

[inetdoc.LINUX]

<http://www.linux-france.org/prj/inetdoc>

Exploration GNU/Linux - Séance 5

Comptes utilisateurs & Identités

Modules d'authentification PAM

Services syslog et cron



Philippe Latu

philippe.latu@linux-france.org

IUT 'A' Paul Sabatier - STRI

Services du système GNU/Linux

- Objectifs.
 - Gérer les comptes utilisateurs locaux
 - Identifier les services de connexion
 - ▶ PAM : Pluggable Authentication Module
 - Exploiter les messages systèmes
 - ▶ syslog
 - Gérer la planification des tâches
 - ▶ cron

Comptes utilisateurs

- Tout objet du système de fichiers doit avoir
 - Un propriétaire
 - Un groupe
- Tout utilisateur du système doit avoir
 - Un identifiant propriétaire unique appelé «uid»
 - ▶ Fichier `/etc/passwd`
 - ▶ Correspondance nom de connexion vs uid numérique
 - Un identifiant groupe unique appelé «gid»
 - ▶ Fichier `/etc/group`
 - ▶ Correspondance nom de groupe vs gid numérique

Comptes utilisateurs

- Plages de validité des «uid» et «gid»

- ▶ <http://www.debian.org/doc/debian-policy/ch-opersys.html#s9.2.2>

- Utilisateurs «système»

- ▶ 0-99 et 100-999 : Comptes réservés aux services

- Utilisateurs «normaux»

- ▶ 1000-29999 : Comptes usuels

- Exemples extraits du fichier /etc/passwd

- ▶ Serveur Web Apache : uid=33

```
$ grep www-data /etc/passwd
```

```
www-data:x:33:33:www-data:/var/www:/bin/sh
```

- ▶ Utilisateur etu : uid=1000

```
$ grep etu /etc/passwd
```

```
etu:x:1000:1000:Etudiant,,,:/home/etu:/bin/bash
```

```
$ ls -l ~/.bashrc
```

```
-rw-r--r-- 1 etu etu 1422 2004-12-12 14:08 /home/etu/.bashrc
```

```
$ ls -ln ~/.bashrc
```

```
-rw-r--r-- 1 1000 1000 1422 2004-12-12 14:08 /home/etu/.bashrc
```

Comptes utilisateurs

- Contrôle d'accès aux services

- Un groupe système par service
- Exemple : accès aux fonctions audio

- ▶ Chaque membre du groupe 'audio' a accès aux fonctions «son» du système

```
$ grep audio /etc/group
```

```
audio:x:29: etu
```

- ▶ Utilisateur etu

```
$ id
```

```
uid=1000(etu) gid=1000(etu) groupes=4(adm),20(dialout),\  
29(audio),44(video),1000(etu)
```

- ▶ Arborescence des périphériques

```
$ ls -l /dev/snd
```

```
total 0
```

```
crw-rw---- 1 root audio 116, 0 2008-01-16 10:15 controlC0  
crw-rw---- 1 root audio 116, 32 2008-01-16 10:15 controlC1  
crw-rw---- 1 root audio 116, 24 2008-01-16 10:15 pcmC0D0c  
crw-rw---- 1 root audio 116, 16 2008-01-16 10:15 pcmC0D0p  
crw-rw---- 1 root audio 116, 1 2008-01-16 10:15 seq  
crw-rw---- 1 root audio 116, 33 2008-01-16 10:15 timer
```

Comptes utilisateurs

- Commandes adduser et deluser
 - Opérations de création et de configuration
- Application
 - À l'aide des pages de manuel 'adduser'
 - ▶ Créer un nouveau compte utilisateur appelé «test»
 - ▶ Quelle est la valeur de l'uid de ce nouveau compte ?
 - ▶ Où sont placés les répertoires utilisateur dans l'arborescence ?
 - ▶ Que contient le répertoire /etc/skel ?
 - ▶ Comment ajouter cet utilisateur au groupe audio ?
 - ▶ Quelles conditions d'activation des nouvelles attributions ?

