Système d'exploitation

LINUX : Les services

IUT G.T.R

2ème Année

Sylvain MERCHEZ

PLAN DU COURS

LINUX : Les services

- Impression
- CRON
- Réseau
- NFS
- NIS
- FTP
- Samba
- Web et Messagerie : cf cours réseau

INSTALLER LINUX : Les services

Le CRON

Le démon crond exécute des commandes utilisateurs . L 'heure et la date d 'exécution sont régies par :

La périodicité qd elles sont soumises par la commande crontab

Le démon atd exécute les commandes différées selon :

L 'échéance qd elle est soumise par la commande at

A leur tour et des que possible qd soumise par batch

Les démons crontd et atd définissent des principes et des contraintes d 'utilisation qui sont toujours valables quel que soit le mode de soumission

INSTALLER LINUX : Les services

Le CRON

- **Pour soumettre une requête :**

Il faut être un utilisateur autorisé : /etc/cron.allow, cron.deny, at.allow et at.deny (pour at et batch)

.deny précise les utilisateurs interdits du service

.allow précise les utilisateurs autorisés du service

Si pas de fichiers, soit tous peuvent utiliser soit seul root

- **Crond mémorise l 'historique des commandes exécutées dans /var/log/cron**

INSTALLER LINUX : Les services

Le CRON

Lorsque le démon exécute une commande, il définit un environnement composé des variables HOME, LOGNAME, SHELL qui vaut par défaut /bin/sh et PATH réduit à /bin:/usr/bin.

Les commandes qui ont besoin d 'un environnement plus complet peuvent être appelées dans un script qui crée les autres variables.

Pour les commandes qui nécessitent une entrée standard il est nécessaire de prévoir une redirection explicite en entrée. A défaut, les sorties sont dirigées dans la boite aux lettres.

Les répertoires des requêtes des démons crond et atd sont /var/spool/cron et /var/spool/at

Le fichier copié porte le nom de l 'utilisateur, max 1 fichier actif par utilisateur

INSTALLER LINUX : Les services

Le CRON

- **Un fichier crontab :**

Min Heure Jour Mois JourSemaine Commande

crontab -e	**édite le crontab**
crontab -l	**liste le crontab**
crontab -r	**supprime le crontab**

Utilisation des variables HOME, SHELL, MAILTO pas LOGAME

Une valeur indique le moment d 'exécution,

Une liste de valeurs séparés par des virgules ou un intervalle indiquent les moments, * signifie le plus grand intervalle

INSTALLER LINUX : Les services

Le CRON

- **Un fichier crontab :**

Exemple :

```
0   21     *      *      *      who
0   0      1      *      1-6    cal
30  12     3,8,15 3-10   *      touch .profile
       6-20/2
```

Le caractère % indique l 'entrée standard

Pour soumettre: crontab moncron
crontab -u utilisateur moncron

7

INSTALLER LINUX : Les services

Le CRON

- **Le fichier crontab :**

En plus des fichiers de requêtes du répertoire /var/cron le démon crond exécute le fichier /etc/crontab

- **La commande at**

La commande at permet de faire exécuter à une date et à ne heure précise (démon atd)
Elle lit les commandes à exécuter depuis l 'entrée standard

at now + 3 hours < fcommande
at 1500 <fcommande (signifie à 15h)
at -l : liste les travaux soumis
at -d : supprime un travail (ou atrm)

8

INSTALLER LINUX : Les services

Le CRON

- **La commande batch**

La commande batch utilise le même schéma de fonctionnement que at, mais on précise pas d 'heure ni de date. Le travail est mis en attente dans une FIFO et sera exécuté à son tour et quand la charge du système le permettra.

