Le système d'exploitation

Cours Windows 2008-2009

Franck Rupin - Laurent Gydé

Architecture et mécanismes internes.

1 Les différentes versions de Windows.

2 Définition des concepts et de la terminologie.

3 Architecture du système.

4 Mécanismes internes.

Les différentes versions de windows

1 MS-DOS

2 Windows 95/98/Me

3 Windows NT

4 Windows 200x/Xp/vista

Les différentes versions de windows

1981 IBM sort le Personal computer (PC) accompagné d'un système
d'exploitation appelé MSDOS 1.0 fourni par Microsoft.

Caractéristiques:

- système 16 bits
- interface en ligne de commande
- monoutilisateur
- monotâche
- taille 8Ko

Les différentes versions de windows

1983 Msdos 2.0 est disponible:
taille 24 Ko
fournit un interpréteur de commandes « shell »

1986 Msdos 3.0 tient dans 36 Ko

Évolution régulière depuis, avec une interface toujours en ligne de commande.

Les différentes versions de windows

Microsoft, inspiré par Apple, décide de doter Ms-dos d'une interface graphique.

Windows sort en 1985 sans grand succès.

En 1987 une version 2.0 dédiée au PC/AT d'IBM n'a pas plus de succès.

À partir de 1990 les versions 3.0, 3.1 et 3.11, vont connaitre un vif succès.

Les différentes versions de windows

Windows 3.x n'est alors qu'un simple habillage graphique de Ms-dos.

C'est ms-dos qui contrôle la machine et le système de fichiers.

Les différentes versions de windows

1995 sortie de windows 95

Cette version n'élimine pas encore Ms-dos

Cette version de Windows et la dernière version de MS-dos 7.0, voient l'arrivée de nouvelles caractéristiques:

- gestion de la mémoire virtuelle
- gestion des processus
- multiprogrammation

Les différentes versions de windows

Windows 95 n'est pas encore entièrement un système 32 bits.

Il utilise encore le système de fichiers Ms-dos mais apporte une amélioration: les noms de fichiers longs à la place du traditionnel système 8.3 de Ms-dos.

Les différentes versions de windows

1998 Sortie de windows 98.

Ce dernier n'élimine pas encore Ms-dos présent dans sa version 7.1.

Une nouvelle gestion des disques permet d'avoir des partitions de taille plus grande.

La différence principale vient de l'intégration d'internet dans l'interface utilisateur.

Les différentes versions de windows

En 2000, Microsoft commercialise une version majeure de windows 98: Windows Me.

Les améliorations portent sur la gestion et le partage d'imprimantes, la musique et les images, la messagerie instantanée, les jeux.

Possibilité de restaurer son système dans un état sauvegardé.

Les différentes versions de windows

Windows NT (Nouvelle Technologie) est une série de systèmes d'exploitation multitâche, préemptif multi-utilisateur et multiprocesseur.

Cette génération de systèmes d'exploitation ne repose pas sur Ms-dos.

Windows NT 3.1	Workstation, Advanced Server	juillet 1993
Windows NT 3.5	Workstation, Server	septembre 1994
Windows NT 3.51	Workstation, Server	mai 1995
Windows NT 4.0	Workstation, Server, Server Enterprise Edition, Terminal Server, Embedded	juillet 1996
Windows 2000	Professional, Server, Advanced Server, Datacenter Server	février 2000
Windows XP	Home, Professional, Media Center, Tablet PC, Starter, Embedded	août 2001
Windows Server 2003	Standard, Enterprise, Datacenter, Web, XP Pro x64 (build 3790)	mars 2003
Windows Vista	Édition Familiale Basic, Édition Familiale Premium, Professionnel, Entreprise, Édition Intégrale	février 2007

Les différentes versions de windows

Windows NT ciblait les applications professionnelles, dans un contexte ou les systèmes d'informations étaient dominés par les systèmes mainframe.

Des caractéristiques de haute disponibilité et de sécurité étaient intégrées à windows NT.

La première évolution majeure fut la version 4.0 de NT. C'est cette version qui va rencontrer le plus succès, car proche de l'interface de windows 95.

Les différentes versions de windows

Caractéristiques:

- Système entièrement 32 bits
- Système sécurisé
- Espace d'adressage privé pour chaque processus Ms-dos
- Support unicode
- Support multiprocesseur
- Code de système d'exploitation réentrant
- Système de fichiers NTFS
- Données critiques du système non modifiables par l'utilisateur

Les différentes versions de windows

Windows 2000 est le successeur de windows NT4, à l'origine son nom aurait dû être NT5.

Windows 2000 sorti en Décembre 1999.

Ce produit fut considéré uninaniment comme étant le plus stable des systèmes de Microsoft.

