      0,00      1,00      0,00      0,00     99,00
11:02:16        all      0,00      0,00      1,00      0,00      0,00     99,00
11:02:17        all      0,00      0,00      0,00      8,08      0,00     91,92
11:02:18        all      0,00      0,00      1,00      0,00      0,00     99,00
11:02:19        all      1,00      0,00      0,00      0,00      0,00     99,00
11:02:20        all      0,00      0,00      1,00      0,00      0,00     99,00
11:02:21        all      0,00      0,00      1,01      0,00      0,00     98,99
11:02:22        all      0,00      0,00      1,00      0,00      0,00     99,00
11:02:23        all      0,00      0,00      0,00      0,00      0,00    100,00
11:02:24        all      1,00      0,00      2,00      0,00      0,00     97,00
Moyenne :       all      0,20      0,00      0,80      0,80      0,00     98,19
```

Pour obtenir des informations sur l'activité mémoire :

```
# sar -r 1 10
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

11:02:38    kbmemfree kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit
11:02:39      1641844    488696     22,94     27672    238288    451508     10,24
11:02:40      1641844    488696     22,94     27672    238288    451508     10,24
11:02:41      1641844    488696     22,94     27672    238288    451508     10,24
11:02:42      1641844    488696     22,94     27680    238284    451508     10,24
11:02:43      1641844    488696     22,94     27680    238288    451508     10,24
11:02:44      1641844    488696     22,94     27680    238288    451508     10,24
11:02:45      1641844    488696     22,94     27680    238288    451508     10,24
11:02:46      1641844    488696     22,94     27680    238288    451508     10,24
11:02:47      1641844    488696     22,94     27680    238288    451508     10,24
11:02:48      1641844    488696     22,94     27680    238288    451508     10,24
Moyenne :     1641844    488696     22,94     27678    238288    451508     10,24
```

Pour obtenir des informations sur l'activité réseau :

```
# sar -n DEV 1 5
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_        (1 CPU)

11:05:02        IFACE   rxpck/s   txpck/s    rxkB/s    txkB/s   rxcmp/s   txcmp/s  rxmcst/s
11:05:03           lo      0,00      0,00      0,00      0,00      0,00      0,00      0,00
11:05:03         eth0      1,02      1,02      0,07      0,07      0,00      0,00      0,00
```

Pour afficher toutes les informations :

```
# sar -A
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    23/01/2015      _x86_64_       (1 CPU)

09:17:48          LINUX RESTART

09:20:02        CPU      %usr     %nice      %sys   %iowait    %steal      %irq     %soft    %guest     %idle
09:30:01        all      0,84      0,00      0,70      1,07      0,00      0,07      0,02      0,00     97,30
09:30:01          0      0,84      0,00      0,70      1,07      0,00      0,07      0,02      0,00     97,30

09:30:01        CPU      %usr     %nice      %sys   %iowait    %steal      %irq     %soft    %guest     %idle
09:40:01        all      0,24      0,00      0,31      0,71      0,00      0,04      0,02      0,00     98,68
09:40:01          0      0,24      0,00      0,31      0,71      0,00      0,04      0,02      0,00     98,68
```

L'option -f permet de lire les informations au format sar à partir d'un fichier.

```
# sar -d -f /var/log/sa/sa23
Linux 3.10.0-693.2.2.el7.x86_64 (centos-uefi)   23/10/2017      _x86_64_        (2 CPU)

11:55:05          LINUX RESTART

12:00:02          DEV       tps  rd_sec/s  wr_sec/s  avgrq-sz  avgqu-sz     await     svctm     %util
12:10:01       dev8-32      2,16    130,09     26,62     72,69      0,06     29,14      3,06      0,66
12:10:01       dev8-16      0,00      0,00      0,00      0,00      0,00      0,00      0,00      0,00
```

Surveillance système

La commande vmstat

- vmstat -a
- vmstat 1 10
- vmstat -s

La commande vmstat

La commande vmstat renvoie des informations sur la mémoire, les processus, la pagination, etc..

Elle fait partie du package procps. Il faut installer le package si vous n'avez pas cette commande à disposition.

```
# rpm -qf /usr/bin/vmstat
procps-3.2.8-25.el6.x86_64
```

L'option '-a' de vmstat permet d'avoir des statistiques sur l'utilisation des ressources à l'instant t. Sans option, elle affiche les statistiques depuis le dernier démarrage.

```
# vmstat -a
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu-----
 r  b   swpd   free  inact active   si   so    bi    bo   in   cs us sy id wa st
 0  0      0 1494120 248364 273036    0    0   115    34  165   96 13  1 85  2  0
```

procs	signification
r	le nombre de processus en attente d'exécution
b	le nombre de processus endormis non interruptible

memory	signification
swpd	la quantité de mémoire virtuelle utilisée
free	la quantité de mémoire libre
buff	la quantité de mémoire utilisée par les buffers
cache	la quantité de mémoire utilisée comme cache
inact	la quantité de mémoire inactive (option -a)
active	la quantité de mémoire active (option -a)

swap	signification
si	la quantité de mémoire swappée depuis le disque (unité: octets/s)
so	la quantité de mémoire swappée sur le disque (unité: octets/s)

io	signification
bi	blocks reçus depuis un périphérique en mode bloc (unité: blocks/s)
bo	blocks envoyés à un périphérique en mode bloc (unité: blocks/s)

system	signification
in	le nombre d'interruptions par seconde
cs	le nombre de changement de contexte par seconde

CPU	signification
us	temps d'exécution du code qui n'est pas du code noyau (user time)
sy	temps d'exécution du code noyau (system time)
id	disponibilité du processeur (idle time)
wa	temps d'attente pour les entrées/sorties (wait time)
st	temps "volé" par une machine virtuelle (stolen time)

Afficher la sortie toutes les 2 secondes avec 5 affichages :

```
# vmstat 2 5
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0      0 1485996  36488 354720    0    0    55    17  257  119 23  1 76  1  0
 2  0      0 1485988  36488 354720    0    0     0     0 1011  351 100  1  0  0  0
 2  0      0 1485988  36488 354720    0    0     0     0 1006  349 100  1  0  0  0
 2  0      0 1485988  36488 354720    0    0     0    18 1015  350 99  1  0  0  0
 2  0      0 1485988  36488 354720    0    0     0     0 1005  353 100  0  0  0  0
```

L'option '-t' permet d'afficher l'horodatage (champ timestamp) :

```
# vmstat -t 2 5
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu------ ---timestamp---
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0      0 1485996  36496 354720    0    0    54    17  262  121 23  1 75  1  0      2015-01-22 13:46:17 CET
 2  0      0 1485988  36496 354720    0    0     0     0 1005  351 100  1  0  0  0      2015-01-22 13:46:19 CET
 2  0      0 1485988  36496 354720    0    0     0     0 1010  347 100  0  0  0  0      2015-01-22 13:46:21 CET
 2  0      0 1485988  36496 354720    0    0     0     0 1008  350 99  1  0  0  0      2015-01-22 13:46:23 CET
 2  0      0 1485988  36496 354720    0    0     0     0 1007  351 100  1  0  0  0      2015-01-22 13:46:25 CET
```

Pour afficher le résultat en méga-octets (en kilo-octets par défaut) :

```
# vmstat -S M 1 3
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 3  0      0   1436     36    358    0    0    48    17  348  152 32  1 66  1  0
 3  0      0   1436     36    358    0    0     0     0 1014  526 75 25  0  0  0
 3  0      0   1436     36    358    0    0     0     0 1011  517 76 24  0  0  0
```

Pour afficher une synthèse générale des statistiques :

```
# vmstat -s
      2130540  total memory
       644544  used memory
       277040  active memory
       251032  inactive memory
      1485996  free memory
        36504  buffer memory
       354720  swap cache
      2277368  total swap
            0  used swap
      2277368  free swap
       180189 non-nice user cpu ticks
            2 nice user cpu ticks
         4423 system cpu ticks
       553353 idle cpu ticks
         7002 IO-wait cpu ticks
          351 IRQ cpu ticks
          154 softirq cpu ticks
            0 stolen cpu ticks
       401193 pages paged in
       124917 pages paged out
            0 pages swapped in
            0 pages swapped out
      2016769 interrupts
       921439 CPU context switches
   1421923388 boot time
         2887 forks
```

L'option '-d' permet d'afficher l'activité des disques :

```
# vmstat -d
disk- ------------reads------------ ------------writes----------- -----IO------
       total merged sectors      ms  total merged sectors      ms    cur    sec
sda     9345   6750  785068   92477   4322  31560  283202  559010      0    103
sdb      362   1123    2746    2274      0      0       0       0      0      2
sdc      336     50    3088    2480      0      0       0       0      0      2
sdd      331     50    3048    2713      0      0       0       0      0      2
sde      337     50    3096    2722      0      0       0       0      0      2
sdf      342     50    3136    2823      0      0       0       0      0      2
dm-0   14641      0  774290  192471  35423      0  283160 41695824      0    101
dm-1     297      0    2376    2820      0      0       0       0      0      1
```

reads	signification
total	le nombre total de lectures réussies
merged	lectures regroupées (résultat sur une entrée/sortie)
sectors	le nombre de secteurs lus avec succès
ms	le temps passé en milli secondes de toutes les lectures

writes	signification
total	le nombre total d'écritures réussies
merged	écritures regroupées (résultat sur une entrée/sortie)
sectors	le nombre de secteurs écrits avec succès
ms	le temps passé en milli secondes de toutes les écritures

io	signification
cur	les entrées/sorties actuellement en cours
s	le temps passé en milli-secondes des entrées/sorties

Surveillance système

La commande iostat

- iostat
- iostat 1 10
- iostat -p sda
- iostat -N

La commande iostat

La commande iostat fait partie du package sysstat. Elle permet notamment d'afficher l'activité des entrées/sorties (I/O) au niveau des disques durs ou de la partition.

La commande iostat renvoie des informations sur les statistiques CPU et les entrées/sorties sur les périphériques et les partitions.

```
# iostat
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          37,46    0,00    4,22    0,73    0,00   57,59

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
scd0              0,01         0,04         0,00        428          0
sda               1,78        85,28        32,71     819374     314276
sdb               0,04         0,29         0,00       2746          0
sdc               0,03         0,32         0,00       3088          0
sdd               0,03         0,32         0,00       3048          0
sde               0,04         0,32         0,00       3096          0
sdf               0,04         0,33         0,00       3136          0
dm-0              6,00        84,16        32,70     808594     314224
dm-1              0,03         0,25         0,00       2376          0
```

avg-cpu	signification
%user	affiche le pourcentage d'utilisation CPU au niveau utilisateur (application)
%nice	affiche le pourcentage d'utilisation CPU au niveau utilisateur avec une priorité nice
%system	
%idle	affiche le taux de disponibilité du CPU

device	signification
tps	affiche le nombre de transferts par seconde
Blk_read/s	affiche la quantité de données lue en blocks par seconde
Blk_wrtn/s	affiche la quantité de données écrite en blocks par seconde
Blk_read	affiche la quantité de blocs lue
Blk_write	affiche la quantité de blocs écrite

Pour l'affichage en kilo-octets à la place des blocs : utiliser l'option '-k' (-m en mega-octets) :

```
# iostat -k
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          39,56    0,00    9,52    0,64    0,00   50,28

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
scd0              0,01         0,02         0,00        214          0
sda               1,59        37,23        14,51     409719     159750
sdb               0,03         0,12         0,00       1373          0
sdc               0,03         0,14         0,00       1544          0
sdd               0,03         0,14         0,00       1524          0
sde               0,03         0,14         0,00       1548          0
sdf               0,03         0,14         0,00       1568          0
dm-0              5,30        36,74        14,51     404329     159724
dm-1              0,03         0,11         0,00       1188          0
```

```
# iostat -m
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          39,82    0,00    9,48    0,63    0,00   50,06

Device:            tps    MB_read/s    MB_wrtn/s    MB_read    MB_wrtn
scd0              0,01         0,00         0,00          0          0
sda               1,59         0,04         0,01        400        156
sdb               0,03         0,00         0,00          1          0
sdc               0,03         0,00         0,00          1          0
sdd               0,03         0,00         0,00          1          0
sde               0,03         0,00         0,00          1          0
sdf               0,03         0,00         0,00          1          0
dm-0              5,28         0,04         0,01        394        155
dm-1              0,03         0,00         0,00          1          0
```

Pour afficher toutes les 2 secondes (CTRL+C pour arrêter) :

```
# iostat 2
```

Pour afficher les statistiques 4 fois toutes les 3 secondes :

```
# iostat 3 4
```

L'option '-c' permet d'afficher que les statistiques CPU :

```
# iostat -c 1 3
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          41,72    0,00    9,20    0,61    0,00   48,47

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          99,00    0,00    1,00    0,00    0,00    0,00

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          98,00    0,00    2,00    0,00    0,00    0,00
```

L'option '-p' permet un affichage par partition :

```
# iostat -p
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          41,19    0,00    9,28    0,62    0,00   48,91

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
scd0              0,01         0,04         0,00        428          0
sda               1,56        72,43        28,35     819438     320716
sda1              0,07         0,56         0,00       6324         52
sda2              1,42        71,76        28,34     811882     320664
sdb               0,03         0,24         0,00       2746          0
sdb1              0,03         0,22         0,00       2442          0
sdc               0,03         0,27         0,00       3088          0
sdc1              0,01         0,05         0,00        520          0
sdc9              0,01         0,05         0,00        584          0
sdd               0,03         0,27         0,00       3048          0
sdd1              0,01         0,05         0,00        520          0
sdd9              0,01         0,05         0,00        584          0
sde               0,03         0,27         0,00       3096          0
sde1              0,01         0,05         0,00        568          0
sde9              0,01         0,05         0,00        584          0
sdf               0,03         0,28         0,00       3136          0
sdf1              0,01         0,05         0,00        568          0
sdf9              0,01         0,05         0,00        584          0
dm-0              5,17        71,48        28,34     808658     320664
dm-1              0,03         0,21         0,00       2376          0
```

L'option '-p' peut prendre en argument un disque pour afficher que les statistiques de ce disque :

```
# iostat -p sda
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          42,14    0,00    9,13    0,61    0,00   48,12

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               1,54        71,25        27,95     819438     321396
sda1              0,07         0,55         0,00       6324         52
sda2              1,40        70,60        27,94     811882     321344
```

L'option '-N' affiche les statistiques concernant LVM :

```
# iostat -N
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          42,47    0,00    9,08    0,61    0,00   47,84

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
scd0              0,01         0,04         0,00        428          0
sda               1,53        70,84        27,80     819438     321540
sdb               0,03         0,24         0,00       2746          0
sdc               0,03         0,27         0,00       3088          0
sdd               0,03         0,26         0,00       3048          0
sde               0,03         0,27         0,00       3096          0
sdf               0,03         0,27         0,00       3136          0
vg_formateur-lv_root     5,07        69,91        27,79     808658     321488
vg_formateur-lv_swap     0,03         0,21         0,00       2376          0
```

```
# iostat -N vg_formateur-lv_root
Linux 2.6.32-358.18.1.el6.x86_64 (formateur)    22/01/2015      _x86_64_        (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          42,59    0,00    9,07    0,60    0,00   47,74

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
vg_formateur-lv_root     5,06        69,77        27,74     808658     321552
```

Surveillance système

La commande top

- top
- top -u user
- top -d 4
- top -n 5

La commande top

Elle effectue du monitoring en temps réel. Les commandes internes à top dépendent de la version de top.