Comptes utilisateurs

- Niveaux de personnalisation
 - Niveau système et création de compte
 - ▶ Fichiers copiés depuis `/etc/skel`
 - Niveau système et compte existant
 - ▶ Fichiers édités : `/etc/bash.bashrc` et `/etc/profile`
 - Niveau individuel
 - ▶ Fichiers `~/.bash*`
- Personnalisation des applications
 - Fichiers ou Répertoires spécifiques
 - ▶ Sous le répertoire utilisateur
 - ▶ Répertoire `~/.mozilla` ou fichier `~/.vimrc`
- Variables d'environnement
 - Définies au niveau Shell
 - Commandes `export`, `env` et `set`
 - ▶ Localisation : `export LC_ALL='C'`

Service de gestion des connexions

- Contexte historique UNIX
 - Toute connexion était gérée via '/etc/passwd'
 - Réécriture des logiciels à chaque évolution
- PAM : Pluggable Authentication Module
 - Mécanisme flexible d'authentification des utilisateurs
 - Appel dynamique de modules chargés de l'authentification
 - Chaque service possède sa propre configuration
 - ▶ Répertoire /etc/pam.d/
- Services
 - login, su, ssh, kerberos, LDAP, cifs, etc.

Service de gestion des connexions

- 4 champs par service

- Authentification

- ▶ Identifiant/Authentifiant de l'utilisateur

- Account

- ▶ Informations sur le compte
- ▶ Restrictions horaires, expiration, etc.

- Password

- ▶ Mise à jour du jeton d'authentification

- Session

- ▶ Tâches à effectuer lors de la connexion/déconnexion

- Application

- Retrouver les paramètres des services

- ▶ login
- ▶ ssh
- ▶ common

Changement d'identité

- Commande 'su'

- Appartient au paquet login
- Module PAM
- Depuis un compte utilisateur normal
 - ▶ Accès au niveau super utilisateur

```
$ su
```

```
:/home/etu#
```

- ▶ Accès à un autre compte utilisateur après authentification

```
$ su test
```

```
$ set |grep USER
```

```
PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
```

```
USER=test
```

- Depuis le niveau super utilisateur

- ▶ Accès à tous les comptes utilisateur sans authentification

```
# su test
```

```
$ cd ~ ; pwd
```

```
/home/test
```

Changement d'identité

- Commande 'sudo'

- Paquet Debian sudo
- Fichier de configuration
 - ▶ /etc/sudoers
- Exécution d'une commande sous une autre identité
- Exemple
 - ▶ Analyse réseau sous l'identité root à partir du compte etu
 - ▶ Configuration dans /etc/sudoers avec l'éditeur visudo

Captures sur les interfaces réseau sans mot de passe

```
etu ALL = NOPASSWD: /usr/bin/wireshark, /usr/bin/tshark
```

- ▶ Utilisation de la commande

```
$ sudo /usr/bin/tshark -i eth0
```

Messages systèmes

- Service syslog

- Formule consacrée

«La vérité n'est pas ailleurs, elle est dans les logs !»

