Administration Linux

OULD DEYE

Dept. de Mathématiques et Informatique
FST - UCAD

20 mars 2009

Plan

Plan

Le rôle de l'administrateur

- **Créer, modifier, supprimer un user**
- **Gérer les fichiers et les disques**
- **Surveiller l'espace disque**
- **Organiser les sauvegardes**
- **Ajouter un périphérique**
- **Améliorer les performances du système**
- **Installer de nouveaux produits**
- **Veiller à la sécurité du système**
- **Paramétrer le démarrage et l'arrêt du système**

Quelques éléments de méthodologie 1/5

Il faut sauvegarder son système :

Votre système est fragile. Un logiciel peut etre bogué, vous pouvez faire des erreurs d'exploitation, un disque ou votre ordinateur peut tomber en panne. A tout moment il faut êre capable de réinstaller votre système tel qu'il était avant le problème

Il faut tenir à jour un journal de bord :

Dans lequel vous consignez les opérations importantes d'exploitation : ajout de peripheriques, mise à jour du système, installation de logiciel, sauvegarde complète du système, ainsi que les evenements anormaux (lenteur inhabituelle du système, messages d'erreurs système ...)

Quelques éléments de méthodologie 2/5

Il faut agir de manière réversible :

Chaque fois que l'on onstalle un péripherique, un logiciel, que l'on met à jour des données, il faut pouvoir revenir en arrière, car l'opération peut être accomplie incorrectement

- Entre deux solutions à un problème d'administration, choisissez toujours la solution réversible
- Il faut conserver l'historique des modification :
  `cp /etc/group /etc/group.001`

Il faut automatiser les procédures :

Toutes les procédures répétitives (sauvegarde, installation d'un poste client, création de comptes ...) doivent être automatisés via des scripts. A défaut de scripts, les procedures manuelles d'exploitation doivent être consigées noir sur blanc

Quelques éléments de méthodologie 3/5

Il faut anticiper les problèmes :

Gouverner, c'est prévoir. Il faut imaginer les événements qui peuvent survenir et qui peuvent affecter l'exploitation

- Vous pouvez tomber malade, l'exploitation doit continuer
- Votre machine ne démarre plus, que faire ?
- Une nouvelle version majeure de votre système est imminente, remet-elle en cause les procedures actuelles ?
- Le local technique brûle, comment redémarrer l'exploitation au plus tôt ?

Quelques éléments de méthodologie 4/5

Avant l'installation :

- **Quel sera l'emploi de la machine ?**
- **Comment sera-t-elle connectée au réseau ?**
- **Qui seront les utilisateurs ?**
- **Quels sont les programmes nécessaires ?**

Quelques éléments de méthodologie 5/5

Être assez large avec ses partitions

- / : système
- swap
- /home : répertoires utilisateurs
- /usr : logiciels

- Les partitions sur lesquelles les utilisateurs ont le droit d'écriture doivent être séparées des autres « /home, /tmp, /var ...»

- Eviter des attaques deny of services (logger,...)

Comment administrer

- **Les commandes d'administration**
- **Les fichiers de configuration**
- **Les scripts**
- **Les outils intégrés d'administration**

La documentation

- **Les pages de manuel**
- **La documentation des paquetages**
- **Les HOWTO et les FAQ :** Issues du projet de documentation de Linux LPD(Linux Project Documentation) http ://www.tldp.org
- **Les pages info :** Une documentation en mode hypertexte disponible dans /usr/share/info
- **La commande locate :** Pratique pour rechercher des fichiers et des répertoires

Plan

Les commandes de gestion des utilisateurs

- `useradd, usermod, userdel` Gèrent les comptes utilisateur
- `groupadd, groupmod, groupdel` Gèrent les comptes de groupe
- `passwd` Modifier le mot de passe d'un utilisateur
- `id` Connaitre son identité
- `who` Affiche les utilisateurs connectés sur le système
- `su` Permet de se connecter à un compte
- `newgrp` Changement de groupe
- `chsh` Change le shell d'un utilisateur

La création d'un utilisateur

Quelques options utiles :

- -c commentaire
- -g initial groupe
- -s shell
- -d home directory
- -m

Ajout d'un utilisateur 'mejdi' dans le groupe 'chefs' avec le shell 'tcsh' :

- `useradd -c 'Mejdi le chef' -g 'chefs' -s '/bin/tcsh' mejdi`

Pour activer le compte, l'administrateur doit définir un mot de passe pour le compte :

