Windows et Active Directory

Généralités
Architecture
Modèle de sécurité

SR v2022

Windows et Active Directory

Généralités

SR v2022

SYSTÈMES D'EXPLOITATION MICROSOFT

De 1981 à 2000 : MS-DOS et Windows

ANNÉE	OS	ANNÉE	OS
1981	MS-DOS 1.0	1995	Windows 95
1983	MS-DOS 2.0	1998	Windows 98
1984	MS-DOS 3.0	1999	Windows 98 SE
1985	Windows 1.0	2000	Windows Me
1987	Windows 2.0		
1988	MS-DOS 4.0		
1990	Windows 3.0		
1991	MS-DOS 5.0		
1992	Windows 3.1		
1993	MS-DOS 6.0 Windows 3.11		
1994	MS-DOS 6.22		

SYSTÈMES D'EXPLOITATION MICROSOFT

De 1993 à 2022 : Windows NT

ANNÉE	NOYAU	OS	TYPE	ANNÉE	NOYAU	OS	TYPE
1993	3.1	Windows NT 3.1	W/S	2009	6.1	Windows 7	W
1994	3.5	Windows NT 3.5	W/S			Windows Server 2008 R2	S
1995	3.51	Windows NT 3.51	W/S	2012	6.2	Windows 8	W
1996	4.0	Windows NT 4.0	W/S	2012		Windows Server 2012	S
2000	5.0	Windows 2000	W/S	2013	6.3	Windows 8.1	W
2001	5.1	WIndows XP	W	2013		Windows Server 2012 R2	S
2003	5.2	Windows Server 2003	S	2015	10.0	Windows 10	W
2005		Windows XP x64	W	2016		Windows Server 2016	S
2006		Windows Server 2003 R2	S	2018	10.0	Windows Server 2019	S
2007	6.0	Windows Vista	W	2021	10.0	Windows 11	W
2008		Windows Server 2008	S	2021	10.0	Windows Server 2022	S

WINDOWS NT

Quelques caractéristiques

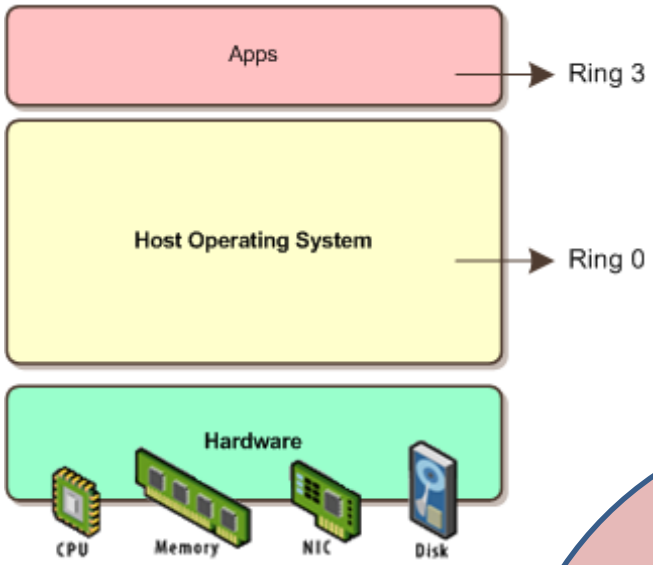
- Multi-utilisateurs
- Multitâche préemptif / Multithread
- Ouverture de session obligatoire
- Protection de la mémoire
- Contrôle d'accès discrétionnaire
- Audit
- A l'origine, portabilité (x86, Alpha, PowerPC et MIPS)
  - Support à l'origine de Windows NT mais abandon avec Windows 2000
  - x86 : non supporté sur les serveurs depuis 2008 R2
  - x64 : toute version depuis XP
  - ARM : Windows 8 RT ou Windows 10 on ARM
  - Itanium : XP, 2003 et 2008/2008 R2
- Fonctionnalités serveurs : Hyper-V, DNS, DHCP, IIS, AD, DFS, etc…

