Table des matières

GESTION DES UTILISATEURS ET GROUPES LOCAUX

I. PRÉSENTATION DES COMPTES UTILISATEURS

Les comptes utilisateurs ainsi que les groupes locaux sont importants en matière de sécurité sous Windows 7, car ils permettent de déterminer des droits d'accès et des autorisations sur les différentes ressources d'un ordinateur.
Pour accéder à un ordinateur, les utilisateurs doivent fournir un nom d'utilisateur et un mot de passe. Si l'authentification est correcte, Windows 7 crée un jeton d'accès qui correspond à l'identification locale de l'utilisateur.
Les paramètres de sécurité associés à un compte utilisateur permettent de contrôler l'accès aux ressources et l'exécution des taches systèmes.
Microsoft Windows 7 propose trois types différents de comptes d'utilisateurs: des comptes d'utilisateurs locaux, des comptes d'utilisateurs de domaine et des comptes d'utilisateurs prédéfinis.
Les comptes d'utilisateurs locaux permettent à un utilisateur de se connecter à un ordinateur et d'accéder aux ressources de cet ordinateur à partir d'un autre ordinateur distant.
Les comptes d'utilisateurs de domaine permettent à un utilisateur de se connecter à un domaine pour accéder aux ressources réseau. Ce type de compte est étudié lors de la formation Windows Server.
Les comptes d'utilisateurs prédéfinis sont créés automatiquement lors de l'installation de Windows 7. Il existe deux comptes prédéfinis : Administrateur et
Invité.

II. COMPTES UTILISATEURS LOCAUX

Lorsque vous créez un compte d'utilisateur sur un ordinateur, Windows 7 inscrit le compte dans sa base locale de sécurité, appelée base SAM (*Security Account Manager*) stockée dans : \Windows\System32\config.
Windows 7 ne réplique les informations du compte d'utilisateur local sur aucun autre ordinateur. Une fois le compte créé, l'ordinateur interroge sa base de données locale de sécurité pour authentifier l'utilisateur au moment où il tente de se connecter soit localement, soit à partir d'un ordinateur distant.
Au contraire de l'utilisateur d'un domaine où à l'ouverture de session l'authentification est unique, l'utilisateur disposant d'un compte local doit préciser à chaque connexion sur un ordinateur distant le nom d'utilisateur et le mot de passe référencés dans le gestionnaire SAM de cet ordinateur.

III. COMPTES UTILISATEURS PRÉDÉFINIS

Il existe deux comptes prédéfinis : Administrateur et Invité qui ne peuvent en aucun cas être supprimés.

ADMINISTRATEUR

Le compte Administrateur qui appartient au groupe Administrateurs est désactivé par défaut Vous ne pouvez pas le supprimer, ou le retirer du groupe

Administrateurs. Il est conseillé de lui attribuer un mot de passe « renforcé » et de le renommer en utilisant un nom qui ne le désigne pas explicitement afin de garantir un plus haut niveau de sécurité. Les tâches effectuées par ce compte comprennent la gestion des comptes utilisateurs et des groupes locaux, la gestion des stratégies de sécurité, l'installation et la configuration d'imprimantes, l'attribution des autorisations et des droits associés pour permettre l'accès aux ressources, la sauvegarde et la restauration de données.

INVITÉ

Le compte prédéfini **Invité** est utilisé pour autoriser des utilisateurs occasionnels à se connecter et à accéder aux ressources. A l'issue de l'installation de Windows 7, ce compte est désactivé par défaut et ne peut pas être supprimé.

Créer des utilisateurs avec 5 méthodes différentes.

