MODULE R3

Chapitre 3
Service,
Partage,
Démarrage

R&T 1ère année

Sylvain
MERCHEZ

Plan

ADMINISTRER UN SYSTEME SERVEUR (2)

- Services
- Partages
- Démarrage

Service

Définition

Peut-être exécuté dès le démarrage de la machine, arrêter ou redémarrer très simplement. Ses évenements sont très souvent inscrit dans un journal d'événement.

Utilité variable et parfois source de vulnérabilité

Attention aux dépendances de certains services

Services sous Windows

Conseils

- Utilisez la console "services.msc" de configuration,
- La configuration des services vaut pour tous les utilisateurs.
- Règlez les services un par un ou plusieurs à la fois, mais JAMAIS tous à la fois,
- Lisez bien les descriptions des services...

Pour modifier les propriétés d'un service (le désactiver ou le réactiver), clic droit puis proopriété : demarrage "Automatique", "desactivé" et "manuel".

Liste des Services sous XP

- http://www.depannetonpc.net/article252-comprendre-et-configurer-les-services-windows.html
- Avec un bon paramétrage, le gain en mémoire vive peut être important

Principaux services (serveur)

- Impression
- Réseau
- Partage de fichiers (NFS)
- FTP
- Samba
- Web et Messagerie : cf Module TR2

Impression

- Ajouter, supprimer un travail (job)
- Gère plusieurs imprimantes (locales ou distantes)
- Son nom :
  - Print spooler (windows)
  - Lpd ou cups (Linux)

Taches planifiées

- Son nom :
  - Planificateur de tâches ou Task Scheduler (sous Windows)
  - Cron (Linux)

Taches planifiées sous Linux

- Le démon exécute des commandes utilisateurs. L'heure et la date d'exécution sont régies par :
  - La périodicité qd elles sont soumises par la commande
- Le démon exécute les commandes différées selon:
  - L'échéance qd elle est soumise par la commande
  - A leur tour et dès que possible qd soumise par
- Les démons crontd et atd définissent des principes et des contraintes d'utilisation qui sont toujours valables quel que soit le mode de soumission

Taches planifiées sous Linux

- Pour soumettre une requête :
  - .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

Taches planifiées sous Linux

- Lorsque le démon exécute une commande, il définit un 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 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
- Les répertoires des requêtes des démons crond et atd
- Le fichier copié porte le nom de l'utilisateur, max 1 fichier actif par utilisateur

Taches planifiées sous Linux

- Un fichier crontab :
  - crontab -e édite le crontab
  - crontab -l liste le crontab
  - crontab -r supprime le crontab
- Utilisation des variables HOME, SHELL, MAILTO pas LOGNAME
- Une valeur indique le moment d'exécution,

Taches planifiées sous Linux

- 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

Taches planifiées sous Linux

- Le fichier crontab :

En plus des fichiers de requêtes du répertoire /var/cron le démon

- La commande at

La commande at permet de faire exécuter à une date et à une heure précise (démon atd)

- Elle lit les commandes à exécuter depuis l'entrée standard
  - at now + 3 hours < fcommande
  - at -d : supprime un travail (ou atrm)

Taches planifiées sous Linux

- La commande batch

La commande batch utilise le même schéma de fonctionnement que at, mais on précise pas d'heure ni de date. et

  - Batch < fcommande

Services Réseaux

- Sous windows :
  - Serveur : partage de fichiers
  - Connexions réseau (Network Connections)
  - Gestionnaire de connexion Automatique d'accès distant (Remote Access Auto Connection Manager)
  - Gestionnaire de connexions d'accès distant (Remote Access Connection Manager)
- Sous Linux :
  - Inetd, xinetd, ... (Linux)

Services Réseaux sous Linux

- **Le service inetd**

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

  - 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

Services Réseaux sous Linux

- **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

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).
in.ftpd dédié à cette connexion et dont la durée de vie est celle de la session FTP.

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

Services Réseaux sous Linux

- **Le « Wrapper » tcpd**

Un « wrapper » offre une couche de protection. Il

- 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.

- 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

Services Réseaux sous Linux

- **Xinetd : /etc/xinetd.conf**

Exécution soit de inetd ou de xinetd au démarrage

Ce fichier ne contient pas les services directement mais

chaque service. Ce fichier remplace une ligne du fichier inetd.conf

id, socket_type (stream ou dgram), protocole (tcp ou udp), port (n° port, par défaut /etc/services), wait/nowait (1 serveur/client ou plusieurs), user (indique le propriétaire de l'appli serveur), server (chemin d'accès au serveur), servers_args (arguments transmis au serveur), disable (actif ou non)

Services Réseaux sous Linux

- **Les commandes remote**

Pratiques lors d'une session ou dans un script

- rcp copie des fichiers entre ordinateurs

  rcp fichier host:fichier.copie

  rlogin host

  host$ commande

  $host exit

Services Réseaux sous Linux

- **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

qui contient les hôtes.

Les communications réseaux

- **Les Remote Procedure Call (RPC)**

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

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

- rcpinfo permet de voir les tables et de voir les rpc actifs sur une machine.

Les répertoires partagés

- Possibilité de monter des volumes distants
- Extension : partage de ressources (dvd, ...)

- Sous Windows
  - Clic droit et partager : définir le nom de partage et les autorisations correspondantes
  - Serveur (Server),
- Sous Linux

Le service NFS (sous Linux)

NFS serveur

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

Format : rép client(droits)

Le service NFS (sous Linux)

NFS client

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

Test : rpcinfo

showmount affiche les clients NFS d'un serveur ou ressources exportées

nfsstat affiche les statistiques concernant les RPC et NFS

L'authentification

Nécessité pour le poste client d'appartenir à un domaine déclaré et fonctionnel (serveur de domaine en état de fonctionnement)

- Ouverture de session réseau ou Net Logon (windows)

Network Information Service

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

- /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.