Batch < fcommande

9

INSTALLER LINUX : Les services

Les services réseaux

- **Le service inetd**

Le daemon principal du réseau est configuré via les fichiers /etc/services et /etc/inetd.conf

Dans le fichier services, un service est associé à un numéro de port. Les requêtes destinées à un serveur sont identifiées par le numéro de port. Le fichier associe un nom à un numéro de port

Le paramètre nowait indique qu 'il y aura un serveur par client comme in.telnetd

Le paramètre wait indique qu 'il y a un seul serveur pour les clients comme in.talkd

10

INSTALLER LINUX : Les services

Les services réseaux

- **Le service inetd (suite)**

Port : 21 FTP, 23 telnet, 53 DNS, 80 http

Quand un client émet une demande de connexion (FTP par ex) la requête est émise via une socket attachée à un port d 'un numéro supérieur à 1023 alloué dynamiquement pour la session. La requête de connexion reçue, sur le serveur distant, par le démon inetd contient le numéro du port de service demandé (ici 21). Le démon exécute alors un démon serveur in.ftpd dédié à cette connexion et dont la durée de vie est celle de la session FTP.

La modif du fichier inetd.conf => signal 1 au démon inetd

La commande netstat permet de visualiser les connexions actives, les adresses IP et les numéros de port.

11

INSTALLER LINUX : Les services

Les services réseaux

- **Le « Wrapper » tcpd**

Un « wrapper » offre une couche de protection. Il contrôle l 'accès à des services réseaux grâce à des fichiers contenant des listes de contrôles d 'accès (ACL). La plupart de services réseaux sont activés à travers tcpd.

Ex à chq fois qu'une requête est adressée au service FTP, le démon principal du réseau inetd active tcpd plutôt que in.ftpd directement.

Tcpd met à jour un journal de bord et vérifie que le client est autorisé à utiliser le service. Si oui tcpd exécute le service demandé Les listes de contrôle d 'accès sont conservées dans les fichiers /etc/hosts.allow et /etc/hosts.deny S 'ils sont vides, pas de contrôle.

Ex : in.ftpd : LOCAL, societe.com

12

INSTALLER LINUX : Les services

Les services réseaux

- **xinetd**

  Destiné à remplacer inetd. Nouvelles possibilités de configuration et de paramétrage plus fin.

  Exécution soit de inetd ou de xinetd au démarrage : /etc/xinetd.conf

  Ce fichier ne contient pas les services directement mais les répertoires dans lesquels des fichiers décrivent chaque service. Ce fichier remplace une ligne du fichier inetd.conf

id, socket_type (stream pour TCP ou dgram pour UDP), protocole (tcp ou udp), port (n° de port à défaut celui de /etc/services), wait (1 serveur par client si no ou plusieurs sinon), user indique le compte sous lequel s 'exécute l 'appli serveur, server chemin d 'accès au serveur, servers_args arguments transmis au serveur, disable actif ou non

INSTALLER LINUX : Les services

Les services réseaux

- **Les commandes Remote**

  Destinées à faire exécuter une action sur une machine distante sans recourir au service telnet ou ftp.

  Pratiques lors d 'une session ou dans un script

rcp copie des fichiers entre ordinateurs
rcp fichier host:fichier.copie

rlogin permet de se connecter à une machine distante (nécessite le démon in.rlogind qui écoute le port 513
rlogin host
host$ commande
$host exit

INSTALLER LINUX : Les services

Les services réseaux

- **Les commandes Remote**

rsh permet d 'exécuter 1 commande sur une machine distante (nécessite le démon in.rshd qui écoute le port 514)
rsh host commande

rwho donne la liste des utilisateurs connectés au réseau.

Pour que les commandes s 'exécutent sans donner de mot de passe, il faut déclarer des équivalences entre utilisateurs de machines différentes : /etc/hosts.equiv qui contient les hôtes.

Sinon il suffit de mettre les machines dans .rhosts de l 'utilisateur.

INSTALLER LINUX : Les services

NFS (RPC)

- **Les RPC**

  RPC utilise les sockets pour faire dialoguer des applications client-serveur, échange de données et renvoi de résultats.

  Les données échangées sont au format eXternal Data Representation
  La version RPC serveur doit êtres supérieure au client

  /etc/rpc établit une correspondance entre n° prog et nom symbolique

  Le lien entre n° prog et n° port est réalisé par le démon portmap

  rcpinfo permet de dialoguer avec un portmapper et de voir les tables et de voir les rpc actifs sur une machine.