- Service universel

- ▶ RFC 3164

- Principes

- Démon syslogd

- ▶ Collecte et classe les informations émises par les processus

- Messages émis par les processus

- ▶ Indicateurs d'état

- ▶ Messages d'erreurs

- Configuration du démon

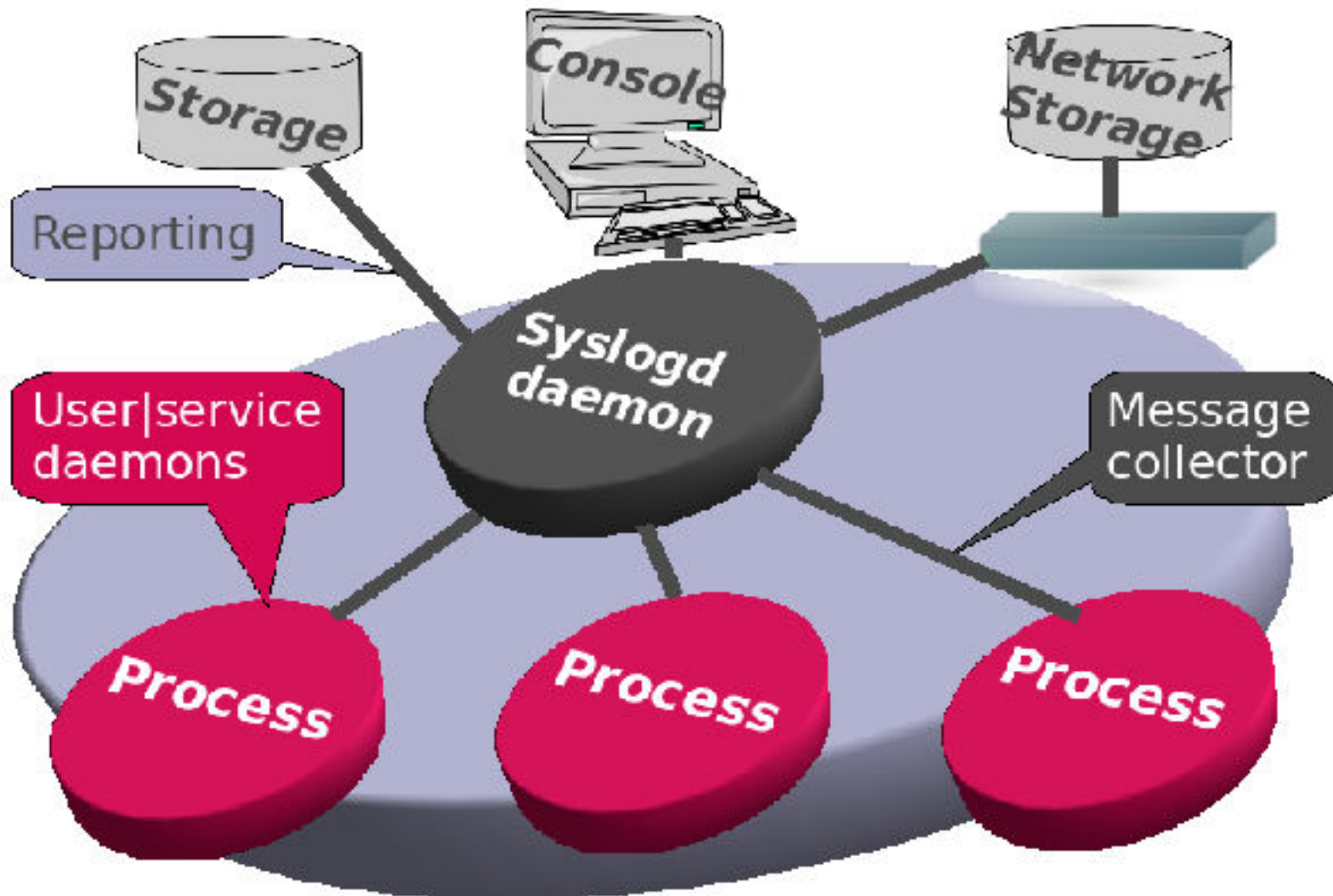
- ▶ Informations à reproduire

- ▶ Niveau de détails

- ▶ Destination : fichier, console, réseau

Messages systèmes

- Principes



Messages systèmes

- Configuration du démon syslogd
 - Fichier /etc/syslog.conf

\$ man syslog.conf

- Syntaxe sur 2 colonnes
 - 1ère colonne - SELECTORS
 - 2ème colonne - ACTIONS
- SELECTORS
 - Sélection des informations journalisées
 - Décomposition en 2 champs : 'facility'. 'level'
 - ▶ 'facility' - type de demande de journalisation
 - ▶ 'level' - niveau de détail