- `passwd mejdi`

Les options par défaut de useradd

- **Les options par défaut** se trouvent dans le fichier /etc/default/useradd (où sont listées par l'option -D de useradd)

- `useradd -D`

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
```

groupadd, gpasswd

Pour ajouter un groupe :

- `groupadd chefs`

Pour gérer les utilisateur dans un groupe, on utilise la commande gpasswd :

- -a ajout d'un utilisateur
- -d retrait d'un utilisateur
- -A affectation d'un administrateur du groupe

- `gpasswd -a nicolas chefs`

Les fichiers de configuration 1/3

/etc/passwd :

- Contient les informations des utilisateurs structurées en sept champs sur une ligne séparés par le caractère ’ :’
  1. Username
  2. Mot de passe, encrypté
  3. user id numérique
  4. group id numérique
  5. Nom complet ou autre description du compte
  6. Répertoire d’accueil
  7. Shell de login (programme lancé au login)

Les fichiers de configuration 2/3

/etc/group :

- Contient les informations des groupes structurées en quatre champs sur une ligne séparés par le caractère ’ :’
  1. Nom du groupe
  2. mot de passe du groupe ou ’x’ s’il existe un fichier /etc/gshadow
  3. GID
  4. Liste des utilisateurs du groupe

/etc/shadow :

- Contient les mots de passe chiffrés
- Ne peut être lu que par root
- `pwconv` pour mettre à jour le shadow après la modification de passwd

Les fichiers de configuration 3/3

/etc/skel :

- Contient les fichiers qui seront recopiés automatiquement dans le répertoire des utilisateurs lors de sa création (.bashrc, .bash_profile ...)

- L'administrateur système peut créer des fichiers dans /etc/skel qui fourniront un bon environnement initial pour les utilisateurs

- Cependant, il est préférable de mettre la configuration globale dans des fichiers globaux, comme /etc/profile

Bloquer un compte

- Un moyen simple et de faire précéder le mot de passe par un ’ !’ dans le fichier de configuration

- Lors de l’utilisation d’un fichier /etc/shadow, on peut remplacer également le ’x’ dans le fichier /etc/passwd par un ’*’

- Une autre méthode :
  - `passwd -l` (-u pour débloquer)
  - `usermod -L` (-U pour débloquer)

La meilleure méthode :

- Consiste à changer le shell en un programme spécial qui affiche simplement un message
  - Directement dans le fichier de configuration
  - Ou avec la commande `chsh`

Atelier 1 (1/2)

Exercice 1

- Décrire les étapes nécessaires pour une création manuelle d'un utilisateur ?
- Expliquer avec des exemples à quoi sert le fichier /etc/login.defs ?

Exercice 2

- Est ce que l'utilisateur bin existe, si oui, quel est son UID ?
- Comment feriez-vous pour vous connecter sous le compte bin ?
- Existe-t-il d'autres comptes possédant les droits de root ?
- A quels groupes appartient l'utilisateur bin ?

Exercice 3

- Créez avec `useradd`, en gardant toutes les valeurs par défaut, l'utilisateur pierre. Quel est le groupe de pierre ?

Atelier 1 (2/2)

Exercice 3 (suite)

- Ajoutez pierre au groupe staff. Au besoin, créez ce groupe.
- Afficher les groupes de pierre.
- Connectez-vous au compte pierre nouvellement créé de deux manières, à la connexion et grâce à la commande `su`. Expliquez les deux résultats.
- Que faut-il faire pour pouvoir se connecter au compte pierre ?

Exercice 4

- Ecrivez un script bash qui affiche les deux lignes suivantes :
  `Ce compte a été desactivé!!`
  `Veuillez contacter votre administrateur.`
- Utilisez ce script pour bloquer le compte pierre précédement créé.

Plan

L'arborescence des fichiers 1/2

- / : répertoire racine (contient tous les autres)
- /root : répertoire personnel de l'utilisateur root
- /home : répertoires utilisateurs
- /etc : fichiers de configuration
- /bin : exécutables indispensables au fonctionnement du système
- /sbin : comme /bin mais pour les commandes d'administration
- /usr : principalement le répertoire des commandes du système
  - /usr/bin et /usr/sbin : exécutables non vitaux
  - /usr/man, /usr/doc et /usr/info : manuel, documentation et infos
  - /usr/local : place pour installer des logiciels
  - /usr/include : pour le compilateur C
  - /usr/src/linux : sources du noyau
  - /usr/X11R6 : X-Window Système

L'arborescence des fichiers 2/2

- /var : fichiers variables changés par le système
  - /var/run :fichiers contenat les PID des services actifs
  - /var/log : journaux divers (ex : syslog, auth.log à lire régulièrement pour voir les tentatives de piratages)
  - /var/spool/cron : fichiers de données du service cron
  - /var/spool/lpd : fichiers de données du service d'impression
  - /var/spool/mail : le répertoire des boîtes aux lettres
- /dev : fichiers périphériques
  - /dev/fd0 : lecteur de disquette
  - /dev/hda : 1er disque IDE (hdb, hdc ...)
  - /dev/hda1 : première partition sur /dev/hda
  - /dev/sda : 1er disque SCSI (sdb, sdc ...)
- /proc : utilisé par le système pour mémoriser les processus
- /tmp : utilisé par des commandes pour créer des fichiers de travail

Les types d'accès

Droits normaux :

- (r : en lecture, w : en écriture, x : en exécution)
  - Un fichier est exécuté avec les privilèges de l'utilisateur qui l'exécute

Droits spéciaux :

- (s : SUID, s : SGID, t : sticky bit)
  - Lorsque des programmes ont besoin d'autorisations plus élevées que celles possédées par l'utilisateur
  - Les fichiers dont le bit SUID ou SGID est activé sont exécutés avec les privilèges de l'utilisateur ou du groupe possédant ce fichier, et non avec ceux de l'utilisateur qui exécute le fichier

Les droits spéciaux 1/3

Le SUID : Set-User-Id bit