Les différentes versions de windows

Windows 2000 serveur offre les avantages de Windows NT serveur mais aussi des fonctionnalités et possibilités supplémentaires.

- Active directory, un système de gestion centralisée des services réseau, supportant la norme Ldap
- Prise en charge de nombreux protocoles industriels standards et de normes de sécurité (DNS, kerberos...)
- Une interopérabilité avec d'autres systèmes d'exploitation (unix).
- La gestion centralisée des clients.
- Des interfaces de gestion personalisables (mmc)

Les différentes versions de windows

Microsoft Windows XP

Windows XP est le successeur de Windows Me et de Windows 2000

La version Home, est le premier système d'exploitation familial Microsoft basé sur le noyau et l'architecure NT. Il s'agit de la version 5.1 de NT

Windows XP est sorti en 2001.
La version Pro, est une édition destinée à l'entreprise.

Les différentes versions de windows

Fonctions offerte par Windows XP Professionnel :

- Possibilité d'être membre d'un domaine
-Support de NTFS et des ACL
-Contrôle à distance de l'ordinateur par le bureau à distance
-une fonction qui permet de faire une copie automatique des fichiers d'un autre ordinateur ;
-EFS, qui est le système de cryptage intégré des fichiers
-Support de plusieurs processeurs, le support des processeurs bi-cœurs

Les différentes versions de windows

Windows XP offre un certain nombre de nouveautés:

Mise en veille et redémarrage rapide,
La possibilité d'intégrer de nouveaux pilotes,
Changement rapide d'utilisateur,
Le bureau à distance,
Le support de la plupart des connexions par modems ADSL, WIFI, ou firewire.

Les différentes versions de windows

Windows XP a reçu beaucoup de critiques pour sa vulnérabilité aux virus et autres menaces.

Les utilisateurs de l'édition Familiale se voient attribuer par défaut, des droits d'administrateur. donnant un accès illimité au système.

Windows est la cible privilégiée de pirates et créateurs de virus. Une faille de sécurité est souvent invisible jusqu'à son exploitation,

Microsoft publie des patchs corrigeant les failles de sécurité nouvellement découvertes.

Les différentes versions de windows

Sorti en 2003, windows 2003 serveur fait suite à Windows 2000 serveur.

Windows 2003 Server améliore la compatibilité avec Active Directory et offre un meilleur support de déploiement.]

Le niveau de sécurité par défaut a été amélioré notamment grâce au pare-feu intégré la désactivation des services par défaut.

Le gestionnaire de serveur : Un outil de gestion des rôles du serveur.

Les différentes versions de windows

Améliorations d'Active Directory.
Gestion améliorée des stratégies de groupe.

La gestion des disques a été améliorée: possibilité de sauvegarde depuis une copie de fichiers.

Améliorations du scripting et des outils en ligne de commande.

Technologie watchdog timer permettant un redémarrage du système après un délai de non-réponse.

Les différentes versions de windows

Windows Server 2003 R2

Mise à jour de Windows 2003 Server publiée en Décembre 2005.

La mise à jour R2 est disponible pour les versions x86 et x64 mais pas pour les versions Itanium.

Les différentes versions de windows

Microsoft Windows Server 2008

Dernier système d'exploitation serveur de Microsoft.

Successeur de Windows server 2003

La sortie du produit date de février 2008. Comme Windows vista, Windows Server 2008 est basé sur le noyau windows NT version 6.0.

Les différentes versions de windows

Réécriture de la couche réseau.

Améliroation du déploiement, des outils de supervision, de diagnostique, de la journalisation, de la sécurité et du pare feu, bitlocker pour le chiffrement des données.

Amélioration des fonctions du noyau comme la gestion mémoire, le système de fichiers, la gestion des disques...

Le Sp1 de vista apporte une grosse partie de la réécriture du noyau introduite par Windos 2008 server.

Les différentes versions de windows

Core Serveur

offre la possibilité d'installation ramenée au strict minimum.
La configuration s'effectue en ligne de commande, ou à distance par mmc.

Un Core Serveur peut être configuré pour certains rôles de base:

- Contrôleur de Domaine/Active Directory Domain Services
- Serveur DNS,
- Serveur DHCP,
- Serveur de fichiers et serveur d'impression,
- Serveur Windows media,
- Terminal services
- Serveur web IIS 7
- Serveur virtuel Hyper-V

Architecture et mécanismes internes.