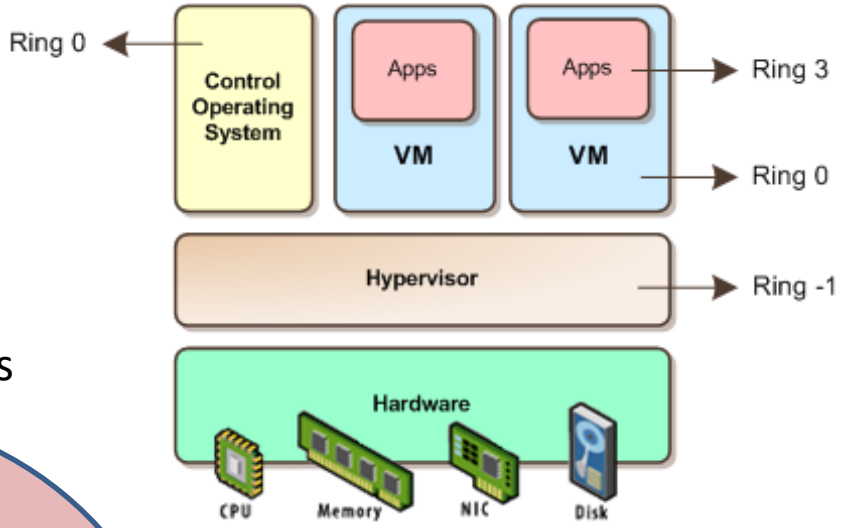
Windows et Active Directory

Architecture

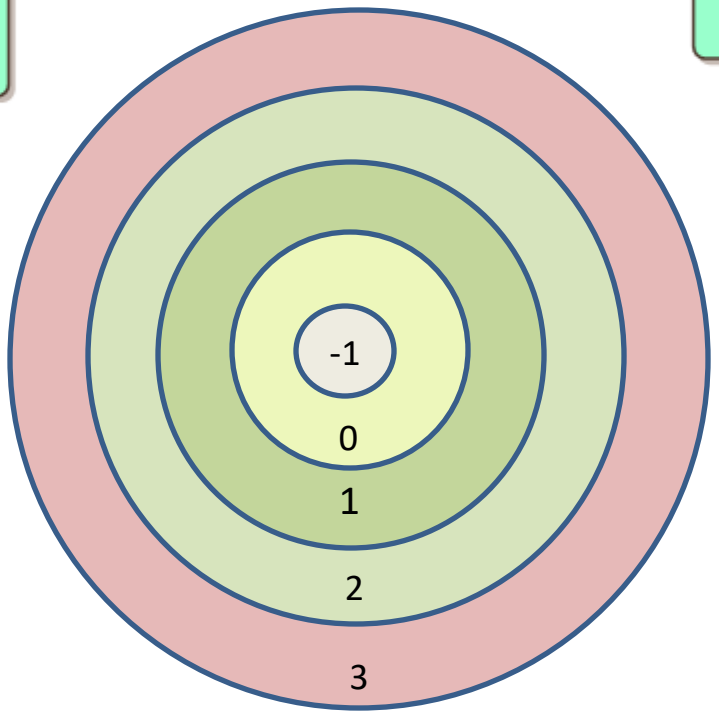
SR v2022

ARCHITECTURE

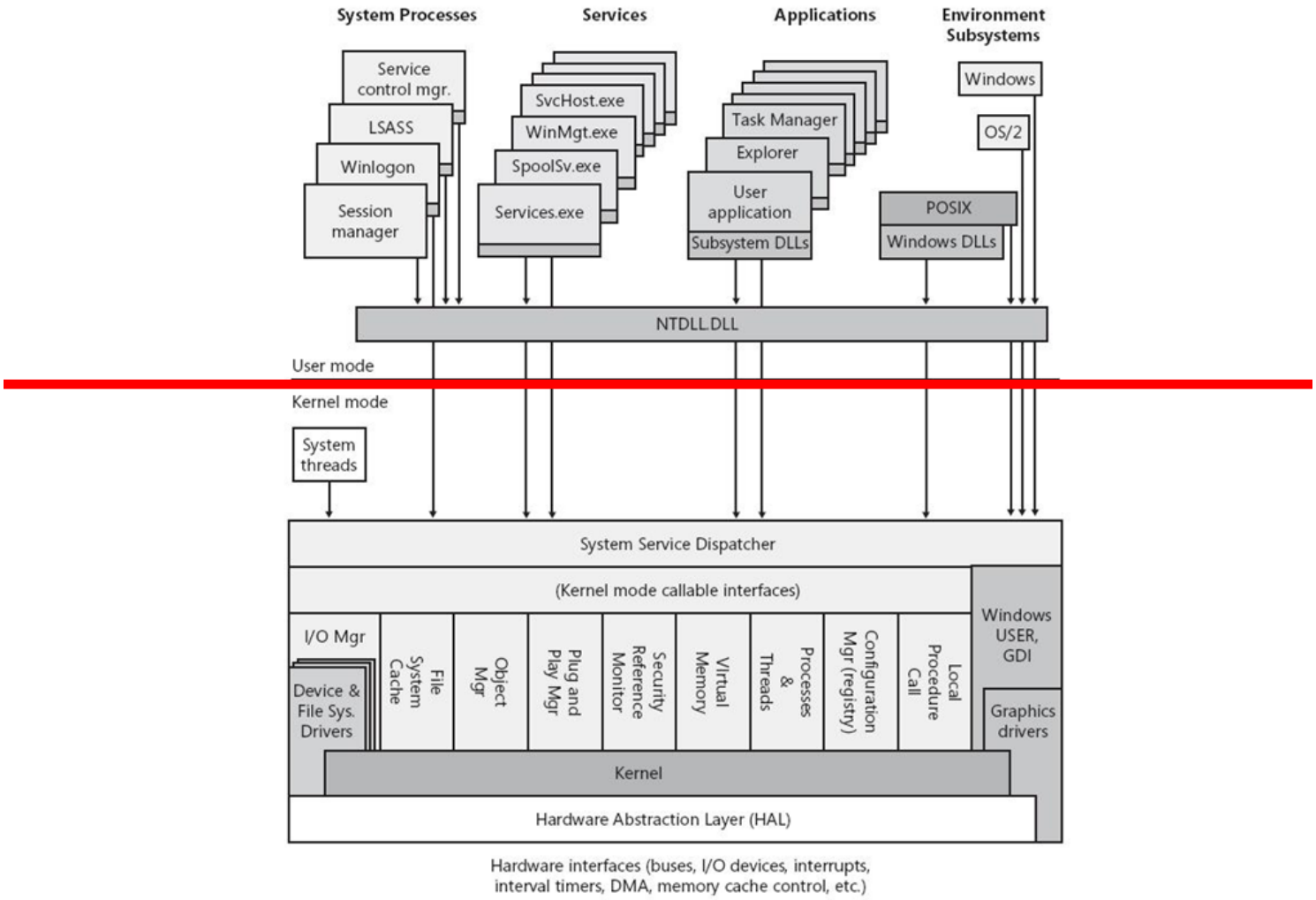




Protection Rings

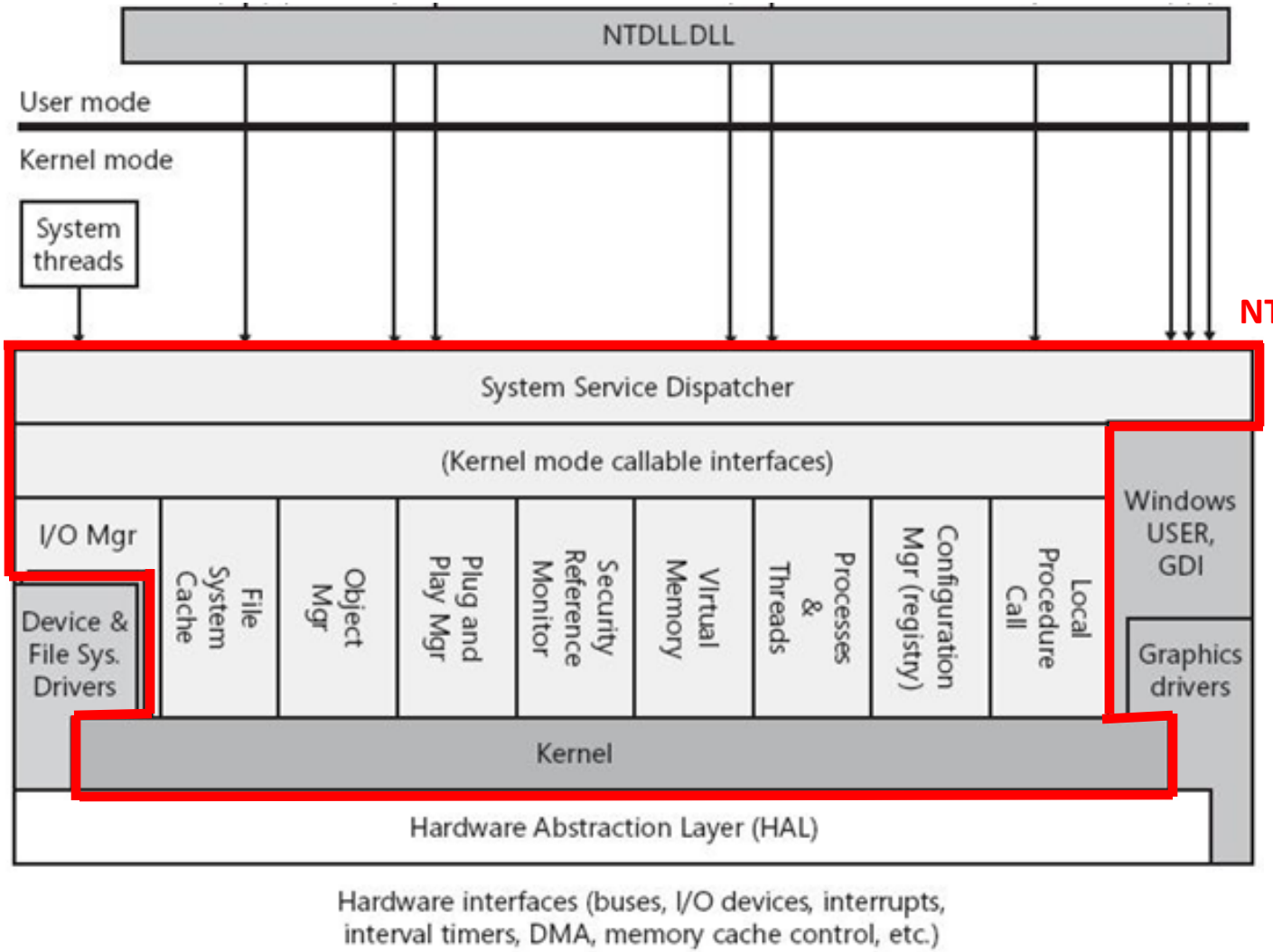


ARCHITECTURE



ARCHITECTURE

Kernel Mode

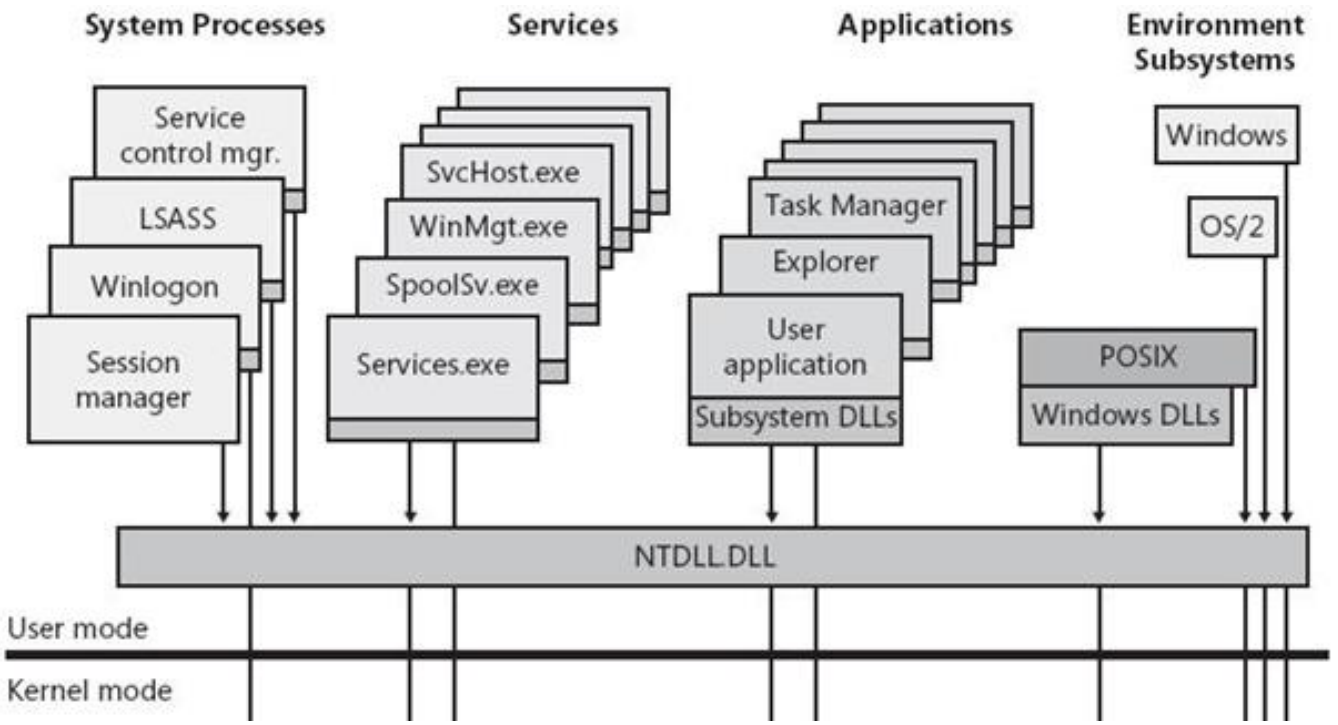


ARCHITECTURE
Kernel Mode

- Composants intégrés à Ntoskrnl.exe
  - L'executive : fonctions « haut-niveau »
    - Fonctions des appels systèmes
    - Managers et bibliothèques statiques
  - Le noyau : fonctions « bas-niveau »
- Pilotes
- Système graphique (Win32k.sys)
