

Quelques considérations sur le compte Administrateur.

Quel est l'utilité du compte Grand Administrateur ? Qu'est-ce qu'il peut faire qu'un compte (petit ? :-D) Administrateur ne peut pas faire ?

Réponse de JCB (Jean-Claude Bellamy)

C'est du grand n'importe quoi !!!!!

Qui dénote de la part de certains des connaissances parcelles et très approximatives, ce qui est une horreur en informatique, domaine privilégié du BINAIRE (OUI/NON, 0/1, Vrai/Faux,...) et qui ne supporte pas le "flou" (et qu'on ne m'objecte pas la "logique floue", qui n'est autre qu'un délire verbal de journaliers n'ayant rien compris)

Il existe 3 catégories de compte, correspondant à un niveau de privilèges donné :

- les administrateurs
- les utilisateurs
- les invités

Pour info, cette information est dans la structure USER_INFO_1 (DWORD usri1_priv) utilisée en particulier par la fonction "NetUserGetInfo" de l'API NetAPI32.dll

[http://msdn.microsoft.com/en-us/library/aa370654\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa370654(VS.85).aspx)

[http://msdn.microsoft.com/en-us/library/aa371109\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa371109(v=VS.85).aspx)

USER_PRIV_GUEST (=0)

-> Guest

USER_PRIV_USER (=1)

-> User

USER_PRIV_ADMIN (=2)

-> Administrator

A l'installation de Windows, DEUX comptes sont systématiquement créés, et NE SONT PAS SUPPRIMABLES :

- le compte "Administrateur", de SID se terminant par 500
(usri1_priv=USER_PRIV_ADMIN)
- le compte "Invité", de SID se terminant par 501
(usri1_priv=USER_PRIV_GUEST)

Par ailleurs, toujours au cours de cette installation, un autre compte utilisateur est créé, qui sera généralement dans la catégorie des administrateurs. Son SID se termine par 1000 ou plus.

Quand un compte ouvre une session, il est doté d'un "jeton" (token en anglais) qui est, pour faire simple, la liste des privilèges accordés au compte concerné. Et chaque fois que le système a besoin de faire quelque chose sous l'égide de ce compte, il consulte le jeton pour voir si c'est possible ou non.

Cela est valable dans toutes les versions de Windows NT, depuis NT4 (bien que l'ayant testé, je n'ai plus de souvenirs suffisamment précis pour NT 3.1 et NT 3.5x) jusqu'à Windows 7.

MAIS à PARTIR de Vista est apparu "UAC" (User Account Control), afin de renforcer la sécurité.

Cela se caractérise par une modification concernant UNIQUEMENT les comptes appartenant au groupe des Administrateurs.

Quand un compte admin ouvre une session, il est doté de DEUX jetons au lieu d'un seul :

- un avec les privilèges d'un compte lambda
- un avec les privilèges d'un compte administrateur

Mais à un instant donné, UN SEUL jeton est actif.
Et par défaut, c'est le jeton "lambda" qui est retenu!

Si bien que lorsque que l'utilisateur (admin) a besoin d'exécuter un processus nécessitant des privilèges élevés, un dialogue émis par le système apparaît demandant si on confirme ou non l'élévation de privilèges. Cela interdit donc à une "cochonnerieware", lancée à l'insu du plein gré de l'utilisateur, de faire n'importe quoi.

(NB: le dialogue en question est émis dans un AUTRE "bureau", donc interdit au processus "alien" de jouer automatiquement l'action sur les boutons, ce qui explique le passage par un écran noir. Mais c'est très gênant dans le cas de prise de main à distance, par VNC ou autre)

Si l'utilisateur a confirmé l'élévation de privilèges, c'est le jeton "admin" qui est alors utilisé, mais uniquement pour le processus concerné (et ses processus "fils" éventuels). Dès que le processus est terminé, c'est à nouveau le jeton "lambda" qui est actif.

(Ce qui est au passage la source d'énervement des utilisateurs admins contraints de confirmer l'élévation de privilèges à tout bout de champ!)

PAR DÉFAUT (car c'est modifiable), LE compte "Administrateur" (donc de SID se terminant par 500) ne se voit attribuer qu'UN SEUL jeton, à savoir celui d'admin.

Donc il détient toujours le maximum de privilèges.

MAIS il NE POSSÈDE PAS davantage de privilèges qu'un autre compte administrateur (quand il a confirmé l'élévation de privilèges)!

C'est pourquoi ces expressions de "Super-administrateur" ou de "Grand administrateur" m'insupportent au plus haut point.

Elles ne correspondent à rien de tangible.

Jusqu'à XP ou W2K3, il n'y a AUCUNE différence entre LE compte "Administrateur" et UN compte du groupe des administrateurs (à part le fait que LE compte "Administrateur" ne peut pas être supprimé)

Et à partir de Vista, on peut très bien unifier cela :

1) La désactivation de UAC

= clef

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA à 0

confère aux comptes admins un UNIQUE jeton "Administrateur" en permanence

2) La soumission du compte "Administrateur" à UAC

= clef

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken à 1

fait que ce compte "Administrateur" est soumis aux approbations d'élévation de privilèges comme les autres administrateurs.

