

# Introduction aux systèmes GNU/Linux

S23E04 inetdoc.net



Philippe Latu / Université Toulouse 3

Document sous licence GNU FDL v1.3  
<http://www.gnu.org/licenses/fdl.html>

# Plan séance 5

- Séance 5 - Comptes utilisateurs - journalisation & planification
  - Gérer les comptes utilisateurs locaux
  - Identifier les services d'authentification
    - PAM : Pluggable Authentication Module
  - Exploiter les messages systèmes → syslog
  - Gérer la planification des tâches → cron
- Manipuler sur machines virtuelles & conteneurs
  - Personnaliser les comptes utilisateurs & sécuriser les droits

# Comptes utilisateurs locaux

- Tout objet du système de fichiers doit avoir
  - Un compte utilisateur propriétaire
  - Un groupe propriétaire
- Tout utilisateur du système doit avoir
  - Un identifiant **propriétaire** unique appelé **uid**
    - Fichier /etc/passwd → correspondance entre nom de connexion et **uid** numérique
  - Un identifiant **groupe** unique appelé **gid**
    - Fichier /etc/group → correspondance entre nom de groupe et **gid** numérique

```
$ grep etu /etc/passwd  
etu:x:1000:1000:etudiant,,,:/home/etu:/bin/bash
```

Identifiant numérique groupe

Identifiant numérique utilisateur

```
$ grep etu /etc/group  
adm:x:4:etu  
cdrom:x:24:etu  
floppy:x:25:etu  
audio:x:29:etu,pulse  
dip:x:30:etu  
src:x:40:etu  
video:x:44:etu  
plugdev:x:46:etu  
staff:x:50:etu  
etu:x:1000:
```

Identifiant numérique groupe

# Comptes utilisateurs locaux

- Plages de validité des **uid** et **gid**
  - Valeurs numériques divisées en classes
    - <http://www.debian.org/doc/debian-policy/ch-opersys.html#s9.2.2>
  - Utilisateurs & groupes **ystème**
    - 0-99 et 100-999
    - Comptes réservés aux services | processus
  - Utilisateurs & groupes «normaux»
    - 1000-59999
    - Comptes alloués dynamiquement
- Cas particulier : utilisateur **nobody** & groupe **nogroup**
  - Valeur réservée 65534

# Comptes utilisateurs locaux

- Contrôle d'accès aux ressources
  - Un groupe système par ressource
  - Exemple : fonctions audio

```
# grep audio /etc/group  
audio:x:29:etu
```

Les membres du groupe audio ont accès aux fonctions «son» du système

- Cas de l'utilisateur **etu**

```
$ id  
uid=1000(etu) gid=1000(etu) groupes=1000(etu),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
```

- Arborescence des périphériques

```
$ ls -l /dev/snd/  
total 0  
crw-rw---T+ 1 root audio 116, 1 mai 31 08:28 seq  
crw-rw---T+ 1 root audio 116, 33 mai 31 08:28 timer
```

# Comptes utilisateurs locaux

- Serveur Web apache2
  - Identification des processus

Identité des processus

```
$ ps faux | grep apache2
root      1408  0.0  1.5 204424 15488 ?        Ss   11:38   0:00 /usr/sbin/apache2 -k start
www-data  1608  0.0  0.9 204448  9716 ?        S    11:38   0:00 \_ /usr/sbin/apache2 -k start
www-data  1609  0.0  0.9 204448  9716 ?        S    11:38   0:00 \_ /usr/sbin/apache2 -k start
www-data  1610  0.0  0.9 204448  9716 ?        S    11:38   0:00 \_ /usr/sbin/apache2 -k start
www-data  1611  0.0  0.9 204448  9716 ?        S    11:38   0:00 \_ /usr/sbin/apache2 -k start
www-data  1612  0.0  0.9 204448  9716 ?        S    11:38   0:00 \_ /usr/sbin/apache2 -k start
```

- Informations compte utilisateur

```
$ grep www-data /etc/passwd
www-data:x:33:33:www-data:/var/www:/bin/sh
```

```
$ grep www-data /etc/group
www-data:x:33:
```

