au fonctionnement du noyau dont :

- Le processus csrss.exe (*Client/Server Runtime Subsystem*) qui gère les fenêtres et les éléments graphiques de Windows.
- Le processus Lsass.exe (*Local Security Authority Subsystem Service*) qui gère les mécanismes de sécurité locale et d'authentification des utilisateurs via le service WinLogon.
- Le processus Lsm.exe (*Local Session Manager*) qui gère l'ouverture de session locale.
- Le processus wmiprvse.exe (*Windows Management Instrumentation*) qui gère les fonctionnalités WMI.
- Le processus Wininit.exe qui gère le démarrage de Windows.
- Le processus Winlogon.exe (*Windows Logon Process*) qui gère l'ouverture et la fermeture des sessions.
- Le processus SearchIndexer qui gère l'indexation des fichiers pour les fonctionnalités de recherche.
- Le processus svchost.exe qui est un nom de processus hôte générique pour exécuter des services à partir de bibliothèques dynamiques (DLL). Vous verrez plusieurs instances de ce processus qui correspondent à autant de services Windows démarrés.

SERVICE RESEAU : ce compte est utilisé par les services qui ont besoin de s'authentifier auprès des autres machines présentes sur le réseau sans avoir besoin de privilèges particulièrement étendus.

SERVICE LOCAL : c'est le même type de compte à la différence près qu'il ne peut accéder qu'aux ressources réseau qui autorisent un accès anonyme. Il permet notamment le lancement de processus liés à la gestion des périphériques et de certains services liés au réseau comme, par exemple, la résolution des noms NetBIOS (LmHosts).

Restricted : il permet de définir une ACE dans une ACL impliquant une permission de type Refuser pour tous les jetons d'accès restreints. Soit cette entité se voit attribuer une permission de type "Refuser", soit l'autorisation accordée est de type "Lecture". Dans les deux cas, les groupes ou les utilisateurs restreints n'ont pas d'accès à la ressource puisque les ACE négatives prennent le pas sur les ACE positives. Pour d'autres entrées, ils ne posséderont qu'un accès en lecture seule.

Trusted Installer : la technologie WRP (*Windows Resource Protection*) agit comme une sorte d'autorité suprême empêchant tout changement dans les fichiers, répertoires et clés du Registre considérés comme étant nécessaires au bon fonctionnement de votre système. Seul, dans ce cas, le service Trusted Installer peut opérer des changements dans les ressources qui sont protégées par ce service.

b. Les groupes d'utilisateurs

Administrateurs : regroupe les membres possédant des privilèges d'administrateur.

Administrateurs Hyper-V : regroupe les membres possédant des privilèges administrateurs pour les fonctionnalités de Hyper-V.

Duplicateurs : les membres de ce groupe disposent de droits pour assurer la réplication des fichiers dans le domaine.

IIS_IUSRS : les membres de ce groupe prédéfini disposent de droits étendus sur les ressources et fichiers du système pour acter des pools IIS en tant que comptes de service. Si un compte de service est affecté à un pool IIS, il devient automatiquement membre de ce groupe.

Invités : les membres du groupe Invités disposent par défaut du même accès que les membres du groupe Utilisateurs, à l'exception du compte Invité qui dispose d'autorisations restreintes.