Messages systèmes

- **SELECTORS**

- Types de demande de journalisation

auth - messages de connexion/déconnexion

console - messages normalement destinés à la console système

cron - messages du planificateur système

daemon - fourre-tout pour tous les démons systèmes

kern - messages du noyau

lpr - messages du service d'impression

mail - messages du service de courrier

user - fourre-tout pour les programmes utilisateur

- Niveaux de détails par ordre décroissant

debug - informations développeur

info - informations générales

err - erreurs diverses

warning - avertissements divers

notice - informations générales ne nécessitant pas d'intervention

Messages systèmes

- ACTIONS

- Traitement des informations
- 3 destinations possibles
- Fichier
 - ▶ Répertoire /var/log
- Console
 - ▶ Terminal /dev/tty?[0-9] ou /dev/xconsole
- Hôte réseau
 - ▶ Adresse @loghost.domain
 - ▶ Protocole UDP et port 514

Messages systèmes

- Syntaxe et wildcards

- Remplacement d'un champ SELECTOR : '*'

journalisation de tous les messages du service de courrier

mail.* /var/log/mail.log

- Exclusion d'un type : ';'

journalisation de tous les messages sauf les accès utilisateur

.;authpriv.none /var/log/all.log

- Sélection d'une priorité individuelle : '='

journalisation de tout le trafic du service de courrier

mail.info /var/log/mail.log

journalisation du debugging

mail.=debug /var/log/mail.debug

- Accès temporisé au fichier : '-'

journalisation temporisée des messages du noyau

kern.* -/var/log/kern.log

Messages systèmes

- Exploitation directe

```
# less /var/log/syslog      # consultation du fichier  
# tail -150 /var/log/syslog # affichage des 150 dernières lignes  
# /bin/cat /dev/xconsole | /usr/bin/lwatch -i-
```

- Exploitation via logcheck

- Émission périodique de rapports par mail
- Recherches d'empreintes spécifiques
 - ▶ Commande egrep
- Spécificités Debian
 - ▶ Jeux de règles fournies avec les paquets
 - ▶ Très pratique pour le débutant

- Exploitation via logwatch

- Un rapport quotidien par mail
- Outil plus synthétique que logcheck

Messages systèmes

- Applications

- À quel groupe appartiennent les fichiers de logs ?

```
# ls -l /dev/xconsole
```

```
prw-r----- 1 root adm 0 2005-05-04 15:52 /dev/xconsole
```

- ▶ Ajouter l'utilisateur etu à ce groupe
- Retrouver l'initialisation de la connexion réseau
 - ▶ Fichiers daemon.log et syslog
 - ▶ Commandes cat, less et grep
- Ouvrir une console graphique de journalisation
 - ▶ Éditer le fichier /etc/syslog.conf
 - ▶ Redémarrer le service

```
# /etc/init.d/syslogd restart
```

- ▶ Utiliser le pseudo terminal /dev/xconsole

```
$ xconsole -daemon -savelines 20 -file /dev/xconsole
```

Messages systèmes

- Applications

- Installer le paquet logwatch
- Reconfigurer le gestionnaire de courrier

dpkg-reconfigure postfix

- ▶ Courrier délivré localement
- ▶ Courriers systèmes transmis à l'utilisateur 'etu'
- ▶ Courriers délivrés avec procmail
- Consulter un rapport
 - ▶ Générer un rapport immédiat

/usr/sbin/logwatch --mailto etu@localhost

- ▶ Utiliser mail ou mutt pour consulter le rapport
- Quelles sont les sections du rapport ?
 - ▶ Identifier les services utilisés sur le système