  - Fonctions USER et GDI
  - Windows 10 : win32kbase.sys et win32kfull.sys
- Bibliothèques dynamiques : fichiers .dll

ARCHITECTURE

User Mode



ARCHITECTURE
User Mode

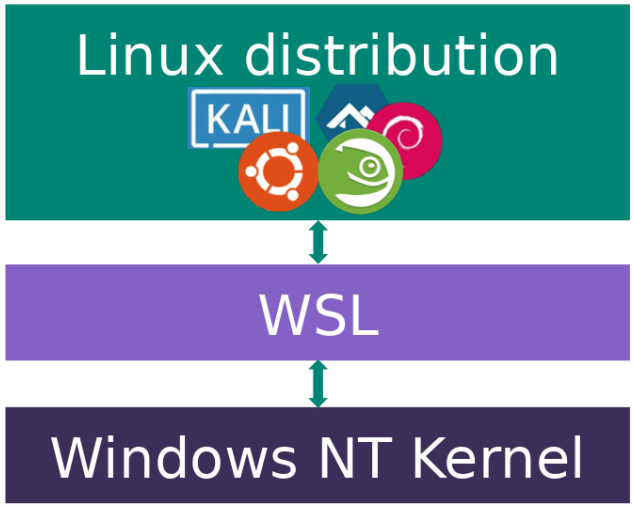
- Windows (csrss.exe)
  - Sous-système obligatoirement démarré
  - Environnement d'exécution des programmes Windows 32/64 bits et Windows 3.1/MS-DOS 16 bits via NTVDM.EXE
- Serveurs hébergés :
  - csrsrv.dll : initialisation et divers
  - basesrv.dll : thread, process, VDM
  - winsrv.dll : console, user services
  - sxssrv.dll : Side-by-Side
  - consrv.dll : console - Transféré dans ConHost.exe depuis Windows 7