```
# top
Tasks: 174 total,   1 running, 173 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.7%sy,  0.0%ni, 96.7%id,  2.3%wa,  0.3%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   612468k used,  1518072k free,    33172k buffers
Swap:  2277368k total,        0k used,  2277368k free,   350672k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2579 root      20   0 15024 1336  968 R  0.7  0.1   0:00.10 top
 2305 theo      20   0  493m  12m 8004 S  0.3  0.6   0:00.30 gnome-settings-
 2496 root      20   0 98.0m 4408 3412 S  0.3  0.2   0:00.16 sshd
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.03 ksoftirqd/0
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
    6 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    7 root      20   0     0    0    0 S  0.0  0.0   0:00.25 events/0
    8 root      20   0     0    0    0 S  0.0  0.0   0:00.00 cgroup
    9 root      20   0     0    0    0 S  0.0  0.0   0:00.00 khelper
```

Pour quitter l'utilitaire il faut appuyer sur 'q'.

Appuyer sur la touche f pour trier la sortie en fonction de certains champs. Puis naviguer pour sélectionner les champs à afficher. La lettre d ou la barre d'espace permet de selectionner des champs.

```
Fields Management for window 1:Def, whose current sort field is %MEM
   Navigate with Up/Dn, Right selects for move then <Enter> or Left commits,
   'd' or <Space> toggles display, 's' sets sort.  Use 'q' or <Esc> to end!

* PID     = Process Id             DATA    = Data+Stack (KiB)
* USER    = Effective User Name    nMaj    = Major Page Faults
* PR      = Priority               nMin    = Minor Page Faults
* NI      = Nice Value             nDRT    = Dirty Pages Count
* VIRT    = Virtual Image (KiB)    WCHAN   = Sleeping in Function
* %MEM    = Memory Usage (RES)     Flags   = Task Flags <sched.h>
* RES     = Resident Size (KiB)    CGROUPS = Control Groups
* SHR     = Shared Memory (KiB)    SUPGIDS = Supp Groups IDs
* S       = Process Status         SUPGRPS = Supp Groups Names
* %CPU    = CPU Usage              TGID    = Thread Group Id
* SUID    = Saved User Id          ENVIRON = Environment vars
* TIME+   = CPU Time, hundredths   vMj     = Major Faults delta
* COMMAND = Command Name/Line      vMn     = Minor Faults delta
  PPID    = Parent Process pid     USED    = Res+Swap Size (KiB)
  UID     = Effective User Id      nsIPC   = IPC namespace Inode
  RUID    = Real User Id           nsMNT   = MNT namespace Inode
  RUSER   = Real User Name         nsNET   = NET namespace Inode
  SUSER   = Saved User Name        nsPID   = PID namespace Inode
  GID     = Group Id               nsUSER  = USER namespace Inode
  GROUP   = Group Name             nsUTS   = UTS namespace Inode
  PGRP    = Process Group Id
  TTY     = Controlling Tty
  TPGID   = Tty Process Grp Id
  SID     = Session Id
  nTH     = Number of Threads
  P       = Last Used Cpu (SMP)
  TIME    = CPU Time
  SWAP    = Swapped Size (KiB)
  CODE    = Code Size (KiB)
```

Afficher les processus d'un utilisateur :

```
# top -u theo
Tasks: 173 total,   1 running, 172 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.3%sy,  0.0%ni, 99.7%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   613328k used,  1517212k free,    33596k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352284k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2220 theo      20   0  146m 3768 3036 S  0.0  0.2   0:00.01 gnome-keyring-d
 2229 theo      20   0  247m 7632 6024 S  0.0  0.4   0:00.20 gnome-session
 2237 theo      20   0 20032  784  516 S  0.0  0.0   0:00.00 dbus-launch
 2238 theo      20   0 21796 1272  612 S  0.0  0.1   0:00.12 dbus-daemon
 2265 theo      20   0  196m 1912 1420 S  0.0  0.1   0:00.00 VBoxClient
 2273 theo      20   0  198m 1660 1136 S  0.0  0.1   0:00.00 VBoxClient
 2278 theo      20   0  130m 1232  c808 S  0.0  0.1   0:00.00 VboxClient
```

Remarque: Pour afficher en couleur seulement les processus actifs appuyez sur la lettre 'z'.

Pour afficher le chemin absolu d'un processus actif appuyer sur la lettre 'c' :

```
top - 11:54:35 up 36 min,  4 users,  load average: 0.86, 1.00, 0.47
Tasks: 174 total,   1 running, 173 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.3%us,  0.6%sy,  0.0%ni, 99.1%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   614460k used,  1516080k free,    33748k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352656k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2617 root      20   0 15024 1352  984 R  0.6  0.1   0:00.30 top
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 /sbin/init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 [kthreadd]
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 [migration/0]
    4 root      20   0     0    0    0 S  0.0  0.0   0:00.06 [ksoftirqd/0]
    5 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 [migration/0]
```

Pour modifier le temps de rafraîchissement (3 secondes par défaut, appuyer sur la lettre 'd' puis indiquer le temps en secondes) :

```
top - 11:56:21 up 37 min,  4 users,  load average: 0.15, 0.70, 0.42
Tasks: 174 total,   1 running, 173 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.3%us,  0.3%sy,  0.0%ni, 99.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   614088k used,  1516452k free,    33756k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352656k cached
Change delay from 3.0 to: 1
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2619 root      20   0 15024 1336  968 R  0.7  0.1   0:00.04 top
 2390 theo      20   0  258m 7188 5220 S  0.3  0.3   0:00.58 gnome-screensav
 2496 root      20   0 98.0m 4408 3412 S  0.3  0.2   0:00.81 sshd
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
```

Pour envoyer un signal à un processus, appuyer sur la lettre 'k' :

```
top - 11:58:11 up 39 min,  4 users,  load average: 0.24, 0.53, 0.38
Tasks: 174 total,   2 running, 172 sleeping,   0 stopped,   0 zombie
Cpu(s): 99.0%us,  1.0%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   614212k used,  1516328k free,    33772k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352656k cached
PID to kill: 2620
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2620 theo      20   0 98.5m  588  500 R 99.5  0.0   0:15.21 yes
```

```
 2619 root      20   0 15024 1352  984 R  1.0  0.1   0:00.13 top
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
```

Puis, préciser le signal à envoyer (signal 15 SIGTERM par défaut) :

```
top - 11:58:11 up 39 min,  4 users,  load average: 0.24, 0.53, 0.38
Tasks: 174 total,   2 running, 172 sleeping,   0 stopped,   0 zombie
Cpu(s): 99.0%us,  1.0%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   614212k used,  1516328k free,    33772k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352656k cached
Kill PID 2620 with signal [15]: 9
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2620 theo      20   0 98.5m  588  500 R 99.5  0.0   0:15.21 yes
 2619 root      20   0 15024 1352  984 R  1.0  0.1   0:00.13 top
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
```

Pour modifier la priorité d'un processus appuyez sur la lettre 'r' :

```
top - 12:03:04 up 44 min,  4 users,  load average: 0.05, 0.37, 0.36
Tasks: 173 total,   1 running, 172 sleeping,   0 stopped,   0 zombie
Cpu(s): 16.2%us,  1.1%sy,  0.0%ni, 80.8%id,  1.9%wa,  0.1%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   614080k used,  1516460k free,    33892k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352684k cached
PID to renice: 2637
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 2637 root      20   0 15020 1228  872 R  3.9  0.1   0:00.02 top
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 migration/0
```

Puis indiquer la nouvelle priorité :

```
Tasks: 173 total,   1 running, 172 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.7%sy,  0.0%ni, 99.0%id,  0.0%wa,  0.3%hi,  0.0%si,  0.0%st
Mem:   2130540k total,   614080k used,  1516460k free,    33900k buffers
Swap:  2277368k total,        0k used,  2277368k free,   352684k cached
Renice PID 2637 to value: +10
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 1754 root      20   0 20212 1328 1148 S  0.3  0.1   0:01.77 hald-addon-stor
 2637 root      30  10 15024 1340  972 R  0.3  0.1   0:00.08 top
    1 root      20   0 19228 1476 1184 S  0.0  0.1   0:01.06 init
    2 root      20   0     0    0    0 S  0.0  0.0   0:00.00 kthreadd
```

Pour afficher l'aide à l'intérieur de top, appuyer sur la lettre 'h' :

```
Help for Interactive Commands - procps-ng version 3.3.10
Window 1:Def: Cumulative mode Off.  System: Delay 3,0 secs; Secure mode Off.

  Z,B,E,e   Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale
  l,t,m     Toggle Summary: 'l' load avg; 't' task/cpu stats; 'm' memory info
  0,1,2,3,I Toggle: '0' zeros; '1/2/3' cpus or numa node views; 'I' Irix mode
  f,F,X     Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width

  L,&,<,> . Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right
  R,H,V,J . Toggle: 'R' Sort; 'H' Threads; 'V' Forest view; 'J' Num justify
  c,i,S,j . Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify
  x,y     . Toggle highlights: 'x' sort field; 'y' running tasks
  z,b     . Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
  u,U,o,O . Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria
  n,#,^O  . Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)
  C,...   . Toggle scroll coordinates msg for: up,down,left,right,home,end

  k,r       Manipulate tasks: 'k' kill; 'r' renice
  d or s    Set update interval
  W,Y       Write configuration file 'W'; Inspect other output 'Y'
  q         Quit
          ( commands shown with '.' require a visible task display window )
Press 'h' or '?' for help with Windows,
Type 'q' or <Esc> to continueh Windows,
any other key to continue
```

Pour quitter automatiquement top après un certain nombre d'affichages, utiliser l'option '-n nombre' :

```
# top -n 3
```

Surveillance système

La commande lsof

- lsof
- lsof -u user
- lsof -i TCP:22
- lsof -p PID

La commande lsof : list open files

Elle affiche notamment les fichiers ouverts et les processus. Les fichiers ouverts comprennent les fichiers basés sur disque, les sockets réseaux, les pipes, les périphériques et les processus. Cette commande est pratique quand vous ne pouvez pas démonter un système de fichiers pour savoir si des processus y accèdent.

Sans options, la commande lsof affiche tous les fichiers ouverts :

```
# lsof
COMMAND    PID      USER   FD      TYPE             DEVICE SIZE/OFF       NODE NAME
init         1      root  cwd       DIR              253,0     4096          2 /
init         1      root  rtd       DIR              253,0     4096          2 /
init         1      root  txt       REG              253,0   150352      11543 /sbin/init
init         1      root  mem       REG              253,0    65928     654112
/lib64/libnss_files-2.12.so
init         1      root  mem       REG              253,0  1916568     654096
/lib64/libc-2.12.so
init         1      root  mem       REG              253,0    90784     654083
/lib64/libgcc_s-4.4.7-20120601.so.1
```

```
# lsof /data
```

FD (File Descriptor)	signification
cwd:	le répertoire de travail courant (current working directory)
rtd:	le répertoire de root (root directory)
txt:	le programme texte (code et données)
mem:	le fichier en mémoire (memory mapped file)
2u:	le descripteur de fichier 2 r: pour un accès en lecture w: pour un accès en écriture u: pour une accès en écriture et lecture

TYPE	type de fichier
DIR	répertoire (directory)
REG	fichier ordinaire (regular file)
CHR	fichier spécial en mode caractère (character special file)
FIFO	premier entrée, premier sortie (First In First Out)

Pour lister que les fichiers ouverts par un utilisateur.

```
# lsof -u theo | more
COMMAND    PID USER   FD   TYPE             DEVICE SIZE/OFF       NODE NAME
gnome-key 2220 theo  cwd    DIR              253,0     4096      13902 /var/gdm
gnome-key 2220 theo  rtd    DIR              253,0     4096          2 /
gnome-key 2220 theo  txt    REG              253,0   688248     795320 /usr/bin/gnome-
keyring-daemon
gnome-key 2220 theo  mem    REG              253,0    90784     654083 /lib64/libgcc_s-
4.4.7-20120601.so.1
gnome-key 2220 theo  mem    REG              253,0    14584     654128 /lib64/libutil-
2.12.so
gnome-key 2220 theo  mem    REG              253,0    95872     805389
/usr/lib64/libgvfscommon.so.0.0.0
...sortie tronquée
```

Pour lister les fichiers qui ne sont pas utilisés par un utilisateur (^ nom_user pour exclure) :

```
# lsof -i -u ^theo | more
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind   1598     rpc    7u  IPv4   9664      0t0  UDP *:925
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598     rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
rpcbind   1598     rpc   10u  IPv6   9669      0t0  UDP *:925
```

Pour afficher les processus utilisant un port particulier :

```
# lsof -i TCP:22
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd    1871 root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
sshd    1871 root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
sshd    2516 root    3r  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd    2518 theo    3u  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd    2800 root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
```

Pour afficher les processus UDP utilisant un intervalle de ports :

```
# lsof -i UDP:1-500
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind  1598  rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind  1598  rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
dhclient 1655 root    6u  IPv4   9983      0t0  UDP *:bootpc
```

Pour afficher les processus TCP utilisant un intervalle de ports :

```
# lsof -i TCP:1-500
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598  rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598  rpc   11u  IPv6   9670      0t0  TCP *:sunrpc (LISTEN)
sshd      1871 root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
sshd      1871 root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
xinetd    1879 root    5u  IPv6  11031      0t0  TCP *:telnet (LISTEN)
master    1962 root   12u  IPv4  11225      0t0  TCP *:smtp (LISTEN)
master    1962 root   13u  IPv6  11227      0t0  TCP *:smtp (LISTEN)
clock-app 2420 theo   21u  IPv4  21584      0t0  TCP formateur.home:58675->a23-200-87-
214.deploy.static.akamaitechnologies.com:http (CLOSE_WAIT)
sshd      2516 root    3r  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2518 theo    3u  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2800 root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
sshd      3179 root    3r  IPv4  25331      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:pehelp (ESTABLISHED)
```

Pour afficher seulement les processus utilisant ipv4 :

```
# lsof -i 4
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind   1598     rpc    7u  IPv4   9664      0t0  UDP *:925
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpc.statd 1642 rpcuser    5r  IPv4   9874      0t0  UDP *:970
rpc.statd 1642 rpcuser    8u  IPv4   9883      0t0  UDP *:47166
rpc.statd 1642 rpcuser    9u  IPv4   9887      0t0  TCP *:55090 (LISTEN)
dhclient  1655    root    6u  IPv4   9983      0t0  UDP *:bootpc
cupsd     1684    root    7u  IPv4  10081      0t0  TCP localhost:ipp (LISTEN)
cupsd     1684    root    9u  IPv4  10084      0t0  UDP *:ipp
sshd      1871    root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
master    1962    root   12u  IPv4  11225      0t0  TCP *:smtp (LISTEN)
clock-app 2420    theo   21u  IPv4  21584      0t0  TCP formateur.home:58675->a23-200-87-
214.deploy.static.akamaitechnologies.com:http (CLOSE_WAIT)
sshd      2516    root    3r  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2518    theo    3u  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2800    root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
```

Pour afficher seulement les processus utilisant ipv6 :

