Administration Unix

Matthieu Pérotin

30 janvier 2006

Notion de bases

- Un réseau founit un moyen de communication entre plusieurs ordinateurs
- Pour communiquer les ordinateurs ont besoin de se mettre d'accord sur la façon de communiquer
- On appel protocole un "langage" utilisable par un ordinateur
- Un certain nombre de normes existent et permettent l'interopérabilité des systèmes et ordinateurs

Le modèle TCP/IP

- Le modèle TCP/IP fournit une modélisation du fonctionnement logique d'un réseau
- Il est basé sur la notion de couches
- Il permet aux applications de s'abstraire du processus physique qui a lieu pour la transmission des messages

Le Modèle TCP/IP

4	Couche Application
3	Couche Transport
2	Couche Internet
1	Couche Accès Réseau

La couche Application

- Regroupe l'ensemble des logiciels accédant au réseau
- Tous les mécanismes d'authentification, session etc.
- Exemple : Navigateur internet, client mail...

La couche Transport 1/2

- Assure l'acheminement des données à la bonne application
- Contient les informations concernant l'état de la transmission

La couche Transport 2/2

- Assure le multiplexage et le démultiplexage des informations
- À cet effet elle introduit la notion de port
- Chaque application d'une machine écoute sur un port donné
- Un port est identifiant numérique

La couche Internet

- Assure la segmentation des données
- Assure l'adressage

La couche Accès Réseau

- Couche la plus bas niveau
- Essentiellement matérielle
- Exemple de couche Accès Réseau : Ethernet

La couche Accès Réseau

- Acheminement des données sur la liaison
- Coordination de la transmission de données
- Format des données
- Conversion des signaux (analogique/numérique)
- Contrôle des erreurs à l'arrivée

Passage des couches

- Construction du message

Message

- Couche transport

E3	Message

- Couche Internet

E2	Data1

E2	Data2

E2	Data3

- Couche Accès réseau

E1	E2	Data1

E1	E2	Data2

E1	E2	Data3

Exemple

Lorsque l'on envoie un courrier au service informatique de l'EPU-DI :

- On commence par écrire le courrier
- On colle un post-it avec le destinataire : SI EPU-DI
- On écrit ensuite l'adresse : 64 av Jean Portalis 37200 Tours
- On confie le tout à La Poste

Exemple 2

Lorsque l'on souhaite envoyer un message à travers un réseau à destination d'un serveur donné :

- On commence par construire le message (Couche application)
- On établit ensuite le service concerné : numéro de port (Couche Transport)
- On rajoute l'adresse IP du destinataire (Couche Internet)
- On envoie le tout dans le cable (Couche Accès réseau)

Un réseau local pour quoi faire ?

- Un réseau local est un ensemble de machines connectées par un réseau
- Un réseau local n'a pas une amplitude géographique très grande (de l'ordre de quelques centaines de mètres)
- Améliore le confort d'utilisation des ressources informatiques
- Partage d'un certain nombre de ressources critiques
- Tout à fait indispensable !

Classiquement

Les services suivants sous fournis par un réseau local

- Partage de fichiers
- Partage de connexion internet
- Authentification centralisée
- Messagerie (e-mail, IM)

Mais aussi ...

Mettre en place un réseau local ce n'est pas seulement mettre en place un certain nombre de services

- Structurer logiquement les ressources matérielles
- Structurer logiquement les moyens humains
- Garantir une qualité de service

Internet ?

- La plupart des services fournis par un réseau local peuvent l'être par Internet
- Un réseau local n'est pas un milieu hostile
- Un réseau local est "rapide"
- Internet est un ensemble de solutions techniques permettant d'interconnecter des réseaux locaux

Structure classique d'un réseau local

Quelques définitions

- On appelle service un logiciel fournissant des fonctionnalités à d'autres logiciels
  Exemples de services :
  - Service web
  - Service mail
  - Service ftp
- On appelle serveur une machine faisant tourner un ou plusieurs services
- Par abus de langage on parle aussi de serveur web, mail, ...

Un serveur comment ça marche ?

- Un serveur écoute sur un port donné
- À la réception d'un message
  - Il l'analyse
  - Il effectue l'action qui lui est demandée
  - Il compose un nouveau message
  - Il envoie ce message au client

L'authentification

- Identifier les utilisateurs
- Problème clef de tout réseau
- Chaque utilisateur n'a accès qu'à un sous ensemble restreint des ressources du réseau
- Identifier les utilisateurs correctement est un des défis de l'administration

Un utilisateur sous Unix

Un utilisateur est identifié par plusieurs informations

- Un nom (aussi appelé login)
- Un mot de passe
- Un identifiant numérique (UID)
- Un identifiant de grouep (GID)
- Un répertoire personnel (Home Directory)
- Un shell par défaut

Utilités

- Le nom et le mot de passe servent au mécanisme d'accréditation (login)
- l'UID et le GID servent à la manipulation des fichiers
- Le répertoire personnel et le shell par défaut donnent les informations nécessaires à la phase de post accréditation

La Phase d'accréditation

- Un utilisateur rentre un login et un mot de passe par le biais d'un programme de login
- Ces informations sont transmises au système d'authentification
- Il compare le mot de passe tapé à celui présent dans sa base de donnée
- Il transmet l'information Succès ou Échec au programme de login
- En cas de succès le shell par défaut est exécuté avec les privilèges de l'utilisateur, et il est placé dans le répertoire personnel.