Groupe des développeurs Web

```
# mkdir /var/www/mywebsite
# chown www-data.www-data /var/www/mywebsite/
# chmod 2770 /var/www/mywebsite
# ls -l /var/www/ | grep mywebsite
drwxrws--- 2 www-data www-data 4096 mai 31 11:54 mywebsite
# ls -ln /var/www/ | grep mywebsite
drwxrws--- 2 33 33 4096 mai 31 11:54 mywebsite
```

# Comptes utilisateurs locaux

- Opérations de création et de configuration
  - Commandes `adduser` et `deluser`
  - Applications
    - À quel paquet appartient la commande `adduser` ?
    - Comment créer un nouveau compte utilisateur `webuser` ?
    - Quelles sont les valeurs `uid` et `gid` de ce nouveau compte ?
    - Où sont placés les répertoires utilisateurs dans l'arborescence ?
    - Comment ajouter ce nouveau compte au groupe `adm` ?
    - Quelles sont les conditions d'activation des attributions de groupe ?
    - Comment faire pour que l'utilisateur `webuser` devienne développeur web ?

# Comptes utilisateurs locaux

- Personnalisation d'un compte
  - 3 niveaux distincts
    - Lors de la création d'un compte → copie des fichiers du répertoire `/etc/skel`
    - À l'échelle système → édition des fichiers `/etc/bash.bashrc` ou `/etc/profile`
    - Au niveau individuel → éditions des fichiers `~/.bash*`
- Personnalisation des applications d'un compte
  - Fichiers ou répertoires «cachés» dans l'arborescence utilisateur

```
$ sudo apt install git fonts-powerline  
$ bash -c "$(wget https://raw.githubusercontent.com/ohmybash/oh-my-bash/master/tools/install.sh -O -)"
```

## ▪ Variables d'environnement

```
$ echo $PATH  
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

Gestion de la configuration  
avec Oh my bash !

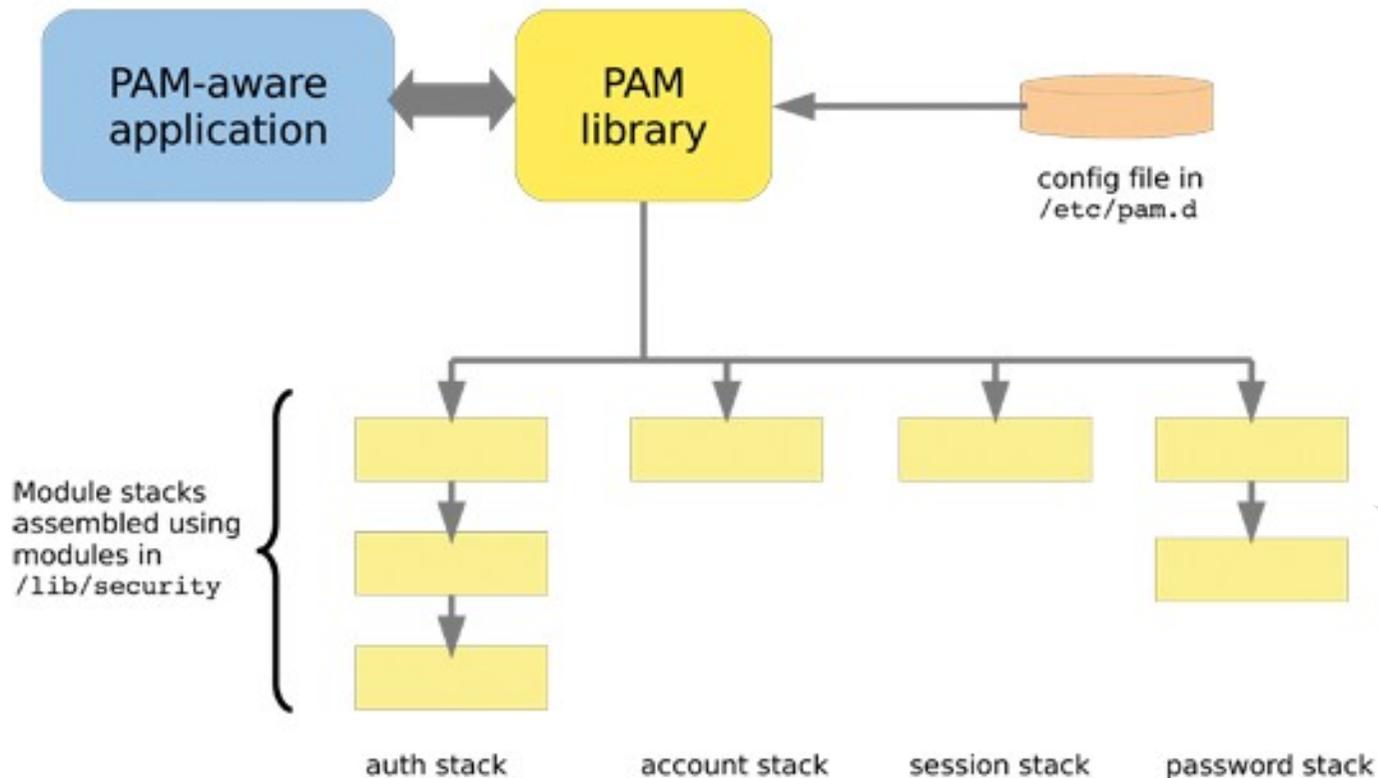
Chemin de recherche des  
programmes exécutables

## ▪ Alias