1 Les différentes versions de Windows.

2 Définition des concepts et de la terminologie.

3 Architecture du système.

4 Mécanismes internes.

• Définition des concepts et de la terminologie

1 API Win32

2 Processus, Threads, Jobs, fibres

3 Mémoire virtuelle

4 Mode utilisateur / Mode noyau

5 Objets

Définition des concepts et de la terminologie

Processus :

Programmes et processus sont deux notions à distinguer. En effet un programme peut être considéré comme un jeu d'instructions statiques, alors qu'un processus contient les ressources employées pendant l'exécution du programme.

Définition des concepts et de la terminologie

Un processus est caractérisé par plusieurs éléments:

- Un espace d'adressage virtuel privé: ensemble d'adresses mémoires virtuelles utilisables par le processus
- Un programme exécutable: définit le code et les données et qui est mappé dans l'espace d'adressage virtuel.
- Liste de Handles: Pointeurs vers d'autres ressources système.
- Un contexte de sécurité: appelé jeton d'accès.
- Un identifiant: ID processus (PID sous unix)
- Au moins un thread d'exécution.

Définition des concepts et de la terminologie

Chaque processus pointe vers le processus parent. Si le processus Parent se termine avant le processus enfant, il n'y a pas d'actualisation de cette information, car elle n'est pas primordiale.

Il n'y a pas la même notion de hiérarchie de processus comme sous unix.

Le gestionnaire de tâches est l'outil de surveillance des processus par excellence sous Windows.

Définition des concepts et de la terminologie

Thread :

Dans un processus c'est le Thread qui est l'entité ordonnancée par le système d'exploitation.

Composants d'un thread:

Contenu d'un jeu de registres qui représentent l'état du processeur.

Deux piles une pour l'exécution en mode noyau et une pour l'exécution en mode utilisateur.

Une zone de stockage Privée (Thread-local Storage) utilisable par les sous-systèmes et les bibliothèques exécutables et les dll.

Un ID unique.

Définition des concepts et de la terminologie

Les threads ont parfois leurs propre contexte de sécurité: utilisé par les serveurs multithread.

Les threads partagent l'espace d'adressage du processus.

Les threads d'un processus peuvent lire et écrire dans la mémoire d'un autre thread du processus.

Définition des concepts et de la terminologie

Notion de Job:

Un objet Job permet de regrouper un ensemble de processus et de les gérer comme un tout. L'objet Job compense le manque d'arborescence telle qu'elle existe sous unix.

Définition des concepts et de la terminologie

Mémoire virtuelle

Sous Windows l'espace d'adressage de mémoire virtuelle est linéaire. Chaque processus à l'illusion de disposer d'un espace privé considérable.

Le gestionnaire de mémoire, avec une aide matérielle, mappe les adresses virtuelles avec les adresses physiques.

Le système d'exploitation prévient les conflits entre processus ainsi que l'intégrité des données.

Définition des concepts et de la terminologie

La mémoire physique est généralement inférieure à la mémoire virtuelle, le gestionnaire de mémoire transfert donc une partie de la mémoire vers le disque: c'est la pagination.

Quand un thread accède à une adresse de mémoire qui a été paginée, le gestionnaire de mémoire recharge en mémoire la page.

Le transfert mémoire/disque est aussi appelé swap.
La taille théorique de l'espace d'adressage virtuel, sur un système 32 bits est de 4Go.

Définition des concepts et de la terminologie

Le système partage cet espace pour moitié aux processus pour leur stockage privé, et l'autre moitié, pour la mémoire protégée du système.

Windows 64 bits offre un espace d'adressage pour les processus de 8192 GO et de 6657 Go pour le système sur les architectures x64, 7152 GO IA-64 et 6144 GO sur les architecures Itanium.
Cela ne représente que les limites d'implémentation, et pas les limites d'architecture.

Définition des concepts et de la terminologie

mode noyau/ mode utilisateur

Windows utilise deux modes d'accès au processeur: mode utilisateur et mode noyau.

Le code des applications est exécuté en mode utilisateur.

Le mode noyau donne accès à toute la mémoire du système et à toutes les instructions du processeur.

L'utilisation de ces deux modes d'exécution, préserve l'intégrité du système en garantissant qu'une application problématique ne viendra pas endommager le système.

Définition des concepts et de la terminologie

Le code système et le code des pilotes de périphériques, s'exécutent en mode noyau.

Une fois en mode noyau, il n'y a plus de mécanisme de protection. C'est pourquoi il faut faire très attention quand on charge un pilote tierce partie, car s'il est mal écrit il peut compromettre l'intégrité du système.
C'est l'une des raisons qui a poussé Microsoft vers la signature des pilotes.

Les applications utilisateurs, effectuent souvent des commutations de contexte afin de basculer dans le mode noyau pour effectuer certaines opérations privilégiées.

