

## M3.22.4 Services

Jean-François Berdjugin  
IUT 1, Département SRC L'Isle  
d'Abeau

## Références

<http://www.microsoft.com/technet/>  
[http://www.laboratoire-  
microsoft.org/articles/win/boot\\_process/](http://www.laboratoire-microsoft.org/articles/win/boot_process/)

## Services ?

- Besoin de lancer des processus (une application) qui s'exécutent sans être rattaché à un terminal ou à un utilisateur logué

=>

Sous Windows les services

Sous Linux les daemons

## Services Windows

Exemple : Affichage des messages

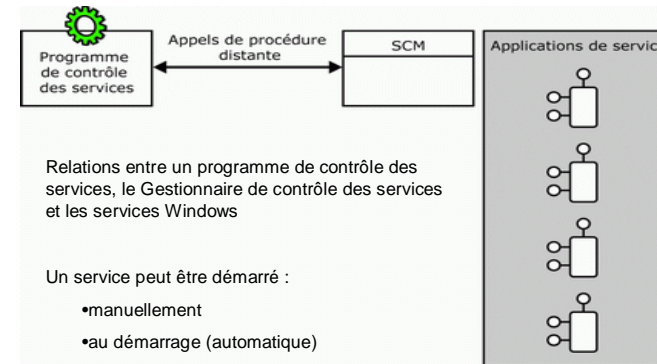
- Description : Ce service donne la possibilité d'envoyer des messages vers d'autres ordinateurs distants (*net send*).
- Configuration : désactivé
- Dépendance :
  - Services dont il dépend
    - Interface NetBIOS (NetBIOS Interface)
    - Plug and Play
    - Appel de procédure distante (Remote Procedure Call)
    - Station de Travail (Workstation)
  - Services dépendants de lui : aucun

## Services Windows

Exemple : WebClient

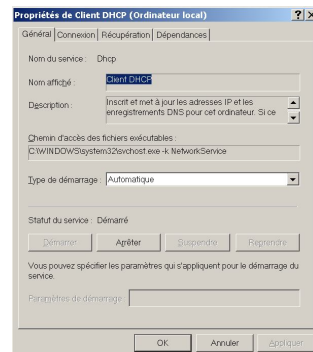
- Description : Permet à un programme fonctionnant sous Windows (généralement un programme Microsoft ou .NET Framework) de créer, modifier et accéder à des fichiers Internet. Nous l'utiliserons pour WebDAV.
- Configuration : désactivé (2003 Server), activé (XP).
- Dépendance :
  - Services dont il dépend : aucun
  - Services qui dépendent de lui : aucun

## Services Windows

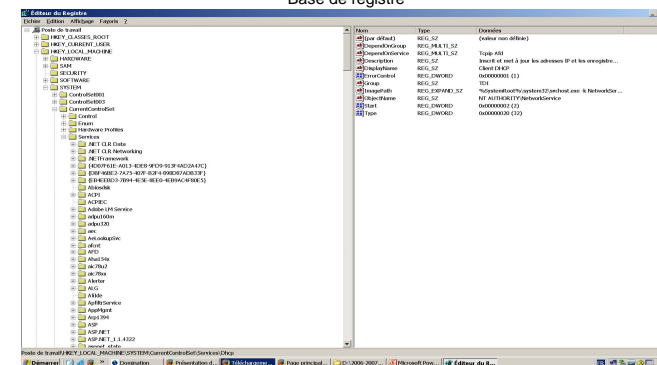


## Services Windows

- Un service Windows inclut un
  - fichier exécutable,
  - un annuaire pour stocker des composants d'application et
  - des paramètres de Registre définissant les paramètres de service.



## Base de registre



HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services (démarré par windows)  
 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\NT\CurrentVersion\svchost (seul dans un processus)  
 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll (plusieurs dans le même processus)

## Services Control

Cette commande permet de communiquer avec le contrôleur de services et les services installés, elle permet la création, l'administration et la suppression des services.

- sc query
- État de tous les services
- sc query dhcp
- État d'un service
- sc stop dhcp
- Arrête le client dhcp
- sc query type= drivers
- État de tous les services de type drivers
- ...
- Rem : un GUI existe : services.msc

## Services Windows

Démarrage d'un service :

1. Récupération des informations de compte stockées dans la base de données des services
2. Connexion du compte du service
3. Création du service en état de veille
4. Attribution du jeton d'accès au processus (politique de sécurité)
5. Autorisation de l'exécution du processus

## IIS

Internet Information Server installe et lance un ensemble de services :

- Service de publication World Wide Web: démon Web,
- Service de publication FTP: démon FTP,
- Simple Mail Transfer Protocol (SMTP): démon SMTP
- Service d'administration IIS: Service nécessaire à l'administration de IIS y compris via le réseau,
- ...