ARCHITECTURE
User Mode

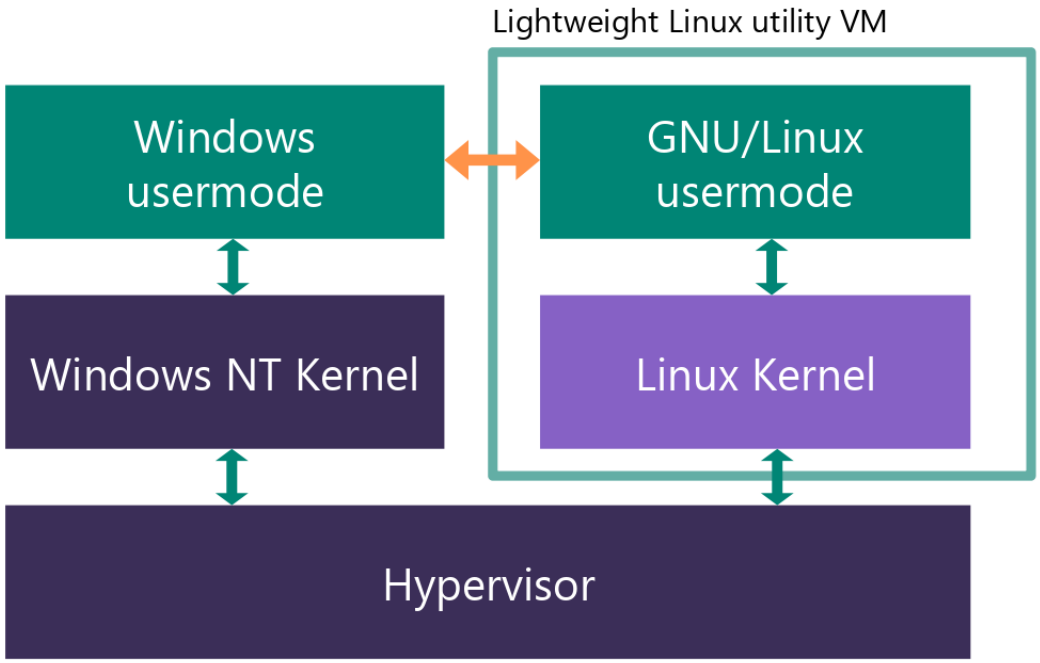
- POSIX (psxss.exe) :
  - Environnement d'exécution des programmes POSIX (32 bits)
  - Remplacé par Windows Services For UNIX (SFU) sous XP/2003
  - Remplacé par Windows Subsystem for Unix-based Applications (SUA) (32/64 bits) sous Vista
  - Supprimé depuis Windows 8/2012
  - Remplacé par Windows Subsystem for Linux (WSL1 puis WSL2) sous Windows 10 et Windows Server 2016
- OS/2 (os2ss.exe) :
  - Environnement d'exécution des programmes OS/2 en invite de commande uniquement
  - Supprimé depuis XP/2003

