

Chapitre 10

NOTIONS SUR WINDOWS NT

Le système d'exploitation WINDOWS NT (*New Technology*) a été conçu par Microsoft entre 1988 et 1993. Cinq objectifs étaient poursuivis en créant ce nouveau SE :

- offrir une interface homme-machine conviviale et standard pour tous ceux qui étaient familiers de l'environnement Windows sous MS-DOS, voire d'Apple

- conception modulaire du SE permettant son évolution

- portabilité du code sur toute machine utilisant un espace d'adressage sur 32 bits

- compatibilité **binaire** avec toutes les applications Microsoft existantes et compatibilité au niveau source avec la norme POSIX (Portable Operating System Interface for Computer Environment, 1988 et 1990). Cette norme est destinée à rendre les applications compatibles avec les différentes versions d'UNIX

- optimisation des services système et mécanisme d'échanges à grande vitesse pour accroître les performances

Outre la version de base pour postes de travail de gamme convenable, WINDOWS NT existe dans la version *Advanced Server* qui offre des services étendus de partage de ressources et d'administration.

1. CARACTERISTIQUES DE WINDOWS NT

4 caractéristiques principales permettent à WINDOWS NT d'être considéré comme un descendant évolué d' OS/2 d'IBM, de VMS de DEC et d'UNIX :

1.1 Utilisation du modèle client-serveur

Il assure l'accès transparent aux services de WINDOWS NT pour les clients hétérogènes WINDOWS, MS-DOS, OS/2 ou POSIX. Le dialogue entre clients et serveur se fait par échange de messages.

1.2 Modèle en couches

Il est utilisé notamment dans le système d'E/S et dans la partie de plus bas niveau : le noyau et la couche d'abstraction du matériel (Hardware Abstraction Layer, **HAL**)

1.3 Modèle de traitement symétrique

SMP (Symmetric MultiProcessing) permet de mieux exploiter la puissance du processeur physique, notamment tous les processeurs à architecture CISC (Complex Instruction Set Computer) tel que le 486 ou le Pentium d'INTEL ou à architecture RISC (Reduced Instruction Set Computer).

1.4 Utilisation des objets

L'utilisation des objets pour représenter les ressources du système permet de gérer les ressources de façon homogène et sécurisée.

Windows NT peut travailler selon deux modes :

- **le mode utilisateur** : mise en œuvre des sous-systèmes protégés ou serveurs, ainsi que des applications clientes

- **le mode noyau** : exécution des fonctions système ou exécutif NT

2. MODE UTILISATEUR

Dans ce mode, on accède à l'exécutif NT (code système) uniquement à travers ses services. Les sous-systèmes ou serveurs sont protégés.

Les communications entre sous-systèmes se font par échange de messages et plus rarement par partage de mémoire. Chaque serveur dispose d'une interface de programmation d'application (Application Programming Interface ou **API**) que les clients et autres serveurs peuvent appeler.

On distingue deux classes de sous-systèmes protégés ou serveurs :

2.1 Les sous systèmes d'environnement

Ils offrent un pseudo-environnement Windows, MS-DOS, OS/2 ou POSIX et proposent chacun une API spécifique avec un espace d'adressage privé pour être protégés les uns des autres :

- le sous-système **Win 32** offre l'API de Windows et l'interface graphique de WindowsNT (fenêtres). Il gère aussi les saisies utilisateur et les sorties de données de toutes les applications. Il est le lien entre l'utilisateur et le reste du SE. Lors du lancement d'une application, Win 32 crée un processus et en donne le contrôle au sous-système concerné

- le sous-système **POSIX** offre une API pour applications UNIX

- le sous-système **OS/2** offre une API pour applications OS/2

- le sous-système **MS-DOS** (Virtual DOS Machine ou **VDM**, client de Win 32) offre aux applications MS-DOS le contexte d'un processus appelé machine virtuelle DOS 5.0, avec un processeur virtuel Intel x86, sans son SGF propre , mais avec espace d'adressage privé et pilotes