1ère Méthode :

Menu Démarrer / Panneau de configuration/ comptes d'utilisateur /créer un compte

2ème Méthode :

Le même éditeur peut être lancé en exécutant directement la commande :
CONTROL USERPASSWORDS

3ème Méthode :

Un troisième éditeur plus avancé en exécutant directement la commande :
CONTROL USERPASSWORDS2

4ème Méthode :

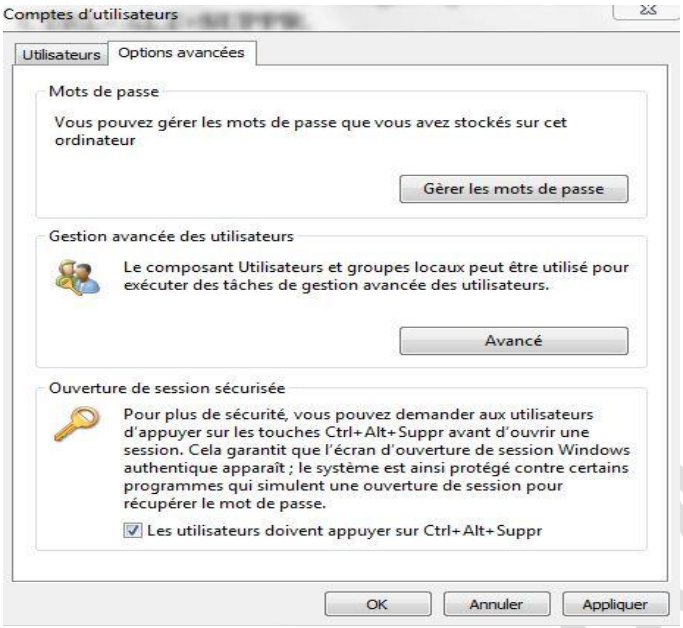
Un quatrième éditeur en exécutant directement la commande :
Lusrmgr.msc

5ème Méthode :

Un cinquième éditeur similaire à celui de la 4ème méthode :
Menu Démarrer / Click droit sur poste de travail / Gérer /utilisateurs et groupes

IV. Activer la commande Ctrl + Alt + Suppr à l'écran d'accueil.

Par défaut Windows utilise l'écran d'accueil pour afficher les comptes utilisateurs présents dans la base de données locale de sécurité. Le problème c'est que certains programmes peuvent remplacer cet écran d'accueil afin de recueillir les mots de passe
De ces comptes. Afin d'ajouter une couche supplémentaire de sécurité à l'ouverture de session il vous suffit de modifier la manière dont vous ouvrez une session. Il va donc falloir activer la séquence de clavier SAS (Secure Attention Séquence), **CTRL+ALT+SUPPR.**
Pour ce faire il suffit d'allez dans le menu **Démarrer** puis **Exécuter** et saisissez **CONTROL USERPASSWORDS2** / Onglet option avancée / cocher **les utilisateurs doivent appuyer sur CTRL+ALT+SUPPR.**



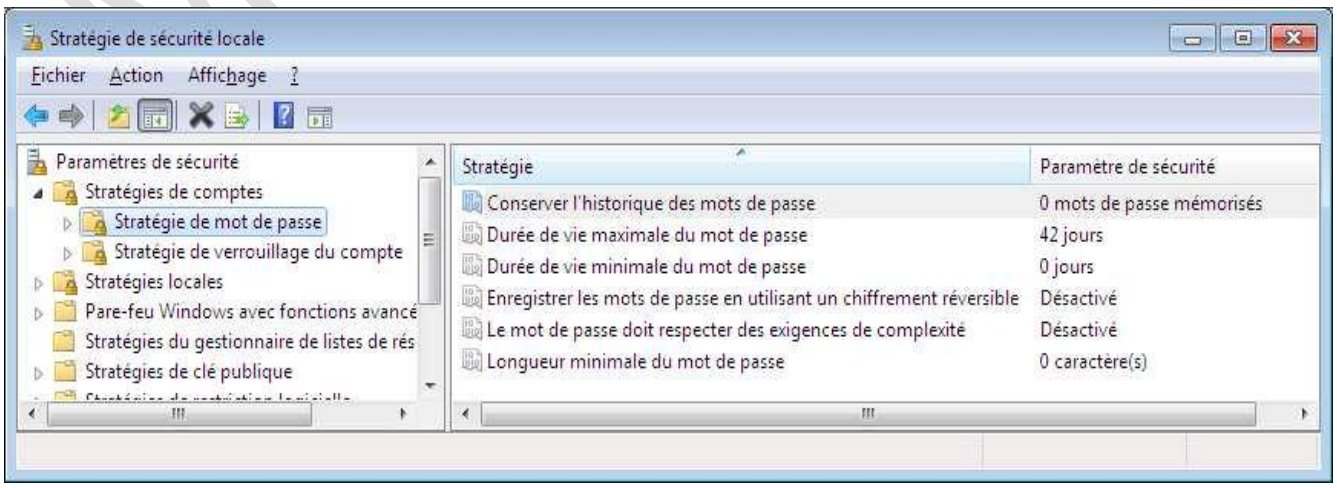
Désormais avant d'ouvrir une session vous devrez appuyer simultanément sur la combinaison de touches **CTRL+ALT+SUPPR**. Ce qui activera l'écran d'ouverture de session sécurisée de Windows.