ARCHITECTURE

User Mode



WSL1



WSL2

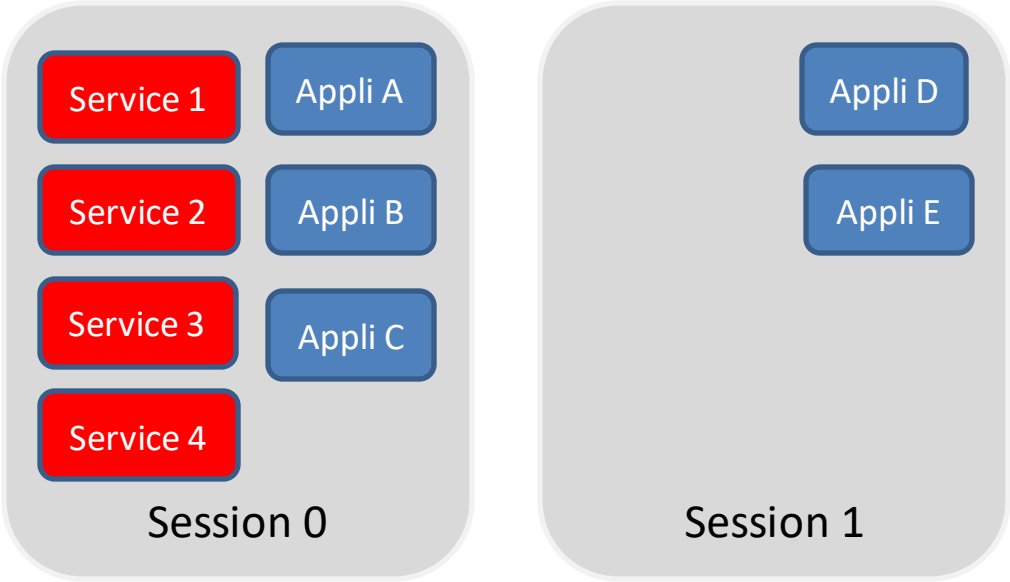
ARCHITECTURE
Sessions

- Apparues sous Windows NT 4 TSE (Terminal Server Edition)
- Permettre la connexion simultanée de plusieurs utilisateurs sur un même système
  - Chaque processus est associé à un numéro de session (SessionID)
  - Des processus dans des sessions différentes sont « isolés »
  - Les sessions sont mises en œuvre par le mécanisme Terminal Services et utilisées par :
    - Le Fast User Switching
    - Le bureau à distance (accédé par le protocole RDP)
    - Les sessions « étendues » (Enhanced Session Mode) d'Hyper-V

ARCHITECTURE

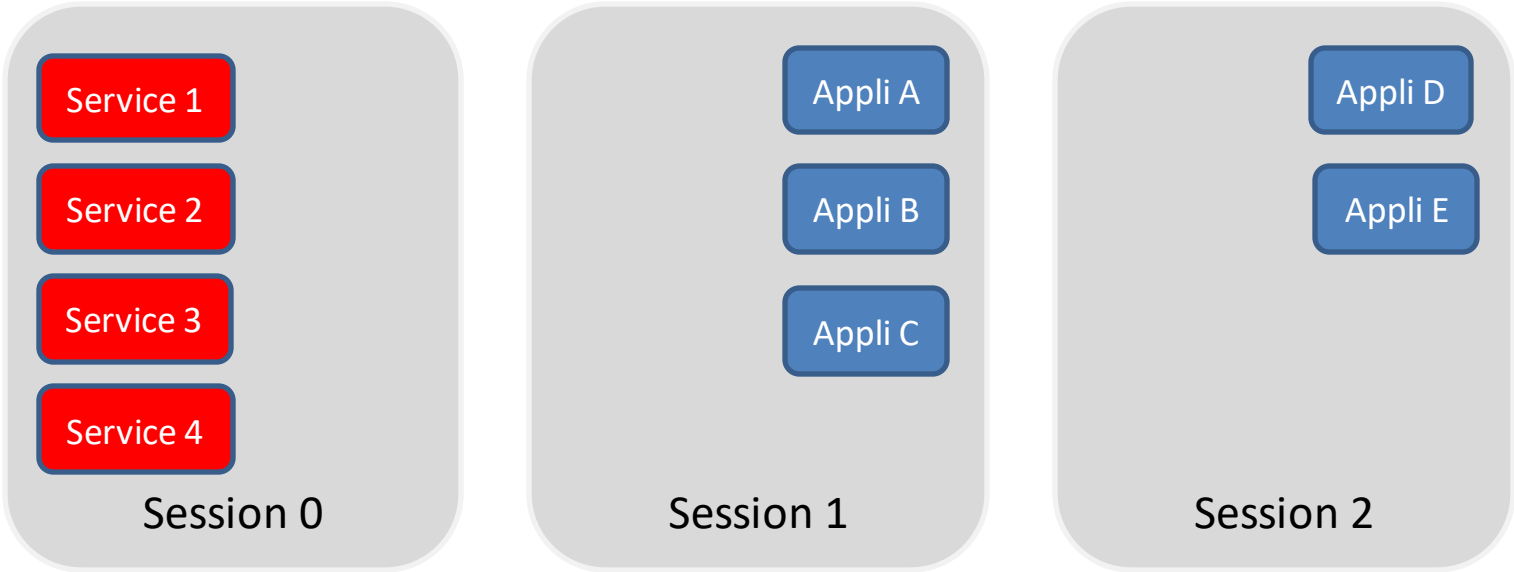
Sessions

- Windows Server 2003
  - Console : session 0
  - Session TSE : sessions 1…n
- Windows XP avec Fast User Switching
  - 1er utilisateur : session 0
  - Utilisateurs suivants : session 1…n



ARCHITECTURE
Sessions

- Windows Vista
  - Isolation de la session 0 en la réservant aux processus critiques du système et aux services
  - La session 0 devient de fait non-interactive



