TP-2 Unix :

Les niveaux de démarrage, et les logs :

NIVEAUX D'INIT

Il existe plusieurs niveaux de démarrage (d'init, de 0 (halt) à 6 (reboot) en passant par 1(single), puis 2-3-4-5 qui sont libres et configurables. Utilisez **runlevel** pour connaître votre niveau de démarrage

utilisez **runlevel** pour connaître votre niveau de démarrage. C'est le niveau normal.
avec **init**, changez de niveau de démarrage : Passez en mode **single(init 1)** afin de faire des réglages, puis revenez en mode normal...
Que se passe t il ?
Basculer de niveaux en niveaux. Que se passe t il dans chaque niveau, concernant vos services ?

Le répertoire /etc/init.d contient l'ensemble des scripts qui permettent le contrôle des services. Ces scripts acceptent en général en argument les valeurs suivantes : **start stop restart reload**
consulter ce répertoire.
Quels sont les services que vous reconnaissez ?
Essayez d'invoquer un script en lui passant des arguments.
consultez un script afin de lister les valeurs acceptées...

Le lancement et l'arrêt des services de chaque niveau de démarrage est contrôlé par les répertoires **/etc/rcX.d** (ou le X vaut le niveau)
Consultez ces répertoires (**/etc/rc1.d/** puis **/etc/rc2.d/** et ainsi de suite): Que constatez vous ?
Quel est le rôle du S et du K ?
A quoi servent les numéros ?

Pour définir les services à lancer ou à arrêter, il suffit de faire un lien symbolique avec la bonne lettre et le numéro voulu vers le vrai script. Ainsi, on dispose de plusieurs démarrages possibles, avec différents services.

Définissez sur papier une liste de service que vous voulez lancer dans deux niveaux différents : Par exemple : niveau 3 : **apache, mysql, gdm**, et dans le niveau 4 : **ssh et apache**.
Modifiez votre machine en conséquence (Nota : en debian, un outil permet de définir le démarrage. Comme d'habitude, il s'agit update-rc.d. Exemple

d'utilisation : **update-rc.d foobar start 25 245 stop 30 0136** ajoute le lancement du service foobar en 25ème position dans les niveau 2 4 et 5, et l'arrêt en 30ème dans les niveau 0,1,3 et 6)
A quoi sert le service rmnologin ? Supprimez le lancement du service **rmnologin**. Coupez brutalement le courant, puis essayez de vous connecter en simple utilisateur. Que constatez vous ? Quel est le message ? Connectez vous en tant que root. Consultez le contenu du fichier /etc/nologin. Que contient il ? Lancez le service **rmnologin**. Que se passe t il ? A votre avis, à quoi sert ce service ?

Pour tenter de modifier le mot de passe du root, on peut essayer de booter la machine en mode **single** (en tapant **linux single** lors du boot).
Pourquoi la debian est elle protégée contre cette manipulation ? Comment enlever cette protection ?

Le lancement du système est contrôlé par **init** (programme dont le PID est 1). Le fichier qui définit le comportement de init est **/etc/inittab**.
Consultez ce fichier.
Comment faire pour rajouter des consoles ? (tty8, tty9, etc)
Pourquoi n'y a t il pas de consoles en mode 1,4 et 5 ?
Comment changer le niveau de démarrage par défaut ?
Pour les courageux, essayez de suivre le raisonnement de la machine : Que fait le programme **/etc/init.d/rc** ?

LES LOGS

Les logs sont les fichiers contenus dans **/var/log**. Ils contiennent les informations que les services ont voulu vous communiquer. Le rangement dans ces fichiers obéit au paramétrage du fichier **/etc/syslog.conf.**
Les services émettent des messages : ceux-ci sont typés, selon deux critères : la « **facility** » (type de l'émetteur : auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, syslog, user), et la « **priority** » (la gravité : de debug, info, notice, warning, err, crit, alert, emerg)
Pour chacun des ces couples facility-priority, on pourra définir une action :
Une action consiste en le rangement du message dans un fichier (par exemple /**var/log/messages**), un ecran (/**dev/console**, /**dev/tty12**), une liste d'utilisateurs, voire sur une machine du réseau.
On peut ranger à plusieurs endroits en même temps (par exemple, dans /**dev/console** et dans /**var/log/messages**).

Consultez le fichier de configuration.
Essayez de repérer quelques couples facility-priority, et notez les réglages
Consultez les fichiers, afin de connaître les messages
Y'a t il un fichier qui contient tous les logs ?
Que contient le fichier **/var/log/messages** ?

logger est un outil qui permet de générer des logs : C'est très pratique dans les scripts par exemple (message de début de script, de fin de scripts, de

connexion, etc). C'est **syslogd** (le démon) qui rangera à l'endroit voulu le message, selon son type.

En consultant le man de **logger**, essayez de générer des messages de différents types.
Consultez les logs correspondants

Modifiez le fichier de configuration afin d'envoyer une copie de tous les messages de niveau warning et supérieur sur l'écran numéro 8 (**/dev/tty8**)
Même chose pour un fichier **/var/log/alarm**
Les deux en même temps.
A l'utilisateur **root**

En réseau.

Il est possible de réaliser un serveur de logs. Pour cela, vous devez lancer le service de logs avec l'option -r (voir le **man**), puis sur chaque client, configurer le syslog.conf afin qu'il s'adresse au serveur (voir **man syslog.conf**).
Vous pouvez définir ce que vous envoyez au serveur. C'est le serveur lui même qui, selon sa configuration, dispatchera dans les fichiers choisis par son admin.

ATTENTION : Il y a une petite difficulté : Dans l'installation de base, le serveur de log n'écoute pas le réseau. Il faut le régler !:
Arrêtez le serveur à la main (**kill**), puis lancer le à la main, avec l'option idoine !!! Vérifiez le bon fonctionnement (avec un **tail -f** par exemple). Comment reconnaît on nos logs de ceux des machines clientes ?
Après vérification, cherchez comment faire pour que le programme de logs (syslogd) soit lancé automatiquement avec la bonne option (réfléchissez : Qui lance ce programme ? Quel rapport avec ce tp ?)

LOGROTATE

Les logs, c'est très bien. Mais n'est ce pas trop envahissant ?
Logrotate est la pour vous. Il organise la rotation des logs, afin de limiter leurs tailles, de permettre différents archivages, voir même de mailer de logs. On peut organiser la rotation de log par semaine, par taille, définir le nombre de copies que l'on désire garder, comment les compresser, ce qu'il faut faire après la rotation, etc..
Consultez le fichier de configuration, et regarder les réglages. En parallèle avec le man, expliquez les réglages actifs.
Modifiez le réglage pour mysql, afin que l'on garde sur 5 occurrences les fichiers de logs, qui ne seront soumis à rotation que si ils dépassent 100Ko