Et la prochaine fois que je vois quelqu'un parler de "gnagnagna-administrateur", aux quatre coins de l'Albret je le dynamite, disperse, ventile!

;-)

Belle et saine colère, Jean-Claude ;-)

Mais que penses-tu de ça ?

Un article du site « Comment ça marche »

<http://www.commentcamarche.net/faq/5963-utiliser-l-administrateur-cache-de-vista>

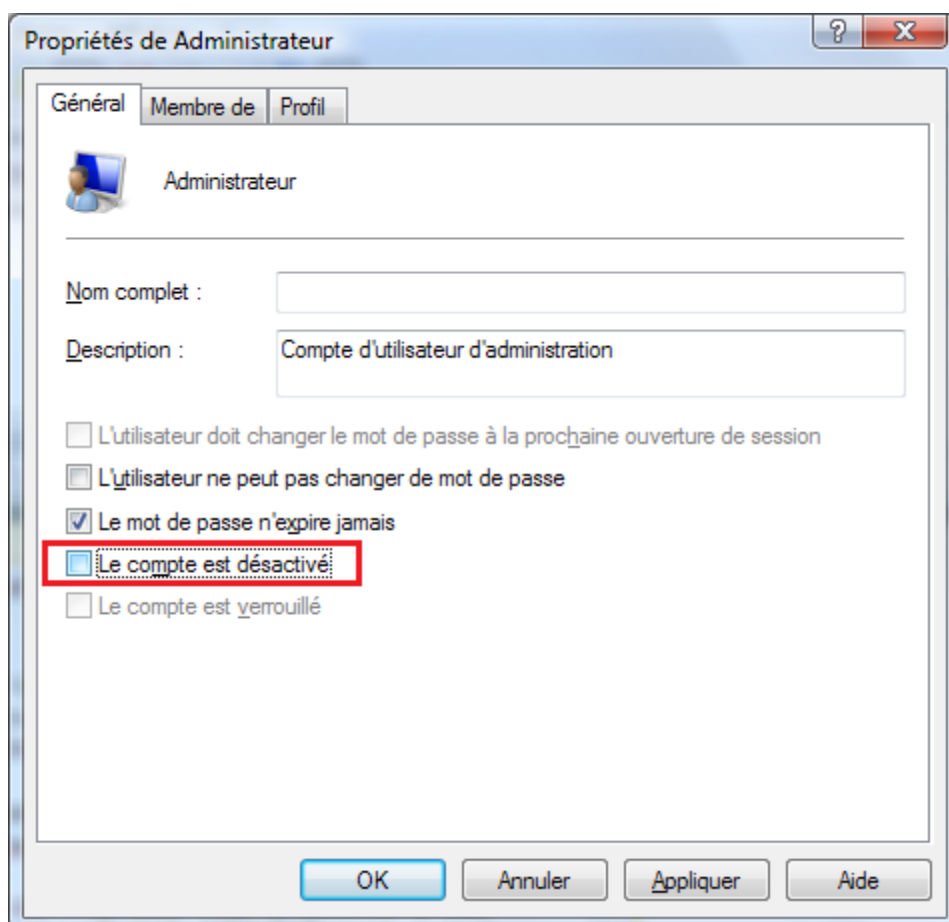
Utiliser l'Administrateur caché de Vista

Vista, comme XP, possède un compte nommé "Administrateur" mais il est caché et non activé par défaut.

Pour que ce compte apparaisse dans la liste des utilisateurs à l'écran d'accueil, la méthode est différente selon que l'on utilise une version "familiale" de Vista ou une version professionnelle (ou Intégrale).

Pour les versions Pro (ou Intégrales) le plus simple est de passer par Utilisateurs et groupes locaux.

- Dans la barre de recherche du menu Démarrer, taper `lusrmgr.msc` et valider.
- Cliquer sur Utilisateurs.
- Dans la fenêtre qui est à droite, faire Administrateur puis Propriétés et décocher la case "Le compte est désactivé"



Pour les versions "familiales" il faut procéder en deux temps :

- Créer la clef Administrateur dans la base de registre.
- Activer le compte Administrateur.

Création de la clé Administrateur dans la base de registre

- [Sauvegarder votre base de registre](#) (en cas de problème).
- [Ouvrir l'éditeur de registre](#).
- Se rendre à :

`HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon`

- Clic-droit sur Winlogon -> Nouveau -> Clé, lui donner le nom *SpecialAccounts* et valider.
- Répéter la même opération par clic-droit sur *SpecialAccounts* pour créer une sous-clé *UserList* et valider.
- Dans la fenêtre à droite en face de *UserList*, clic-droit -> Nouveau -> Valeur DWORD (32 bits) et lui attribuer le nom *Administrateur* avec la valeur *1* en cochant *Décimale* (clic-droit -> Modifier).
- Fermer l'éditeur...