```
# lsof -i 6
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
rpcbind   1598     rpc   10u  IPv6   9669      0t0  UDP *:925
rpcbind   1598     rpc   11u  IPv6   9670      0t0  TCP *:sunrpc (LISTEN)
rpc.statd 1642 rpcuser   10u  IPv6   9891      0t0  UDP *:33844
rpc.statd 1642 rpcuser   11u  IPv6   9895      0t0  TCP *:55198 (LISTEN)
cupsd     1684    root    6u  IPv6  10080      0t0  TCP localhost:ipp (LISTEN)
sshd      1871    root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
xinetd    1879    root    5u  IPv6  11031      0t0  TCP *:telnet (LISTEN)
master    1962    root   13u  IPv6  11227      0t0  TCP *:smtp (LISTEN)
```

Pour afficher les informations sur les fichiers ouverts par un utilisateur via le réseau :

```
# lsof -i -u theo | egrep '/etc| ping'
bash      3237    theo  cwd    DIR              253,0     4096     130819 /etc
ping      3280    theo  cwd    DIR              253,0     4096     130819 /etc
```

On constate que l'utilisateur theo est positionné dans le répertoire /etc et utilise la commande ping.

L'option '-i' permet d'afficher toutes les connexions réseaux :

```
# lsof -i | more
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind   1598     rpc    7u  IPv4   9664      0t0  UDP *:925
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598     rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
rpcbind   1598     rpc   10u  IPv6   9669      0t0  UDP *:925
... sortie tronquée
```

```
# lsof -i | grep ESTABLISHED
sshd      2800    root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
sshd      3179    root    3r  IPv4  25331      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:pehelp (ESTABLISHED)
sshd      3214    root    3r  IPv4  25679      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:sdclient (ESTABLISHED)
sshd      3234    root    3r  IPv4  25772      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:messageservice (ESTABLISHED)
sshd      3236    theo    3u  IPv4  25772      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:messageservice (ESTABLISHED)
```

```
# lsof -i | grep LISTEN
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598     rpc   11u  IPv6   9670      0t0  TCP *:sunrpc (LISTEN)
rpc.statd 1642 rpcuser    9u  IPv4   9887      0t0  TCP *:55090 (LISTEN)
rpc.statd 1642 rpcuser   11u  IPv6   9895      0t0  TCP *:55198 (LISTEN)
cupsd     1684    root    6u  IPv6  10080      0t0  TCP localhost:ipp (LISTEN)
cupsd     1684    root    7u  IPv4  10081      0t0  TCP localhost:ipp (LISTEN)
sshd      1871    root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
sshd      1871    root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
xinetd    1879    root    5u  IPv6  11031      0t0  TCP *:telnet (LISTEN)
master    1962    root   12u  IPv4  11225      0t0  TCP *:smtp (LISTEN)
master    1962    root   13u  IPv6  11227      0t0  TCP *:smtp (LISTEN)
```

L'option '-p' permet d'afficher tous les fichiers ouverts par un PID particulier :

```
# lsof -p 1
COMMAND PID USER   FD   TYPE             DEVICE SIZE/OFF   NODE NAME
init      1 root  cwd    DIR              253,0     4096      2 /
init      1 root  rtd    DIR              253,0     4096      2 /
init      1 root  txt    REG              253,0   150352  11543 /sbin/init
init      1 root  mem    REG              253,0    65928 654112 /lib64/libnss_files-
2.12.so
init      1 root  mem    REG              253,0  1916568 654096 /lib64/libc-2.12.so
init      1 root  mem    REG              253,0    90784 654083 /lib64/libgcc_s-4.4.7-
20120601.so.1
init      1 root  mem    REG              253,0    43832 654124 /lib64/librt-2.12.so
init      1 root  mem    REG              253,0   142464 654120 /lib64/libpthread-2.12.so
init      1 root  mem    REG              253,0   265728 654149 /lib64/libdbus-1.so.3.4.0
init      1 root  mem    REG              253,0    39896 654216 /lib64/libnih-
dbus.so.1.0.0
init      1 root  mem    REG              253,0   101920 654218 /lib64/libnih.so.1.0.0
init      1 root  mem    REG              253,0   154504 654477 /lib64/ld-2.12.so
init      1 root    0u   CHR                1,3      0t0   3656 /dev/null
init      1 root    1u   CHR                1,3      0t0   3656 /dev/null
init      1 root    2u   CHR                1,3      0t0   3656 /dev/null
init      1 root    3r  FIFO                0,8      0t0   7047 pipe
init      1 root    4w  FIFO                0,8      0t0   7047 pipe
init      1 root    5r   DIR               0,10        0      1 inotify
init      1 root    6r   DIR               0,10        0      1 inotify
init      1 root    7u  unix 0xffff88003781a680      0t0   7048 socket
init      1 root    9u  unix 0xffff8800379a7380      0t0   9743 socket
```

Pour envoyer un signal à tous les processus d'un utilisateur. Par exemple avec le signal SIGKILL (-9), on peut supprimer tous les processus d'un utilisateur :

```
# kill -9 `lsof -t -u theo`
```

Remarque: l'option '-t' de la commande lsof renvoie le PID des processus.

Vérification :

```
# lsof -u theo
```

Notes

Administration réseau

Dans ce chapitre, nous allons étudier l'administration réseau d'un serveur Linux et les commandes d'analyse de performances.

Table des matières

Administration du réseau

Les interfaces réseaux et la commande ifconfig

- Lister les interfaces
- ifconfig -a
- ifconfig eth0

Les interfaces réseaux et la commande ifconfig

La commande ifconfig affiche les interfaces actives de votre système. L'option -a les listent toutes, ainsi que celles qui sont inactives.

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A2:D4:ED
          inet adr:192.168.1.6  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fea2:d4ed/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:621 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:191549 (187.0 KiB)  TX bytes:105329 (102.8 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:6740 (6.5 KiB)  TX bytes:6740 (6.5 KiB)
```

Le nommage des périphériques dépend du type de cartes réseau physique installé sur la machine. La 1ère carte réseau porte le nom du pilote (eth, qfe, hme, ..) suivi du chiffre 0 (eth0 par exemple). Si plusieurs interfaces identiques sont présentes elles sont incrémentées (eth1, eth2,...). L'interface lo représente l'adresse de bouclage (loopback). La commande lsmod permet de visualiser les pilotes chargés en mémoire.

```
# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:A2:D4:ED
          inet adr:192.168.1.6  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fea2:d4ed/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1798 errors:0 dropped:0 overruns:0 frame:0
          TX packets:628 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:193938 (189.3 KiB)  TX bytes:107099 (104.5 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:1E:4E:D5
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1013 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:114839 (112.1 KiB)  TX bytes:1152 (1.1 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:CA:FC:FE
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1583 errors:0 dropped:0 overruns:0 frame:0
          TX packets:469 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:172425 (168.3 KiB)  TX bytes:83886 (81.9 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:6740 (6.5 KiB)  TX bytes:6740 (6.5 KiB)
```

Administration du réseau

Configuration réseau

- Le fichier /etc/sysconfig/network
- Les fichiers /etc/sysconfig/network-scripts/*
- Basculement d'un adressage fixe en DHCP

Les fichiers de configuration

Le fichier /etc/sysconfig/network contient le nom de la machine (la variable HOSTNAME=<nom_machine>) pour les versions antérieures à CentOS 7. Depuis CentOS 7, le nom de la machine est stocké dans le fichier /etc/hostname (/etc/HOSTNAME pour une distribution Suse).

Versions antérieurs à CentOS 7 :

```
# more /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=formateur
```

Depuis CentOS 7 :

```
# more /etc/hostname
form1
```

Chaque carte réseau possède un fichier de configuration dans le répertoire /etc/sysconfig/network-scripts qui porte le nom ifcfg-<nom_de_la_carte>.

```
# ls /etc/sysconfig/network-scripts
ifcfg-enp0s3  ifdown-ipv6    ifdown-Team      ifup-eth    ifup-post      ifup-tunnel
ifcfg-lo      ifdown-isdn    ifdown-TeamPort  ifup-ippp   ifup-ppp       ifup-wireless
ifdown        ifdown-post    ifdown-tunnel    ifup-ipv6   ifup-routes    init.ipv6-global
ifdown-bnep   ifdown-ppp     ifup             ifup-isdn   ifup-sit       network-
functions
ifdown-eth    ifdown-routes  ifup-aliases     ifup-plip   ifup-Team      network-
functions-ipv6
ifdown-ippp   ifdown-sit     ifup-bnep        ifup-plusb  ifup-TeamPort
```

Le fichier de configuration d'une carte réseau :

```
# more /etc/sysconfig/network-scripts/ifcfg-enp0s3
HWADDR="08:00:27:EE:E2:B9"
TYPE="Ethernet"
BOOTPROTO="dhcp"
DEFROUTE="yes"
PEERDNS="yes"
PEERROUTES="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
IPV6_FAILURE_FATAL="no"
NAME="enp0s3"
UUID="914b83e6-80cc-47f2-9eef-b61aff13400c"
ONBOOT="yes"
```

Dans cet exemple, l'adresse IP de la carte réseau est donnée par le serveur DHCP.

```
# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.4  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feee:e2b9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ee:e2:b9  txqueuelen 1000  (Ethernet)
        RX packets 663  bytes 71417 (69.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 523  bytes 85359 (83.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Pour basculer en adressage IP fixe, il faut configurer correctement le fichier ifcfg-enp0s3.
Le fichier après modification :

```
# more /etc/sysconfig/network-scripts/ifcfg-enp0s3
HWADDR="08:00:27:EE:E2:B9"
TYPE="Ethernet"
BOOTPROTO="static"
IPADDR=192.168.1.104
NETMASK=255.255.255.0
GATEWAY=192.168.1.254
DNS1=192.168.1.254
DNS2=8.8.8.8
DEFROUTE="yes"
PEERDNS="yes"
PEERROUTES="yes"
IPV4_FAILURE_FATAL="no"
NAME="enp0s3"
UUID="914b83e6-80cc-47f2-9eef-b61aff13400c"
ONBOOT="yes"
```

Puis il faut désactiver et activer la carte réseau :

```
# ifdown enp0s3
# ifup enp0s3
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/2)
```

Remarque : les commandes ifup et ifdown ne fonctionnent que sur les interfaces réseaux ayant un fichier de configuration dans le répertoire /etc/sysconfig/network-scripts.

Vérification :

```
# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.104  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:feee:e2b9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ee:e2:b9  txqueuelen 1000  (Ethernet)
        RX packets 1251  bytes 129507 (126.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 925  bytes 143178 (139.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
# more /etc/resolv.conf
# Generated by NetworkManager
domain home
search home
nameserver 192.168.1.254
nameserver 8.8.8.8
```

Administration du réseau

La commande ip

- ip link ip link show
- ip a ip addr ip addr show
- ip route

La commande ip

Remarques:

La commande ip supporte les options raccourcis (l pour linf, a pour addr, ...)

L'option 'show' est le comportement par défaut de beaucoup d'options de la commande ip (link, addr, …).

Afficher les interfaces réseaux :

```
# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode
DEFAULT qlen 1000
    link/ether 08:00:27:df:f2:61 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode
DEFAULT qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode
DEFAULT qlen 1000
    link/ether 52:54:00:5d:d9:00 brd ff:ff:ff:ff:ff:ff
5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
mode DEFAULT qlen 1000
    link/ether 52:54:00:5d:d9:00 brd ff:ff:ff:ff:ff:ff
```

Afficher la configuration IP.

```
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:df:f2:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 86341sec preferred_lft 86341sec
    inet6 fe80::4f8c:c790:26de:6302/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.7/24 brd 192.168.1.255 scope global dynamic enp0s8
       valid_lft 86343sec preferred_lft 86343sec
    inet6 fe80::933:576e:329d:ca02/64 scope link
       valid_lft forever preferred_lft forever
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN qlen
1000
    link/ether 52:54:00:5d:d9:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN
qlen 1000
    link/ether 52:54:00:5d:d9:00 brd ff:ff:ff:ff:ff:ff
```

Afficher la configuration d'une carte.

```
# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:df:f2:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 84687sec preferred_lft 84687sec
    inet6 fe80::4f8c:c790:26de:6302/64 scope link
       valid_lft forever preferred_lft forever
```

Supprimer l'adresse ip d'une carte.

```
# ip addr del 192.168.1.7/24 dev enp0s8
# ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
    inet6 fe80::933:576e:329d:ca02/64 scope link
       valid_lft forever preferred_lft forever
```

Configurer une adresse ip sur une interface réseau.

```
# ip addr add 192.168.1.10 dev enp0s8
# ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/32 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::933:576e:329d:ca02/64 scope link
       valid_lft forever preferred_lft forever
```

Remarque : Contrairement à la commande ifconfig, la commande ip n'affecte pas un netmask correspondant à la classe d'adresse. Avec ip le netmask par défaut est toujours 255.255.255.255.

```
# ip addr del 192.168.1.10/32 dev enp0s8
# ip addr add 192.168.1.10/24 dev enp0s8
# ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::933:576e:329d:ca02/64 scope link
       valid_lft forever preferred_lft forever
```

Désactiver une interface réseau.

```
# ip link set enp0s8 down
# ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
```

Activer une interface réseau.

```
# ip link set enp0s8 up
# ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:50:63:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.7/24 brd 192.168.1.255 scope global dynamic enp0s8
       valid_lft 86392sec preferred_lft 86392sec
    inet6 fe80::933:576e:329d:ca02/64 scope link
       valid_lft forever preferred_lft forever
```

Afficher la table de routage.

```
# ip route
default via 192.168.1.254 dev enp0s3  proto static  metric 101
192.168.1.0/24 dev enp0s3  proto kernel  scope link  src 192.168.1.3  metric 100
192.168.122.0/24 dev virbr0  proto kernel  scope link  src 192.168.122.1
```

Ajouter une route.

```
# ip route add 192.168.2.0/24 dev enp0s8
# ip route
default via 192.168.1.254 dev enp0s3  proto static  metric 101
192.168.1.0/24 dev enp0s3  proto kernel  scope link  src 192.168.1.3  metric 100
192.168.2.0/24 dev enp0s8  scope link
192.168.122.0/24 dev virbr0  proto kernel  scope link  src 192.168.122.1
```

Supprimer une route.

```
# ip route del 192.168.2.0/24 dev enp0s8
```

Ajouter une passerelle.

```
# ip route add 192.168.2.0/24 via 192.168.2.10
```

Administration du réseau

La résolution de noms, client DNS

- Le fichier /etc/hosts
- Le fichier /etc/resolv.conf
- Paramétrer la passerelle et le client DNS
- Le fichier /etc/nsswitch.conf

La résolution de noms, client DNS

Le fichier /etc/hosts est un fichier qui permet d'effectuer la résolution de nom en local. Il est constitué d'au moins 2 champs. Le 1er champ est l'adresse ip de la machine, le second champ est le nom de la machine, les champs suivant sont des noms d'alias pour la machine.

```
# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.6 formateur pc1
```

Le fichier /etc/resolv.conf contient les adresses des serveurs DNS. Chaque serveur DNS est identifié avec l'entrée 'nameserver'. Ils sont interrogés dans l'ordre chronologique d'apparition dans le fichier. Les mots clefs 'domain' ou 'search' permettent de spécifier un suffixe DNS.

```
# more /etc/resolv.conf
# Generated by NetworkManager
domain home
search home
nameserver 192.168.1.254
```

La passerelle est identifiée par le paramètre GATEWAY qui peut être défini dans le fichier /etc/sysconfig/network (peu utilisé car dans ce cas toutes les cartes utilisent la même passerelle). Usuellement, la passerelle est indiquée dans chaque fichier de configuration des cartes réseaux. (/etc/sysconfig/network-scripts/ifcfg-<nom_de_la_carte>. Si la carte est configurée pour un adressage via un serveur DHCP, c'est le serveur qui fournit l'adresse IP de la passerelle.