V. LES STRATÉGIES DE COMPTES

Les stratégies de comptes permettent d'améliorer la sécurité des mots de passe des utilisateurs et de paramétrer le verrouillage d'un compte utilisateur.
Les stratégies de comptes sont accessibles exclusivement aux membres du groupe *Administrateurs* à partir du menu *Outils d'administration* / *Stratégie de sécurité locale* / *Stratégies de comptes* ou directement depuis la console
« secpol.msc ».
Le dossier *Stratégies de compte* se subdivise en 2 sous dossiers *Stratégie de mot de passe* et *Stratégie de verrouillage du compte*.

STRATÉGIE DE MOT DE PASSE

La stratégie de mot de passe est utilisée pour paramétrer la création et la gestion des mots de passe.
Vous exécutez la commande SECPOL.MSC cette fenêtre si dessus s'ouvre



Et vous donne la possibilité de faire ces paramètres ci après :

✓ Conserver l'historique des mots de passe

Nombre de mots de passe à conserver dans l'historique.
La valeur par défaut est 0, ce qui signifie qu'aucun historique n'est conservé.
Cette valeur comprise entre 0 et 24, définit le nombre de nouveaux mots de passe qu'un utilisateur doit employer avant de réutiliser un ancien mot de passe.

✓ Durée de vie maximale d'un mot de passe

Nombre de jours pendant lequel un utilisateur peut employer un mot de passe avant de devoir le changer.
La plage de valeurs est comprise entre 0 et 999.
La valeur 0 indique que le mot de passe n'expire pas.
La valeur par défaut est 42.

✓ Durée de vie minimale du mot de passe

Nombre de jours minimum pendant lequel un utilisateur doit conserver son mot de passe avant de le changer.
La valeur par défaut 0 signifie que le mot de passe peut être modifié immédiatement après un changement.

✓ Enregistrer les mots de passe en utilisant un chiffrement réversible.

Les options disponibles sont Activées et Désactivé.
La valeur par défaut est Désactivée.
Cette stratégie est destinée aux applications qui utilisent des protocoles nécessitant la connaissance du mot de passe de l'utilisateur à des fins d'authentification. Le stockage des mots de passe avec un chiffrement réversible est fondamentalement identique au stockage des versions des mots de passe en texte clair. Pour cette raison, cette stratégie ne doit être activée que si les impératifs de l'application prévalent sur la nécessité de protéger les informations des mots de passe.