Comment marche le système d'authentification

- Comme une boite noire !
- Sur un système non connecté à un réseau, les informations sont stockées dans les fichier `/etc/passwd` et `/etc/shadow`
- `toto :x :1003 :1003 :,,, :/home/toto :/bin/bash`
- `toto :$1$fGnA5lkH$/vzJIS49fgiVb04yBKryX. :13177 :0 :99999`

Système basique

- Repose sur deux fichiers particuliers qui sont propres à chaque machine
- Si l'utilisateur a accès a plusieurs machine, il doit changer de mot de passe sur toutes les machines
- Si il change de groupe, on doit changer le groupe sur toutes les machines
- Vite lourd et contraignant

Systèmes avancés

À partir d'un certain nombre d'utilisateurs/machines

- on met en place un système centralisé
- Résoud une partie des problèmes liés à l'accès direct aux machines

Tout est fichier !

- Unix propose une abstraction généralisée de l'ensemble des ressources d'une machine
- **Tout est fichier !**
- Evidemment les fichiers "conventionnels" sont des fichiers
- De façon plus étonnantes les périphériques aussi sont des fichiers

Pas si fou que ça ...

- Si l'on considère une souris :
  - Le système lit des informations envoyées par la souris
  - Ne paraîtrait-il pas logique que la souris écrive dans un fichier ?
- Un dique dur n'est qu'une longue suite de 0 et de 1
- Un fichier est une suite de 0 et de 1

Importance de ce modèle

- Ce modèle unique permet un accès uniforme, quelque soit la ressource
- Aucune différence de gestion dépendemment du périphérique
- La partie bas niveau est cachée dans le driver matériel
- Les périphériques apparaissent tous dans le système de fichier virtuel monté dans /dev

Qu'est-ce qu'un fichier ?

- Un fichier est un objet dans lequel on peut lire ou écrire des données
- Un fichier est la propriété d'un utilisateur et d'un groupe

Revenons sur les permissions

- On appelle permission un ensemble de règles limitant l'accès à une ressource donnée
- Deux types de permissions
  - Les permissions sur les fichiers
  - Les permissions sur le réseau

Permissions sur les fichiers

- Trois types d'opérations sur les fichiers
  - Les droits de lecture
  - Les droits d'écriture
  - Les droits d'exécution
- Un individu donné peut se voir accorder telle permission ou telle autre
- Ces informations sont stockées au niveau du système de fichier

Problème...

- Stocker des permissions individuelles pour chaque fichier induit un espace disque plus important
- Unix propose un modèle à taille fixe
  - Permission du propriétaire
  - Permission du groupe
  - Permission des autres
- Pour chacune de ces catégories, on peut fixer les trois types de droit

Exemple

- La commande ls -la donne toutes les informations disponibles sur un fichier
- ls -la main.tex produit le résultat
- -rw-r–r– 1 matteo matteo 13856 2006-01-29 19 :00 main.tex

Agir sur les permissions

- On peut agir sur les permissions d'un fichier à l'aide de la commande chmod
- Changer le propriétaire et le groupe avec la commande chown

Le superutilisateur

- Il existe un superutilisateur (root)
- Root est au dessus de tous les droits

Le modèle est contraignant

- Il est parfois difficile de donner des permissions fines
- D'autres mécanismes existent, les ACL (Access Control List)
- Mais le système du triplet est simple et la plupart du temps suffisant

Partager des fichiers

- C'est rendre possible l'échange de fichiers entre plusieurs ordinateurs
- Faire en sorte que les données d'un utilisateurs sont accessibles quelque soit le poste qu'il utilise
- Avoir un espace de stockage centralisé

Plusieurs méthodes

- Juste un mécanisme de transfert de fichier (FTP)
  - Un utilisateur peut rappatrier ses données en local
  - Renvoyer des versions modifiées sur le serveur
- Un système de fichier réseau (NFS)
  - Un partage réseau est monté de façon transparente
  - Abstraction totale du mode d'accès

Bénéfices

- Quelque soit le poste sur lequel l'utilisateur se log, il a accès à ses données
- Les données sont sur un serveur unique (Pb d'accès physique aux machines)
- Plus facile à sauvegarder

Points importants

- Les données sont sur un serveur unique ...
- Politique de sécurité rigoureuse nécessaire

Objectifs

- Offrir une plateforme utilisable pour les prochains cours de MIMATS

Moyens

- Une petite dizaine de machines aux performances inégales
- une 40 aine d'heures de travail
- Pas mal d'huile de coude et de bonne volonté :)

Contraintes

- Le projet doit aboutir
- Les machines doivent rester utilisables

Planification

- Installation des systèmes de base
- Configuration du réseau
- Mise en place du partage de fichier
- Mise en place d'une authentification centralisée

Phase critique

- La phase d'installation est la phase réellement critique du projet
- Pas le droit à l'erreur . . .

Concernant la phase d'installation

- Rien de trop difficile en fait
- Il y a cependant une phase d'enquête à mener
  - Quels seront les utilisateurs de la salle ?
  - Quels sont les besoins logiciels ?
- À vous de jouer