```
# more /etc/sysconfig/network-scripts/ifcfg-enp0s3
HWADDR="08:00:27:EE:E2:B9"
TYPE="Ethernet"
BOOTPROTO="static"
IPADDR=192.168.1.104
NETMASK=255.255.255.0
GATEWAY=192.168.1.254
DNS1=192.168.1.254
DNS2=8.8.8.8
DEFROUTE="yes"
PEERDNS="yes"
PEERROUTES="yes"
IPV4_FAILURE_FATAL="no"
NAME="enp0s3"
UUID="914b83e6-80cc-47f2-9eef-b61aff13400c"
ONBOOT="yes"
```

Le fichier /etc/nsswitch.conf définit l'ordre dans lequel les services de noms seront scrutés. Donc, toute la politique de résolution de noms dépend de ce fichier.

```
# grep hosts /etc/nsswitch.conf
hosts:      files   dns
```

Cette ligne indique que pour la résolution de nom des noms de machines, le système vérifie d'abord le fichier local, c'est à dire /etc/hosts. Si le système ne trouve pas la réponse, il va interroger le serveur dns.

Comparatif des commandes ifconfig et ip		
Afficher la configuration	ifconfig ifconfig -a	ip addr show ip link ip a
Activer une interface	ifconfig eth0 up	ip link set eth0 up
Désactiver une interface	ifconfig eth0 down	ip link set eth0 down
Affecter une adresse IP	ifconfig eth0 192.168.1.2 ifconfig eth0 192.168.1.2/16	ip addr add 192.168.1.2 dev eth0 ip addr add 192.168.1.2/16 dev eth0
Suppimer une addresse IP	non supporté	ip addr del 192.168.1.10/16 dev eth0
Ajouter un alias	ifconfig eth0:1 10.1.1.1/8	ip addr add 10.1.1.1/8 dev eth0 label eth0:1
Ajouter une entrée arp	arp -i eth0 -s 192.168.1.2 00:11:22:33:44:55	ip neigh add 192.168.1.2 lladdr 00:11:22:33:44:55 nud permanent dev eth0
Désactiver la résolution arp	ifconfig -arp eth0	ip link set dev eth0 arp off
Afficher les routes	route	ip route show
Afficher la route sortante	non supporté	ip route get 10.20.30.40
Ajouter une route	route add -net 192.168.2.0/24 dev eth1	ip route add 192.168.2.0/24 dev eth1
Supprimer une route	route del -net 192.168.2.0/24 dev eth1	ip route del 192.168.2.0/24 dev eth1
Ajouter une passerelle	route add -net 192.168.2.0/24 gw 192.168.2.254	ip route add 192.168.2.0/24 via 192.168.2.254

Administration du réseau

Les commandes d'analyse du réseau

- lsof
- netstat
- tcpdump
- iptraf
- ethtool
- dstat
- ss

Les commandes d'analyse du réseau

La commande lsof

La commande lsof : list open files

Cette commande permet notamment d'afficher les fichiers ouverts par des processus.

Pour afficher les processus utilisant un port particulier :

```
# lsof -i TCP:22
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd    1871 root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
sshd    1871 root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
sshd    2516 root    3r  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd    2518 theo    3u  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd    2800 root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
```

Pour afficher les processus utilisant un intervalle de ports :

```
# lsof -i UDP:1-500
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind  1598  rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind  1598  rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
dhclient 1655 root    6u  IPv4   9983      0t0  UDP *:bootpc
```

```
# lsof -i TCP:1-500
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598  rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598  rpc   11u  IPv6   9670      0t0  TCP *:sunrpc (LISTEN)
sshd      1871 root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
sshd      1871 root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
xinetd    1879 root    5u  IPv6  11031      0t0  TCP *:telnet (LISTEN)
master    1962 root   12u  IPv4  11225      0t0  TCP *:smtp (LISTEN)
master    1962 root   13u  IPv6  11227      0t0  TCP *:smtp (LISTEN)
clock-app 2420 theo   21u  IPv4  21584      0t0  TCP formateur.home:58675->a23-200-87-
214.deploy.static.akamaitechnologies.com:http (CLOSE_WAIT)
sshd      2516 root    3r  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2518 theo    3u  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2800 root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
sshd      3179 root    3r  IPv4  25331      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:pehelp (ESTABLISHED)
```

Pour afficher seulement les processus utilisant ipv4 :

```
# lsof -i 4
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind   1598     rpc    7u  IPv4   9664      0t0  UDP *:925
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpc.statd 1642 rpcuser    5r  IPv4   9874      0t0  UDP *:970
rpc.statd 1642 rpcuser    8u  IPv4   9883      0t0  UDP *:47166
rpc.statd 1642 rpcuser    9u  IPv4   9887      0t0  TCP *:55090 (LISTEN)
dhclient  1655    root    6u  IPv4   9983      0t0  UDP *:bootpc
cupsd     1684    root    7u  IPv4  10081      0t0  TCP localhost:ipp (LISTEN)
cupsd     1684    root    9u  IPv4  10084      0t0  UDP *:ipp
sshd      1871    root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
master    1962    root   12u  IPv4  11225      0t0  TCP *:smtp (LISTEN)
clock-app 2420    theo   21u  IPv4  21584      0t0  TCP formateur.home:58675->a23-200-87-
214.deploy.static.akamaitechnologies.com:http (CLOSE_WAIT)
sshd      2516    root    3r  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2518    theo    3u  IPv4  16653      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:vpvc (ESTABLISHED)
sshd      2800    root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
```

Pour afficher seulement les processus utilisant ipv6 :

```
# lsof -i 6
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
rpcbind   1598     rpc   10u  IPv6   9669      0t0  UDP *:925
rpcbind   1598     rpc   11u  IPv6   9670      0t0  TCP *:sunrpc (LISTEN)
rpc.statd 1642 rpcuser   10u  IPv6   9891      0t0  UDP *:33844
rpc.statd 1642 rpcuser   11u  IPv6   9895      0t0  TCP *:55198 (LISTEN)
cupsd     1684    root    6u  IPv6  10080      0t0  TCP localhost:ipp (LISTEN)
sshd      1871    root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
xinetd    1879    root    5u  IPv6  11031      0t0  TCP *:telnet (LISTEN)
master    1962    root   13u  IPv6  11227      0t0  TCP *:smtp (LISTEN)
```

Pour afficher les informations sur les fichiers ouverts par un utilisateur via le réseau :

```
# lsof -i -u theo | egrep '/etc| ping'
bash      3237    theo  cwd    DIR              253,0     4096     130819 /etc
ping      3280    theo  cwd    DIR              253,0     4096     130819 /etc
```

On constate que l'utilisateur theo est positionné dans le répertoire /etc et utilise la commande ping.

L'option '-i' permet d'afficher toutes les connexions réseaux :

```
# lsof -i | more
COMMAND    PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
rpcbind   1598     rpc    6u  IPv4   9660      0t0  UDP *:sunrpc
rpcbind   1598     rpc    7u  IPv4   9664      0t0  UDP *:925
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598     rpc    9u  IPv6   9667      0t0  UDP *:sunrpc
rpcbind   1598     rpc   10u  IPv6   9669      0t0  UDP *:925
... sortie tronquée
```

```
# lsof -i | grep ESTABLISHED
sshd      2800    root    3r  IPv4  19133      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:xmsg (ESTABLISHED)
sshd      3179    root    3r  IPv4  25331      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:pehelp (ESTABLISHED)
sshd      3214    root    3r  IPv4  25679      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:sdclient (ESTABLISHED)
sshd      3234    root    3r  IPv4  25772      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:messageservice (ESTABLISHED)
sshd      3236    theo    3u  IPv4  25772      0t0  TCP formateur.home:ssh-
>PosteSpherius.home:messageservice (ESTABLISHED)
```

```
# lsof -i | grep LISTEN
rpcbind   1598     rpc    8u  IPv4   9665      0t0  TCP *:sunrpc (LISTEN)
rpcbind   1598     rpc   11u  IPv6   9670      0t0  TCP *:sunrpc (LISTEN)
rpc.statd 1642 rpcuser    9u  IPv4   9887      0t0  TCP *:55090 (LISTEN)
rpc.statd 1642 rpcuser   11u  IPv6   9895      0t0  TCP *:55198 (LISTEN)
cupsd     1684    root    6u  IPv6  10080      0t0  TCP localhost:ipp (LISTEN)
cupsd     1684    root    7u  IPv4  10081      0t0  TCP localhost:ipp (LISTEN)
sshd      1871    root    3u  IPv4  10958      0t0  TCP *:ssh (LISTEN)
sshd      1871    root    4u  IPv6  10962      0t0  TCP *:ssh (LISTEN)
xinetd    1879    root    5u  IPv6  11031      0t0  TCP *:telnet (LISTEN)
master    1962    root   12u  IPv4  11225      0t0  TCP *:smtp (LISTEN)
master    1962    root   13u  IPv6  11227      0t0  TCP *:smtp (LISTEN)
```

La commande netstat

La commande netstat permet d'afficher des statistiques réseaux. Elle est remplacée par la commande ss au fur à mesure de l'évolution des systèmes d'exploitation.

L'option '-a' permet de lister tous les ports (TCP & UDP) :

```
# netstat -a | more
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
... sortie tronquée
```

L'option '-n' permet un affichage numérique :

```
# netstat -an | more
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
```

L'option '-t' permet de lister que le protocole TCP :

```
# netstat -at | more
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
```

L'option '-u' permet de lister que le protocole UDP :

```
# netstat -au | more
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:ipp                       *:*
udp        0      0 *:44285                     *:*
```

L'option '-l' permet d'afficher toutes les connections qui sont dans l'état LISTENING :

```
# netstat -l | more
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
```

```
tcp        0      0 localhost:ipp               *:*                         LISTEN
....
Sockets du domaine UNIX actives(seulement serveurs)
Proto RefCpt Indicatrs   Type       Etat          I-Node Chemin
unix  2      [ ACC ]     STREAM     LISTENING     12931  /tmp/keyring-eWbmKt/socket
unix  2      [ ACC ]     STREAM     LISTENING     10202  @/var/run/hald/dbus-Z8nKfYFaGn
unix  2      [ ACC ]     STREAM     LISTENING     13817  /tmp/orbit-theo/linc-8dc-0-
2e5de3a8b89eb
```

Ne lister que les ports TCP en écoute :

```
# netstat -lt | more
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
```

Ne lister tous les ports UDP en écoute :

```
# netstat -lu | more
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:ipp                       *:*
udp        0      0 *:44285                     *:*
udp        0      0 *:899                       *:*
```

Ne lister que les ports UNIX en écoute :

```
# netstat -lx | more
Sockets du domaine UNIX actives(seulement serveurs)
Proto RefCpt Indicatrs   Type       Etat          I-Node Chemin
unix  2      [ ACC ]     STREAM     LISTENING     12931  /tmp/keyring-eWbmKt/socket
unix  2      [ ACC ]     STREAM     LISTENING     10202  @/var/run/hald/dbus-Z8nKfYFaGn
unix  2      [ ACC ]     STREAM     LISTENING     13817  /tmp/orbit-theo/linc-8dc-0-
2e5de3a8b89eb
unix  2      [ ACC ]     STREAM     LISTENING     13928  /tmp/orbit-theo/linc-8e1-0-
154e47713696c
```

Pour afficher les statistiques par protocole :

```
# netstat -s
Ip:
    1984 total packets received
    0 forwarded
    0 incoming packets discarded
    1798 incoming packets delivered
    1254 requests sent out
Icmp:
    0 ICMP messages received
    0 input ICMP message failed.
    Histogramme d'entrée ICMP
    0 ICMP messages sent
    0 ICMP messages failed
    Histogramme de sortie ICMP
Tcp:
    14 active connections openings
    7 passive connection openings
    4 failed connection attempts
    1 connection resets received
```

Pour afficher les statistiques pour le protocole TCP :

```
# netstat -st
Tcp:
    14 active connections openings
    7 passive connection openings
    4 failed connection attempts
    1 connection resets received
    2 connections established
```

Pour afficher les statistiques pour protocole UDP :

```
# netstat -su
Udp:
    98 packets received
    0 packets to unknown port received.
    0 packet receive errors
    97 packets sent
UdpLite:
IpExt:
    InMcastPkts: 9
    InBcastPkts: 377
```

Pour afficher le nom du service et le PID des connexions actives :

```
# netstat -tp | more
Connexions Internet actives (sans serveurs)
Proto Recv-Q Send-Q Local Address         Foreign Address             State
PID/Program name
tcp        1      0 formateur.home:32970  a23-200-87-142.deploy.:http CLOSE_WAIT
2369/clock-applet
tcp        0     52 formateur.home:ssh    PosteSpherius.hom:kofax-svr ESTABLISHED
2414/sshd
```

```
# netstat -tulpn | more
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Local Address         Foreign Address      State       PID/Program
name
tcp        0      0 0.0.0.0:111           0.0.0.0:*            LISTEN      1572/rpcbind
tcp        0      0 0.0.0.0:21            0.0.0.0:*            LISTEN      2552/vsftpd
tcp        0      0 0.0.0.0:22            0.0.0.0:*            LISTEN      1885/sshd
tcp        0      0 127.0.0.1:631         0.0.0.0:*            LISTEN      1658/cupsd
tcp        0      0 0.0.0.0:25            0.0.0.0:*            LISTEN      1975/master
tcp        0      0 0.0.0.0:44345         0.0.0.0:*            LISTEN      1623/rpc.statd
```

Pour obtenir un fichage avec un rafraîchissement toutes les 3 secondes. L'option '-c' sans argument effectue un affichage en continue (CTRL-C pour arrêter).

```
# netstat -ac 3
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
```

Pour afficher la table de routage du noyau :

```
# netstat -r | more
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
192.168.1.0     *               255.255.255.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
default         gestionbbox.lan 0.0.0.0         UG        0 0          0 eth0
```

```
# netstat -nr | more
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre irtt Iface
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
192.168.1.254   0.0.0.0         0.0.0.0         UG        0 0          0 eth0
```

Pour afficher les transactions des paquets réseaux :

```
# netstat -i
Table d'interfaces noyau
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0     2823      0      0      0     1700      0      0      0 BMRU
lo        16436   0        8      0      0      0        8      0      0      0 LRU
```

Pour afficher la table d'interface du noyau (similaire à la commande ifconfig) :

```
# netstat -ie
Table d'interfaces noyau
eth0      Link encap:Ethernet  HWaddr 08:00:27:E2:B4:2E
          inet adr:192.168.1.7  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fee2:b42e/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2843 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1709 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:526119 (513.7 KiB)  TX bytes:421344 (411.4 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)
```

Pour afficher les groupes multicast dans les formats IPV4 et IPV6 :

```
# netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      all-systems.mcast.net
lo              1      ff02::1
eth0            1      ff02::202
eth0            1      ff02::1:ffe2:b42e
eth0            1      ff02::1
```

La commande tcpdump

La commande d'analyse réseau tcpdump permet de capturer les paquets transitant sur le réseau.