- Permet à un fichier exécutable binaire de s'exécuter sous l'identité et donc les droits de son propriétaire, à la place des droits de l'utilisateur actuel qui l'exécute
- `chmod u+s fichier`
- `chmod 4??? fichier`

- L'exemple le plus flagrant est celui de la commande `passwd` (rws- -x- -x) qui appartient à l'utilisateur root
- `passwd` sert à modifier les mots de passe stockés dans le fichier /etc/shadow (r- - - - - - - -)

Les droits spéciaux 2/3

Le SGID, Set-Group-Id bit

- Fonctionne différemment selon qu'il est affecté à un fichier exécutable ou à un répertoire
  - Exécutable : Le SGID est similaire au droit SUID sauf qu'il donne à un utilisateur les droits du groupe auquel appartient le propriétaire de l'exécutable et non plus les droits du propriétaire
  - Répertoire : Tout nouveau fichier créé dans un répertoire marqué par le SGID sera de groupe non pas celui du propriétaire du fichier mais celui du propriétaire du répertoire
- `chmod g+s fichier`
- `chmod 2??? fichier`

Les droits spéciaux 3/3

Sticky Bit

- Permet d'interdire à tout utilisateur (sauf le root) de supprimer un fichier dont il n'est pas le propriétaire, quelque soient ses droits
- `chmod o+t repertoire`
- `chmod 1??? repertoire`

Contrôler les autorisations 1/2

Les programmes SUID et SGID

- Un binaire SUID ou SGID mal écrit peut être utilisé pour augmenter rapidement et facilement les privilèges d'un user
- Un assaillant ayant déjà obtenu un accès root peut cacher des binaires SUID un peu partout sur le système
- `find / \( -perm -4000 -o -perm -2000 \) -type f`

Répertoires modifiables par tout le monde

- `find / -type d \( -perm -g+w -o -o+w \)`

Contrôler les autorisations 2/2

Fichiers sans propriétaires

- `find / -nouser -o -nogroup`

Permissions particulières

- Certains fichiers doivent posséder des permissions particulières pour éviter les problèmes de sécurité
  - /etc/shadow : **en mode 400**
  - /etc/passwd , /etc/group : **doit être en mode 644**
  - Les fichiers périphériques **en mode 600**
  - **...**

Les ACL (Access Control List) 1/7

- N'apportent pas une sécurité supplémentaire au système
- Réduisent la complexité de gestion des autorisations
- Stockées sous forme d'attributs étendus au sein des métadonnées du système de fichiers
- Permettent de définir des listes qui accordent ou refusent des accès à un fichier selon les critères que vous indiquez

Les ACL (Access Control List) 2/7

Exemple :

- Soit le fichier /fst.mpasse dont les droits sont les suivants :
  -rw-r- - - - - 1 root root 18 oct 12 12 :10 /fst.mpasse
- Imaginons qu'on veuille le rendre accessible en lecture aux utilisateurs **ndiaye** et **cheikh**, en lecture et écriture à **khadija** et **fatou** et bien sûr rien pour les autres !
- Comment faire ?

Les ACL (Access Control List) 3/7

- Vérifier si le noyau a été compilé avec le support des ACL
  - `grep "ACL" /boot/config-version-du-noyau`
- Activer la prise en charge des ACL par le système de fichiers
  - /etc/fstab : /dev/hda2 /var ext3 defaults,acl 0 0
  - mount : `mount -o remount,acl /var`
- Utiliser les commandes `setfacl` et `getfacl`

Les ACL (Access Control List) 4/7

ACL « minimale » :

- La traduction « en ACL » des droits d'accès traditionnels Unix
  - `touch test.acl`
  - `ls -l test.acl`
    -rw-r--r-- 1 sow tdsi 0 oct 12 12 :10 test.acl
  - `getfacl test.acl`
    #file : test.acl
    #owner : sow
    #group : tdsi
    user : :rw-
    group : :r--
    other : :r--

Les ACL (Access Control List) 5/7

Modifier ACL minimale :

- `setfacl -m u::---,g::---,o::--- test.acl`
- `ls -l test.acl`
  ---------- 1 sow tdsi 0 oct 12 12 :10 test.acl
- `getfacl test.acl`
  #file : test.acl
  #owner : sow
  #group : tdsi
  user : :---
  group : :---
  other : :---

- Composée exclusivement d'éléments de type **propriétaire**, **groupe** et « **reste du monde** »

Les ACL (Access Control List) 6/7

ACL étendue : Prolonge les droits de l'ACL minimale

- Elle contient au moins un élément de type mask et peut contenir des éléments de type utilisateur et/ou groupe
- `setfacl -m u::rw-,u:deye:r test.acl`
- `ls -l test.acl`
  -rw-r-----+ 1 sow tdsi 0 oct 12 12 :10 test.acl
- `getfacl test.acl`
  #file : test.acl
  #owner : sow
  #group : tdsi
  user : :rw-
  user :deye :r--
  group : :---
  mask : :r--
  other : :---

Les ACL (Access Control List) 7/7

ACL par défaut :

- Les ACL par défaut ne peuvent être appliquées qu'aux répertoires et définissent de quels droits un objet du système de fichiers devra hériter (de son répertoire parent) lors de sa création
- `mkdir monrep`
- `setfacl -m d:u:deye:rw- monrep`
- `getfacl monrep`

  ...

  ...

  default :user : :rwx
  default :user :deye :rw-
  default :group : :r-x
  default :mask : :rwx
  default :other : :r-x

Les attributs des fichiers 1/2

- Les attributs d'un fichier sont des caractéristiques supplémentaires qui viennent s'ajouter, dans le système de fichiers ext2, aux caracteristiques habituelles

Les principaux attributs :

- `a` : Le fichier ne peut, en écriture, qu'être ouvert en ajout (Fichier log)
- `i` : Le fichier ne peut pas être modifié, déteruit, renommé (Fichier non modifiable)
- `S` : Les écritures dans les fichiers sont immédiatement effectuées sur le disque (Fichier synchrone)
- `A` : L'heure et la date de dernier accès ne sont plus modifiées (souci de performance)

Les attributs des fichiers 2/2

Les commandes :

- `chattr` Modifier les attributs
- `lsattr` Afficher les attributs

- `chattr +Ss f2`
- `chattr +i f1`
- `lsattr`