- le sous-système **Windows 16 bits** (**WOW**, Windows on Win 32, client de Win 32) est une VDM multitâches dont chaque tâche fait tourner une application Windows 16 bits. Le code du noyau de Windows 3.1 est chargé au-dessus du code de MS-DOS. La gestion des fenêtres est faites par l'API Win 32

2.2 Les sous systèmes intégraux

Ils exécutent les fonctions de base du SE :

- les sous-systèmes **réseau** gèrent les demandes d'E/S sur le réseau
- le sous-système de **sécurité** maintient une base de données contenant des informations de sécurité sur les comptes utilisateurs locaux ou distants. Il est chargé de l'authentification des utilisateurs lors d'une tentative de connexion locale ou via le réseau.

Ainsi, dès qu'un utilisateur ouvre une session dans WINDOWS NT après avoir fourni un nom de compte et un mot de passe corrects, le sous-système de sécurité construit un objet appelé ***jeton d'accès*** et l'attache en permanence au processus utilisateur lancé à la connexion. Un jeton d'accès comprend l'identificateur personnel de sécurité de l'utilisateur (Security Identifier ou **SID**) et la liste des groupes dont il fait partie. Le jeton d'accès identifie tout processus et ses tâches (threads) auprès du SE.

Lorsqu'on crée un objet partageable par plusieurs processus, un descripteur de sécurité est créé dans l'en-tête de l'objet. Il s'agit d'un pointeur sur une liste de contrôle d'accès (Access Control List ou **ACL**) dont chaque élément (Access Control Entry ou **ACE**) comporte deux champs : un utilisateur ou un groupe, une liste de droits d'accès à l'objet (cf. exemple ci-dessus). Pour des raisons d'efficacité, les contrôles sont effectués à l'ouverture d'un objet et non pas à chaque utilisation.

3. MODE NOYAU

C'est le mode dans lequel tourne le code système ou **exécutif** de WINDOWS NT. On ne peut accéder dans ce mode au matériel et à la mémoire.

L'exécutif est le moteur du SE. Il peut gérer un nombre quelconque de processus serveurs.

L'exécutif NT est composé de plusieurs éléments :

3.1 Le gestionnaire d'objets

gère les structures de données de l'exécutif, modélisant les ressources du SE. Elles sont utilisées par les programmes en mode utilisateur au travers des services.

3.2 Le moniteur de référence de la sécurité

surveille les ressources du SE en contrôlant l'accès aux objets par les processus. Quand un processus demande l'ouverture d'un objet, le moniteur consulte la liste de contrôle d'accès de l'objet et le jeton d'accès du processus.

3.3 Le gestionnaire de processus

crée, termine les processus et les tâches (**threads**), suspend et relance l'exécution des tâches, gère leurs données

3.4 L'appel de procédures locales

LPC (Local Procedure Call) transmet les messages entre client et serveur sur la même machine

3.5 Le gestionnaire de mémoire virtuelle

gère la pagination, fournit un espace privé d'adresses mémoire pour chaque processus et en protège l'accès

3.6 Le noyau

traite les interruptions, réalise l'ordonnancement des tâches, synchronise les processus, fournit des objets et des interfaces de bas niveau au reste de l'exécutif

3.7 Le système d'E/S

Il comprend :

- le gestionnaire d'E/S qui gère des modèles d'E/S indépendants des périphériques
- les pilotes de fichiers (drivers) qui traduisent les demandes d'E/S fichiers
- le redirecteur et le serveur du réseau : pilotes spécifiques qui transmettent et reçoivent des demandes d'E/S avec une autre machine du réseau
- les pilotes de périphériques (device drivers) gèrent la lecture ou l'écriture sur un périphérique physique ou un réseau
- le gestionnaire de mémoire cache

3.8 La couche d'abstraction du matériel (HAL)

masque à WINDOWS NT les détails d'implémentation de la plate-forme : contrôleurs d'interruption, mécanismes de communication multiprocesseur, interfaces d'E/S, etc...