```
# yum -y install tcpdump
```

Pour afficher les interfaces disponibles :

```
# tcpdump -D
1.eth0
2.usbmon1 (USB bus number 1)
3.any (Pseudo-device that captures on all interfaces)
4.lo
```

Pour capturer les paquets sur l'interface eth0 (CTRL-C pour arrêter) :

```
# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:38:38.497076 IP formateur.home.ssh > PosteSpherius.home.sdclient: Flags [P.], seq
1286564342:1286564538, ack 1880827162, win 178, length 196
15:38:38.497658 IP formateur.home.58385 > gestionbbox.lan.home.domain: 28311+ PTR?
1.1.168.192.in-addr.arpa. (42)
15:38:38.498265 IP PosteSpherius.home.sdclient > formateur.home.ssh: Flags [.], ack 196,
win 251, length 0
15:38:38.506344 IP gestionbbox.lan.home.domain > formateur.home.58385: 28311* 1/0/0 PTR
PosteSpherius.home. (74)
15:38:38.506732 IP formateur.home.54691 > gestionbbox.lan.home.domain: 19559+ PTR?
7.1.168.192.in-addr.arpa. (42)
15:38:38.515665 IP gestionbbox.lan.home.domain > formateur.home.54691: 19559* 1/0/0 PTR
formateur.home. (70)
15:38:38.515842 IP formateur.home.41651 > gestionbbox.lan.home.domain: 27300+ PTR?
254.1.168.192.in-addr.arpa. (44)
15:38:38.516646 IP formateur.home.ssh > PosteSpherius.home.sdclient: Flags [P.], seq
196:392, ack 1, win 178, length 196
15:38:38.524473 IP gestionbbox.lan.home.domain > formateur.home.41651: 27300* 1/0/0 PTR
gestionbbox.lan.home. (78)
15:38:38.525845 IP formateur.home.ssh > PosteSpherius.home.sdclient: Flags [P.], seq
392:1356, ack 1, win 178, length 964
15:38:38.526660 IP formateur.home.ssh > PosteSpherius.home.sdclient: Flags [P.], seq
1356:1520, ack 1, win 178, length 164
... sortie tronquée
```

L'option '-c' permet de capturer le nombre de paquets spécifiés :

```
# tcpdump -c 4 -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:42:40.476651 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags   [P.],
seq 2904686810:2904687006, ack 3818110767, win 18144, length 196
15:42:40.477192 IP formateur.home.50025 > gestionbbox.lan.home.domain: 22806+ PT  R?
1.1.168.192.in-addr.arpa. (42)
15:42:40.477840 IP PosteSpherius.home.appleugcontrol > formateur.home.ssh: Flags   [.],
ack 196, win 63992, length 0
15:42:40.485892 IP gestionbbox.lan.home.domain > formateur.home.50025: 22806* 1/  0/0 PTR
PosteSpherius.home. (74)
4 packets captured
9 packets received by filter
0 packets dropped by kernel
```

L'option '-A' pour un affichage en mode ASCII :

```
# tcpdump -A -c 2 -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:43:45.817672 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 2904688950:2904689146, ack 3818112031, win 18144, length 196
E.....@.@.............   ."     6....P.F..7....9.....3.a..)...^......w.M..>.:.
{hy.^.Hh...2..#.H..T.p..s..m.Z.r....9'.M.+ZB.bK...T...L
r.b.p.......+......5.7<.d`l.......      ..K.T.~..       R..%......
+J.KO3..X.g3..c.`....6<ql..I.3..,.....=.`.Q.B....vYh
15:43:45.818320 IP formateur.home.36455 > gestionbbox.lan.home.domain: 30492+ PTR?
1.1.168.192.in-addr.arpa. (42)
E..F..@.@.............g.5.2..w............1.1.168.192.in-addr.arpa.....
2 packets captured
9 packets received by filter
0 packets dropped by kernel
```

L'option '-XX' pour un affichage ASCII et hexadécimal :

```
# tcpdump -XX -c 2 -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:44:18.755696 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 2904691222:2904691418, ack 3818113279, win 18144, length 196
        0x0000:  f8b1 56e4 626f 0800 27e2 b42e 0800 4510  ..V.bo..'.....E.
        0x0010:  00ec caaf 4000 4006 ebf3 c0a8 0107 c0a8  ....@.@.........
        0x0020:  0101 0016 0920 ad22 1216 e393 c8ff 5018  ........."......P.
        0x0030:  46e0 8437 0000 45e0 2f25 bb65 cb9b 22d0  F..7..E./%.e..".
        0x0040:  db5e d9f1 da5c bc53 e17a 1775 ea47 21ad  .^...\.S.z.u.G!.
        0x0050:  7c45 2a68 de88 06f7 a406 bd30 bb61 de3a  |E*h.......0.a.:
        0x0060:  7289 2cfc b044 27e7 be21 ee86 6734 80db  r.,..D'..!..g4..
        0x0070:  99b3 e0ae 25aa eb3f f595 79b6 55d3 7f72  ....%..?..y.U..r
        0x0080:  55ba f22d 827a 7e68 1439 6ec9 1ebf 2d86  U..-.z~h.9n...-.
        0x0090:  3d18 f5f9 38b9 23d5 1047 33f6 3b81 4151  =...8.#..G3.;.AQ
        0x00a0:  36fd d911 c639 fc42 1561 193f 86a2 91b4  6....9.B.a.?....
        0x00b0:  d7d2 d93b 7408 832d 9ac3 d83b 5075 ce92  ...;t..-...;Pu..
        0x00c0:  bd40 32cc 1656 ada1 c131 8652 5369 c90d  .@2..V...1.RSi..
        0x00d0:  386a f5bd 26b2 034f 2cc7 abd1 dfc9 e87b  8j..&..O,......{
        0x00e0:  8896 3792 03cc 03f9 bf82 427a bd00 ed55  ..7.......Bz...U
        0x00f0:  e685 f772 d213 16e4 4f5f                 ...r....O_
15:44:18.756191 IP formateur.home.59371 > gestionbbox.lan.home.domain: 443+ PTR?
1.1.168.192.in-addr.arpa. (42)
        0x0000:  9001 3bcf e859 0800 27e2 b42e 0800 4500  ..;..Y..'.....E.
        0x0010:  0046 395f 4000 4011 7cf2 c0a8 0107 c0a8  .F9_@.@.|.......
        0x0020:  01fe e7eb 0035 0032 8499 01bb 0100 0001  .....5.2........
        0x0030:  0000 0000 0000 0131 0131 0331 3638 0331  .......1.1.168.1
        0x0040:  3932 0769 6e2d 6164 6472 0461 7270 6100  92.in-addr.arpa.
        0x0050:  000c 0001                                ....
2 packets captured
9 packets received by filter
0 packets dropped by kernel
```

L'option '-w nom_fichier' permet de sauvegarder la sortie dans un fichier au format .pcap. :

```
# tcpdump -w snif -c 3 -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

```
# file snif
snif: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535
```

L'option '-r' permet de lire ce fichier :

```
# tcpdump -r snif
reading from file snif, link-type EN10MB (Ethernet)
15:47:42.819677 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 2904702590:2904702722, ack 3818119639, win 20832, length 132
15:47:42.820806 IP PosteSpherius.home.appleugcontrol > formateur.home.ssh: Flags [.], ack
132, win 63900, length 0
15:47:42.921083 IP theo-spherius.home.50070 > 239.255.255.250.ssdp: UDP, length 133
```

L'option '-n' pour un affichage numérique (sans résolution de noms) :

```
# tcpdump -n -c 2 -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:49:35.823786 IP 192.168.1.7.ssh > 192.168.1.1.appleugcontrol: Flags [P.], seq
2904706882:2904707078, ack 3818122807, win 22176, length 196
15:49:35.824769 IP 192.168.1.7.ssh > 192.168.1.1.appleugcontrol: Flags [P.], seq 196:392,
ack 1, win 22176, length 196
2 packets captured
3 packets received by filter
0 packets dropped by kernel
```

Pour afficher que les paquets TCP :

```
# tcpdump -c 2 -i eth0 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:50:08.706649 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 2904708954:2904709150, ack 3818124211, win 22176, length 196
15:50:08.707880 IP PosteSpherius.home.appleugcontrol > formateur.home.ssh: Flags [.], ack
196, win 65040, length 0
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Pour afficher que les paquets UDP :

```
# tcpdump -c 2 -i eth0 udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:51:17.996615 IP Baranger-PC.home.64618 > 239.255.255.250.ssdp: UDP, length 133
15:51:17.997388 IP formateur.home.36521 > gestionbbox.lan.home.domain: 25022+ PTR?
250.255.255.239.in-addr.arpa. (46)
2 packets captured
9 packets received by filter
0 packets dropped by kernel
```

Pour afficher que les paquets sur un port spécifique :

```
# tcpdump -c 2 -i eth0 port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:52:32.526643 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 2904712054:2904712250, ack 3818126031, win 23520, length 196
15:52:32.527880 IP PosteSpherius.home.appleugcontrol > formateur.home.ssh: Flags [.], ack
196, win 65040, length 0
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Pour afficher que les paquets provenant d'une adresse IP spécifique :

```
# tcpdump -c 2 -i eth0 src 192.168.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:53:52.651740 IP PosteSpherius.home.appleugcontrol > formateur.home.ssh: Flags [.], ack
2904714166, win 65040, length 0
15:53:52.882321 IP PosteSpherius.home.appleugcontrol > formateur.home.ssh: Flags [.], ack
165, win 64876, length 0
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Pour afficher que les paquets sortant vers une adresse IP spécifique :

```
# tcpdump -c 2 -i eth0 dst 192.168.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:55:16.300711 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 2904715758:2904715954, ack 3818128319, win 23520, length 196
15:55:16.319693 IP formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.],
seq 196:392, ack 1, win 23520, length 196
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

L'option '-v' permet un affichage verbeux :

```
# tcpdump -v -c 1 -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:55:49.235983 IP (tos 0x10, ttl 64, id 52272, offset 0, flags [DF], proto TCP (6),
length 92)
    formateur.home.ssh > PosteSpherius.home.appleugcontrol: Flags [P.], cksum 0x83a7
(incorrect -> 0xe48f), seq 2904718850:2904718902, ack 3818130659, win 23520, length 52
1 packets captured
7 packets received by filter
0 packets dropped by kernel
```

Exemple de capture avec un protocole non sécurisé :

```
# tcpdump -A src 192.168.1.1 and dst 192.168.1.7 and port ftp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
16:27:06.221115 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [S], seq
3666606626, win 8192, options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
E..4..@...]W........    ......"...... ..f..............
16:27:06.222050 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [.], ack
2604983982, win 8192, length 0
E..(..@...]b........    ......#.D..P. ..........
16:27:06.424666 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [.], ack 21,
win 8172, length 0
E..(..@...]a........    ......#.D..P............
16:27:07.849910 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [P.], seq
0:11, ack 21, win 8172, length 11
E..3..@...]T........    ......#.D..P.......USER theo

16:27:08.058578 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [.], ack 55,
win 8138, length 0
E..(..@...]].........    ........D..P....#........
16:27:08.826026 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [P.], seq
11:22, ack 55, win 8138, length 11
E..3..@...]P........    ........D..P.......PASS theo

16:27:09.137973 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [.], ack 78,
win 8115, length 0
E..(..@...]Y........    ......9.D..P............
16:27:19.690718 IP PosteSpherius.home.netadmin > formateur.home.ftp: Flags [R.], seq
878613020, ack 2770135450, win 0, length 0
E..(. @...]W........    ...4^......P............
16:27:21.478084 IP PosteSpherius.home.madge-ltd > formateur.home.ftp: Flags [P.], seq
22:28, ack 78, win 8115, length 6
E...."@...]O........    ......9.D..P....k..XPWD
```

Le login (theo) et le mot de passe (theo) sont visibles ainsi que la commande tapée (pwd).

La commande ss

La commande ss est destinée à remplacer la commande netstat. Elle permet notamment une analyse plus fines des sockets réseaux.

Elle permet de lister toutes les connexions.

```
# ss | more
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
u_str  ESTAB      0      0      @/tmp/dbus-gA3NXMZM6o 26316                 * 26315
u_str  ESTAB      0      0      /run/systemd/journal/stdout 17418                 * 17417
u_str  ESTAB      0      0      /run/systemd/journal/stdout 74298                 * 74294
u_str  ESTAB      0      0                    * 25436                 * 25437
u_str  ESTAB      0      0                    * 21225                 * 21226
u_str  ESTAB      0      0      /var/run/dbus/system_bus_socket 28732                 *
28731
u_str  ESTAB      0      0                    * 27930                 * 27931
u_str  ESTAB      0      0                    * 26770                 * 26773
u_str  ESTAB      0      0      /run/user/1000/pulse/native 26538                 * 26537
u_str  ESTAB      0      0      /run/systemd/journal/stdout 71344                 * 71343
u_str  ESTAB      0      0                    * 19240                 * 19241
u_str  ESTAB      0      0                    * 26412                 * 26413
```

Pour lister que les connexions tcp :

```
# ss -t | more
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
ESTAB      0      64            192.168.1.5:ssh           192.168.1.2:piccolo
```

L'option n permet un affichage numérique :

```
# ss -nt | more
State      Recv-Q Send-Q        Local Address:Port          Peer Address:Port
ESTAB      0      64              192.168.1.5:22            192.168.1.2:2787
```

Pour lister que les connexions udp :

```
# ss -u | more
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
```

```
# ss -ua | more
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
UNCONN     0      0                      *:bootpc                  *:*
UNCONN     0      0                      *:sunrpc                  *:*
UNCONN     0      0                      *:ntp                     *:*
UNCONN     0      0                      *:7309                    *:*
UNCONN     0      0                      *:50342                   *:*
UNCONN     0      0                      *:mdns                    *:*
UNCONN     0      0                      *:34044                   *:*
UNCONN     0      0                127.0.0.1:rpki-rtr               *:*
UNCONN     0      0                      *:mcns-sec                *:*
UNCONN     0      0                127.0.0.1:859                   *:*
UNCONN     0      0                     :::sunrpc                 :::*
UNCONN     0      0                     :::ntp                    :::*
UNCONN     0      0                     :::47322                  :::*
UNCONN     0      0                    ::1:rpki-rtr                :::*
UNCONN     0      0                     :::mcns-sec                :::*
UNCONN     0      0                     :::16150                  :::*
```

Remarque: L'option '-a' liste toutes les connexions mêmes celles qui ne sont pas établies.
Pour lister les sockets unix :

```
# ss -x | more
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
u_str  ESTAB      0      0      @/tmp/dbus-gA3NXMZM6o 26316                * 26315
u_str  ESTAB      0      0      /run/systemd/journal/stdout 17418               * 17417
u_str  ESTAB      0      0      /run/systemd/journal/stdout 74298               * 74294
u_str  ESTAB      0      0                    * 25436                 * 25437
u_str  ESTAB      0      0                    * 21225                 * 21226
u_str  ESTAB      0      0      /var/run/dbus/system_bus_socket 28732                *
28731
u_str  ESTAB      0      0                    * 27930                 * 27931
u_str  ESTAB      0      0                    * 26770                 * 26773
```

Pour lister les connexions dans l'état LISTENING :

```
# ss -lt
State       Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
LISTEN      0      100                                         127.0.0.1:smtp
*:*
LISTEN      0      128                                           *:44040
*:*
LISTEN      0      128                                           *:sunrpc
*:*
LISTEN      0      128                                           *:ssh
*:*
LISTEN      0      128                                         127.0.0.1:ipp
*:*
LISTEN      0      100                                        ::1:smtp
:::*
LISTEN      0      128                                         :::sunrpc
:::*
LISTEN      0      128                                         :::47407
:::*
LISTEN      0      128                                         :::ssh
:::*
LISTEN      0      128                                        ::1:ipp
:::*
```