INSTALLER LINUX : Les services

NFS (RPC)

- **NFS serveur**

  NFS est un service qui permet le partage de fichiers à distance

  Les démons : (niveau3)

portmap	permet d 'adresser un service RPC
rpc.mountd	réalise le montage demandé par un client
rpc.nfsd	exécute les requêtes NFS

  Le fichier /etc/exports indique les arborescences qui peuvent être montées à distance. Format : rép client(droits)

  Si modif des fichiers de configuration relancer les démons

INSTALLER LINUX : Les services

NFS (RPC)

- **NFS client**

  Le montage sur le client d'un répertoire distant partagé par le serveur se fait par la commande mount de type nfs

  mount -t nfs host:rep_exporte pt_montage

  ajouter la ligne dans /etc/fstab pour le monter au démarrage.
  Ou mount pt_montage

Test : rpcinfo

showmount	affiche les clients NFS d 'un serveur ou ressources exportées
nfsstat	affiche les statistiques concernant les RPC et NFS

INSTALLER LINUX : Les services

NIS

- **Network Information Service**

  Service réseau qui permet l 'administration centralisée de bases de données de configuration (utilisateurs, groupe, …)

  Les bases de données gérées s 'appellent « NIS map ». Les maps sont utilisées en complément des fichiers /etc/passwd et /etc/group

  Tout fichier structuré en champs peut être géré par NIS

  /etc/hosts et /etc/services sont gérés à travers de maps

  NIS est organisé en domaines. Un client NIS demande à un serveur un champ d'une base de données en fournissant une clé.

  Les maps sont distribuées sur les serveurs du domaine NIS, 1 seul serveur maître par domaine, il est garant de l 'unicité des infos. Les serveurs esclaves contiennent des copies

  Les applications NIS reposent sur les bibliothèques RPC et peuvent donc être utilisées en mode sécurisé (cryptage et authentification)

INSTALLER LINUX : Les services

NIS

- **Network Information Service**

  L 'utilisation de NIS est indispensable pour un parc important utilisant NFS. L 'authentification repose sur un UID et un GID. Il faut s 'arranger pour que les utilisateurs aient les mêmes numéros de sorte que les droits soient identiques sur les machines. NIS résout ce pb en ne créant qu 'un seul utilisateur du domaine.

  NIS ou « Yellow Pages »

Les MAPS

L 'arborescence d 'un serveur NIS est situé dans le répertoire /var/yp et les maps dans /var/yp/domaine. Plusieurs clés de recherche peuvent être définies et 1 fichier de configuration se retrouve alors en plusieurs exemplaires. Ex passwd.byname, passwd.byuid, group, host

La commande make depuis /var/yp/domaine reconstruit les maps.

INSTALLER LINUX : Les services

NIS

- **Configuration d 'un client**

  Installation des paquetages yp-tools et ypbind

  Définir le nom de domaine : domainname nom

  Lancer ypbind (/etc/rc.d/init.d/ypbind)

  L 'ordre de recherche est fixé par /etc/nsswitch.conf

  Ex : /etc/nsswitch.conf

  passwd: files nis
  shadow: files nis
  group: files nis
  hosts: files nis dns

INSTALLER LINUX : Les services

NIS

- **Configuration du serveur maître**

  Installation des paquetages yp-tools, ypserv et ypbind

  Définir le nom de domaine : domainname nom

  Créer les maps, lancer make depuis /var/yp (modifier Makefile ?)
  Préciser les fichiers à gérer :

  all : passwd group hosts rpc services netid protocoles netgrp mail shadow publickey networks ethers bootparams ….