Création :

- IUSR\_[nom\_ordinateur]

Utilisation du compte :

- Système local (un compte local prédéfini )

## Processus vs Service

- Un processus peut héberger un ou plusieurs services
- Tasklist
- Tasklist /svc

## Étape d'un boot Windows

1. Power On Self Test  
BIOS (Basic Input Output System)  
MBR (Master Boot Record) scan pour trouver la partition puis secteur 0 et bootstrap
  2. Sélection de l'OS  
Ntdr fait passer le processeur du mode réel (16 bits) au mode mémoire linéaire 32 bits.  
Ntdr démarre les pilotes de système de fichiers approprié (FAT ou NTFS).  
Ntdr lit Boot.ini et affiche les sélections.  
Ntdr charge l'OS sélectionné.  
Si NT est sélectionné, Ntdr charge Ntdelect.com (sinon, Bootsect.dos).  
Ntdr charge Ntoskrnl.exe, Hal.dll et la ruche "system".
  3. Chargement du Noyau (Kernel)  
ntoskrnl.exe et hal.exe  
Chargement des pilotes du matériel : HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services valeur 0x0
  4. Initialisation du noyau  
Valeur 0x1
  5. Chargement des Services  
Entrée BootExecute  
Winlogon.exe  
Local Security Administration (Lsass.exe)  
Valeur 0x2
  6. Ouverture de session
- Rem :
- Centre d'aide et support -> support -> utilitaire de configuration système
  - /SOS dans le boot.ini pour voir les services chargés

## Vocabulaire

Windows :

Processus une zone  
mémoire dans lequel  
un thread s'exécute

Unix :

Processus s'exécute  
dans son espace  
mémoire

Un thread est un  
processus léger

## Daemon

Un daemon est un processus qui s'exécute en arrière plan, il vient de l'anglais : Disk And Execution MONitor (Moniteur de disque et d'exécution).

Lancé :

- à la main
- au démarrage (rc)
- à la demande (xinetd)

Communique :

- avec des fichiers de log (/var/log/syslog)

Rem:

- netstat -ntap
- /etc/services (référéncés non forcement lancés)

## RunLevel

- Le premier des processus init a pour tâche de lancer les autres processus
- L'ordre des premiers processus (fils de init) est donné par le « runlevel »
- Le fichier /etc/inittab est utilisé
  - Code\_sequence: niveau\_execution:traitement:chemin de commande
  - Selon le runlevel du niveau d'exécution un script dans le /etc/init.d/rc (ou /etc/rc) avec une valeur pour argument a pour but de lancer tous les processus contenus dans /etc/rcX.d (X=valeur du runlevel)

## /etc/inittab

```
#
# inittab This file describes how the INIT process should set up
#         the system in a certain run-level.
#
# Author:   Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#         Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by Mandrakelinux are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

## Optimisation

- Un daemon occupe de la mémoire est utilise du temps processeur, pourquoi ne pas le lancer à la demande ? Et comment procéder ?

=>

- Utiliser un super daemon qui lancera les autres

## Inetd

- L'ancêtre, un chargeur de démon à la demande aussi nommé super serveur de démons
- Les démons sont lancés lorsqu'ils sont appelés et arrêtés après une période paramétrable d'inactivité
- /etc/inetd.conf
- Facile mais comment
  - restreindre l'accès à des machines (filtrer les adresses IP) => utiliser tcpd (tcp Wrapper) qui filtre en fonction des fichiers /etc/hosts.allow et /etc/hosts.deny
  - Restreindre l'accès en fonction de l'heure, de l'interface
  - Limiter la charge des services, le nombre de services
  - Accéder facilement au log d'accès à mes daemons => iptables, PortSentry, ...
- Ou utiliser Xinetd

## Xinetd

Extended Internet Service Daemon

Fichier de configuration : /etc/xinetd.conf