Network Information Service

-

est garant de l'unicité des infos. Les serveurs esclaves contiennent des copies

- 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 »

Network Information Service

- **Les MAPS**

Plusieurs clés de recherche peuvent être définies et 1 fichier de configuration se retrouve alors en plusieurs exemplaires. Ex passwd.byname, passwd.byuid, ...

Network Information Service

- **Configuration d'un client**

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

Network Information Service

- **Configuration du serveur maître**

– 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 ….

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

Network Information Service

- **Configuration du serveur esclave**
  - Modifier sur le maître le fichier /var/yp/ypservers de sorte que le serveur esclave apparaisse. Exécuter make ypservers
  - Mise à jour des maps des serveurs esclaves
  - idem depuis les esclaves : ypxfr
- Supprimer le NIS d'un client

Network Information Service

- **La sécurité**

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

- 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

Network Information Service

- **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

Network Information Service

- **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

Le service FTP

- **FTP est un service qui permet le transfert de fichiers entre machines distantes**
- **Sous windows :**
  - ajouter le service FTP comme composant logiciel et configurer le serveur (ie. Préciser l'emplacement de l'arborescence accessible et les méthodes d'accès) cf. TP2

Le service FTP

- **Sous Linux**
  - La commande in.ftpd permet de configurer le serveur
    - -l sauvegarde dans un fichier de log via syslog
    - -d des infos supplémentaires envoyées à syslog
    - -a utilise le fichier de configuration ftpaccess
  - Les fichiers de configuration :
    - /etc/ftpusers précise la liste des utilisateurs interdits de ftp

Le service FTP

- **Sous Linux**

Pour faire du ftp anonyme, créer l'utilisateur ftp

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 passwd et group dans ./etc

4 : Copie de la commande ls et de ses bibliothèques

5 : Déposer les fichiers partagés dans ./pub

Le service DHCP

- **Le protocole Dynamic Host configuration Protocol permet à une station lors de son démarrage d'obtenir dynamiquement des informations de configuration réseau (ex adresse IP, DNS, ...)**
  - Au démarrage, la station émet un message de

    la totalité des serveurs qui propose ce service (DHCP offer) reçoivent cette demande

    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.

Le service DHCP

- **Un serveur a 3 façons d'allouer**
  - Manuelle : alloue une adresse IP à une adresse MAC
  - 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 ...

Le service DHCP

- **Sous windows**
  - Configurer la plage d'adresses allouables
  - Définir les restrictions ou réservations (en fontion de l'adresse MAC par exemple)

  cf. TP2

Le service DHCP

- **Sous Linux**
  - Installer le paquetage dhcp-*.rpm

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

Le service SAMBA

- 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
- Pour que le client associe une lettre à la ressource partagée
  - La commande net : Net use u: \\iut-gtr2\home

Le service SAMBA

- **Les composants :**
- **Les commandes :**
  - 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

Le service SAMBA

- **Lancement et arrêt du service**
  - Ou utiliser /usr/sbin/samba : samba start; samba stop
- **La configuration**
  - Section entre crochets [global][homes][printers]
  - 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

Le service SAMBA

- **La configuration d'une ressource disque Linux**
  - Comment =« » : commentaire affiché (voisinage réseau)
  - 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

Le service SAMBA

- **La configuration d'une ressource disque Linux**
  - Only guest (=yes) : seul le compte invite peut accéder
  - Read only =yes|no; writable = yes|no;
  - Create mask = 0744 : idem que umask

Le service SAMBA

- **La configuration d'une ressource disque windows**

- **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

Le service SAMBA

- **La sécurité : 2 niveaux essentiels**

  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

  Même droits pour tous les utilisateurs; il suffit de connaître le mot de passe associé à la ressource.

- Cryptage des mots de passe sauvegardé dans /etc/smbpasswd, le chemin est précisé dans smb.conf

Le service 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
  - 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

Le service SAMBA

- **Samba comme Serveur (controleur) de domaine**
  - Les postes Windows peuvent faire partie d'un domaine.

Le service SAMBA

- **Samba comme Serveur (controleur) de domaine**
- Sur le serveur :
  - [global]
  - Workgroup = DOMAIN
  - Security = user
  - Encrypt passwords = yes
  - Smb passwd file = /etc/smbpasswd

Le service SAMBA

- **Samba comme Serveur (controleur) de domaine**
- Pour ajouter des scripts de démarrage, sur le serveur :
  - Public = no
  - Writable = no
  - Browsable = no
  - Mkdir /export/samba/logon
  - Chmod 770 /export/samba/logon

Le service SAMBA

- **Samba comme Serveur (controleur) 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, 2000 ou XP
  - Pour chaque machine créer un compte
    - Nom$:*:PID:GID:Comment:/dev/null:/dev/null
    - Créer le mot de passe : smbpasswd –a-m nom

Le service SAMBA

- **Samba comme Serveur (controleur) de domaine**
- Samba et les journaux de bord
  - 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
    - 2 les avertissements
    - 3 Remarques
    - 4 Informations
- Syslog only= yes|no : samba n'utilise pas ses propres journaux de bord

Le courrier électronique

- **Sendmail (Linux)**
  - A voir dans les modules de TR2
- **Serveur de messagerie (Windows)**
  - A voir dans les modules de TR2

Serveur DNS

- **Named (Linux)**
  - A voir dans les modules de RT2
- **Rôle DNS (Windows)**
  - A voir dans les modules de RT2

Serveur Web

- **Apache (Windows et Linux)**
  - cf. TP3
  - A voir dans les modules de RT2