Définition des concepts et de la terminologie

Objets

le concept d'objet est fondamental dans les systèmes Windows 200x

Les ressources système comme les processus, threads... sont représentés par des objets.

Ils fournissent une interface standard pour accéder et manipuler les ressources et les structures de données du système.

Définition des concepts et de la terminologie

Cette interface standard se caractérise par:

- le nommage de l'objet
- un handle
- L'accès via le gestionnaire d'objets.

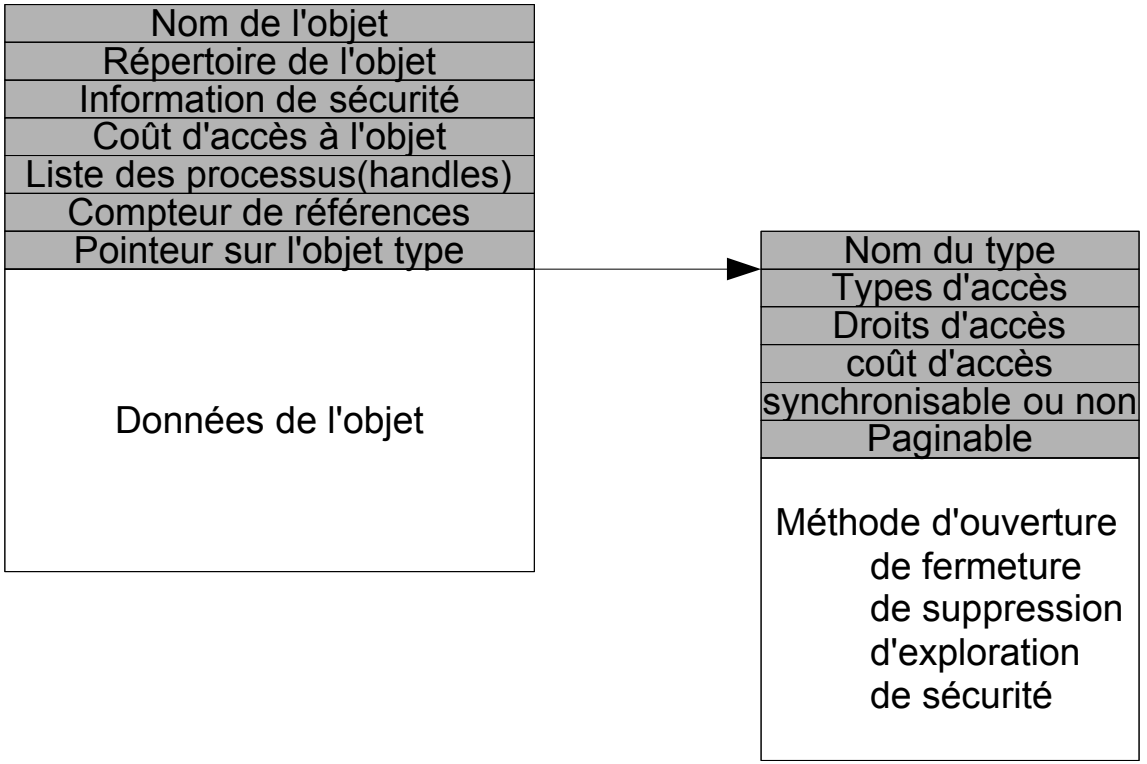
Le gestionnaire d'objets permet de localiser les contrôles de sécurité.

Le partage d'objets est pris en charge de manière uniforme.

Possibilité de savoir à tout instant quels sont les objets utilisés.

Définition des concepts et de la terminologie

Structure d'un objet:



Définition des concepts et de la terminologie

un en-tête formé d'informations communes à tous les objets

Le champs coût d'ouverture: en fonction du capital alloué à un job auquel appartient un processus, le cout déterminera le nombre maximum de l'objet qu'il pourra ouvrir.

Le mécanisme de récupération de mémoire est chargé de libérer la mémoire qu'occupe un objet.
Utilise le compteur de références.
Si compteur de références = 0 alors aucun programme ne référence l'objet.
Un compteur de références de l'exécutif est aussi utilisé.

Si les deux compteurs de références = 0 alors l'objet peut être détruit.

Définition des concepts et de la terminologie

Les objets sont typés, cela signifie qu'ils possèdent des propriétés communes en fonction de leur type.

exemple de types d'objets:

Process, Thread, Open File, Key, Device driver...

l'objet type possède des pointeurs vers des méthodes standard du type comme: open close delete...

Architecture et mécanismes internes.