```
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/
```

```
defaults
{
    instances      = 60
    log_type       = SYSLOG authpriv
    log_on_success = HOST PID
    log_on_failure = HOST
    cps            = 25 30
}
includedir /etc/xinetd.d
```

Syntaxe : attribut assignement valeur ...

## Xinetd

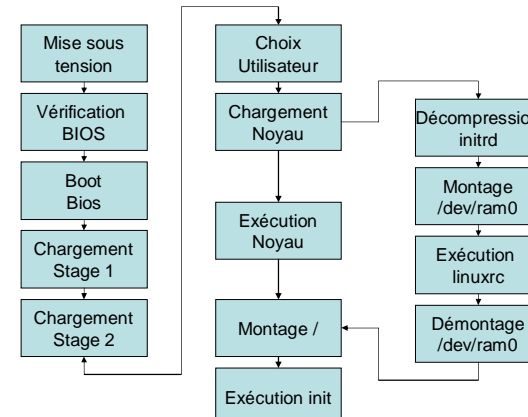
```

/etc/xinetd.d/swat

# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#             to configure your Samba server. To use SWAT, \
#             connect to port 901 with your favorite web browser.
service swat
{
    port          = 901
    socket_type   = stream
    wait         = no
    only_from    = 127.0.0.1
    user         = root
    server       = /usr/sbin/swat
    log_on_failure += USERID
    disable      = yes
}

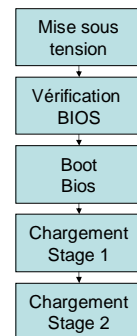
```

## Étapes d'un boot Linux



## Étapes d'un boot Linux - chargement du noyau -

1. BIOS (Basic Input Output System)
  - Inventaire du matériel
  - Choix du périphérique de boot
2. Si disque dur, le MBR (Master Boot Record) contient le code du Boot Loader qui est chargé en mémoire (stage 1)
3. Le MBR charge la configuration du Boot Loader pour savoir sur quelle partition l'OS va s'amorcer (stage 2)



## Grub/LiLo

```

• Linux Loader

/sbin/lilo qui installe le boot loader sur le MBR

/etc/lilo.conf le fichier de configuration

boot=/dev/hda //lilo sur le MBR du premier disque IDE
map=/boot/map //fichier qui contient les infos sur les différents OS
install=/boot/bootb //fichier on place la deuxième partie du programme Lilo.
default=linux
prompt
timeout=50
message=/boot/message //affiche /boot/message
other=/dev/hda1
label=windows
table=/dev/hda
image=/boot/vmlinuz
label=linux
root=/dev/hda4
append=""
read-only

Rem : password=mot_de_passe interdit la commande linux single qui permet de changer le mot de passe root

```

## Grub/LiLo

- Grand Unified Bootloader
- /sbin/grub
- /sbin/grub/grub.conf
- ```
# grub.conf fictif
default=0
timeout=10
splashimage=(hd0,1)/grub/splash.xpm.gz
title Red Hat Linux (2.4.18-5)
  root (hd0,1)
  kernel /vmlinuz-2.4.18-5 ro root=/dev/hda6
  initrd /initrd-2.4.18-5.img
title Red Hat Linux (2.4.18-5) vga=791
  root (hd0,1)
  kernel /vmlinuz-2.4.18-5 ro root=/dev/hda6 vga=791
  initrd /initrd-2.4.18-5.img
title Red Hat Linux 7.2 (2.4.9-21) /dev/hdb5 6/3/2002
  root (hd1,4)
  kernel /boot/vmlinuz-2.4.9-21 ro root=/dev/hdb5
title windows 95
  makeactive
  chainloader +1
title windows XP
  rootnoverify (hd0,3)
  chainloader +1
```

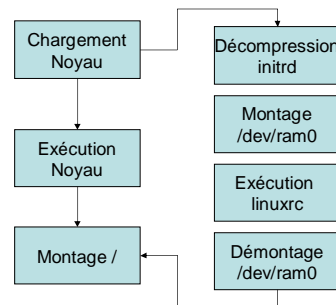
## Autre Boot Loader

- etherboot
- netboot

## Initialisation du noyau

- Le noyau une fois chargé s'exécute et détecte les périphériques :
- Décompression de INITIAL RamDisk, une image d'un noyau minimal dans /dev/ram0
  - Système de fichier initrd est monté puis exécution de linuxrc
  - Montage de / et /root
  - Lancement de /sbin/init le père de tous les processus

Rem: dmesg pour afficher les messages du boot



## Conclusion

Windows/Linux un même besoin : lancer des applications en arrière plan associé à des droits particulier.

Une solution centralisée :

- Gestionnaire de contrôle des services
- Xinetd, inetd

Un ordre de lancement imposé au démarrage