Pour lister les PID associés :

```
# ss -lpt
State       Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
LISTEN      0      100                                         127.0.0.1:smtp
*:*         users:(("master",2522,13))
LISTEN      0      128                                           *:44040
*:*         users:(("rpc.statd",18067,9))
LISTEN      0      128                                           *:sunrpc
*:*         users:(("rpcbind",18271,9))
LISTEN      0      128                                           *:ssh
*:*         users:(("sshd",17774,3))
LISTEN      0      128                                         127.0.0.1:ipp
*:*         users:(("cupsd",17878,12))
LISTEN      0      100                                        ::1:smtp
:::*        users:(("master",2522,14))
LISTEN      0      128                                         :::sunrpc
:::*        users:(("rpcbind",18271,12))
LISTEN      0      128                                         :::47407
:::*        users:(("rpc.statd",18067,11))
LISTEN      0      128                                         :::ssh
:::*        users:(("sshd",17774,4))
LISTEN      0      128                                        ::1:ipp
```

```
:::*        users:(("cupsd",17878,11))
```

Pour afficher le timer :

```
# ss -ot
State       Recv-Q Send-Q                                    Local Address:Port
Peer Address:Port
ESTAB       0      64                                          192.168.1.5:ssh
192.168.1.2:piccolo  timer:(on,381ms,0)
```

Pour afficher les statistiques réseaux :

```
# ss -s
Total: 579 (kernel 597)
TCP:   12 (estab 1, closed 1, orphaned 0, synrecv 0, timewait 0/0), ports 0

Transport Total     IP        IPv6
*         597       -         -
RAW       1         0         1
UDP       16        10        6
TCP       11        6         5
INET      28        16        12
FRAG      0         0         0
```

Pour afficher les connexions dans l'état 'established' :

```
# ss state established
Netid Recv-Q Send-Q                                    Local Address:Port
Peer Address:Port
u_str 0      0                                  @/tmp/dbus-gA3NXMZM6o 26316
* 26315
u_str 0      0                            /run/systemd/journal/stdout 17418
* 17417
u_str 0      0                            /run/systemd/journal/stdout 74298
* 74294
u_str 0      0                                                    * 25436
* 25437
```

Pour afficher les connexions TCP ipv4 dans l'état 'established' :

```
# ss -t4 state established
Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
0      64                                        192.168.1.5:ssh
192.168.1.2:piccolo
```

Pour afficher les connexions ipv6 :

```
# ss -t6 -a
State       Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
LISTEN      0      100                                           ::1:smtp
:::*
LISTEN      0      128                                            :::sunrpc
:::*
LISTEN      0      128                                            :::47407
:::*
LISTEN      0      128                                            :::ssh
:::*
LISTEN      0      128                                           ::1:ipp
:::*
```

Pour afficher les connexions sur le port de destination ou de source 22 :

```
# ss -at '( dport = :22 or sport = :22 )'
State       Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
LISTEN      0      128                                             *:ssh
*:*
ESTAB       0      64                                    192.168.1.5:ssh
192.168.1.2:piccolo
LISTEN      0      128                                            :::ssh
:::*
```

La même chose avec une syntaxe plus synthétique :

```
# ss -at dst :22 or src :22
State       Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
LISTEN      0      128                                             *:ssh
*:*
ESTAB       0      64                                    192.168.1.5:ssh
192.168.1.2:piccolo
LISTEN      0      128                                            :::ssh
:::*
```

Pour lister les connexions sur un hôte :

```
# ss -nt dst 192.168.1.2
State       Recv-Q Send-Q                                    Local Address:Port
Peer Address:Port
ESTAB       0      64                                          192.168.1.5:22
192.168.1.2:2787
```

```
# ss -nt dst 192.168.1.2/24
State       Recv-Q Send-Q                                    Local Address:Port
Peer Address:Port
ESTAB       0      64                                          192.168.1.5:22
192.168.1.2:2787
```

```
# ss -nt dst 192.168.1.2:22
State       Recv-Q Send-Q                                    Local Address:Port
Peer Address:Port
```

```
# ss -nt dst 192.168.1.2:2787
State       Recv-Q Send-Q                                    Local Address:Port
Peer Address:Port
ESTAB       0      64                                          192.168.1.5:22
192.168.1.2:2787
```

```
# ss -nt src 192.168.1.2:22
State      Recv-Q Send-Q                                   Local Address:Port
Peer Address:Port
```

```
# ss -nt src 192.168.1.2:2787
State      Recv-Q Send-Q                                   Local Address:Port
Peer Address:Port
```

```
# ss -nt src 192.168.1.5:22
State      Recv-Q Send-Q                                   Local Address:Port
Peer Address:Port
ESTAB      0      64                                         192.168.1.5:22
192.168.1.2:2787
```

Pour lister les connexions dont le port source est supérieur ou égal à 22 et le port de destination inférieur ou égal à 443 :

```
# ss -t '( sport >= :22 or dport <= :443 )'
State      Recv-Q Send-Q                                  Local Address:Port
Peer Address:Port
ESTAB      0      64                                       192.168.1.5:ssh
192.168.1.2:piccolo
```

Administration réseau

Le filtrage de paquets réseaux: netfilter et iptables

- Présentation de netfilter
- La table filter
- Les commandes iptables
- Sauvegarder sa configuration iptables

Le filtrage de paquets réseaux : netfilter et iptables

Netfilter s'exécute au niveau du noyau pour identifier l'action à entreprendre lorsqu'il reçoit un paquet. Sa fonction primaire est de jouer le rôle d'un pare-feu (table filter: table par défaut). Il peut jouer le rôle de traduction d'adresses (table NAT) pour partager une connexion internet. Il peut aussi masquer des machines du réseau local ou rediriger les connexions (table forward).

La commande permettant de configurer netfilter est iptables.

Les commandes iptables sont assez complexes lorsqu'on n'est pas familiarisé avec. Créer des règles de filtrage avec l'interface graphique puis analyser les commandes correspondantes est une bonne manière pour se familiariser avec la syntaxe de la commande iptables.

Pour la table filter il existe par défaut 3 chaînes de filtrage :

- chaîne INPUT : filtrer les paquets entrants,

- chaîne OUPUT : filtrer les paquets sortants,

- chaîne FORWARD : filtrer les paquets à transférer.

Lorsqu'un paquet arrive dans une chaîne, netfilter agit de la façon suivante :

- comparaison avec la 1ère règle,

- si correspondance, netfilter applique l'action (drop, reject, accept, log, …),

- si pas de correspondance, comparaison avec la règle suivante, jusqu'à la dernière règle,

- si aucune règle ne correspond, application de la politique par défaut. ATTENTION : la politique par défaut est souvent d'accepter le paquet.

Les actions ou cibles sont :

ACCEPT : accepter le paquet,

REJECT : refuser le paquet en avertissant le demandeur,

DROP : refuser le paquet sans avertir le demandeur,

LOG : enregistre les paquets dans les logs systèmes.

Pour visualiser la configuration :

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Entre parenthèses apparaît la politique par défaut (policy ACCEPT).

Modification de l'action par défaut de la chaîne INPUT :

```
# iptables -P INPUT DROP

# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Suppression des règles du pare-feu (attention cela ne modifie pas les politiques par défaut des chaînes) :

```
# iptables -F

# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

Pour autoriser ssh en entrée et en sortie :

```
# iptables -I INPUT -p tcp --dport 22 -j ACCEPT
# iptables -I OUTPUT -p tcp --sport 22 -j ACCEPT

# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
```

L'option -n permet un affichage numérique :

```
# iptables -L -n
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:22
```

```
# iptables -L -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:22
```

Suppression d'une règle :

```
# iptables -D OUTPUT 1
```

Sauvegarde des règles :

```
# service iptables save
iptables : Sauvegarde des règles du pare-feu dans /etc/sysc[  OK  ]tables :

# more /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue Feb  2 16:44:46 2016
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT DROP [2:140]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
COMMIT
# Completed on Tue Feb  2 16:44:46 2016
```

Administration réseau

Le filtrage de paquets réseaux: firewalld

- remplace iptables pour configurer netfilter
- utilisation de zones de confiance
- /etc/firewalld /etc/firewalld/firewalld.conf
- firewall-config: interface graphique de gestion des règles

Le filtrage de paquets : firewalld

Firewalld est le remplaçant de iptables pour configurer le filtrage de paquets avec netfilter. La configuration de firewalld est stocké dans le répertoire /etc/firewalld. Certaines zones sont configurées par défaut avec des règles.

Afficher le statut de firewalld.

```
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
enabled)
   Active: active (running) since ven. 2017-03-10 11:17:12 CET; 30min ago
     Docs: man:firewalld(1)
 Main PID: 715 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─715 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

mars 10 11:17:10 poste-linux systemd[1]: Starting firewalld - dynamic firewall daemon...
mars 10 11:17:12 poste-linux systemd[1]: Started firewalld - dynamic firewall daemon.
```

```
# firewall-cmd --state
running
```

Afficher la zone par défaut

```
# firewall-cmd --get-default-zone
public
```

Afficher les zones actives associés à des interfaces

```
# firewall-cmd --get-active-zone
public
  interfaces: enp0s3 enp0s8
```

Affichez la zone associée à une interface.

```
# firewall-cmd --get-zone-of-interface=eth0
no zone
# firewall-cmd --get-zone-of-interface=enp0s3
public
```

Afficher toutes les zones disponibles.

```
# firewall-cmd --get-zones
work drop internal external trusted home dmz public block
```

Modifier la zone par défaut

```
# firewall-cmd --set-default-zone=home
success
# firewall-cmd --get-default-zone
home
```

Afficher la configuration permanente d'une zone.

```
# firewall-cmd --permanent --zone=public --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
```

```
# firewall-cmd --permanent --zone=home --list-all
home
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client mdns samba-client ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
```

Création d'une zone personnalisée.

```
# firewall-cmd --permanent --new-zone=test_zone
success
```

Rechargement de la configuration.

```
# firewall-cmd --reload
success
```

Ajouter une source à une zone.

```
# firewall-cmd --permanent --zone=dmz --add-source=192.168.2.0/24
success
# firewall-cmd --permanent --zone=dmz --add-source=00:11:22:33:44:55
success
# firewall-cmd --reload
success
```

Afficher les sources associées à une zone

```
# firewall-cmd --permanent --zone=dmz --list-sources
00:11:22:33:44:55 192.168.2.0/24
```

Configurer une plage d'adresses ip et l'associer à une source

```
# firewall-cmd --permanent --new-ipset=my_ip_list --type=hash:ip
success
# firewall-cmd --reload
success
# firewall-cmd  --ipset=my_ip_list --add-entry=192.168.1.100
success
# firewall-cmd  --ipset=my_ip_list --add-entry=192.168.1.101
success
# firewall-cmd  --ipset=my_ip_list --add-entry=192.168.1.102
success
# firewall-cmd --permanent --zone=dmz --add-source=ipset:my_ip_list
success
# firewall-cmd --reload
success
```

```
# firewall-cmd --permanent --zone=dmz --list-sources
00:11:22:33:44:55 192.168.2.0/24 ipset:my_ip_list
```

```
# firewall-cmd --info-zone=dmz
dmz (active)
  target: default
  icmp-block-inversion: no
  interfaces:
  sources: 00:11:22:33:44:55 192.168.2.0/24 ipset:my_ip_list
  services: ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  sourceports:
  icmp-blocks:
  rich rules:
```

La commande iptables permet aussi de visualiser les règles du pare-feu configuré avec firewalld.

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:bootps
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
INPUT_direct  all  --  anywhere            anywhere
INPUT_ZONES_SOURCE  all  --  anywhere           anywhere
INPUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             192.168.122.0/24     ctstate RELATED,ESTABLISHED
ACCEPT     all  --  192.168.122.0/24     anywhere
ACCEPT     all  --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-
unreachable
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-
unreachable
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
FORWARD_direct  all  --  anywhere            anywhere
FORWARD_IN_ZONES_SOURCE  all  --  anywhere           anywhere
FORWARD_IN_ZONES  all  --  anywhere             anywhere
FORWARD_OUT_ZONES_SOURCE  all  --  anywhere           anywhere
FORWARD_OUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootpc
OUTPUT_direct  all  --  anywhere            anywhere

Chain FORWARD_IN_ZONES (1 references)
target     prot opt source               destination
FWDI_public  all  --  anywhere             anywhere             [goto]
FWDI_public  all  --  anywhere             anywhere             [goto]
FWDI_public  all  --  anywhere             anywhere             [goto]

Chain FORWARD_IN_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_OUT_ZONES (1 references)
target     prot opt source               destination
FWDO_public  all  --  anywhere             anywhere             [goto]
FWDO_public  all  --  anywhere             anywhere             [goto]
FWDO_public  all  --  anywhere             anywhere             [goto]

Chain FORWARD_OUT_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_direct (1 references)
target     prot opt source               destination

Chain FWDI_public (3 references)
target     prot opt source               destination
FWDI_public_log  all  --  anywhere             anywhere
FWDI_public_deny  all  --  anywhere             anywhere
```

```
FWDI_public_allow  all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere

Chain FWDI_public_allow (1 references)
target     prot opt source               destination

Chain FWDI_public_deny (1 references)
target     prot opt source               destination

Chain FWDI_public_log (1 references)
target     prot opt source               destination

Chain FWDO_public (3 references)
target     prot opt source               destination
FWDO_public_log  all  --  anywhere             anywhere
FWDO_public_deny  all  --  anywhere             anywhere
FWDO_public_allow  all  --  anywhere             anywhere

Chain FWDO_public_allow (1 references)
target     prot opt source               destination

Chain FWDO_public_deny (1 references)
target     prot opt source               destination

Chain FWDO_public_log (1 references)
target     prot opt source               destination

Chain INPUT_ZONES (1 references)
target     prot opt source               destination
IN_public  all  --  anywhere             anywhere            [goto]
IN_public  all  --  anywhere             anywhere            [goto]
IN_public  all  --  anywhere             anywhere            [goto]

Chain INPUT_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain INPUT_direct (1 references)
target     prot opt source               destination

Chain IN_public (3 references)
target     prot opt source               destination
IN_public_log  all  --  anywhere             anywhere
IN_public_deny  all  --  anywhere             anywhere
IN_public_allow  all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere

Chain IN_public_allow (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh ctstate NEW

Chain IN_public_deny (1 references)
target     prot opt source               destination

Chain IN_public_log (1 references)
target     prot opt source               destination

Chain OUTPUT_direct (1 references)
target     prot opt source               destination
```

Notes

Présentation de services réseaux

Dans ce chapitre, nous allons étudier la configuration de certains services et le partage de fichiers via NFS.

Table des matières

Présentation de services réseau

Le super-démon réseau xinetd

- Le répertoire /etc/xinetd.d
- Activer un service sous le contrôle de xinetd

Le super-démon réseau xinetd

Le répertoire /etc/xinetd.d contient une liste de services réseaux qui sont sous le contrôle de xinetd.

Chaque service a un fichier de configuration qui porte son nom. Lorsque l'on installe un nouveau service, le paramètre disable est positionné sur yes par défaut. Il faut le positionner à no pour activer le service. Puis le démon xinetd doit être rechargé.

Exemple avec le fichier de configuration de telnet serveur après installation du package :

```
# more /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Pour activer telnet, on modifie le fichier de configuration et on relance xinetd.

```
# more /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
}
```

```
# service xinetd reload
Rechargement de la configuration :                         [  OK  ]
```

Le port 23 de telnet est bien dans l 'état LISTEN, donc actif en écoute du réseau :

```
# netstat -atnl | more
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:40550               0.0.0.0:*                   LISTEN
tcp        1      0 192.168.1.6:49814           23.200.86.151:80            CLOSE_WAIT
tcp        0     64 192.168.1.6:22              192.168.1.1:5559            ESTABLISHED
tcp        0      0 :::111                      :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::23                       :::*                        LISTEN
tcp        0      0 ::1:631                     :::*                        LISTEN
tcp        0      0 ::1:25                      :::*                        LISTEN
tcp        0      0 :::38396                    :::*                        LISTEN
```

Remarque : depuis la version 7 de RedHat, telnet n'est pas sous le contrôle de xinetd mais de systemd. Pour démarrer votre serveur telnet :

```
# systemctl start telnet.socket
# netstat -tulpn | grep ':23'
tcp6       0      0 :::23                   :::*                    LISTEN      1/systemd
```

Présentation de services réseau

Le partage d'arborescence entre machines Linux: NFS

Serveur NFS

Service

Démon

Fichiers de configuration

Les commandes

Le partage d'arborescence entre machines Linux: NFS

NFS (Network FileSystem) est le système de partage d'arborecence sous Linux. Un serveur NFS met à disposition une ressource qui est un répertoire. Ce répertoire peut-être partagé pour toutes les machines du réseau ou pour des machines spécifiques. Des options NFS permettent de contrôler le comportement du partage. Le fichier contenant les partages NFS est le fichier /etc/exports.