```
---i-- ./f1
s-S--- ./f2
```

- `rm f1`

```
rm : détruire le fichier protégé en écriture
'f1' ? o
rm : Ne peut enlever 'f1' : opération non
permise
```

sudo 1/5

- Les privilèges du root ne peuvent pas être répartis (sur Unix classique)
- Il est relativement difficile d'autoriser certains users à effectuer une tâche particulière (par exemple sauvegarde) sans fournir à ces derniers un accès complet au système
- sudo permet aux administrateurs systèmes de donner à certains utilisateurs ou groupes d'utilisateurs, la possibilité d'exécuter une ou plusieurs commandes en tant que root ou en tant qu'un autre utilisateur

sudo 2/5

/etc/sudoers

- La configuration de sudo s'effectue via la commande `visudo` en root qui va éditer le fichier /etc/sudoers : contient la liste des personnes autorisées à utiliser sudo, ainsi que les commandes qui peuvent être exécutées sur chaque hôte

- Définition des groupes d'utilisateurs à qui on veut donner des droits particuliers via la syntaxe **`User_Alias`**

- Définition des groupes de machines à partir desquelles il est possible d'exécuter les commandes définies via la syntaxe **`Host_Alias`**

- Définition des commandes que les utilisateurs vont pouvoir exécuter via la syntaxe **`Cmnd_Alias`**

sudo 3/5

Exemple :

