Les comptes d'utilisateurs

Nous distinguons les comptes prédéfinis des comptes interactifs, qui permettent aux utilisateurs d'ouvrir une session sur la machine. Les comptes prédéfinis de type Administrateur ou Invité vous permettent de tirer profit de certaines fonctionnalités du système d'exploitation. Ce type de compte ne correspond donc pas directement à un utilisateur réel. À l'inverse, un compte d'utilisateur interactif correspond à une personne physique. Le système lui renvoie donc une image, appelée profil, qui est stockée à cet emplacement : C:\Utilisateurs\<Nom Utilisateurs>.

Chaque utilisateur appartient à un groupe générique (prédéfini). Comme il est possible de créer des utilisateurs, vous pouvez également définir de nouveaux groupes.

À chaque groupe correspond un jeu de privilèges et de restrictions. En termes clairs, si le groupe des administrateurs dispose des pleins pouvoirs, celui des invités évolue dans une sorte de liberté surveillée.

La gestion des comptes d'utilisateurs est accessible depuis le **Panneau de configuration**, dans la section **Comptes d'utilisateurs**. Notez que sous Windows 10, la gestion des comptes utilisateurs est aussi accessible depuis l'utilitaire de gestion des paramètres du PC. Vous pouvez aussi utiliser la console de gestion avancée des utilisateurs en saisissant la commande `netplwiz` depuis la zone de recherche du menu **Démarrer**.

Si vous désirez réinitialiser le mot de passe d'un compte, depuis la console de gestion avancée des utilisateurs, cliquez sur le bouton **Réinitialiser le mot de passe**. Notez que cette option sera désactivée si vous êtes connecté avec un compte Microsoft. En effet, la modification se fera en ligne.

Pour accéder aux propriétés d'un utilisateur et visualiser son groupe d'appartenance, c'est-à-dire le type et le niveau d'accès du compte, cliquez sur le bouton **Propriétés**.

Sélectionnez l'onglet **Options avancées**, puis dans la section **Gestion avancée des utilisateurs**, cliquez sur le bouton **Avancé**. La console de gestion des comptes d'utilisateurs s'affiche. Cette console est également accessible en saisissant la commande `lusrmgr.msc` depuis la zone de recherche du menu **Démarrer**.

Lors de l'installation de Windows, nous avons vu qu'il était possible de configurer un compte d'utilisateur de type Compte Microsoft afin d'intégrer les fonctionnalités de cloud offertes par le nouveau système d'exploitation de Microsoft, comme le courrier, les contacts ou SkyDrive. Excepté le mot de passe, la gestion de ce type de compte est identique aux comptes utilisateurs locaux de l'ordinateur.

Dans Windows 10, l'intégration du cloud pour les comptes utilisateurs permet de synchroniser les éléments de configuration des paramètres personnalisés.

1. Fonctionnement des profils d'utilisateurs

Au démarrage de l'ordinateur, il vous est demandé de vous connecter sur votre session. À chaque nom de session correspond un utilisateur. Lors de la première ouverture de session sur un système fraîchement installé, un profil d'utilisateur par défaut (ou modèle) est utilisé pour créer votre propre profil. Ce profil est décrit dans cette arborescence du Registre : HKEY_USERS. Par la suite, et au fur et à mesure des retouches que vous apporterez à votre environnement de travail, chacune de vos préférences sera mémorisée. De fait, votre profil d'utilisateur va se peaufiner au fil du temps.

Sous les systèmes NT, on utilise aussi des profils itinérants (on parle plutôt de profils "errants") : dans un environnement où un utilisateur se sert de différents ordinateurs, il pourra retrouver son même environnement de travail quel que soit l'ordinateur sur lequel il a ouvert une session.

Par ailleurs, il est possible d'assigner un profil obligatoire pour un utilisateur ou un groupe d'utilisateurs, ou de modifier le profil par défaut qui sera affecté à chaque nouvel utilisateur. En d'autres termes, il vous est possible de

copier un profil d'utilisateur d'un compte à l'autre de la même manière qu'on fabrique plusieurs petites figurines à partir d'un même moule.

Windows 10 introduit une nouvelle version de gestion du profil d'utilisateur Windows. Ce profil disposera d'une portabilité sur différents dispositifs supérieure à ses prédécesseurs. Néanmoins, la version des profils Windows 10 (v5) est incompatible avec la version des profils des versions antérieures de Windows. Il faudra donc laisser activé le Contrôle de version des profils. La gestion des fichiers et dossiers du profil utilisateur est toujours localisée par défaut dans le dossier C:\Users ou C:\Utilisateurs.

2. Les groupes prédéfinis

Il y a un certain nombre de groupes d'utilisateur qui sont paramétrés par défaut sur le système. Nous nous sommes limités aux plus répandus.

a. Les entités de sécurité intégrées

ANONYMOUS LOGON : représente les utilisateurs et les services qui accèdent à un ordinateur sans utiliser un nom de compte, un mot de passe ou un nom de domaine.

CREATEUR PROPRIETAIRE : représente l'utilisateur ayant créé ou pris possession d'un objet.