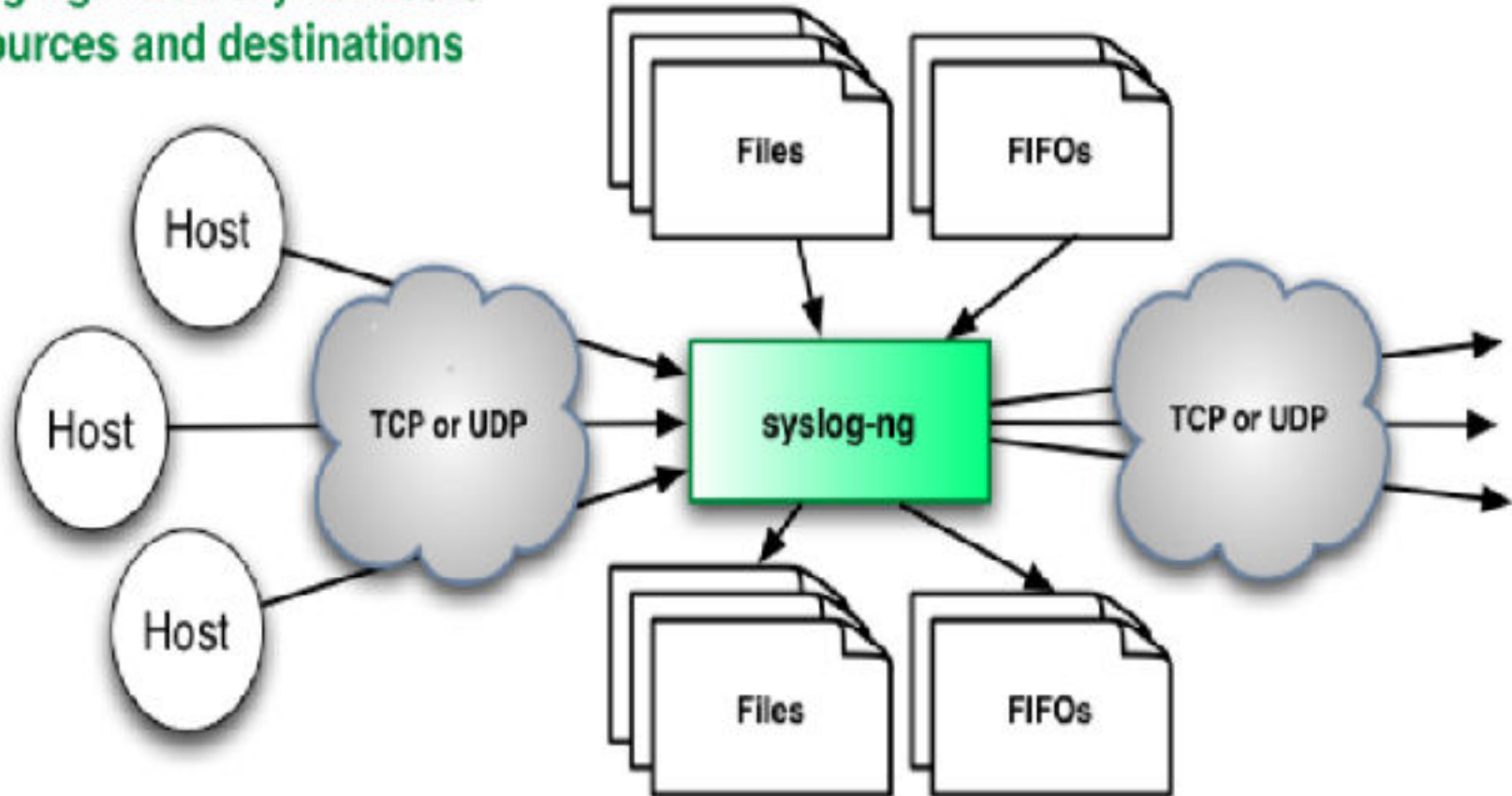
Messages systèmes

- Centralisation des logs

- Démon syslog-ng

- ▶ Sélection des sources par adresses IP
- ▶ Transmission via TCP/UDP et SSL/TLS

Syslog-ng: Arbitrary numbers of sources and destinations



Messages systèmes

- Rotation des logs avec logrotate
 - Contrôle du volume des logs
 - Exemple du service Web Apache

```
# cat /etc/logrotate.d/apache2
```

```
/var/log/apache2/*.log { # traitement sur tous les fichiers du répertoire
    weekly              # rotation hebdomadaire
    missingok           # pas de rapport d'erreur si le fichier est absent
    rotate 52           # rotation sur 52 semaines
    compress            # compression des fichiers d'archives
    delaycompress       # attendre un tour avant la compression
    notifempty         # pas de compression si le fichier est vide
    create 640 root adm # permissions et propriétaire des archives
    sharedscripts      # traitement après rotation
    postrotate         # redémarrage du service s'il est actif
        if [ -f /var/run/apache2.pid ]; then
            /etc/init.d/apache2 reload > /dev/null
        fi
    endscript
}
```

