

Systemes clients Microsoft

Module 05 – Les utilisateurs et les groupes



1

1

Les utilisateurs et les groupes

Objectifs

- Prendre conscience de l'importance de la notion d'utilisateur
- Distinguer les utilisateurs et leurs profils
- Gérer les utilisateurs et les groupes
- Découvrir les outils de gestion
- Assimiler le fonctionnement de l'UAC



2

2

Les objets utilisateurs et groupes

- Notion d'utilisateurs
- Les profils d'utilisateurs
- Les groupes
- Le contrôle de compte utilisateurs



La notion d'utilisateur

- Le système d'exploitation client Windows est une porte ouverte sur le système d'information de l'entreprise
- Êtes-vous une personne de confiance ?
 - Identifiant ?
 - Mot de passe ?
 - Accès en lecture ? En modification ? À quelques fichiers ? À l'ensemble du réseau ?
 - Simple utilisateur ? Technicien informatique ? Administrateur de l'entreprise ?



La notion d'utilisateur

- 1 **collaborateur** de l'entreprise = 1 **utilisateur** du système d'information
- Accès au SI validé par :
 - Le couple **Identifiant** + **Mot de passe**
 - Biométrie (Windows Hello)
 - Objet tiers (carte à puce, badge...)
 - 2^{de} authentification possible dans certains contextes spécifiques (SMS, lien de validation, etc.)



Gestion des utilisateurs

Utilisateur local

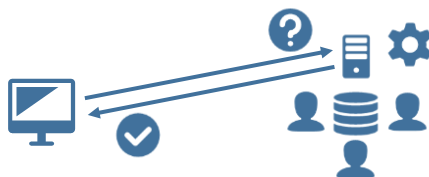
- Propre à chaque ordinateur
- Stocké dans la base de données locale SAM (Base Security Account Manager)
- L'utilisateur ne peut exploiter que les ressources de l'ordinateur source



Gestion des utilisateurs

Utilisateur du domaine

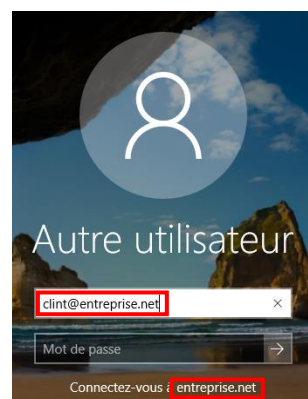
- Stocké dans une base de données commune (annuaire Active Directory)
 - Sur un serveur de l'entreprise (contrôleur de domaine)
 - Externalisé chez un prestataire (Microsoft Azure ou autre)
- Authentification Kerberos sécurisée par le réseau
- Un utilisateur peut ouvrir une session sur tous les ordinateurs du domaine
- Un utilisateur (local, de domaine) est identifié par le système grâce à son **SID** (Security Identifier)



Gestion des utilisateurs

Ouverture de session

- Pour les utilisateurs locaux
 - Utiliser un compte présent dans la base SAM
 - Sont affichés par défaut sur l'écran d'accueil
- Pour les utilisateurs du domaine
 - Jonction du poste au domaine de l'entreprise indispensable au préalable
 - Domaine sélectionné par défaut
 - Possibilité de s'authentifier grâce à l'annuaire d'un autre domaine



ATTENTION, la liste des utilisateurs locaux n'apparaît plus une fois l'ordinateur joint au domaine de l'entreprise !



Les catégories d'utilisateurs

- **Standard**

- Pour **utiliser** les ressources de l'ordinateur
- Être membre du groupe **Utilisateurs**

- **Administrateur**

- Pour **utiliser** et **modifier** les ressources de l'ordinateur
- Être membre du groupe **Administrateurs**
- L'utilisateur créé à l'installation du système est membre du groupe Administrateurs
- Le compte *administrateur* est désactivé par défaut

- **Le compte Invité**

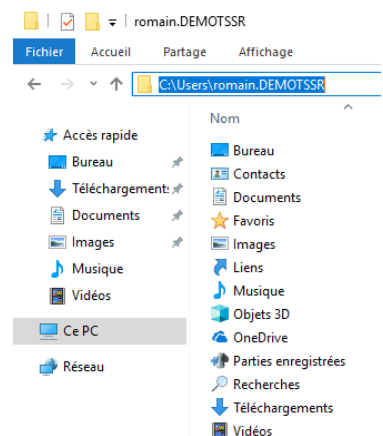
- Pour une **utilisation restreinte** des ressources de l'ordinateur
- Pas besoin de mot de passe pour accéder aux ressources
- Ce compte est désactivé par défaut