  Exécuter /usr/lib/yp/ypinit -m pour créer les tables

  Démarrer le service ypserv (/etc/rc.d/init.d)

  Lancer ypbind (/etc/rc.d/init.d/ypbind)

INSTALLER LINUX : Les services

NIS

- **Configuration du serveur escalve**

  Modifier sur le maître le fichier /var/yp/ypservers de sorte que le serveur esclave apparaisse. Exécuter make ypservers

  Sur l 'esclave, lancer domainname et ypinit -s

- **Mise à jour des maps des serveurs esclaves**

  Propager les maps du serveur maître vers les esclaves : yppush

  idem depuis les esclaves : ypxfr

- **Supprimer le NIS d 'un client**

  Ajouter les informations liées à la machine dans les fichiers de configuration. Arrêter ypbind

INSTALLER LINUX : Les services

NIS

- **La sécurité**

  Le contrôle d'accès des clients : /var/yp/securenets définit les clients autorisés à se connecter (netmask/réseau)

  La sécurité des maps : /etc/ypserv.conf configure l 'accès aux maps du serveur pour ypserv et rpc.ypxfrd

  option: [yes|no]

  host:map:security:mangle[:filed]

  Les commandes :

  nisdomainname, ypinit, yppasswd, ypcat

  ypwich : affiche le nom du serveur NIS et la liste des maps

  ypmatch affiche les valeurs des clés d 'une map NIS

  ypbind, yppush, ypxfr

INSTALLER LINUX : Les services

NIS

- **Utilisation de NIS pour gérer les comptes utilisateurs**

Exemple 1 : Créer un compte NIS mais rep de connexion sur la machine
Sur serveur : useradd -M nomUtilisateur, passwd nomUtilisateur
cd /var/yp; make; ypmatch nomUtilisateur passwd
Sur l'hote: mkdir /home/nomUtilisateur; cp -r /etc/skel/* /home/nomU
chown nomU /home/nomU

Exemple 2 : Utilisateur connu d 'un hôte, le déclarer en NIS
Sur serveur : useradd -M nomUtilisateur, passwd nomUtilisateur
cd /var/yp; make; ypmatch nomUtilisateur passwd
Sur l'hote: userdel nomUtilisateur

INSTALLER LINUX : Les services

NIS

- **Utilisation de NIS pour gérer les comptes utilisateurs**

Exemple 3 : Serveur NIS devient serveur NFS centralisant les comptes
Sur serveur : S'assurer que le service NFS est démarré et que le répertoire de login est exporté (exportfs)
Ajouter dans le Makefile auto.master et auto.home au lieu de /etc/auto.master et /etc/auto.home
Exécuter la commande make depuis /var/yp

Sur l'hote: Démarrer le service d 'automontage (autofs)
Se connecter avec un utilisateur NIS

INSTALLER LINUX : Les services

FTP

FTP est un service qui permet le transfert de fichiers, le démon ftpd joue le rôle de serveurs de fichiers (démarré par inetd)

- **Le démon in.ftpd**

in.ftpd commandes serveur
-l sauvegarde dans un fichier de log via syslog
-d des infos supplémentaires sont envoyées à syslog
-a utilise le fichier de configuration ftpaccess

- **Les fichiers de configuration**

/etc/ftpusers précise la liste des utilisateurs interdits de ftp
FTPLIB/ftpaccess fichier qui configure l 'accès au service

INSTALLER LINUX : Les services

FTP

- **Le ftp anonyme**

Par défaut, il faut s'identifier et correspondre au fichier /etc/passwd
Pour l 'anonyme, créer l 'utilisateur ftp
Pour sécuriser, le démon in.ftpd exécute chroot sur le répertoire ~ftp
Ainsi, l'utilisateur ne peut remonter dans l 'arborescence ~ftp/pub
1 : Création de /home/ftp; chmod 555 /home/ftp
2 : Création des répertoires bin, lib, etc et pub avec les droits
3 : Copie des fichiers d 'administration passwd et group dans ./etc
4 : Copie de la commande ls et de ses bibliothèques
5 : Déposer les fichiers partagés dans ./pub

INSTALLER LINUX : Les services

DHCP

Le protocole Dynamic Host configuration Protocol permet à une station lors de son démarrage d 'obtenir dynamiquement des informations de configuration (ex adresse IP)

Au démarrage, la station émet un message de diffusion (DHCP discover) de demande d 'adresse IP, la totalité des serveurs qui propose ce service (DHCP offer) reçoivent cette demande

La station choisit le permier qui a répondu toujours par un message de diffusion (DHCP request) afin d'informer les serveurs. Celui qui a été choisi répond par un message de diffusion (DHCP ACK). La station n 'a toujours pas d 'adresse.