```
$ alias
```

# Gestion des connexions

- AAA → *Authentication, Authorization, Accounting*
- PAM → *Pluggable Authentication Module*



- Bibliothèque partagée
  - Mécanisme d'appel de fonctions AAA
- Un module par service
- Un fichier de configuration par service

```
$ ls /etc/pam.d
atd chpasswd common-account common-password
common-session-noninteractive login other
polkit-1 su xdm chfn chsh common-auth
common-session cron newusers passwd sshd sudo
xscreensaver
```

# Gestion des connexions

- 4 champs par service
  - Authentication
    - Identifiant/Authentifiant de l'utilisateur
  - Account
    - Informations sur le compte
    - Restrictions horaires, expiration, etc.
  - Password
    - Conditions de mise à jour du jeton d'authentification
  - Session
    - Tâches à effectuer lors de la (dé)connexion

# Gestion des connexions

## ▪ Application

- Retrouver les paramètres des services `common`, `login` et `ssh`
- Comment appliquer un masque utilisateur avec la valeur `0027` à chaque nouvelle connexion ?
  - Lire et éditer le fichier `/etc/login.defs`
    - Rechercher la clé `UMASK` et modifier sa valeur
  - Lire et éditer le fichier `/etc/pam.d/common-session`
    - Ajouter la ligne suivante en fin de fichier

```
session optional pam_umask.so
```

- Tester la valeur du masque utilisateur après l'ouverture d'une nouvelle session

# Changement d'identité

- Commande **su**

- Commande fournie avec le paquet login
- Ouverture d'une **session** sous une autre identité

- Exemples

- Accès au niveau super-utilisateur
- Accès à un autre compte utilisateur
  - À partir du niveau «normal» ou à partir du niveau super utilisateur

```
etu@vm:~$ su -  
Mot de passe :  
root@vm:/home/etu#
```

```
etu@vm:~$ su - testuser  
Mot de passe :  
testuser@vm:~$ pwd  
/home/testuser
```

avec  
authentification

```
root@vm:~# su - testuser  
testuser@vm:~$ pwd  
/home/testuser
```

sans  
authentification

# Changement d'identité

- Commande **sudo**

- Commande fournie avec le paquet sudo
- Exécution d'une **commande** sous une autre identité
- Exemple de configuration

- Édition de la configuration avec **visudo**
  - Visualisation du groupe système **sudo**
  - Ajout de l'utilisateur **webuser** au groupe sudo

```
$ sudo grep ^%sudo /etc/sudoers
%sudo    ALL=(ALL:ALL) ALL
```

```
newuser@vm:~$ sudo apt update
```

Nous espérons que vous avez reçu de votre administrateur système local les consignes traditionnelles. Généralement, elles se concentrent sur ces trois éléments :

- #1) Respectez la vie privée des autres.
- #2) Réfléchissez avant d'utiliser le clavier.
- #3) De grands pouvoirs confèrent de grandes responsabilités.