```
# Host alias specification
Host_Alias SECINFO=licpro1, maitrise1
# Définition du groupe administrateurs
User_Alias ADMIN=deye, niang
# Définition du groupe de commandes autorisées
Cmnd_Alias GEST_USER=/usr/sbin/adduser,
/usr/sbin/userdel
# Définition des autorisations
root ALL=(ALL) ALL
ADMIN SECINFO=NOPASSWD :GEST_USER
%bin ALL=(ALL) NOPASSWD : ALL
```

sudo 4/5

Les avantages de sudo :

- La sécurité du système est largement améliorée puisque les commandes sont enregistrées dans un fichier journal
- Vos subalternes peuvent effectuer leur tâches quotidiennes sans posséder les privilèges illimitées de root
- Une seule personne (2 au plus) connaît le mot de passe root réel
- Ces privilèges peuvent être supprimés sans pour autant modifier le mot de passe root

sudo 5/5

Les avantages de sudo : (suite)

- Une liste établie de tous les users qui possèdent les privilèges de root est mise à jour
- Il y a moins de chances pour qu'un shell root soit laissé ouvert par inadvertance
- Vous pouvez utiliser un seul fichier pour contrôler l'accès à un réseau entier

Inconvénient :

- Une brèche dans la sécurité d'une personne qui utilise ce système est équivalent à une faille de sécurité dans le compte root lui-même

Atelier 2 (1/2)

Exercice 1

- Recherchez tous les répertoires accessibles en écriture pour les autres
- En étant connecté en tant qu'administrateur, mettez les droits 700 a l'ensemble des fichiers de l'utilisateur **pierre**
- En utilisant le manuel, retrouvez les différents utilisations du droit **SGID** dans le système linux
- Créez un fichier par la commande `cp` et rendez-le non modifiable. Listez ces attributs . Essayez de le modifier

Atelier 2 (2/2)

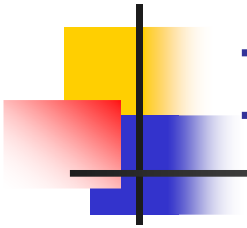
Exercice 2

- Connectez-vous avec le compte pierre et créez une arborescence de fichiers en utilisant les commandes suivantes :