1 Les différentes versions de Windows.

2 Définition des concepts et de la terminologie.

3 Architecture du système.

4 Mécanismes internes.

Architecture du système

La structure du système

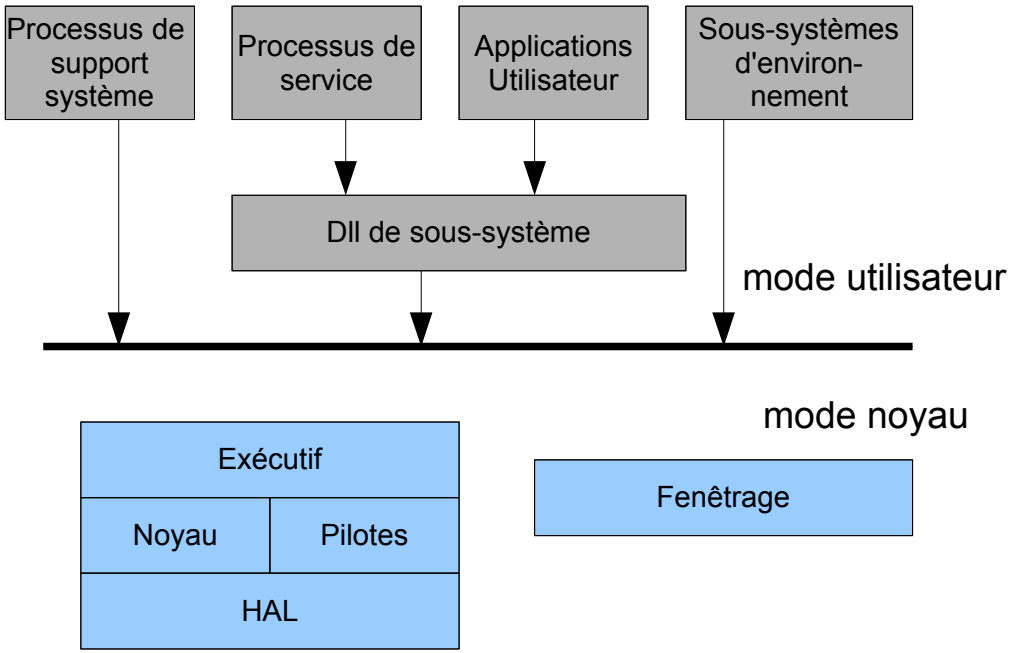
- HAL
- Couche noyau
- Exécutif
- Pilotes

Les sous-systèmes d'environnement

Les processus système

La structure du système

Schéma simplifié



La structure du système

HAL
Hardware Abstraction Layer ou couche d'abstraction matérielle.

Les composants internes de Windows n'accèdent pas directement au matériel, ils passent par les routines de Hal quand ils ont besoin d'informations liées à la plateforme.

Hal masque les détails dépendants du matériel comme les interfaces d'E/S.

HAL assure donc la portabilité du système Windows indépendamment de la plateforme matérielle.

La structure du système

Le Noyau (Ntoskernel.exe)

Ensemble de fonctions qui fournissent les mécanismes fondamentaux utilisés par l'exécutif (ordonnancement des threads),
et les fonctionnalités de bas niveau (ventilation des interruptions).

Le noyau est écrit en C.

La structure du système

Il rend le reste du système d'exploitation indépendant du matériel.

Il fournit un mécanisme de commutation de contexte, il sauvegarde l'ensemble des registres CPU associés à un thread.

c'est lui aussi qui ordonnance les threads.

La structure du système

L'exécutif
C'est la couche supérieure de Ntoskrnl.exe

Il est indépendant de l'architecture.

Il est composé de 10 composants:

- Le gestionnaire d'objets,
- Le gestionnaire d'E/S,
- Le gestionnaire de processus,
- Le gestionnaire de mémoire,
- Le gestionnaire de sécurité,

La structure du système

Le gestionnaire de cache,
Le gestionnaire Plug and Play
Le gestionnaire d'alimentation électrique,
Le gestionnaire de configuration,
Le gestionnaire d'appels de procédures locales

La structure du système

Pilotes de périphériques

Chaque pilote peut contrôler un ou plusieurs périphériques d'E/S.

Les pilotes ne sont pas inclus dans Ntoskrnl.exe, mais dans le registre. Ce dernier est chargé automatiquement au démarrage.

Il existe des pilotes pour des périphériques comme les disques, les imprimantes.... mais aussi pour des périphériques internes: par exemple le système de fichiers est traité comme un périphérique.

La structure du système

Le module de fenêtrage

Il fournit des appels systèmes pour permettre aux applications utilisateurs d'écrire sur l'écran.

Architecture du système

La structure du système

Les sous-systèmes d'environnement

- Ntdll.dll
- Sous-système windows
- sous-système posix
- sous-système os/2

Les processus système

Les sous-systèmes d'environnement

Ntdll.dll

C'est une bibliothèque utilisée par les dll de sous-systèmes qui contient deux types de fonctions:

- des stubs de ventilation de services systèmes pour l'exécutif.