ARCHITECTURE

Processus User Mode

- **Idle et System**
  - Créés par NTOSKRNL.EXE via le Process Manager
  - Pas de processus parent visible
  - SYSTEM a un PID static à 4
  - SYSTEM crée le processus SMSS.EXE
  - 1 seul processus SYSTEM

ARCHITECTURE

Processus User Mode

- **SMSS — Session Manager**
  - Premier processus en user mode
  - Processus parent : SYSTEM
  - Priorité de base : 11
  - \%systemroot%\System32\smss.exe
  - Username: NT AUTHORITY\SYSTEM
  - Charge les KNOWN DLLS
  - Effectue des suppressions et renommages différés des fichiers
  - Crée la session 0 (OS services)
  - Crée la session 1 (User session) et les suivantes si plusieurs utilisateurs
  - Crée les processus CSRSS et WINLOGON (session 1)
  - S'exécute dans la session 0
  - 1 seul processus SMSS.EXE

ARCHITECTURE

Processus User Mode

- **CSRSS.EXE — Client/Server Run**
  - Windows subsystem process.
  - Enfant de SMSS.EXE
  - Priorité de base : 13
  - \%SystemRoot%\system32\csrss.exe
  - Username : NT AUTHORITY\SYSTEM
  - Crée et supprime processus et threads, fichiers temporaires, etc.
  - 1 seul processus CSRSS par session dont 1 en session 0

ARCHITECTURE

Processus User Mode

- **WININIT.EXE — Windows Initialization Process**
  - Parent des processus SERVICES.EXE (Service Control Manager - SCM), LSASS.EXE et LSM.EXE
  - Enfant de SMSS.EXE
  - Priorité de base : 13
  - Username: NT AUTHORITY\SYSTEM
  - \%SystemRoot%\system32\wininit.exe
  - Réalise des opérations d'initialisation en user-mode
  - Crée \%windir%\temp
  - S'exécute en session 0

ARCHITECTURE

Processus User Mode

- **SERVICES.EXE — Service Control Manager**
  - Enfant de WININIT.EXE
  - Parent de services tels que SVCHOST.EXE, DLLHOST.EXE, TASKHOST.EXE, SPOOLSV.EXE, etc.
  - \%SystemRoot%\System32\wininit.exe
  - Username: NT AUTHORITY\SYSTEM
  - Priorité de base : 9
  - Charge en mémoire une table des services
  - S'exécute en session 0
  - 1 seul processus SERVICES.EXE

ARCHITECTURE

Processus User Mode

- **LSASS.EXE — Local Security Authority**
  - Enfant de WININIT.EXE
  - 1 seul processus LSASS.EXE
  - %SystemRoot%\System32\lsass.exe
  - Responsable de la stratégie de sécurité locale dont la gestion des utilisateurs autorisés à se connecter, les stratégies de mot de passe, l'écriture dans le journal des événements de sécurité, etc.
  - Priorité de base : 9
  - Username: NT AUTHORITY\SYSTEM
  - S'exécute en session 0
  - Aucun processus enfant

ARCHITECTURE

Processus User Mode

- **SVCHOST.EXE — Service Hosting Process**
  - Plusieurs instances de SVCHOST.EXE s'exécutent
  - %SystemRoot%\System32\svchost.exe
  - Username : l'un des 3 - NT AUTHORITY\SYSTEM, LOCAL SERVICE, ou NETWORK SERVICE
  - Enfant de SERVICES.EXE
  - Priorité de base : 8
  - S'exécute en session 0

ARCHITECTURE

Processus User Mode

- **LSM.EXE — Load Session Manager Service**
  - Gère l'état des sessions Terminal Server du système local. Envoie les requête de démarrage de nouvelles sessions à SMSS.EXE.
  - Reçoie les logon/off, démarrage et arrêt de l'environnement utilisateur, connexion / déconnexion d'une session et verrouillage / déverrouillage du bureau
  - Enfant de WININIT.EXE
  - Exécuté au sein de SVCHOST.EXE depuis Windows 8
  - Pas de processus enfant
  - %systemroot%\System32\lsm.exe
  - Priorité de base : 8
  - Username: NT AUTHORITY\SYSTEM
  - S'exécute en session 0

ARCHITECTURE

Processus User Mode

- **WINLOGON.EXE — Windows Logon Process**
  - Pas de processus parent
  - Peut avoir comme processus enfant LogonUI si une carte à puce par exemple est utilisée pour s'authentifier
  - LogonUI se terminera une fois que l'utilisateur aura entré son mot de passe. Une fois le mot de passe saisi, la vérification est envoyée à LSASS et vérifiée via Active Directory ou SAM.
  - Priorité de base : 13
  - S’exécute en session 1 et suivante
  - Gère les connexions / déconnexions utilisateur interactives lorsque la combinaison de touches SAS est activée (Ctrl+Alt+Delete)
  - Charge le processus USERINIT.EXE décrit dans la valeur USERINIT de Software\Microsoft\Windows NT\CurrentVersion\Winlogon

ARCHITECTURE

Processus User Mode

- **WINLOGON.EXE — Windows Logon Process**
  - Userinit initialise l'environnement utilisateur incluant l'exécution des GPOs et des logon scripts.
  - Userinit exécute le processus EXPLORER.EXE décrit dans la valeur SHELL de Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
- **EXPLORER.EXE — Windows Explorer**
  - Pas de processus parent
  - Priorité de base : 8
  - Username: utilisateur ayant ouvert la session
  - %Systemroot%\Explorer.exe
  - Multiples processus enfants