INSTALLER LINUX : Les services

DHCP

Un serveur a 3 façons d 'allouer

Manuelle : alloue une adresse IP a une adresse MAC

Automatique : fournit une adresse à partir d'un ensemble d 'adresses réservées à cet effet

Dynamique : idem mais limité dans le temps

Outre l 'adresse, DHCP permet d 'obtenir d 'autres informations comme le netmask, les tables de routage, le DNS, etc ...

INSTALLER LINUX : Les services

GTR

DHCP

- **Configuration d 'un serveur DHCP**
  Installer le paquetage dhcp-*.rpm
  Vérifier que le démon dhcpd est exécuté au démarrage
- **Les fichiers de configuration**

dhcp.conf : fichier de configuration du démon dhcp. Pour chaque sous réseau, il précise les adresses disponibles, la durée du bail et les options de dhcp

dhcp.leases Ce fichier contient les baux en cours

dhcp.leases~ Contient les baux précédents

31

INSTALLER LINUX : Les services

GTR

SAMBA

Samba transforme un système Linux en un véritable serveur de fichiers et d'impression

- **Utilise le protocole Server Message Block (Microsoft) pour accéder aux ressources**
- **Utilise le protocole Netbios RFC pour gérer les noms des ressources et l'échange de données**
- **Ressource accessible sur le réseau grâce à son nom de partage (ex: \\host\rep_partage)**
- **Le client associe une lettre à la ressource partagée**
  Net use u: \\iut-gtr2\home

32

INSTALLER LINUX : Les services

GTR

SAMBA

- **Les composants :**
  - ✓ **Smbd : démon qui fournit les services de partage de fichiers et d'imprimante (lancé au démarrage)**
  - ✓ **Nmbd : démon qui fournit le service netbios et le browser. Il peut servir de serveur wins (lancé au démarrage)**
  - ✓ **Smbclient : permet à linux d'accéder à des ressources d'un serveur smb**
  - ✓ **Testparm : teste la configuration d'un serveur**
  - ✓ **Smbstatus : affiche les connexions en cours**
  - ✓ **Nmblockup : permet d'accéder au Netbios et de connaître le Master Browser**
  - ✓ **Smbpasswd : permet de changer les pots de passe**

33

INSTALLER LINUX : Les services

GTR

SAMBA

- **Lancement et arrêt du service**
  - ✓ **Dans /etc/rc.d/init.d : ./smb start ou ./smb stop**
  - ✓ **Ou utiliser /usr/sbin/samba : samba start; samba stop**
- **La configuration**
  - ✓ **Fichier de configuration : /etc/smb.conf**
  - ✓ **Section entre crochets [global][homes][printers]**
  - ✓ **Spécifier le groupe de travail WORKGROUP**
  - ✓ **Nom du serveur = nom de la machine**
  - ✓ **Serveur wins « wins support = yes »**
  - ✓ **Début de section marque la fin de la précédente; pas de différence entre majuscules et minuscules**

34

INSTALLER LINUX : Les services

GTR

SAMBA

- **La configuration d'une ressource disque Linux**
  - ✓ **Comment =« » : commentaire affiché (voisinage réseau)**
  - ✓ **Path=chemin : précise le chemin d'accès à la ressource**
  - ✓ **Browsable = yes|no : visible ou non dans les ressources disponibles**
  - ✓ **Valid users = liste d'utilisateurs : utilisateurs ou groupe ayant accès à la ressource**
  - ✓ **Invalid users = liste d'utilisateurs : inverse de ci-dessus**
  - ✓ **Public = yes|no : si yes le compte guest est utilisé pour accéder à la ressource**
  - ✓ **Only guest (=yes) : seul le compte invite peut accéder**
  - ✓ **Read only =yes|no; writable = yes|no;**
  - ✓ **Create mask = 0744 : idem que umask**

35

INSTALLER LINUX : Les services

GTR

SAMBA

- **La configuration d'une ressource disque windows**
  - ✓ **Donner un nom de partage**
  - ✓ **Installer ksmbfs paquetage (insmod smbfs.o)**
  - ✓ **Monter le volume :**
    smbmount \\host\rep montage -P passwd
- **Imprimer vers une imprimante Linux**
  - ✓ **La section printers indique le répertoire de la file d'attente de l'imprimante par défaut**
- **Imprimer vers une imprimante windows**
  - ✓ **Smbclient \\server\service -P**

