CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

LE SYSTÈME DE FICHIERS NTFS

LE SYSTÈME DE FICHIERS NTFS

Le système de fichiers de Windows

- Windows NT utilise le système de fichiers NTFS (New Technology File System) qui est le successeur de FAT (File Allocation table)
- Actuellement 5 versions du format NTFS:
  - 1.0 : Win NT 3.1, première version
  - 1.2 : Win NT 3.51, ajout de la compression et des ACLs
  - 3.0 : Win 2000, ajout des quotas, Chiffrement
  - 3.1 : Win XP, ajout de redondance de la MFT
- Depuis Win XP, l'ajout de fonctionnalités a été réalisé sur le driver NTFS.sys sans toucher au format NTFS 3.1

LE SYSTÈME DE FICHIERS NTFS

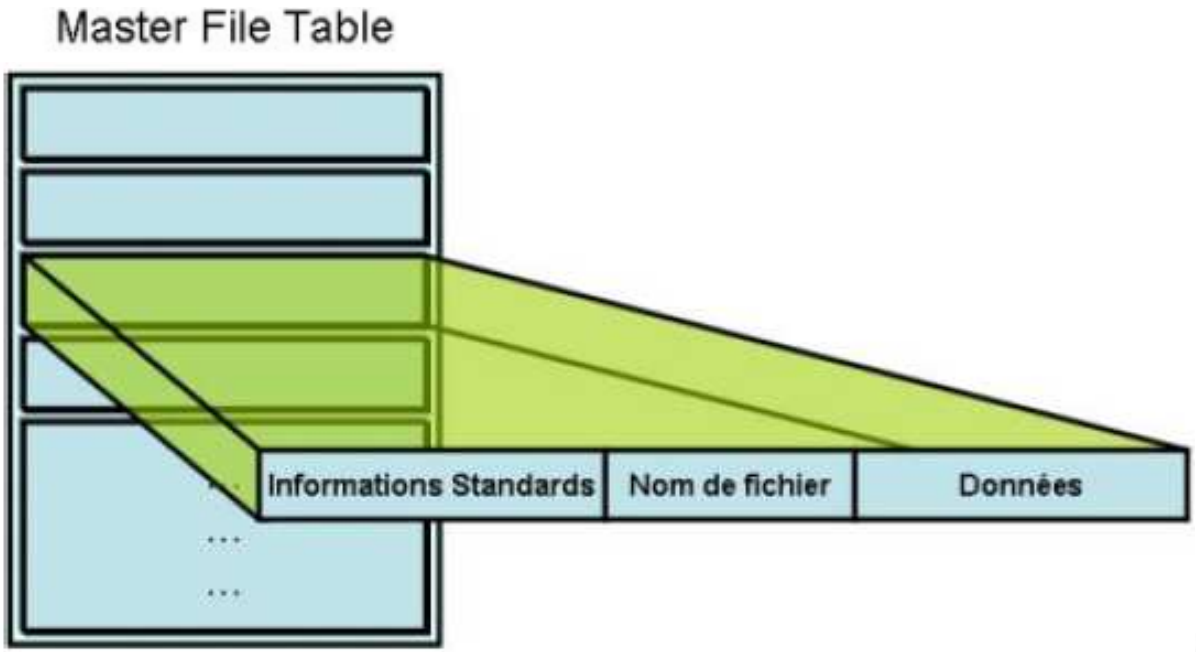
Principales fonctionnalités de NTFS

FEATURE	FAT32	NTFS
Max. Partition Size	2TB	2TB
Max. File Name	8.3 Characters	255 Characters
Max. File Size	4GB	16TB
File/Folder Encryption	No	Yes
Fault Tolerance	No	Auto Repair
Security	Only Network	Local and Network
Compression	No	Yes
Conversion	Possible	Not Allowed
Compatibility	Win 95/98/2K/2K3/XP	Win NT/2K/XP/Vista/7