Windows et Active Directory

Modèle de sécurité

SR v2022

MODÈLE DE SÉCURITÉ

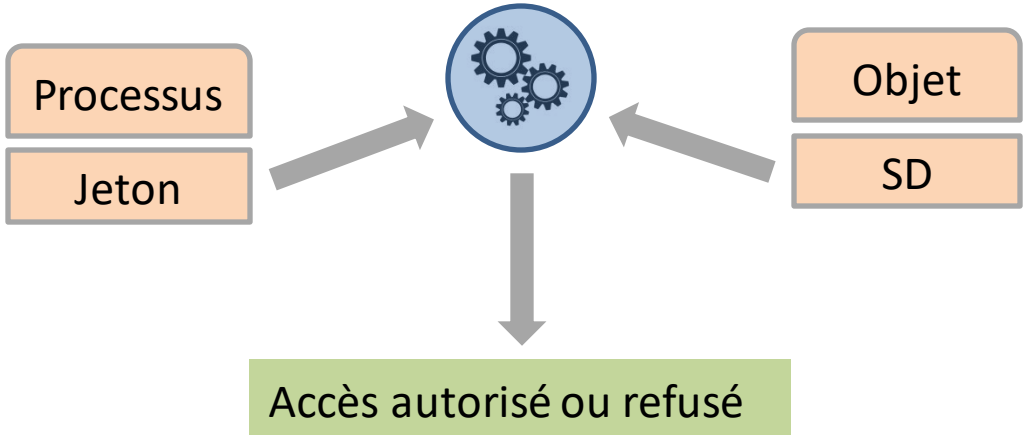
Modèle général

- Windows propose un modèle de sécurité s'appuyant sur un mécanisme de contrôle d'accès discrétionnaire lors de l'accès d'un processus aux objets noyau, aux objets de l'Active Directory et aux composants du système
  - Fichiers/répertoires (NTFS), clés du registre, named pipes, mailslots, window/desktop, jobs, objets de synchronisation (events, mutexes, sémaphores, timers), processus, threads, token, anonymous pipes, file-mapping, partages réseau, imprimantes, services…
- Chacun de ces objets est protégé par un descripteur de sécurité (SD) qui va définir quels types d'accès vont être autorisés de la part des différentes entités.

MODÈLE DE SÉCURITÉ

Modèle général

- Une entité doit au préalable s'authentifier sur le système
  - Un jeton est alors créé et permet de définir le contexte de sécurité de cette entité
  - Tout processus lancé le sera dans ce contexte de sécurité
- Le Security Reference Monitor (SRM) valide les accès aux objets et effectue la journalisation des évènements de sécurité



MODÈLE DE SÉCURITÉ

Notions de SID (Security Identifier)

- Permet d'identifier de façon unique
  - Utilisateur
  - Machine
  - Groupe
  - Domaine
- S – Rev – ID Authority – (Sub…Sub) – RID
  - Rev : révision (actuellement toujours 1)
  - ID A : identifiant de l'autorité émettrice (48 bits)
  - (Sub…Sub) : identifiants des sous-autorités (n x 32 bits)
  - RID : Relative ID (32 bits)

MODÈLE DE SÉCURITÉ

Well-Known SIDs

S-1	0 (SECURITY_NULL_SID_AUTHORITY)	0 (Null SID)	S-1-0-0	Null SID
	1 (SECURITY_WORLD_SID_AUTHORITY)	0 (World)	S-1-1-0	localhost\Tout le monde
	2 (SECURITY_LOCAL_SID_AUTHORITY)	0 (Local)	S-1-2-0	localhost\LOCAL
	3 (SECURITY_CREATOR_SID_AUTHORITY)	0 (Creator Owner ID)	S-1-3-0	CREATEUR PROPRIETAIRE
		1 (Creator Group ID)	S-1-3-1	GROUPE CREATEUR
		2 (Creator Owner ID)	S-1-3-2	CREATOR OWNER SERVER
		3 (Creator Group ID)	S-1-3-3	CREATOR GROUP SERVER
	5 (SECURITY_NT_AUTHORITY)			

MODÈLE DE SÉCURITÉ

Well-Known SIDs : S-1-5 / SECURITY_NT_AUTHORITY

1 (SECURITY_DIALUP_RID (Groupe))	S-1-5-1	LIGNE
2 (SECURITY_NETWORK_RID (Groupe))	S-1-5-2	RESEAU
3 (SECURITY_BATCH_RID (Groupe))	S-1-5-3	TACHE
4 (SECURITY_INTERACTIVE_RID (Groupe))	S-1-5-4	INTERACTIF
5 (SECURITY_LOGON_IDS_RID)	S-1-5-5-X-Y	
6 (SECURITY_SERVICE_RID (Groupe))	S-1-5-6	SERVICE
7 (SECURITY_ANONYMOUS_LOGON_RID)	S-1-5-7	ANONYMOUS LOGON
10 (SECURITY_PRINCIPAL_SELF_RID)	S-1-5-10	SELF
11 (SECURITY_AUTHENTICATED_USER_RID (Groupe))	S-1-5-11	Utilisateurs authentifiés
12 (SECURITY_RESTRICTED_CODE_RID)	S-1-5-12	RESTRICTED
13 (SECURITY_TERMINAL_SERVER_RID (Groupe))	S-1-5-13	UTILISATEUR TERMINAL SERVER
14	S-1-5-14	REMOTE INTERACTIVE LOGON
18 (SECURITY_LOCAL_SYSTEM_RID)	S-1-5-18	SYSTEM ou LocalSystem
32 (SECURITY_BUILTIN_DOMAIN_RID)	S-1-5-32-544	BUILTIN\Administrateurs
	S-1-5-32-545	BUILTIN\Utilisateurs
	S-1-5-32-546	BUILTIN\Invités

MODÈLE DE SÉCURITÉ

Well-Known SIDs : S-1-5-21 / SECURITY_NT_NON_UNIQUE

- Lors de l'installation d'une machine Windows, un SID est généré et lui est affecté : S-1-5-21-X-Y-Z
- SID des comptes et groupes locaux
  - SID de la machine
  - RID unique et incrémental pour chaque compte ou groupe
    - Well-known users :
      - Administrateur : 500 (DOMAIN_USER_RID_ADMIN)
      - Invité : 501 (DOMAIN_USER_RID_GUEST)
      - Autres : >999 (DOMAIN_USER_RID_MAX)
  - Exemple : Machine\Administrateur → S-1-5-21-X-Y-Z-500