✓ Le mot de passe doit respecter des exigences de complexité

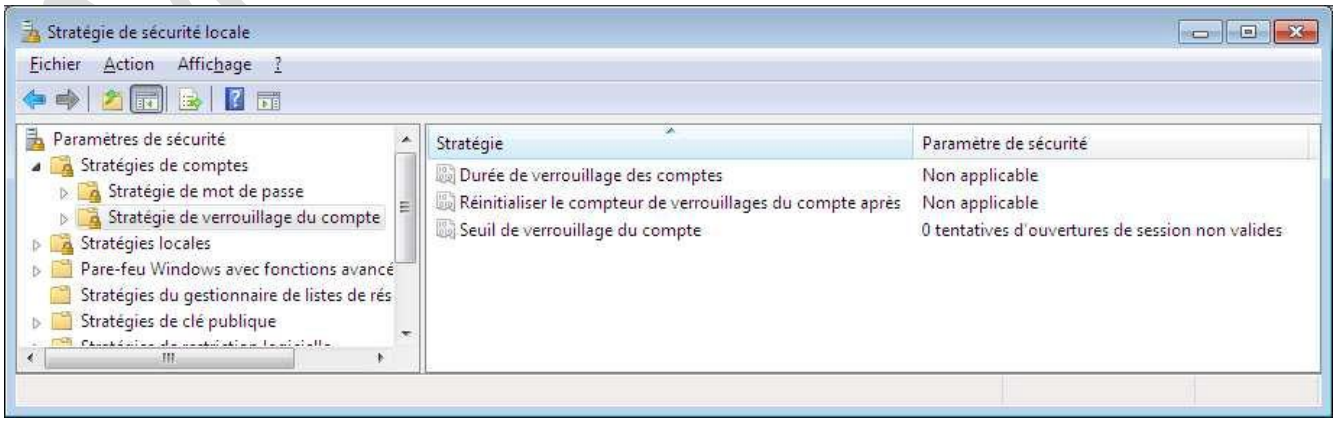
Les options disponibles sont Activées et Désactivé.
La valeur par défaut est Désactivée.
Lorsque l'option Activé est sélectionnée, les mots de passe doivent être de type renforcé (7 caractères minimum, combinaison de majuscules, minuscules, chiffres et symboles,…..).

✓ Longueur minimale du mot passe

Nombre minimal de caractères requis dans le lot de passe.
Ce nombre doit être compris entre **0 et 14 caractères,** la valeur par défaut 0 autorise le mot de passe vide.

STRATÉGIE DE VERROUILLAGE DE COMPTE

La stratégie de verrouillage de compte interdit à un utilisateur l'accès à un ordinateur après un certain nombre de tentatives infructueuses.



✓ Durée de verrouillage des comptes

Nombre de minutes durant lesquelles le compte est verrouillé.
La valeur 0 indique que le compte est verrouillé jusqu'à ce que l'administrateur le déverrouille.
La plage de valeurs est comprise entre 0 et 99999.

✓ Réinitialiser le compteur de verrouillages du compte après

Nombre de minutes qui doivent s'écouler avant que le système réinitialise le compteur de verrouillage du compte.
La plage de valeurs est comprise entre 0 et 99999.

✓ Seuil de verrouillage du compte

Nombre de tentatives d'ouvertures de session non valides avant que le compte utilisateur soit verrouillé.
La valeur 0 indique que le compte ne sera pas verrouillé quel que soit le nombre de tentatives d'ouvertures de session non valides.
La plage de valeurs est comprise entre 0 et 999.

VI. LE CONTRÔLE DE COMPTE UTILISATEUR

Le contrôle de compte utilisateur permet une mise en œuvre de la sécurité par l'utilisateur lui-même.
Un utilisateur est « utilisateur standard » ou « administrateur », pour ne pas être confronté aux contraintes liés à un profil d'utilisateur standard, les utilisateurs étaient déclarés en tant administrateur.
Face à cette situation qui pouvait parfois mettre en péril le système et la sécurité,
Microsoft a proposé UAC (*User Account Control*) au sein de Vista et a implémenté le principe dit de moindre privilège. Ce principe consiste à toujours donner à **Comptes utilisateurs et groupes locaux** l'utilisateur, qu'il soit administrateur ou non, le moins de droits possible, et à les compléter uniquement lorsqu'il en a besoin.
Le contrôle utilisateur fonctionne comme une surcouche système. Il est suffisamment séparé du système pour qu'aucun ne programme ou virus ne puisse y accéder et seuls les messages envoyés légitimement depuis la souris ou le clavier sont autorisés à lui parvenir, afin de bloquer les virus simulant l'appui sur les touches.
Le mécanisme du contrôle utilisateur pour les applications est simple mais efficace. Pour chaque application, une méthode de détection heuristique (Algorithme permettant de rapidement trouver une solution) est utilisée pour détecter si :