Exemple de fichier /etc/exports

```
serverNFS # cat /etc/exports
/export/rep1 *
/export/rep2 *(rw)
/export/rep3 192.168.1.3(rw,no_root_squash)
/export/rep4 *(rw,all_squash,anonuid=1001,anongid=100)
```

Demarrage du service NFS

```
serverNFS # systemctl start nfs.service
```

Visualisation des partages NFS

```
serverNFS # showmount -e
Export list for poste-linux:
/export/rep4 *
/export/rep2 *
/export/rep1 *
/export/rep3 192.168.1.3
```

La commande exportfs permet de visualiser les options de partage.

```
serverNFS # exportfs -v
/export/rep3
192.168.1.3(rw,wdelay,no_root_squash,no_subtree_check,sec=sys,rw,secure,no_root_squash,no
_all_squash)
/export/rep1
<world>(ro,wdelay,root_squash,no_subtree_check,sec=sys,ro,secure,root_squash,no_all_squas
h)
/export/rep2
<world>(rw,wdelay,root_squash,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squas
h)
/export/rep4
<world>(rw,wdelay,root_squash,all_squash,no_subtree_check,anonuid=1001,anongid=100,sec=sy
s,rw,secure,root_squash,all_squash)
```

Visualiser les partages d'un serveur NFS depuis un client

```
clientNFS # showmount -e 192.168.1.5
Export list for 192.168.1.5:
/export/rep4 *
/export/rep2 *
/export/rep1 *
/export/rep3 192.168.1.3
```

Effectuer le montage depuis le client

```
clientNFS # mount -t nfs 192.168.1.5:/export/rep1 /rep1
clientNFS # mount -t nfs 192.168.1.5:/export/rep2 /rep2
clientNFS # mount -t nfs 192.168.1.5:/export/rep3 /rep3
clientNFS # mount -t nfs 192.168.1.5:/export/rep4 /rep4
```

Tester en créant des fichiers

```
clientNFS # touch /rep1/fic1
touch: impossible de faire un touch « /rep1/fic1 »: Système de fichiers accessible en
lecture seulement
clientNFS # touch /rep2/fic1
clientNFS # touch /rep3/fic1
clientNFS # touch /rep4/fic1
clientNFS # ls -l /rep[1-4]
/rep1:
total 0

/rep2:
total 0
-rw-r--r--. 1 nfsnobody nfsnobody 0 23 mars  11:12 fic1

/rep3:
total 0
-rw-r--r--. 1 root root 0 23 mars  11:12 fic1

/rep4:
total 0
-rw-r--r--. 1 1001 users 0 23 mars  11:12 fic1
```

Pour que le montage soit effectif au démarrage de la machine il faut ajouter une entrée dans le fichier /etc/fstab.

```
clientNFS # grep /rep2 /etc/fstab
192.168.1.5:/export/rep2        /rep2           nfs     bg,soft 0 0
```

Evidemment, les options de montage locales sont applicables pour des montages NFS. Par contre, coté client, on ne peut pas outrepasser les limitations fixées coté serveur NFS.

Pour automatiser le montage NFS lors de la séquence de boot, utiliser l'option bg qui permet d'indiquer au système d'effectuer des tentatives de montage en arrière plan lorsque le serveur NFS ne répond pas. Ceci a pour effet d'éviter de bloquer une séquence de démarrage d'un client lorsque le serveur NFS est indisponible. Cette option bg (background) s'oppose à fg (foreground) qui est la valeur par défaut.
Une autre option peut être exploitée, il s'agit de soft qui permet d'indiquer au système qu'après n retry tentatives de connexions NFS qui auraient échouées, il faut abandonner. Elle s'oppose à hard qui est la valeur par défaut et qui tente des connexions de manière infinie.

Présentation de services réseau

Les commandes SSH

- ssh

```
$ ssh  -l theo   mars
$ ssh  theo@mars

$ ssh  root@mars  cat /etc/passwd
```

- scp

```
$ scp  [options_ssh]  user@machine:/fichier_source  /fichier
$ scp  [options_ssh]  /fichier  user@machine:/fichier_destination
```

- sftp

```
$ sftp  [options_ssh]  machine
cd chemin       lcd chemin          exit ou quit ou bye
                get fic         mget fic*
                put fic         mput fic*
```

Les commandes SSH

SSH est un mécanisme qui permet une communication entre machines de façon sécurisé, toute la communication étant cryptée.

Le mécanisme SSH repose sur l'existence d'une pair de clefs : la clef publique et la clef privée.
La clef publique est envoyée sur les serveurs auxquels nous voulons nous connecter, la clef privée étant conservée bien précieusement sur la machine sur laquelle nous nous connectons.

Les commandes clientes SSH (Secure Shell) sont des commandes de communications sécurisées, utilisant des clés d'authentification RSA ou DSA : ssh, scp, sftp.

La commande ssh

La commande ssh sert à ce connecter à une machine distante ou à exécuter une séquence de commande sur une machine distante.

$ ssh -l nom_utilisateur machine_distante [séquence_de_commandes]

$ ssh nom_utilisateur@machine_distante [séquence_de_commandes]

```
$ ssh  -l theo   mars
$ ssh  theo@mars

$ ssh  root@mars  cat /etc/passwd
```

Lors d'une première connexion sur un serveur avec SSH, le système demande si on veut ajouter le serveur à la liste des hôtes connus. En répondant « oui » à cette question, nous sauvegardons la clef publique du serveur dans le fichier $HOME/.ssh/known_hosts. Pour se connecter vous devez fournir le mot de passe de l'utilisateur avec lequel vous essayer de vous connecter sur le serveur.

La commande scp

La commande scp sert à copier des fichiers entre deux machines.

Pour récupérer des fichiers d'une machine distante :

```
$ scp [options_ssh] utilisateur@machine:/fichier_source /fichier_destination
```

Pour recopier des fichiers sur une machine distante :

```
$ scp [options_ssh] /fichier_source utilisateur@machine:/fichier_destination
```

La commande sftp

La commande sftp sert à transférer des fichiers entre deux machines.

```
$ sftp [ options_ssh ] machine
```

Cette commande a les sous commandes équivalentes à la commande 'ftp'.

Quelques sous commandes :

cd chemin	:	pour se déplacer sur l'arborescence de la machine distante.
lcd chemin	:	pour se déplacer sur l'arborescence de la machine locale.
get fichier	:	pour récupérer un fichier.
mget fic*	:	pour récupérer plusieurs fichiers.
put fichier	:	pour déposer un fichier.
mput fic*	:	pour déposer plusieurs fichiers.
exit ou quit ou bye	:	pour quitter ftp.

Les fichiers de configurations

Le fichier de configuration du serveur SSH : /etc/ssh/sshd_config

Le fichier de configuration des commandes clientes SSH : /etc/ssh/ssh_config

Le fichier $HOME/.ssh/authorized_keys : il est présent sur le poste serveur SSH. Il contient la liste des clés autorisées pour l'authentification utilisateur.

Le fichier $HOME/.ssh/known_hosts : il est présent sur le poste client SSH. Il contient la liste des clés autorisées pour l'authentification machine.

Présentation de services réseau

L'utilisation des clefs SSH

- Création de la clef sur le serveur maître

```
Serveur$  cd   $HOME/.ssh
Serveur$  ssh-keygen  -t  rsa  -f  ma_clef
Serveur$  ls  -l
    ma_clef     ma_clef.pub
```

- Mise à jour des serveurs clients

```
Serveur$ cd  .ssh
Serveur$ ssh-copy-id  -i ma_clef.pub  user1@Client

user1:Client$ cat  $HOME/.ssh/authorized_keys
```

- Vérification

```
user1:Client$ cat  $HOME/.ssh/authorized_keys
```

L'utilisation des clefs SSH

Les clefs doivent être créées sur le poste qui exécute la commande ssh, en l'occurrence sur le serveur maître. La clef publique sera localisée au sein du fichier authorized_keys des serveurs clients.

La clef ne sera pas nommée avec le nom par défaut (id_rsa ou id_dsa) mais avec un nom particulier (comm_serveur_key). L'avantage est de disposer d'une clef spécifique utilisée pour un usage bien particulier dans un contexte donné. Chaque application réseau disposera de sa propre clef de sécurité qui pourra être gérée de manière complètement autonome.

Création de la clef sur le serveur maître :

```
Serveur$  cd   $HOME/.ssh
Serveur$  ssh-keygen  -t  rsa  -f  ma_clef
Serveur$  ls  -l
    ma_clef     ma_clef.pub
```

Mise à jour des serveurs clients :

```
Serveur$ cd  .ssh
Serveur$ ssh-copy-id  -i ma_clef.pub  user1@Client

user1:Client$ cat  $HOME/.ssh/authorized_keys
```

Vérification :

```
Serveur$ ssh    -i $HOME/.ssh/ma_clef    user1@Client
```

Présentation de services réseau

Les serveurs DNS, DHCP et LDAP

- DNS Service de noms
- DHCP Service d'adressage réseau
- LDAP Service d'annuaire

Les serveurs DNS, DHCP, NFS et LDAP

Serveur DNS **Domain Name System**

Un serveur DNS est un serveur de noms de domaines.

Une machine a besoin de l'adresse IP d'une machine distante pour communiquer avec elle. Lorsqu'une commande utilise un nom de machine, il est donc nécessaire de récupérer l'adresse IP correspondante. Si cette résolution d'IP n'est pas faite un locale, un serveur DNS peut le faire.

Un serveur DNS centralise la correspondance entre des noms de machines et des adresses IP. Un serveur DNS se charge d'un domaine ou nom de domaine. Plusieurs serveurs DNS peuvent communiquer entre eux pour la résolution entre différents domaines.

L'infrastructure du web fonctionne avec ce type de serveurs.

Serveur DHCP **Dynamic Host Configuration Protocol**

Un serveur DCHP délivre des adresses IP aux machines clientes du réseau. C'est donc un fournisseur d'adressage réseau dynamique.

Ainsi, à chaque démarrage d'une machine cliente DHCP, le serveur lui fournira son adresse IP et sa configuration réseau.

L'intérêt est que la configuration réseau d'une machine n'est pas définie en locale, mais centralisée sur un serveur. Cela simplifie la gestion, l'administration et la maintenance des configurations réseaux des postes clients.

Serveur LDAP **Lightweight Dirctory Access Protocol**

Un serveur LDAP est un annuaire qui fournit des informations à la demande des clients LDAP.
Ces serveurs sont optimisés pour les opérations de lectures, donc pour répondre rapidement aux sollicitations des clients.

Ce type d'annuaire peut être configuré pour contenir un grand nombre d'informations de différents types. Il peut centraliser beaucoup de données de configuration indispensables à des machines clientes, telles que :

- la résolution de noms de machines en adresse IP,
- la définition des comptes utilisateurs,
- la résolution pour les numéros de réseaux,
- la correspondance entre des protocoles et des ports réseaux,
- etc...

Cette centralisation d'informations en simplifie la gestion, l'administration et la maintenance pour l'équipe d'administration de l'infrastructure informatique et réseau de l'entreprise.

Présentation de services réseau

Le serveur web: apache

- Installation des packages
- Le fichier de configuration d'apache : /etc/httpd/conf/httpd.conf
- Démarrage du serveur apache

Le serveur web: apache

Apache est un logiciel libre. Apache est un serveur http. Il permet d'héberger la configuration des sites internet. Apache inclut la fonctionnalité d'hôtes virtuels (virtualhosts) permettant d'héberger la configuration de plusieurs sites internet sur le même hôte physique.

Distribution Linux : CentOS 6.4

```
# cat /etc/redhat-release
CentOS release 6.4 (Final)
```

Version d'apache: 2.2

```
# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   Oct 16 2014 14:48:21
```

Site de documentation d'apache: http://httpd.apache.org/docs/

Le fichier de configuration d'apache s'appelle httpd.conf. Il se trouve dans le répertoire /etc/httpd/conf.

```
# cd /etc/httpd
# ls
conf  conf.d  logs  modules  run
# cd conf
# ls
httpd.conf  magic
```

Apache est un serveur modulaire. Les principales fonctionnalités sont intégrées dans le binaire. Les fonctionnalités supplémentaires sont appelées grâce à des modules externes.
Le répertoire 'modules' est un lien symbolique vers /usr/lib64/httpd/modules. Ce répertoire contient les modules utilisés par apache.

Les modules peuvent être inclus lors de la compilation d'apache ou être appelés de manière dynamique lorsque le serveur s'exécute. Il fait alors appel aux DSO (Dynamic Shared Object: objets partagés dynamiques). Pour cela, apache doit être compilé avec le module 'so' en plus du module 'core'.

Visualisation des modules avec lequels un serveur apache a été compilé. Ceci est possible avec les commandes httpd ou apachectl :

```
# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   Oct 16 2014 14:48:21
```

```
# httpd -l
Compiled in modules:
  core.c
  prefork.c
  http_core.c
  mod_so.c
```

```
# apachectl -v
Server version: Apache/2.2.15 (Unix)
Server built:   Oct 16 2014 14:48:21
```

```
# apachectl -l
Compiled in modules:
  core.c
  prefork.c
  http_core.c
  mod_so.c
```

Configuration d'apache pour héberger un site web :

Durant ce tutoriel, nous allons enregistrer un site web en local et y accéder. Par défaut, apache héberge qu'un seul site à la fois, sauf si on utilise des hôtes virtuels.