LE SYSTÈME DE FICHIERS NTFS

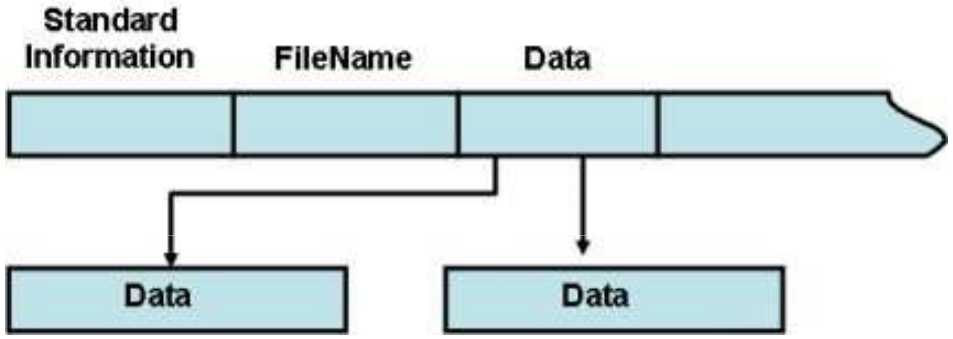
La table de référencement des fichiers

- NTFS utilise une MFT (Master File Table) dans laquelle chaque fichier ou dossier est référencé
- Si le fichier ou le dossier est de petite taille, la donnée est directement stockée dans la MFT



LE SYSTÈME DE FICHIERS NTFS
MFT

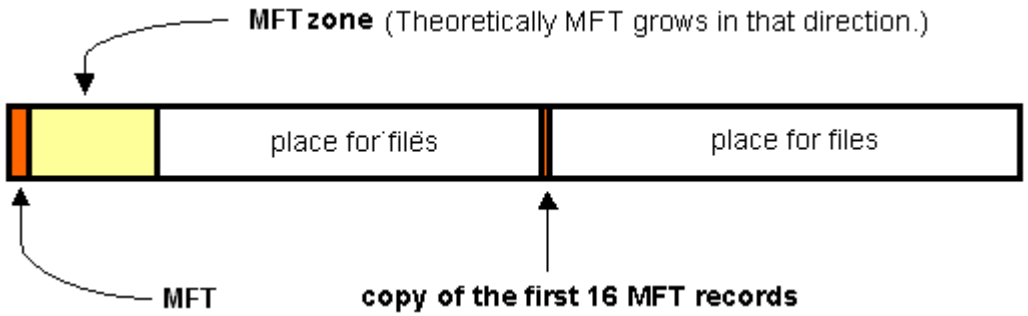
- Dans la cas d'une taille élevée de la donnée, le champ de données contiendra son adresse de stockage



- Un formatage au format NTFS va découper le stockage en clusters de taille fixe (taille de 512o à 64ko)
- Un fichier est découpé en clusters, le dernier ne sera dans la plupart des cas pas rempli

LE SYSTÈME DE FICHIERS NTFS
Structure de la MFT

- La MFT contient les attributs pour chaque élément :
  - Nom du fichier ou du dossier
  - Attributs : caché, lecture seule, compressé, …
  - ACLs
  - Index (si dossier) : liste les fichiers du dossier
  - Données : liste d'adresses et le nombre de clusters
- La MFT étant critique, une réservation de l'espace est réalisée au formatage et une copie est réalisée régulièrement



LE SYSTÈME DE FICHIERS NTFS

Effacement d'un fichier

- Lorsque l'OS demande au driver ntfs.sys de supprimer un fichier, le driver modifie dans la MFT un attribut du fichier pour indiquer qu'il est supprimé
- Le fichier ne sera plus visible par l'OS mais il reste toujours référencé et présent sur le disque
- Cette technique permet de gagner en rapidité lors de la suppression
- Les clusters du fichier supprimé seront réutilisés lors de l'écriture d'un autre fichier
- La réutilisation de l'espace libéré n'est pas prédictible

LE SYSTÈME DE FICHIERS NTFS

Ce qu'il faut retenir pour la suite

- NTFS est le système de fichiers de Windows
- La MFT contient toutes les informations des fichiers et des répertoires, elle est critique
- Un fichier supprimé par l'utilisateur peut être récupéré si n'y a pas écrasement des données du fichier