```
cp /etc/psswd /etc/group ~
mkdir ~/boot
cp /etc/inittab /etc/profile ~/boot
```

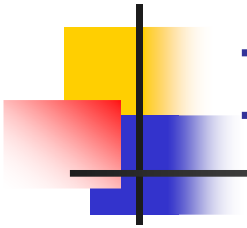
- Listez cette arborescence en utilisant différentes commandes
- Créez un compte utilisateur **invite**. visualisez les ACLs du fichier ~/**boot**/**profile** et attribuez a **invite** le droit de modifier ce fichier. Avant de faire le test d'accès, visualisez à nouveau ces ACLs
- Etendez le droit de l'utilisateur **invite** à toute l'arborescence ~/**boot**. Créez un fichier dans ~/**boot** et visualiser ces ACLs, que constatez-vous ?
- Supprimez les ACLs de l'arborescence.

Plan



Installation de nouveaux logiciels

- Les applications ou logiciels peuvent être installés de deux façons
- Par la compilation des programmes sources
  - tar, gzip, make, gcc
- Par l'installation des paquetages
  - Contiennent les exécutables, fichiers de conf, man pages, licence…
    - **rpm, yum**
    - **dpkg, apt-get**

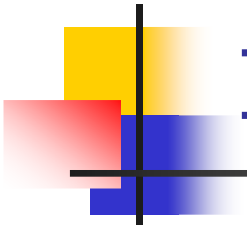


Installation à partir des sources

- Les sources sont composées d'un ou plusieurs fichiers archivés et compressés pour faciliter le transport du programme

- La première étape de l'installation consiste alors à la décompression puis au désarchivage du fichier source
  - Ex : ***tar -xzvf nom-du-programme.tar.gz***
  - Ex : ***tar -xjvf nom-du-programme.tar.bz2***

- L'étape suivante consiste à explorer le programme : les instructions d'installation se trouvent souvent dans le fichier README ou INSTALL ou TODO. Néanmoins, la suite la plus courante de commandes est la suivante :
  - Préparation de la compilation : ***./configure***
  - Compilation de l'application : ***make***
  - Installation de l'application : ***make install***



Installation à partir des sources

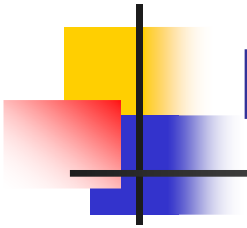
- Un même code source peut être compilé sur n'importe quelle machine UNIX et ce quel que soit son processeur (Intel, Alpha, Risc, PowerPC, etc..)
- Vous pouvez spécifier le répertoire où l'application doit être installée
- Vous pouvez compiler l'application avec des options spécifiques (ajout de modules particuliers, optimisation du binaire en fonction du processeur, etc…)
- Le téléchargement des sources d'une application est beaucoup plus rapide que le téléchargement du binaire ou du paquetage rpm correspondant

Installation avec les paquetages

- La plupart des distributions utilisent un système de gestion de paquetages pour installer, désinstaller ou mettre à jour ses applications

Avantages	Inconvénients
Installation et désinstallation facile	Perte de performance due à la compilation sur une autre plateforme
Mise à jour facile	
Protection des fichiers de configuration	
Gestion des paquetages installés facile	Une corruption de la base de données des paquetages installés peut rendre un système ingérable

- Les deux grandes familles d'outils de gestion de paquetages sont RPM (Redhat Package Manager) et DPKG (Debian packages)

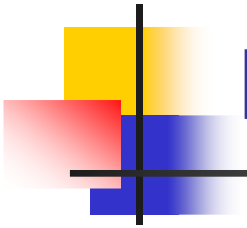


RPM

- RPM garde sa base de données dans le répertoire /var/lib/rpm

- Les options courantes :
  - -i (ou --install) : installe un paquetage
  - -U (ou --update) : met à jour un paquetage déjà installé ou installe si ceci n'est pas encore présent dans le système
  - -e (ou --erase) : désinstalle un paquetage
  - -q (ou --query) : envoie une requête sur un paquetage afin d'afficher des informations

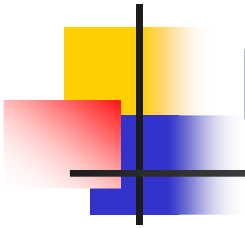
- Ex : ***rpm -ivh xsnow-1.41-1.i386.rpm***



RPM

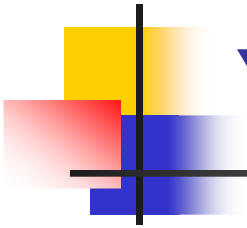
- Options à utiliser avec l'option -q (ou --query)
  - c : affiche la liste des fichiers de configuration d'un paquetage donné
  - f : affiche le nom du paquetage auquel appartient un fichier donné
  - i : affiche les informations relatives à un paquetage
  - l : affiche tous les fichiers et repertoires relatifs à un paquetage
  - p : spécifie que la requête est spécifique au fichier du paquetage

- Afficher la liste de tous les paquetages installés :
  - ***rpm -qa***



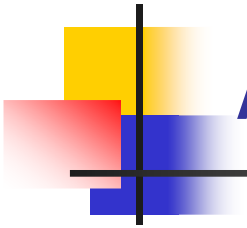
RPM

- Vérifier à partir du nom si un paquetage est déjà installé : ***rpm -qa | grep php***
- Lister le contenu d'un paquetage :
  - ***rpm -ql xsnow-1.41-1***
- Afficher les fichiers de configuration d'un paquetage :
  - ***rpm -qc xsnow-1.41-1***
- Afficher le nom du paquetage auquel appartient un fichier donné : ***rpm -qf /etc/passwd***



Yum

- rpm n'est pas très conviviale notamment du fait qu'il ne prend pas en charge l'installation/désinstallation automatique des dépendances d'un logiciel
- Un gestionnaire de paquetages évolué gérant les dépendances
- Installer plusieurs logiciels
  - ***yum install nom_logiciel_1 nom_logiciel_2 nom_logiciel_3***
- Installer un logiciel en utilisant les caractères jokers
  - ***yum install kde****
- Désinstaller un logiciel
  - ***yum remove nom_logiciel***



Atelier 3

- Utiliser yum pour installer apache, le tester ensuite le désinstaller
- Récupérer maintenant la version source avec wget http://apache.crihan.fr/dist/httpd/apache_1.3.41.tar.gz et l'installer
- Télécharger et installer *john the ripper* ensuite l'utiliser pour tester la rigidité de vos mots de passe

Plan

Plan

Plan

Plan

Plan

Plan

Plan