Activation du compte Administrateur

L'étape suivante consiste à activer la présence du compte Administrateur dans le choix des comptes d'utilisateurs à l'ouverture de session :

- Ouvrir une fenêtre de commande, aller dans le menu Démarrer -> Tous les programmes -> Accessoires -> Clic-droit sur Invite de commande -> Exécuter en tant qu'administrateur.
- Taper

```
net user Administrateur /active:yes
```

(avec un espace entre *Administrateur* et */*) et valider.

- La notification

```
La commande s'est terminée correctement
```

confirme sa bonne exécution.

- Fermer la fenêtre de l'invite des commandes.

Le résultat est immédiat, il n'est pas nécessaire de redémarrer. Il suffit de fermer la session pour voir administrateur dans la liste.

Si l'on désire cacher de nouveau "Administrateur", il suffit de porter la valeur à 0 dans la base de registre.

Important

Attention, comme sous XP, il est préférable de ne pas utiliser ce compte pour le travail courant. Il faut le réserver à des dépannages et/ou à des modifications nécessitant un accès non restreint. Ne pas l'utiliser pour naviguer sur le net car l'ordinateur serait beaucoup plus vulnérable.

Ce n'est pas une nouveauté !

Et cela ne remet pas en cause mes propos.

Tout compte, quel qu'il soit, peut être activé ou désactivé.

Par défaut, sous Vista et au-delà, le compte Administrateur est désactivé, ce qui est une énorme conceté !

Jusqu'à XP PRO, au cours de l'installation de Windows la procédure était la suivante, et je la trouvais EXCELLENTE au demeurant :

- Création automatique du compte Administrateur
- DEMANDE de création de mot de passe pour ce compte
- Activation systématique de ce compte
- ...

Donc ici le compte admin était toujours utilisable, quel que soit le mode (normal ou sans échec), et protégé par mot de passe

Sous XP HOME, une HORREUR et une ERREUR en matière de gestion des comptes, le compte administrateur était créé SANS demande de mot de passe, et utilisable SEULEMENT en mode sans échec (une IDIOTIE TOTALE!)

A partir de Vista, la procédure est devenue la suivante :

- Création automatique du compte Administrateur
- Aucun mot de passe pour ce compte
- Désactivation systématique de ce compte
- ...

Ici le compte admin n'est pas utilisable en mode normal, et l'est en mode sans échec SEULEMENT s'il n'existe pas d'autre compte administrateur, et

non protégé par mot de passe.

Situation grotesque!

En effet, MS ayant décidé de ne pas faire attribuer de mot de passe au compte Administrateur, par défaut, l'a volontairement désactivé, afin qu'on ne puisse pas l'utiliser en fonctionnement normal.

Cela peut à la rigueur empêcher qu'un "alien" s'empare de l'ordinateur en utilisant le compte Administrateur, mais seulement en mode normal!

Par contre, ce qui est hautement fâcheux, c'est la situation (très fréquente comme en témoignent les appels au secours dans les forums Answers p.ex.) où un utilisateur a oublié son mot de passe, alors que son compte fait partie du groupe des admins (cas par défaut), et où il n'y a pas d'autre compte administrateur dont il connaîtrait le mot de passe.

En effet, il ne peut pas ouvrir de session

- ni en mode normal :

- ni avec son compte puisqu'il a oublié son mot de passe
- ni avec LE compte "Administrateur" puisqu'il est désactivé

- ni en mode sans échec :

- ni avec son compte puisqu'il a oublié son mot de passe
- ni avec LE compte "Administrateur" puisqu'il existe un AUTRE compte administrateur.

-> BLOCAGE TOTAL à moins de faire appel à la méthode de Petter NORDHAL d'effacement des mot de passe directement dans la base SAM.

<http://www.bellamyjc.org/fr/pwdnt.html>

DONC dès que j'installe Vista ou Win7, une des toutes premières actions que j'entreprends est l'ACTIVATION du compte "Administrateur", par la commande :

NET USER Administrateur /ACTIVE:YES

et la définition d'un mot de passe (donc non vide) par la commande :

```
NET USER Administrateur *
```

(il y a alors demande de ce mot de passe avec confirmation)

Je retrouve ainsi le fonctionnement de NT4, W2K, XP, W2K3, ..., nettement plus rationnel et plus pratique.

Et tout autant sécurisé ...

De plus, je rappelle que par défaut il est impossible d'ouvrir une session à distance si le mot de passe du compte est vide !

Donc ce compte "Administrateur" sans mot de passe par défaut est, une fois de plus, une super conceté, puisque cela interdit de l'utiliser dans un réseau!

il est à noter que pour le désactiver la commande est :

```
NET USER Administrateur /ACTIVE:NO
```

--

May the Force be with You!

La Connaissance s'accroît quand on la partage

Jean-Claude BELLAMY [MVP]

<http://www.bellamyjc.org> ou <http://jc.bellamy.free.fr>

Voir encore le lien de JF : <http://fspsa.free.fr/echec-ouverture-session-par-service-profil-utilisateur.htm>