INTERACTIF : représente tous les utilisateurs connectés actuellement à un ordinateur et qui accèdent à une ressource donnée sur cet ordinateur (par opposition aux utilisateurs qui accèdent à la ressource sur le réseau). Chaque fois qu'un utilisateur accède à une ressource spécifique sur l'ordinateur auquel il est actuellement connecté, il est ajouté automatiquement au groupe Interactif.

LIGNE : représente n'importe quel utilisateur qui s'est connecté à l'ordinateur en utilisant une connexion d'accès à distance.

REMOTE INTERACTIVE LOGON : représente n'importe quel utilisateur qui s'est connecté à l'ordinateur en utilisant une connexion Bureau à distance.

RESEAU : représente les utilisateurs qui accèdent actuellement à une ressource spécifique sur le réseau (par opposition aux utilisateurs qui accèdent à une ressource en ouvrant une session locale sur l'ordinateur qui contient cette ressource). Chaque fois qu'un utilisateur accède à une ressource spécifique sur le réseau, il est ajouté automatiquement au groupe Réseau.

Tout le monde : représente tous les utilisateurs du réseau actuel, y compris les invités et les utilisateurs d'autres domaines. Chaque fois qu'un utilisateur ouvre une session sur le réseau, il est ajouté automatiquement au groupe Tout le monde.

UTILISATEUR TERMINAL SERVER : représente n'importe quel utilisateur qui accède à l'ordinateur en utilisant une connexion Bureau à distance.

Utilisateurs authentifiés : ce groupe comprend tous les utilisateurs possédant un compte et un mot de passe sur la machine locale ou Active Directory.

TOUS LES PACKAGES D'APPLICATION : cette entité gère les droits d'accès aux ressources système pour les applications Windows Store.

DROITS DU PROPRIÉTAIRE : représente les droits appliqués au propriétaire actuel d'un objet.

SYSTEM : c'est avec cette identité que le cœur système d'exploitation gère l'ensemble des composants essentiels

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.

Lecteurs des journaux d'événements : les membres de ce groupe disposent des droits pour lire les journaux d'événements sur l'ordinateur local.

Opérateurs d'assistance de contrôle d'accès : les membres de ce groupe peuvent interroger à distance les ressources système avancées (permissions et autorisations) sur l'ordinateur local.

Opérateurs de chiffrement : regroupe les membres possédant des privilèges de mise en œuvre des opérations de chiffrement.

Opérateurs de configuration réseau : regroupe les membres possédant un certain nombre de privilèges concernant la configuration des interfaces réseau.

Opérateurs de sauvegarde : regroupe les membres ayant le pouvoir de sauvegarder et de restaurer tous les fichiers d'un ordinateur.

Propriétaires d'appareils : regroupe les membres ayant le pouvoir de modifier les paramètres système de la machine.

System Managed Accounts Group : les membres de ce groupe dédié pour les futures fonctionnalités de Windows 10 sont gérés par le système.

Utilisateurs : les membres de ce groupe ont un accès limité aux ressources et disposent d'un nombre restreint de privilèges. Mais ils peuvent exécuter des applications.

Utilisateurs avec pouvoir : les membres de ce groupe peuvent effectuer un certain nombre de tâches administratives sans pour autant avoir un contrôle total sur la machine. Ce groupe est présent pour des raisons de compatibilité avec les systèmes antérieurs.

Utilisateurs de gestion à distance : regroupe les membres qui accèdent aux ressources WMI via des protocoles de communication compatibles.

Utilisateurs de l'Analyseur de performances : regroupe les membres qui peuvent afficher les données de performance en temps réel dans l'Analyseur de performances.

Utilisateurs du bureau à distance : regroupe les membres possédant les privilèges d'ouverture de session distante.

Utilisateurs du journal de performance : regroupe les membres qui peuvent, en plus de l'affichage des données de performance en temps réel, créer et modifier des ensembles de collecteurs de données dans l'Analyseur de performances.

Utilisateurs du modèle COM distribué : les membres peuvent lancer, activer et utiliser localement les objets COM distribués.

c. Les utilisateurs prédéfinis

Administrateur : ce compte spécial vous permet de vous affranchir du contrôle du compte d'utilisateur. Le jeton d'accès qui lui est accordé est unique. Il est par défaut désactivé dans Windows 10.

DefaultAccount : compte utilisateur dédié, désactivé par défaut. Ce compte est géré par le système.

Invité : ce compte est aussi désactivé par défaut dans Windows 10. Il est utile dans le cas où l'on veut accorder un accès occasionnel pour un utilisateur qui ne disposera de presque aucun privilège ni droit sur les ressources.

WDAG Utility Account : compte utilisateur géré par le système pour les besoins de Windows Defender Application Guard (WDAG), désactivé par défaut.

Vous pouvez réactiver ces comptes en suivant cette procédure :

- Dans la zone de texte **Rechercher** à droite du menu **Démarrer**, saisissez cette commande : `netplwiz`.
- Cliquez sur l'onglet **Options avancées**, puis le bouton **Avancé**.
- Ouvrez la branche **Utilisateurs**, puis le compte que vous souhaitez modifier.
- Décochez la case **Le compte est désactivé**.