MODÈLE DE SÉCURITÉ

Well-Known SIDs : S-1-5-21 / SECURITY_NT_NON_UNIQUE

- SID des comptes et groupes de domaine Active Directory :
  - Création du domaine : un SID est affecté au domaine (SID du 1er DC)
  - RID du domaine gérés par DC / RID Master
  - Pools de RID affectés à chaque DC
  - Chaque DC affecte un RID de son pool à la création d'un Security Principal (utilisateurs, groupes, machines)
  - RID unique et incrémental
  - SID stocké dans l'attribut *objectSid*

MODÈLE DE SÉCURITÉ

Jeton d’accès

- Remis à l’utilisateur après authentification
- Utilisé par ses processus ou threads pendant toute la durée de la session jusqu’à sa fermeture
- Utilisé pour représenter l'utilisateur dans toutes les demandes d'accès aux ressources du système
- Identifie ou liste :
  - l’utilisateur
  - ses groupes d’appartenance
  - ses privilèges accordés
  - la session
  - la session d’authentification

MODÈLE DE SÉCURITÉ

Jeton d'accès

Champ	Description
Token source	Identifiant de la source ayant créé le jeton
Token ID	Identifiant local unique (LUID) que le SRM affecte à un jeton quand celui-ci est créé
Authentication ID	Indique à quelle logon session est relié le jeton. LSASS affecte cet ID.
Expiration Time	Champ non utilisé pour le moment qui pourrait permettre la mise en place réelle de l'expiration d'un compte.
UserAndGroupCount	Nombre d'entrées dans le champ UserAndGroup
UserAndGroups	Liste des SID de l'utilisateur et des groupes d'appartenance
RestrictedSidCount	Nombre d'entrées dans le champs RestrictedSids
RestrictedSids	Liste des SID restreints
PrivilegeCount	Nombre d'entrées dans le champ Privileges
Privileges	Liste des privilèges.
DefaultOwnerIndex	SID du propriétaire par défaut d'un objet créé
PrimaryGroup	SID du groupe propriétaire par défaut d'un objet créée
DefaultDacl	DACL par défaut d'un objet créé
TokenType	Type de Token : TokenPrimary ou TokenImpersonation
ImpersonationLevel	Niveau d'impersonalisation : SecurityAnonymous, SecurityIdentification, SecurityImpersonation ou SecurityDelegation

MODÈLE DE SÉCURITÉ

Jeton d'accès - Attributs

- UserAndGroups
  - SE_GROUP_ENABLED
    - SID activé et pris en compte lors du contrôle d'accès pour les autorisations et les refus
  - SE_GROUP_USE_FOR_DENY_ONLY
    - SID activé et pris en compte lors du contrôle d'accès uniquement pour les refus
- Privileges
  - SE_PRIVILEGE_ENABLED
    - Droit activé
  - Sinon désactivé

MODÈLE DE SÉCURITÉ

Descripteur de sécurité

- Un descripteur de sécurité contient :
  - Un champ « control information » (numéro de version, attributs)
  - Le SID du propriétaire de l'objet
  - Le SID du groupe primaire de l'objet
  - La DACL (Discretionary Access Control List) : liste définissant les autorisations d'accès
  - La SACL (System Access Control List) : liste définissant les audits à générer lors des accès à l'objet ou diverses propriétés de l'objet (niveau d'intégrité, claims, etc.)

MODÈLE DE SÉCURITÉ

Descripteur de sécurité

- DACL et SACL sont constituées d'ACE (Access Control Entries) qui sont composées
  - du type de l'ACE
    - Access-allowed ACE
    - Access-denied ACE
    - System-audit ACE
    - Mandatory label ACE
    - etc.
  - de propriétés : héritage, journalisation (Failed/Success)
  - du SID auquel l'ACE s'applique
  - des autorisations d'accès concernés (AccessMask)

MODÈLE DE SÉCURITÉ

Descripteur de sécurité

- Autorisations standards (communs à tous les types d'objets)
  - WRITE_OWNER : permet de changer le propriétaire de l'objet
  - READ_CONTROL : lire la DACL
  - WRITE_DAC : modifier la DACL
  - DELETE
- Autorisations spécifiques (propres à chaque type d'objets)
  - FILE_WRITE_ATTRIBUTES
  - KEY_CREATE_SUB_KEY
  - TOKEN_ADJUST_PRIVILEGES
  - etc…
- Autorisations génériques : READ, WRITE, EXECUTE, ALL

MODÈLE DE SÉCURITÉ

Descripteur de sécurité

- A noter que
  - SeTakeOwnershipPrivilege accorde l'autorisation
    - WRITE_OWNER
  - SeDebugPrivilege accorde toutes les autorisations sur les processus
  - SeBackupPrivilege accorde les autorisations
    - READ_CONTROL, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_READ, FILE_TRAVERSE
  - SeRestorePrivilege accorde les autorisations
    - WRITE_DAC, WRITE_OWNER, ACCESS_SYSTEM_SECURITY
    - FILE_GENERIC_WRITE, FILE_ADD_FILE, FILE_ADD_SUBDIRECTORY, DELETE
  - SID propriétaire de l'objet dans jeton accorde implicitement les accès
    - READ_CONTROL et WRITE_DAC
  - Descripteur de sécurité sans DACL (null DACL)
    - Accès toujours autorisés
  - DACL sans ACE (empty DACL)
    - Accès toujours refusés (sauf ceux du propriétaire et des privilèges)

MODÈLE DE SÉCURITÉ

Vue globale du contrôle d'accès