La gestion des profils

Un utilisateur ouvre une session pour la première fois, un profil personnel est créé

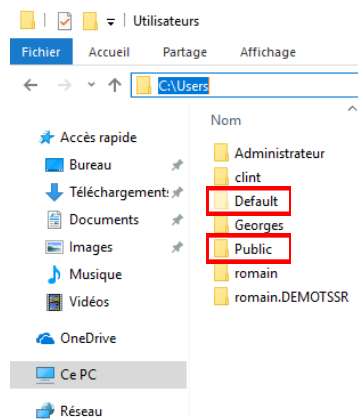
- Dans le dossier **C:\Users**
- Propre à chaque utilisateur
- Contient tous les paramètres et données de l'utilisateur
 - Documents
 - Téléchargement
 - Bureau
 - Images...



La gestion des profils

Un utilisateur ouvre une session pour la première fois, un profil personnel est créé

- Dans le dossier **C:\Users**
- Propre à chaque utilisateur
- Contient tous les paramètres et données de l'utilisateur
 - Documents
 - Téléchargement
 - Bureau
 - Images...
- Profil public : commun à tous les utilisateurs
- Profil par défaut (caché) : modèle pour la création d'un nouveau profil



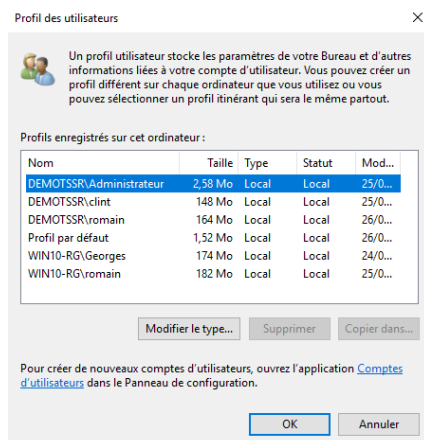
11

11

La gestion des profils

Comment gérer les profils ?

- **La gestion manuelle des profils dans le dossier c:\Users est à proscrire !**
- **sysdm.cpl** onglet **Paramètres systèmes avancés**
 - Supprimer des profils
 - Modifier le type du profil
 - Gestion du profil par défaut



12

12

Gestion des groupes

- Tout utilisateur doit appartenir à au moins un groupe
- Un groupe est identifié par le système grâce à son **SID** (Security IDentifier)
- Le SID du groupe s'ajoute au jeton d'accès de l'utilisateur
 - **Groupes locaux**
 - Pour configurer les autorisations d'accès aux ressources
 - Pour configurer les privilèges d'administration
 - **Groupes prédéfinis**
 - Présent nativement
 - Pour configurer les privilèges et la délégation d'administration (Administrateurs, Opérateurs de sauvegarde...)
 - **Entités intégrées de sécurité**
 - Non visibles dans les consoles
 - Affectation automatique
 - Utilisés par le système pour la gestion des permissions (Tout le monde, Utilisateurs authentifiés...)



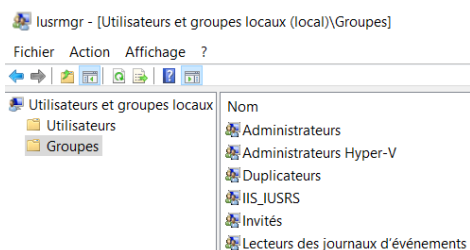
14

14

Gestion des utilisateurs et des groupes

Configuration

- Graphiquement grâce aux consoles MMC
 - lusrmgr.msc (gestion des utilisateurs et groupes locaux)
 - compmgmt.msc (gestion de l'ordinateur)
- Menu **Comptes d'utilisateurs** dans le panneau de configuration (orienté utilisateur)
- En ligne de commande
 - **net user** (**net help user** pour l'aide détaillée)
 - **net localgroup** (**net help localgroup**)



```
C:\>net user /?
La syntaxe de cette commande est :

NET USER
[nom_utilisateur [mot_passe | *] [options]] [/DOMAIN]
nom_utilisateur {mot_passe | *} /ADD [options] [/DOMAIN]
nom_utilisateur [/DELETE] [/DOMAIN]
nom_utilisateur [/TIMES:{heures | ALL}]
nom_utilisateur [/ACTIVE: {YES | NO}]
```