- des fonctions de support interne.

Les sous-systèmes d'environnement

Sous-système windows

Csrss.exe est le processus du sous-système d'environnement qui est chargé de la gestion des éléments suivants:

- Fenêtre console

- Création/suppression des threads et des processus

- Support des processus 16 bits (Virtual Dos Machine)

Les sous-systèmes d'environnement

win2k.sys est le pilote de périphérique mode noyau il contient :

- le gestionnaire de fenêtres
- le GDI (Graphics Device Interface)

Les sous-systèmes d'environnement

Les dll de sous-système traduisent les fonctions de l'API win32 exécutées en mode utilisateur, en appels système exécutés en mode noyau.

Kernel32.dll, Advapi32.dll, user32.dll, gdi32.dll

Les sous-systèmes d'environnement

Le sous-système POSIX

POSIX est un ensemble de normes pour les systèmes de type Unix.

windows implémente la norme POSIX.1 (le système reconnaît par exemple la fonction fork), cependant ce n'est pas un environnement complet de programmation.

Ce sous-système facilite le portage d'application unix vers windows.

Comme les applications posix sont limités à l'ensemble des services définis dans POSIX.1, Microsoft fournit Services Windows pour unix pour contourner cette limitation.

Les sous-systèmes d'environnement

Le sous-système OS/2

OS/2 est l'interface de présentation qu'avait choisi Microsoft au départ pour Windows NT.

Mais c'est Win32 qui a été finalement adopté.

Windows NT respecte la norme OS/2 1.X, c'est à dire OS/2 mode caractère (OS/2 2.X étant le mode graphique).

Les applications disposent de leur propre espace d'adressage et tournent en mode multitâches préemptif.

Architecture du système

La structure du système

Les sous-systèmes d'environnement

Les processus système

- Processus inactifs
- Processus system et threads système
- Gestionnaire de session
- Winlogon Lsass et userinit

Les processus système

Tout système Windows exécute les processus suivants:

- Processus inactifs du système

- Processus system

- Gestionnaire de session (smss.exe)

- Processus d'ouverture de session (winlogon.exe)

- Service Control manager (services.exe) et les processus enfants (svchost.exe)

- Serveur local d'authentification (lsass.exe)

Les processus système

Processus inactifs du système

Il ne s'agit pas réellement d'un processus, car il n'existe pas d'exécutable « processus inactif du système.exe »

Le processus inactif du système (system idle process) correspond aux ressources disponibles du système.

Il représente le taux d'inactivité du processeur.

Les processus système

Processus et threads système

Le processus system contient en fait des threads spéciaux appelés threads system qui s'exécutent uniquement en mode noyau.

Ils exécutent du code chargé dans l'espace système.

Les threads système n'ont pas d'espace d'adressage de processus utilisateur.

Les threads système sont la propriété du processus system, mais un pilote peut créer un thread système dans n'importe quel processus.

Les processus système

Le gestionnaire de session

Premier processus mode utilisateur créé par le système: smss.exe

C'est le thread système mode noyau effectuant la phase finale de l'initialisation de l'exécutif et du noyau. Chargé de la création de variables d'environnement.

Il lance les processus csrss.exe et winlogon.exe

Après avoir effectué les étapes d'initialisation, le thread principal de smss.exe attend les handles des processus de csrss et de winlogon.

Les processus système

Winlogon lsass et userinit

Winlogon gère les ouvertures et fermetures de session interactive.

Winlogon est informé qu'un utilisateur veut entrer sur le système par la combinaison clavier SAS (secure attention sequence) ctrl+alt+supp

Le SAS sert à protéger les utilisateurs contre les logiciels de capture de mots de passe car cette combinaison de touches ne peut pas être interceptée par une application en mode utilisateur.

Les processus système

Les informations d'identification de l'utilisateur sont récoltées par une dll nommée GINA (graphical identification and authentication): msgina.dll

Le login et le mot de passe sont envoyés au processus serveur d'authentification de sécurité locale : lsass.exe

LSASS appelle le module d'authentification implémenté sous forme de dll pour la vérification: dans active directory ou dans la SAM.

Les processus système

Si l'authentification réussit, LSASS appelle une fonction pour créer un jeton d'accès qui contient les informations concernant le profil de sécurité de l'utilisateur (sid privilèges...)

Winlogon utilise ce jeton d'accès pour créer les processus initiaux.

Les processus initiaux sont indiqués par la valeur de registre userinit HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\winlogon.