36

INSTALLER LINUX : Les services

SAMBA

- **La sécurité : 2 niveaux essentiels**
  - ✓ **USER-LEVEL : Chaque utilisateur a des droits propres à chaque ressource. Une Access Control List est associée à chaque ressource. Tout utilisateur doit être déclaré sur le serveur. Sous linux même compte /etc/passwd**
  - ✓ **SHARE-LEVEL : Même droits pour tous les utilisateurs; il suffit de connaître le mot de passe associé à la ressource.**

Dans tous les cas pour accéder à une ressource réseaux il faut s'identifier : nom passwd

Cryptage des mots de passe sauvegardé dans /etc/smbpasswd le chemin est précisé dans smb.conf : la commande smbpasswd mksmbpasswd.sh

INSTALLER LINUX : Les services

SAMBA

- **Les paramètres de la sécurité (en section globale)**
  - ✓ **Security=user|share|server|domain : niveau de sécurité; authentification par un autre serveur (server); domain est équivalent à user**
  - ✓ **Passwd server = nom serveur : adresse du serveur d'authentification**
  - ✓ **Encrypt passwords = yes|no**
  - ✓ **Smb passwd file = /etc/smbpasswd : fichier de mots de passe**
  - ✓ **Null passwords = yes|no : accepte mot de passe vide**
  - ✓ **Guest account = un_compte : compte pour les ressources publiques**
  - ✓ **Map to guest = server|bad user|bad password : que faire en cas d'erreur soit connexion refusée soit guest**

INSTALLER LINUX : Les services

SAMBA

- **Samba comme Serveur de domaine**

Les postes Windows peuvent faire partie d'un domaine NT.

Gestion centralisé des comptes sur le Primary Domain Controler. Le PDC valide alors les connexions

- ✓ **Sur le serveur :**

[global]
Workgroup = DOMAIN
Security = user
Encrypt passwords = yes
Smb passwd file = /etc/smbpasswd
Domain logons = yes (accès au domaine)
Local master = yes; preferred master = yes;
Domain master = yes

INSTALLER LINUX : Les services

SAMBA

- **Samba comme Serveur de domaine**
  - ✓ **Sur le serveur :**

[netlogon]
Comment = « »
Path = /export/samba/logon
Public = no
Writable = no
Browsable = no

Mkdir /export/samba/logon
Chmod 770 /export/samba/logon

INSTALLER LINUX : Les services

SAMBA

- **Samba comme Serveur de domaine**
  - ✓ **Sur le poste windows 95/98 :**

Indiquer que le poste fait partie d'un domaine en précisant le nom

  - ✓ **Sur le poste windows NT ou 2000**

Il faut créer sur le serveur un compte spécial correspondant au nom$ de la machine
Pour chaque machine créer un compte
Nom$:*:PID:GID:Comment:/dev/null:/dev/null
Créer le mot de passe : smbpasswd –a-m nom

INSTALLER LINUX : Les services

SAMBA

- **Samba et les journaux de bord**
  - ✓ **Log file = /var/log/log.%m : fichier de log**
  - ✓ **Max log size = 5000 : fixe la taille du fichier de log en ko**
  - ✓ **Debug level=3 : spécifie le niveau de détails**
  - ✓ **Syslog = 1 : Indique les messages envoyés à syslog**

0 uniquement les erreurs

- ✓ **les avertissements**
- ✓ **Remarques**
- ✓ **Informations**

  - ✓ **Syslog only= yes|no : samba n'utilise pas ses propres journaux de bord**

INSTALLER LINUX : Les services

Le courrier électronique

- **sendmail**
  CF Cours Réseaux

43

INSTALLER LINUX : Les services

Serveur DNS

- **named**
  CF Cours Réseaux

44

INSTALLER LINUX : Les services

Serveur Web

- **Apache**
  CF Cours Réseaux

45