Planification des tâches

- Démon cron

- Exécution périodique de traitements
- Fichier /etc/crontab

```
# m h dom mon dow user  command
```

```
17 * * * * root run-parts --report /etc/cron.hourly
```

```
25 6 * * * root test -x /usr/sbin/anacron || \  
run-parts --report /etc/cron.daily
```

```
47 6 * * 7 root test -x /usr/sbin/anacron || \  
run-parts --report /etc/cron.weekly
```

```
52 6 1 * * root test -x /usr/sbin/anacron || \  
run-parts --report /etc/cron.monthly
```

- Syntaxe de planification

- ▶ minute - heure - jour du mois - mois - jour de la semaine

Planification des tâches

- Démon cron

- Commande run-parts

- ▶ Exécution des scripts présents dans un répertoire

- Périodicité

- ▶ Horaire /etc/cron.hourly
- ▶ Quotidienne /etc/cron.daily
- ▶ Hebdomadaire /etc/cron.weekly
- ▶ Mensuelle /etc/cron.monthly

- Exemple de script

```
$ cat /etc/cron.weekly/man-db
```

```
#!/bin/sh
```

```
#
```

```
# Last modification: Fri, 18 May 2001 13:54:15 +0100
```

```
# man-db cron weekly
```

```
# regenerate man database
```

```
if [ -x /usr/bin/mandb ]; then
```

```
    nice su man -c 'mandb 2>/dev/null >/dev/null'
```

```
fi
```

Planification des tâches

- Application

- Automatisation des mises à jour APT

- ▶ Exemple de script placé dans le répertoire `/etc/cron.daily`

```
#!/bin/sh
```

```
APT=/usr/bin/aptitude
```

```
LOGFILE=/var/log/apt-upgrade.log
```

```
if [ ! -f $LOGFILE ]; then
```

```
    touch $LOGFILE
```

```
    chown root.adm $LOGFILE
```

```
fi
```

```
if [ -x $APT ]; then
```

```
    $APT update >>$LOGFILE 2>&1
```

```
    $APT -y -q safe-upgrade >>$LOGFILE 2>&1
```

```
fi
```

```
exit 0
```

Surveillance des connexions

- **Contrôle périodique des connexions impératif !**
 - Commande 'w'
 - Liste des utilisateurs connectés

\$ w

16:54:37 up 1:35, 1 user, load average: 1,00, 0,75, 0,42

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
etu	:0	-	15:21 ?xdm?	4:33	0.00s	-:0	

- **Journalisation dans /var/log/auth.log**

Jan 14 18:59:55 host kdm: :0[20956]: \

pam_unix(kdm:session): session opened for user etu by (uid=0)

Jan 14 20:56:41 host su[14330]: Successful su for root by etu

Jan 14 20:56:41 host su[14330]: + pts/3 etu:root

Surveillance des connexions

- **Commande lastlog**

sateur	Port	Venant de	Dernière
root	tty1		ven mai 23 09:30:48 +0200 2007
daemon			**Jamais connecté**
bin			**Jamais connecté**
sys			**Jamais connecté**
sync			**Jamais connecté**
www-data			**Jamais connecté**
man			**Jamais connecté**
lp			**Jamais connecté**
mail			**Jamais connecté**

- **Attention !**

- Comptes systèmes utilisés = danger

Synthèse

- Gestion des comptes utilisateurs
 - Fonctionnalités nombreuses
 - Limiter les accès aux comptes systèmes
- Mécanismes d'authentification modulaires
 - Granularité par service ouvert
 - Adaptation à tous les usages
- Messages systèmes
 - Journaux = outil vital pour l'administrateur
 - Documentation Securing Debian Manual
 - ▶ The importance of logs and alerts
 - Outils d'émissions de rapports
 - ▶ logwatch
 - ▶ Compromis coût d'administration / efficacité

Synthèse

- Planification des tâches
 - Optimisation du fonctionnement des services
- Surveillance des connexions
 - Identifier les «intrusions» de premier niveau