Les processus système

Userinit effectue l'initialisation de l'environnement de l'utilisateur (exécution de des scripts d'ouverture de session, application des stratégies de groupe).

Ensuite il consulte la valeur de registre shell de la clé winlogon et crée un processus pour le shell.

Userinit se termine c'est pourquoi explorer est affiché sans parent.

Winlogon est actif aussi lors de la fermeture de session et à chaque fois qu'il intercepte le SAS.

Architecture et mécanismes internes.

1 Les différentes versions de Windows.

2 Définition des concepts et de la terminologie.

3 Architecture du système.

4 Mécanismes internes.

Mécanises internes

Les services

Le registre

L'amorçage

Mécanises internes

Le gestionnaire de service SCM (service control manager)

Le terme service sous windows peut désigner un processus serveur ou encore un pilote de périphérique.

Nous allons traiter des processus en mode utilisateur.

Les services sont comparables aux démons unix.

Ils démarrent automatiquement sans ouverture de session interactive.

En principe ils n'interagissent pas avec l'utilisateur connecté.

Mécanises internes

Le contexte de sécurité d'un service est un point important car il définit les ressources auxquelles il peut accéder.

Le compte **system local** est le compte sous lequel sont exécutés des éléments clés de windows mode utiliateur :

- le gestionnaire de sessions smss.exe,
- les sous-système csrss.exe,
- LSASS.exe

Mécanises internes

Ce compte est extrêmement puissant:

- il est membre du groupe administrateurs locaux
- il dispose de tous les privilèges
- il accès à tous les fichiers et clés de registre
- les processus exécutés sous ce compte disposent du profil HKU\.DEFAULT
- si un système appartient à un domaine le compte inclut le SID de l'ordinateur sur lequel est exécuté un processus de services. un service sera donc authentifié automatiquement sur les autres machines de la même forêt.

Mécanises internes

Compte **service réseau**

ce compte est utilisé par les services qui veulent se faire authentifier sur d'autres machines du réseau via le compte d'ordinateur sans pour autant avoir besoin d'appartenir au groupe administrateur, ni d 'employer autant de privilège que le compte system local.

ce compte est plus restreint que le compte system local.

les processus exécutés sous ce compte utilisent le profil du compte service réseau HKU\S-1-5-20

Mécanises internes

Compte **service local**

ce compte est quasiment identique au compte service réseau sauf qu'il ne peut accéder qu'aux ressources réseau autorisant l'accès anonyme.

Le service d'accès à distance au registre s'exécute sous ce compte par exemple.

Mécanises internes

Le registre

Le registre est une base de données contenant la configuration et le contrôle du système.

C'est un élément fondamental du système.

Sous windows 3.1x les informations de configuration étaient réparties dans des fichiers .ini

À partir de windows 95 l'ensemble de ces informations ont été regroupées dans une base de données appelée Registre.

Mécanises internes

Il faut voir le registre comme une sorte de système de fichiers.

Dans la terminologie du registre un clef représente un répertoire, et une valeur représente un fichier.

Une valeur est composée d'un nom, d'un type, et de la donnée.

Le nom est une chaîne de caractères.

Le type est l'un des 11 types standards.

La donnée contient l'information

Mécanises internes

Le registre est organisé en 6 clefs racines:

HKEY_LOCAL_MACHINE contient toute l'information de configuration du système courant. Elle possède 5 sous-clefs.

HARDWARE: matériel et mappage des matériel sur les pilotes

SAM: Information de sécurité sur les utilisateurs.

SECURITY: règles de sécurité du système

SOFTWARE: Informations sur les applications installées

SYSTEM: Informations sur l'amorçage du système.

Mécanises internes

HKEY_USERS contient le profil de tous les utilisateurs

HKEY_CURRENT_CONFIG contient des informations qui sont mises à jour en temps réel, elles sont régénérées après chaque boot.

HKEY_CLASSES_ROOT (HKCR) contient les informations sur les applications comme les associations entre extensions de fichiers ce qui permet de lancer automatiquement l'exécutable correspondant. Cela correspond à HKEY_LOCAL_MACHINE\SOFTWARE\Classes.

Mécanises internes

HKEY_CURRENT_USER (HKCU) contient les informations concernant l'utilisateur connecté. C'est un lien vers HKEY_USERS.