```
[sudo] Mot de passe de newuser :
```

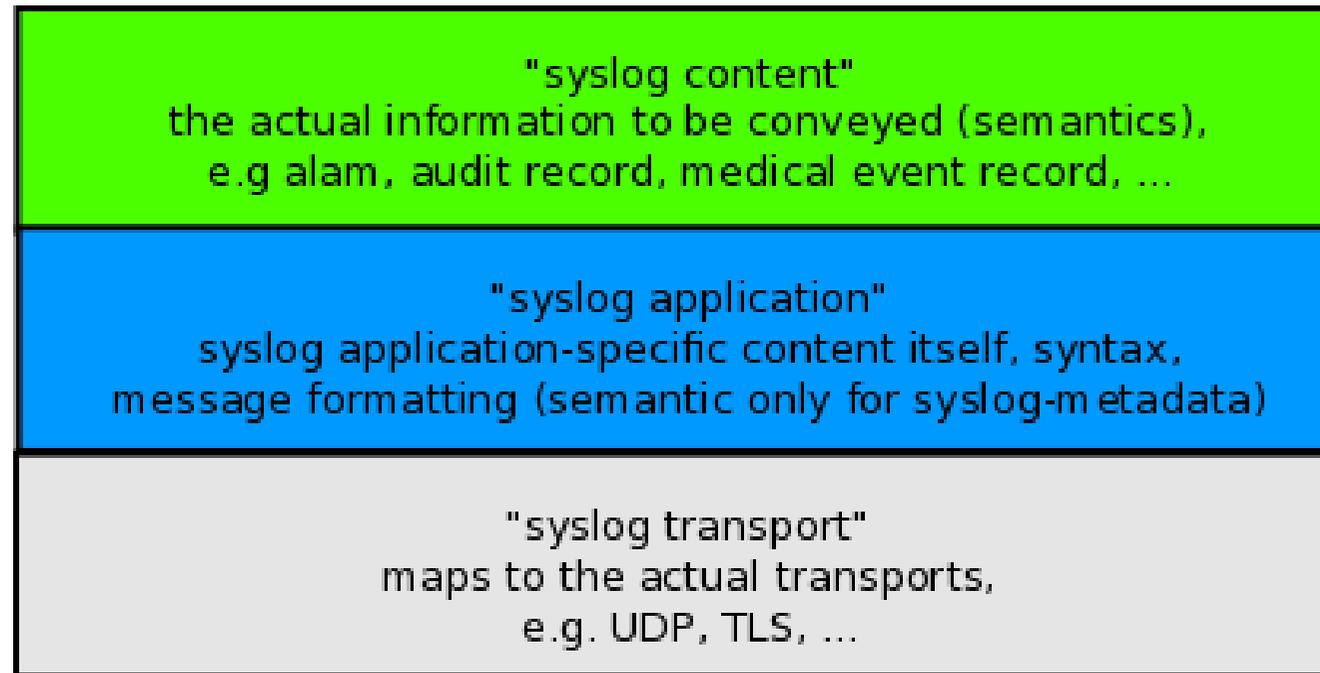
```
$ sudo adduser webuser sudo
```

```
Ajout de l'utilisateur « newuser » au groupe « sudo »
Ajout de l'utilisateur newuser au groupe sudo
Fait.
```

Attribution active après (dé)reconnexion

# Journalisation système

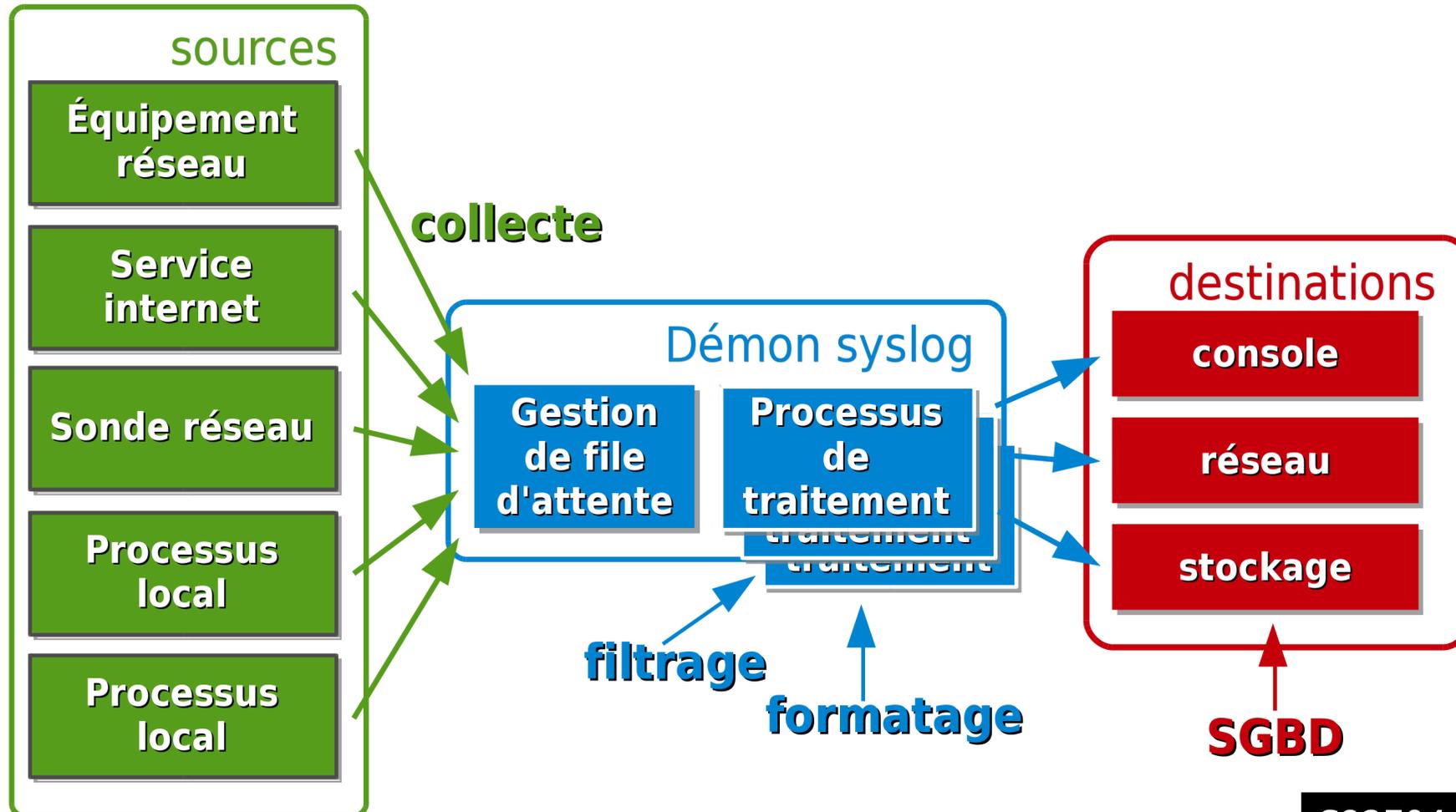
- La vérité n'est pas ailleurs, elle est dans les logs !
- RFC5424 : The syslog protocol
  - <http://en.wikipedia.org/wiki/Syslog>



Source [www.rsyslog.com](http://www.rsyslog.com)

# Journalisation système

- Identification des composants



# Journalisation système

- Application : rsyslog
  - Architecture modulaire
    - Collecte → input modules
    - Destination → output modules
    - Règles conformes aux versions historiques de syslogd
  - Syntaxe composée de 2 colonnes
    - SELECTORS
    - ACTIONS
  - SELECTORS → Sélection des informations journalisées
    - Format → **facility.level**
    - **Facility** → type de demande de journalisation
    - **Level** → niveau de détail

# Journalisation système

## ▪ 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

# Journalisation système

- ACTIONS

- Destinations des informations traités
- Catégories de modules
  - Système de fichiers local → /var/log
  - Réseau → 514/udp
  - Console
- Configuration rsyslog
  - [http://www.rsyslog.com/doc/rsyslog\\_conf.html](http://www.rsyslog.com/doc/rsyslog_conf.html)
  - Paquet `rsyslog-doc`

# Journalisation système

- 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
```

# Journalisation système

- Consultation directe

- Consultation → `journalctl`

Rechercher les messages relatifs à la création du compte `webuser`

- Consultation des nouveaux messages → `journalctl -n 100 -f`

- Consultation après traitement

- Tableaux de bord → Nagios - Centreon - `suite ELK`

- Émission périodique de rapports → `logwatch`

- Recherche permanente du meilleur compromis

- Efficacité du processus métier → la détection d'incident
- Coût humain de traitement des journaux → massification des sources

# Journalisation système

## ▪ Applications

- À quel groupe appartiennent le dossier et les fichiers de logs ?
- Comment retrouver l'initialisation et la configuration de l'interface réseau ?
  - Utiliser la commande `journalctl`
  - Essayer les options : recherche avec `'/'` ou `--since today` ou `--grep=`
- Comment produire un rapport avec `logwatch` ?
  - Rechercher et installer le paquet correspondant
  - Générer l'émission d'un rapport via la commande : `/usr/sbin/logwatch --detail high`
- Comment identifier les consultations de pages Web ?
  - Quel est le fichier de journalisation utile ?
  - Comment comptabiliser les visites ?

# Journalisation système

- Optimisation du stockage → Rotation des journaux
  - Objectif → limiter le volume des données stockées
  - Outil → **logrotate**
  - Exemple du service Web apache

```
/var/log/apache2/*.log {
    daily
    missingok
    rotate 365
    compress
    delaycompress
    notifempty
    create 640 root adm
    sharedscripts
    prerotate
        if [ -d /etc/logrotate.d/httpd-prerotate ]; then
            run-parts /etc/logrotate.d/httpd-prerotate
        fi
    endscript
    postrotate
        if pgrep -f ^/usr/sbin/apache2 > /dev/null; then
            invoke-rc.d apache2 reload 2>&1 | \
                logger -t apache2.logrotate
        fi
    endscript
}
```

Rotation chaque jour sur une durée de 365 jours de tous les fichiers du répertoire avec compression

# Planification des tâches

- Service historique *cron*
  - Exécution périodique d'un ou d'une série de scripts
  - Périodicité prédéfinie
    - Horaire → `/etc/cron.hourly/`
    - Quotidienne → `/etc/cron.daily/`
    - Hebdomadaire → `/etc/cron.weekly/`
    - Mensuelle → `/etc/cron.monthly/`
    - Apériodique → `/etc/cron.d/`
  - Fichier de configuration principal → `/etc/crontab`

```
$ grep -B1 ^[0-9] /etc/crontab
# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
```

# Planification des tâches

- Systemd *timer* associé à un *service*
  - Exécution périodique d'un service
  - Exemple : fstrim (jeter les blocs de stockage non utilisés)

```
$ cat /usr/lib/systemd/system/fstrim.service
[Unit]
Description=Discard unused blocks on filesystems from /etc/fstab
Documentation=man:fstrim(8)
ConditionVirtualization=!container

[Service]
Type=oneshot
ExecStart=/sbin/fstrim --listed-in /etc/fstab:/proc/self/mountinfo --
verbose --quiet-unsupported
PrivateDevices=no
PrivateNetwork=yes
PrivateUsers=no
ProtectKernelTunables=yes
ProtectKernelModules=yes
ProtectControlGroups=yes
MemoryDenyWriteExecute=yes
SystemCallFilter=@default @file-system @basic-io @system-service
```

```
$ cat /usr/lib/systemd/system/fstrim.timer
[Unit]
Description=Discard unused blocks once a week
Documentation=man:fstrim
ConditionVirtualization=!container

[Timer]
OnCalendar=weekly
AccuracySec=1h
Persistent=true
RandomizedDelaySec=6000

[Install]
WantedBy=timers.target
```

# Planification des tâches

- Systemd *timer* associé à un *service*
  - Exécution périodique d'un service
  - Exemple : fstrim (jeter les blocs de stockage non utilisés)

```
$ sudo systemctl enable fstrim.timer  
Created symlink /etc/systemd/system/timers.target.wants/fstrim.timer → /lib/systemd/system/fstrim.timer.
```

```
$ systemctl list-timers --all
```

NEXT	LEFT	LAST	PASSED	UNIT	ACTIVATES
Tue 2020-12-29 17:56:35 CET	3min 50s left	n/a	n/a	systemd-tmpfiles-clean.timer	systemd-tmpfiles-clean.service
Wed 2020-12-30 00:00:00 CET	6h left	n/a	n/a	exim4-base.timer	exim4-base.service
Wed 2020-12-30 00:00:00 CET	6h left	n/a	n/a	logrotate.timer	logrotate.service
Wed 2020-12-30 00:00:00 CET	6h left	n/a	n/a	man-db.timer	man-db.service
Wed 2020-12-30 00:40:31 CET	6h left	Sun 2020-06-28 10:04:12 CEST	6 months 1 days ago	apt-daily.timer	apt-daily.service
Wed 2020-12-30 06:31:02 CET	12h left	Tue 2020-12-29 16:57:23 CET	55min ago	apt-daily-upgrade.timer	apt-daily-upgrade.service
Sun 2021-01-03 03:10:51 CET	4 days left	Mon 2020-12-28 16:18:13 CET	1 day 1h ago	e2scrub_all.timer	e2scrub_all.service
Mon 2021-01-04 00:26:39 CET	5 days left	n/a	n/a	fstrim.timer	fstrim.service

# Surveillance des connexions

- Quels sont les comptes utilisateurs actifs ?
  - Liste des utilisateurs connectés → `w`

```
$ w
10:47:46 up 33 min,  1 user,  load average: 0,00, 0,00, 0,00
USER      TTY      FROM          LOGIN@      IDLE        JCPU        PCPU WHAT
etu       pts/0    fe80::f479:19ff: 11:15      0.00s      0.11s      0.00s w
```

- Journalisation des connexions → `journalctl -u systemd-logind`

```
vm0 sshd[873]: Server listening on :: port 22.
vm0 sshd[882]: Accepted password for etu from fe80::f479:19ff:fed2:b0d3%eth0 port 50420 ssh2
vm0 sshd[882]: pam_unix(sshd:session): session opened for user etu by (uid=0)
vm0 systemd-logind[556]: New session 1 of user etu.
vm0 systemd: pam_unix(systemd-user:session): session opened for user etu by (uid=0)
```

# Surveillance des connexions

- Historique des connexions

- Commande `last`
- Tester les options `-W -S -X`
- !ATTENTION DANGER! → compte système utilisé → `lastlog -u www-data`

```
$ lastlog -t 2
```

Username	Port	From	Latest
etu	pts/0	fe80::8d5:d0ff:f	mar. déc. 29 17:56:34 +0100 2020

```
$ last -s -2days
```

etu	pts/0	fe80::8d5:d0ff:f	Tue Dec 29 17:56	still logged in
reboot	system boot	5.9.0-5-amd64	Tue Dec 29 17:56	still running
etu	pts/0	fe80::84d5:caff:	Mon Dec 28 17:17 - 16:19	(-00:58)
reboot	system boot	5.9.0-5-amd64	Mon Dec 28 17:17 - 16:19	(-00:58)

```
wtmp commence Thu Aug 29 11:38:38 2019
```

# Bilan séance

- Gestion des comptes utilisateurs
  - Respecter les règles définies sur les uids & gids
  - Limiter les accès aux comptes système
- AAA → PAM
  - Importance de la granularité des configurations
- Journalisation système
  - Outil de mise au point des configurations des services
  - Outil essentiel pour la survie de l'administrateur
- Planification des tâches
  - Optimisation des opérations d'administration

# Ressources

- Manuel de référence Debian
  - Authentification
    - <http://www.debian.org/doc/manuals/debian-reference/ch04.fr.html>
  - Journalisation système
    - Analyse de plus haut niveau → suite ELK