15

15

Gestion des utilisateurs et des groupes

- Configuration en PowerShell

Description	verbe	-nom
Affiche la liste des utilisateurs locaux	Get	-LocalUser
Créer un nouvel utilisateur dans la base SAM	New	
Modifier un utilisateur local existant	Set	
Renommer un utilisateur	Rename	
Activer l'utilisateur, il pourra de ce fait utiliser les ressources de l'ordinateur	Enable	
Désactiver un utilisateur	Disable	
Supprimer un utilisateur de la base SAM	Remove	

- Manipulation des groupes et de leurs membres avec les cmdlets

- {Get | Set | New | Remove}-LocalGroup et {Get | Set | Remove}-LocalGroupMember







Démonstration

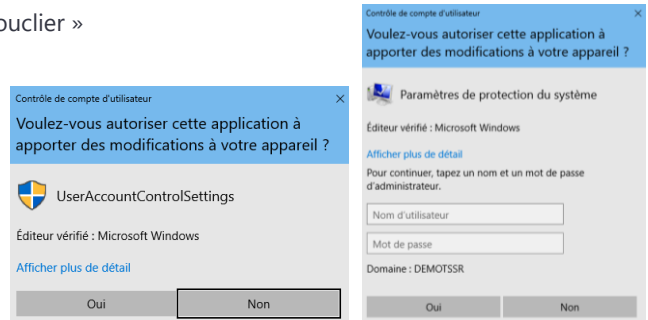


Contrôle de comptes d'utilisateur (UAC)

Sans action particulière, le système loge tous les utilisateurs à la même enseigne ... même les administrateurs !

- Par l'intermédiaire de l'UAC, le système n'accorde les privilèges que lorsque c'est nécessaire
- Élévation de pouvoir symbolisée par le « bouclier »
- Validation requise pour un administrateur
- Authentification requise pour un utilisateur

-  Gestionnaire de périphériques
-  Paramètres d'utilisation à distance
-  Protection du système
-  Paramètres système avancés



18

18

Contrôle de comptes d'utilisateur (UAC)

- Pourquoi ces contrôles ?
 - Lutter contre les actions des programmes malveillants
 - Avertir face à un paramètre sensible du système

Il est donc déconseillé de désactiver l'UAC

- Comment le configurer ?
 - Via le panneau de configuration
 - À l'aide de la stratégie de sécurité locale
 - secpol.msc
 - Stratégies locales > Options de sécurité
 - Valeurs **Contrôle de compte d'utilisateur**

Toujours m'avertir



Ne jamais m'avertir

M'avertir uniquement quand des applications tentent d'apporter des modifications à mon ordinateur (par défaut).

- Ne pas m'avertir lorsque je modifie des paramètres Windows.

i Recommandé si vous utilisez des applications et que vous visitez des sites Web que vous connaissez.

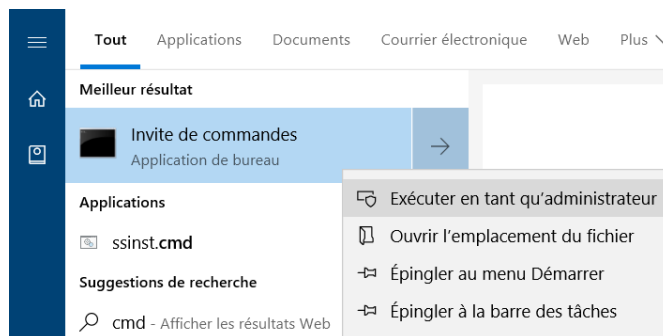
19

19

Contrôle de comptes d'utilisateur (UAC)

Pour certaines actions, il est nécessaire de demander l'élévation

- Graphiquement avec la fonction **Exécuter en tant qu'administrateur**



20

20

Récapitulatif

Un utilisateur est associé à :

- Un nom d'ouverture de session et un mot de passe
- Un profil local
 - Généré à la première ouverture de session
 - Contient les données personnelles et les paramètres de l'utilisateur
- Un identifiant unique (SID)
- Des appartenances de groupe définies dans l'onglet **Membre de**
- L'ensemble des SID constituent le **jeton d'accès**, ouvrant des accès et accordant des privilèges
- Les informations du jeton d'accès sont consultables avec la commande **whoami**

```
C:\Users\Georges>whoami /user
Informations sur l'utilisateur
-----
Nom d'utilisateur SID
win10-rg\georges S-1-5-21-1156289194-385894006-3085599902-1002
```

21

21

Démonstration



22

22

TP



23

23

Conclusion

- Un collaborateur = un utilisateur
- A chacun son métier
- A chacun ses données
- Le système est protégé
- L'identification est la clé de la sécurité