HKEY_PERFORMANCE_DATAgénéré dynamiquement contient des compteurs mesurant les performances du système

Mécanises internes

Les types des valeurs

Chaque clé peut contenir des valeurs parmi les types suivants:

REG_BINARY binaire,
REG_DWORD , nombre codé sur 32 bits
QWORD REG_QWORD nombre codé sur 64 bits
REG_SZ chaîne simple,
REG_EXPAND_SZ, Chaîne extensible qui permet l'utilisation de variables d'environnement

Mécanises internes

REG_MULTI_SZ, Chaîne multiple
REG_NONE donnée non typée
REG_RESOURCE_LIST description de ressource matérielle
REG_RESOURCE_REQUIREMENTS_LIST exigences de la ressource
REG_FULL_RESOURCE_DESCRIPTOR description de ressource matérielle
REG_LINK lien symbolique unicode

Mécanises internes

Les ruches

Les clefs sont la représentation logique du registre, tel qu'il est chargé en mémoire.

Les ruches quant à elles représentent la structure physique du registre, tel qu'il stocké dans le système de fichiers, afin d'y sauvegarder les mises à jour.

À l'amorçage du système, les ruches sont chargée depuis le disque dur, en mémoire.

Mécanises internes

Voici les chemins d'accès de quelques ruches avec leurs clefs correspondantes.

HKEY_LOCAL_MACHINE\SYSTEM \windows\system32\config\system
HKEY_LOCAL_MACHINE\SAM \windows\system32\config\ sam
HKEY_LOCAL_MACHINE\ SECURITY \windows\system32\config\security
HKEY_LOCAL_MACHINE\SOFTWARE \windows\system32\config\software

HKEY_USERS\sid_user \documents and settings\nom user\ntuser.dat

L'amorçage

L'opération préalable au démarrage de windows est la séquence de boot.

Le processus de boot va initialiser les processus de démarrage du système.

Le démarrage matériel consiste à lire le premier secteur du premier disque: Le MBR (master boot record), puis faire un saut à cette adresse.

Le programme est chargé de lire la table des partitions et détermine la partition contenant un système bootable.

L'amorçage

Une fois trouvé il lit le premier secteur (appelé secteur de boot) et effectue un saut à cette adresse.

Le programme du secteur de boot consulte le répertoire racine de sa partition à la recherche d'un fichier nommé ntldr.

Une fois trouvé, il charge en mémoire ntldr et l'exécute, ce qui provoque le chargement de windows.

L'amorçage

ntldr lit le fichier boot.ini, qui donne toutes les versions disponibles de hal.dll et de ntoskrnl.exe.

Il contient d'autres informations comme le nombre de cpu, la quantité de mémoire disponible, l'allocation de mémoire utilisateur, la fréquence de l'horloge temps réel.

ntldr choisit alors hal.dll et ntoskrnl.exe ainsi que le pilote video bootvid.dll

Il consulte le registre pour déterminer les pilotes au boot (clavier souris, composants carte mère).

Enfin il charge tous ces pilotes et passe la main à ntoskrnl.exe

L'amorçage

Une fois démarré le système effectue une initialisation générale.

Il appelle chaque composant de l'exécutif afin qu'il s'initialise.

Le gestionnaire d'objets initialise son espace de nommage.

Le gestionnaire de mémoire initialise la table des pages.

Le premier véritable processus utilisateur va être créé: le gestionnaire de session (smss.exe)

Une fois ce processus activé, le boot est achevé.

L'amorçage

Le gestionnaire de session est un programme natif qui effectue de véritables appels système, sans passer par le sous-système win32 qui n'est pas encore actif à ce moment.

Sa première tâche consiste à lancer cet environnement: crss.exe

Il consulte le registre afin de savoir ce qu'il lui reste à charger, ouvre d'autres dll, crée des fichiers paginés.

Une fois terminé il crée le processus de connexion winlogon.exe.

L'amorçage

Le système est opérationel.

Il faut à présent démarrer les services et autoriser les connexions utilisateur.

Winlogon démarre le serveur local d'authentification lsass.exe ainsi que le gestionnaire de services services.exe.

Le SCM consulte le registre pour obtenir la liste des processus utilisateur à démarrer.

L'amorçage

winlogon gère aussi la connexion des utilisateurs.

Les échanges durant la connexion sont pris en charge par msgina.dll

Après la connexion réussie, winlogon retrouve le profil de l'utilisateur dans le registre et détermine l'interpréteur de commandes à lancer: par défaut explorer.exe

Références

Le cours s'appuie largement sur ces références:

Web:

http://msdn.microsoft.com/en-us/default.aspx

http://technet.microsoft.com/en-us/default.aspx

http://technet.microsoft.com/en-us/sysinternals/default.aspx

Livres spécifiques windows:

La collection des kits de ressources chez microsoft presse:

- -Windows 2000 server (6 ouvrages)
- -Securité windows
- -Au coeur de windows (lecture difficile)

Livres généralistes :

A.Tanenbaum: Systèmes d'exploitation;Architecture de l'ordinateur

Références

Livres électroniques :
http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploy