TP7 d'administration Unix

F. Butelle M. Mayero

2015

Conseil : rédiger un compte rendu de TP.

1 Utilisation de `sudo`

Faites en sorte que l'utilisateur `etudiant` puisse attribuer une adresse IP à sa machine sans avoir à passer root et sans avoir à taper de mot de passe. Lui donner aussi le droit d'exécuter toute commande dans /usr/bin en tant que root mais avec mot de passe. Prenez-vous des risques ?

2 Utilisation de `crontab`

1. Créer au moins un utilisateur de plus avec quelques fichiers dans son répertoire de travail
2. Faites en sorte de sauvegarder, sous la forme d'archive compressée (homes.tgz), les répertoires des utilisateurs toutes les deux minutes.
   Quels sont les défauts de cette solution de sauvegarde ? Nous verrons plus loin comment améliorer un peu le système.

3 Serveur d'audit ou comment centraliser les logs

Nous allons utiliser principalement `rsyslogd`, un démon travaillant avec `systemd-journald`.

1. `systemd-journald` et `rsyslog` sont configurés par défaut pour ne tracer que les événements locaux ; `rsyslog` dispose d'une option lui permettant d'écouter sur un port UDP et donc devenir un véritable serveur d'Audit. Trouver le fichier de configuration de `rsyslog`.
   - Sur le serveur, modifier la configuration pour qu'il démarre par défaut le démon `rsyslogd` en mode écoute réseau. Relancer ce service et vérifier par `netstat` qu'il est bien devenu un service réseau.
   - Sur le client, modifier `/etc/syslog.conf` pour qu'il envoie tous ses logs vers le serveur.
   Relancer le service rsyslog sur le client. Faites quelques manipulations sur le client, comme par exemple essayer de se loguer avec un mauvais mot de passe, et consultez les résultats au niveau du serveur... avec `tail -f /var/log/messages` (et pas `journalctl -f`).
2. A quoi sert le fichier `/etc/logrotate.conf` ?
   On veut garder les 3 dernières sauvegardes des fichiers utilisateurs (homes.tgz), mais pas plus... Comment faire ?