Explication des paramètres par défaut du fichier de configuration :

ServerTokens : indique comment apache s'identifie auprès des clients.
ServerRoot: indique où sont stockés les fichiers de configurations d'apache.
PidFile: indique l'endroit où est stocké le fichier 'pid' d'apache. C'est un chemin relatif par rapport à ServerRoot.
Timeout: indique en secondes le temps pendant lequel le serveur attend des émissions ou réceptions en cours de communication.
KeepAlive: indique qu'apache doit interdire les connexions TCP persistantes (plusieurs demandes par connexion).
MaxKeepAliveRequests: indique le nombre maximum de requêtes auxquelles apache répondra lors de la même connexion TCP.
KeepAliveTimeout: indique le nombre de secondes que doit attendre apache avant de clore une connexion TCP.
StartServers : Indique le nombre de processus httpd exécutés lors du démarrage du serveur.

```
# ps aux | grep httpd
root      7099  0.0  0.2 186224  3896 ?        Ss   15:19   0:00 /usr/sbin/httpd
apache    7102  0.0  0.1 186360  3080 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7103  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7104  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7105  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7106  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7107  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7108  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
apache    7109  0.0  0.1 186360  2448 ?        S    15:19   0:00 /usr/sbin/httpd
root     32463  0.0  0.0 105312   876 pts/1    S+   15:46   0:00 grep httpd
```

MinSpareServers: indique le nombre minimum de processus en écoute.
MaxSpareServers: indique le nombre maximum de processus en écoute.
ServerLimit:indique le nombre maximum de processus qui peuvent être lancés.
MaxClients: indique le nombre maximum de clients supportés (est égal à ServerLimit).
MaxRequestsPerChild: indique le nombre maximum de requêtes pour un processus enfant.

Listen : Indique le port d'écoute du serveur apache.

LoadModule: indique les différents modules qui sont chargés par apache.
Include conf.d/*.conf: indique qu'il faut prendre en compte tous les fichiers se terminant par .conf dans le répertoire /etc/httpd/conf.d.

User: indique à quel utilisateur appartiendront les processus fils apache.
Group: indique à quel groupe appartiendront les processus fils apache.

Modification la configuration du serveur apache pour héberger le site appelé site1 :

```
# diff httpd.conf httpd.conf.origin
277d276
< ServerName formateur.spherius.fr
293c292
< DocumentRoot "/var/www/html/site1"
---
> DocumentRoot "/var/www/html"
318c317
< <Directory "/var/www/html/site1">
---
> <Directory "/var/www/html">
```

```
# httpd -t
Syntax error on line 293 of /etc/httpd/conf/httpd.conf:
DocumentRoot must be a directory
```

Le répertoire /var/www/html/site1 n'a pas encore été créé comme l'indique le message d'erreur ci-dessus.

```
# mkdir /var/www/html/site1
# chmod 777 /var/www/html/site1
# httpd -t
Syntax OK
```

Maintenant, nous allons lancer un navigateur web et enregistrer la page sous le nom d'index.html dans le répertoire /var/www/html/site1 :

```
# ls /var/www/html/site1/
index_fichiers  index.html
```

Il ne reste plus qu'à relancer notre serveur apache et tester l'accès à la page :

```
# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Nous avons créé le premier serveur apache avec un accès non authentifié. Sécurisons notre site pour n'accepter que des utilisateurs qui s'authentifient.

Pour cela, nous allons modifier le fichier de configuration d'apache pour qu'il demande l'authentification. Il faut modifier le paramètre AllowOverride de la section <Directory "/var/www/html/site1"> pour qu'il prenne en compte le fichier .htaccess qui devra être placé dans le répertoire /var/www/html/site1.

```
# diff httpd.conf httpd.conf.origin
277d276
< ServerName formateur.spherius.fr
293c292
< DocumentRoot "/var/www/html/site1"
---
> DocumentRoot "/var/www/html"
318c317
< <Directory "/var/www/html/site1">
---
```

```
> <Directory "/var/www/html">
339c338
<     AllowOverride AuthConfig
---
>     AllowOverride None
```

```
# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

```
# more /var/www/html/site1/.htaccess
AuthType        Basic
AuthName        "Va t'en mannant"
AuthUserFile    /.http/site1/passwd_user
AuthGroupFile   /.http/site1/passwd_group
Require         valid-user
```

AuthType Basic: indique qu'il faut utiliser AuthUserFile pour l'authentification.
AuthName: indique ce qui sera affiché dans la bannière d'authentification.
AuthUserFile: indique le chemin d'accès absolu au fichier qui contiendra les utilisateurs (et les mots de passe) qui seront autorisés à se connecter.
AuthGroupFile: pour les groupes.
Require valid-user: indique qu'on autorise que des personnes authentifiés.

Ajoutons l'utilisateur user1 pour qu'il puisse accéder au site :

```
# htpasswd -c /.http/site1/passwd_user user1
htpasswd: cannot create file /.http/site1/passwd_user
# mkdir -p /.http/site1
# htpasswd -c /.http/site1/passwd_user user1
New password:
Re-type new password:
Adding password for user user1
```

L'option '-c' crée le fichier qui stocke les mots de passes (nota : il l'écrase s'il en existe déjà un).

Ajoutons les utilisateurs user2 et user3:

```
# htpasswd /.http/site1/passwd_user user2
New password:
Re-type new password:
Adding password for user user2
```

```
# htpasswd /.http/site1/passwd_user user3
New password:
Re-type new password:
Adding password for user user3
```

```
# more /.http/site1/passwd_user
user1:GqSDteLDVRWOQ
user2:ExeOdemlS1Abw
user3:bixFSvBOPXGPE
```

Les hôtes virtuels d'apache :

Il existe deux grand types d'hôtes virtuels : ceux basés sur l'adresse IP et ceux basés sur le nom. La plupart des hôtes virtuels sont basés sur le nom. C'est cette solution que nous allons privilégier ici. Nous allons basculer le site1 en hôte virtuel, et nous allons créer un deuxième hôte virtuel pour le site2.

```
# diff httpd.conf httpd.conf.origin
277d276
< ServerName formateur.spherius.fr
992d990
< NameVirtualHost *:80
1005,1014c1003,1006
< <VirtualHost *:80>
<     ServerAdmin root@spherius.fr
<     DocumentRoot /var/www/html/site1
<     ServerName www.site1.spherius.fr
< <Directory "/var/www/html/site1">
<       Options Indexes FollowSymLinks
<       AllowOverride AuthConfig
<       Order   allow,deny
<       Allow from all
< </Directory>
---
> #<VirtualHost *:80>
> #    ServerAdmin webmaster@dummy-host.example.com
> #    DocumentRoot /www/docs/dummy-host.example.com
> #    ServerName dummy-host.example.com
1017c1009
< </VirtualHost>
---
> #</VirtualHost>
```

Vérification que la configuration soit correcte :

```
# httpd -S
VirtualHost configuration:
wildcard NameVirtualHosts and _default_ servers:
*:80                   is a NameVirtualHost
         default server www.site1.spherius.fr (/etc/httpd/conf/httpd.conf:1005)
         port 80 namevhost www.site1.spherius.fr (/etc/httpd/conf/httpd.conf:100
5)
Syntax OK
```

Pour l'instant, le serveur héberge un seul 'vhost'. Nous allons en créer un deuxième :

```
# diff httpd.conf httpd.conf.origin
277d276
< ServerName formateur.spherius.fr
992d990
< NameVirtualHost *:80
1005,1021c1003,1006
< <VirtualHost *:80>
<     ServerAdmin root@spherius.fr
<     DocumentRoot /var/www/html/site1
<     ServerName www.site1.spherius.fr
< <Directory "/var/www/html/site1">
<       Options Indexes FollowSymLinks
<       AllowOverride AuthConfig
<       Order   allow,deny
<       Allow from all
< </Directory>
< #    ErrorLog logs/dummy-host.example.com-error_log
< #    CustomLog logs/dummy-host.example.com-access_log common
< </VirtualHost>
< <VirtualHost *:80>
<     ServerAdmin root@spherius.fr
<     DocumentRoot /var/www/html/site2
<     ServerName www.site2.spherius.fr
---
> #<VirtualHost *:80>
> #    ServerAdmin webmaster@dummy-host.example.com
> #    DocumentRoot /www/docs/dummy-host.example.com
> #    ServerName dummy-host.example.com
1024c1009
< </VirtualHost>
---
> #</VirtualHost>
```

```
# mkdir /var/www/html/site2
# chmod 777 /var/www/html/site2
# httpd -S
VirtualHost configuration:
wildcard NameVirtualHosts and _default_ servers:
*:80                   is a NameVirtualHost
         default server www.site1.spherius.fr (/etc/httpd/conf/httpd.conf:1005)
         port 80 namevhost www.site1.spherius.fr (/etc/httpd/conf/httpd.conf:1005)
         port 80 namevhost www.site2.spherius.fr (/etc/httpd/conf/httpd.conf:1018)
Syntax OK
```

On démarre un navigateur web et on enregistre une page dans le répertoire site2.

Remarque: pour accéder à nos sites web, il faut que les FQDN soient définis au sein du serveur DNS ou dans le fichier local /etc/hosts.

Dans cet exemple, nous mettons à jour le fichier hosts :

```
# more /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.107   formateur formateur.spherius.fr
192.168.1.107   www.site1.spherius.fr
192.168.1.107   www.site2.spherius.fr
```

Nous pouvons accéder à nos sites via les urls : http://www.site1.spherius.fr et http://www.site2.spherius.fr.

Présentation de services réseau

Partage de fichiers entre Windows et Linux: samba

- Installation des packages
- Le fichier de samba : /etc/samba/smb.conf
- Démarrage du serveur samba

Partage de fichiers entre Windows et Linux : samba

Samba est un serveur permettant le partage de fichiers et d'imprimantes entre machines Windows et machines Linux.

Depuis la version 3, Samba peut jouer le rôle d'un contrôleur de domaine. Dans la version 4, la gestion des GPO a été intégrée.

Le fichier de configuration de Samba est au premier abord assez complexe. Des outils ont été développés pour configurer Samba, notamment swat (samba web administration tool) qui fonctionne sur le port 901.

Pour une première configuration de Samba, privilégier l'outil web. Vous pourrez par la suite adapter le fichier généré.

Vérification de la présence des packages :

```
# rpm -qa  | egrep 'samba|smb'
gnome-vfs2-smb-2.24.2-6.el6.x86_64
samba-common-3.6.9-164.el6.x86_64
libsmbclient-3.6.9-164.el6.x86_64
samba4-libs-4.0.0-58.el6.rc4.x86_64
gvfs-smb-1.4.3-15.el6.x86_64
samba-winbind-3.6.9-164.el6.x86_64
samba-winbind-clients-3.6.9-164.el6.x86_64
samba-client-3.6.9-164.el6.x86_64
```

Installation de SWAT :

```
# yum install -y samba-swat
```

Swat est sous le contrôle de xinetd. Il faut modifier le fichier de configuration de swat et passer le paramètre disable à no.

```
# more /etc/xinetd.d/swat
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web browser.
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
        only_from       = 127.0.0.1
        user            = root
        server          = /usr/sbin/swat
        log_on_failure  += USERID
        disable         = no
}
```

Le paramètre only_form indique depuis quelle adresse IP nous pouvons nous connecter sur swat.

Redémarrage de xinetd :

```
# service xinetd restart
Arrêt de xinetd :                                          [  OK  ]
Démarrage de xinetd :                                      [  OK  ]
```

Il ne reste plus qu'à se connecter sur **http://127.0.0.1:901** depuis la machine locale. Sinon indiquer l'adresse IP de votre serveur Samba. L'interface graphique possède plusieurs onglets. Le bouton vue détaillée de certains onglets permet d'avoir la liste de tous les paramètres modifiables.

L'onglet HOME possède des liens vers de la documentation. L'onglet GLOBALS permet d'effectuer un paramétrage global s'appliquant à tous les partages, sauf si le paramètre a été redéfini au niveau du partage. C'est dans cette section que nous indiquons si on est en WORKGOUP ou en DOMAINE et quels sont leur nom. L'onglet SHARES permet de définir les partages. L'onglet PRINTERS permet de partager des imprimantes. L'onglet WIZARD permet de régénérer un fichier de configuration vierge. L'onglet STATUS permet de visualiser les statuts des démons et de les redémarrer. L'onglet VIEW affiche le fichier de configuration de Samba. L'onglet PASSWORD permet de gérer les utilisateurs Samba (création, suppression, modification du mot de passe).

Avec l'interface graphique, on peut créer un partage qui s'appelle 'rep' et qui partage le répertoire /export/rep. Pour cela, on met un commentaire et on rend le partage disponible (Available à yes).

```
# ls /etc/samba

lmhosts  smb.conf  smbusers
```

Le fichier lmhosts contient la correspondance entre une adresse IP et un nom NETBIOS.

Le fichier smbusers contient la correspondance entre un nom d'utilisateur unix et un nom d'utilisateur Samba (donc windows).

Le fichier smb.conf contient la configuration du serveur.

```
# more /etc/samba/smb.conf
# Samba config file created using SWAT
# from UNKNOWN (192.168.1.1)
# Date: 2016/02/02 14:38:57

[global]
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        idmap config * : backend = tdb
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        print ok = Yes
        browseable = No

[rep]
        comment = test de samba
        path = /export/rep
```

```
# service smb start
Démarrage des services SMB :                               [  OK  ]
```

Ajout d'utilisateurs Samba (l'utilisateur doit déjà être un utilisateur unix) :

```
# smbpasswd -a root
New SMB password:
Retype new SMB password:
Added user root.
```

```
# smbpasswd -a theo
New SMB password:
Retype new SMB password:
Added user theo.
```

Visualisation des partages Samba :

```
# smbclient -L 192.168.1.4
Enter root's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.6.23-24.el6_7]

        Sharename       Type      Comment
        ---------       ----      -------
        rep             Disk      test de samba
        IPC$            IPC       IPC Service (Samba Server Version 3.6.23-24.el6_7)
        root            Disk      Home Directories
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.6.23-24.el6_7]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

L'option -U permet de spécifier l'utilisateur :

```
# smbclient -L 192.168.1.4 -U theo
Enter theo's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.6.23-24.el6_7]

        Sharename       Type      Comment
        ---------       ----      -------
        rep             Disk      test de samba
        IPC$            IPC       IPC Service (Samba Server Version 3.6.23-24.el6_7)
        theo            Disk      Home Directories
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.6.23-24.el6_7]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

On peut se connecter à ce partage avec la commande smbclient. Les commandes internes sont après similaires à ftp :

```
# smbclient //192.168.1.4/rep -U theo
Enter theo's password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.6.23-24.el6_7]
smb: \> help
?              allinfo        altname        archive        blocksize
cancel         case_sensitive cd             chmod          chown
close          del            dir            du             echo
exit           get            getfacl        geteas         hardlink
help           history        iosize         lcd            link
lock           lowercase      ls             l              mask
md             mget           mkdir          more           mput
newer          open           posix          posix_encrypt  posix_open
posix_mkdir    posix_rmdir    posix_unlink   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    ..
!
smb: \> pwd
Current directory is \\192.168.1.4\rep\
smb: \> !pwd
/var/tmp
smb: \> ls
  .                                   D        0  Tue Feb  2 14:52:58 2016
  ..                                  D        0  Tue Feb  2 14:37:50 2016
  fic1                                         0  Tue Feb  2 14:52:58 2016
  fic2                                         0  Tue Feb  2 14:52:58 2016

                35292 blocks of size 524288. 9718 blocks available
smb: \> get fic1
getting file \fic1 of size 0 as fic1 (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
```

Notes

Fin de session de Formation

Je vous recommande de relire ce support de cours d'ici les deux semaines à venir, et de refaire des exercices.

Il ne vous reste plus qu'à mettre en œuvre ces nouvelles connaissances au sein de votre entreprise.

Merci, et à bientôt.

Jean-Marc Baranger

Theo Schomaker