- L'application est bloquée par une stratégie de sécurité ou si son éditeur est bloqué.
- L'éditeur est le système lui-même.
- L'éditeur est un éditeur vérifié.
- L'éditeur n'est pas connu.

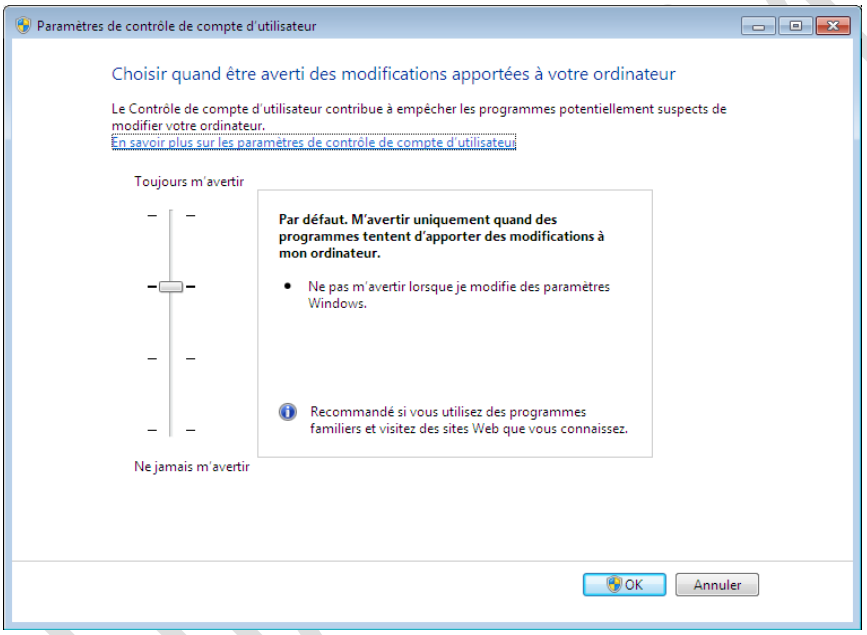
Pour chacune de ces vérifications, une fenêtre d'alerte s'affiche, demandant à l'utilisateur de valider.

✓ LE PRINCIPE DE MOINDRE PRIVILÈGE

Avec le mécanisme du moindre privilège, un utilisateur, lors de sa connexion au système, reçoit un jeton (en anglais *token*) définissant les rôles qu'il possède.
Avec le mécanisme du moindre privilège, il reçoit uniquement les jetons qui correspondent à des rôles ne comportant que peu de risques pour le système (incapables de modifier le registre ou les fichiers système, par exemple).
Ainsi, lorsque l'utilisateur tente d'accéder à une console d'administration système telle que la console de stratégies locales, le système vérifie ses jetons. Comme l'utilisateur ne porte avec lui qu'une partie de ses jetons d'accès, s'il ne possède pas les jetons nécessaires à l'exécution d'une tâche ou d'un programme, le système vérifie dans la liste complète des jetons de l'utilisateur s'il possède celui qui permet d'utiliser la console. Dans le cas où l'utilisateur possède un jeton directement valide, le système lui demande juste de valider s'il souhaite réellement accéder à cette console.
Si l'utilisateur ne possède pas le jeton nécessaire, une boîte de dialogue lui demande de saisir les identifiants de connexion administrateur.

✓ CONFIGURER LE CONTRÔLE UTILISATEUR

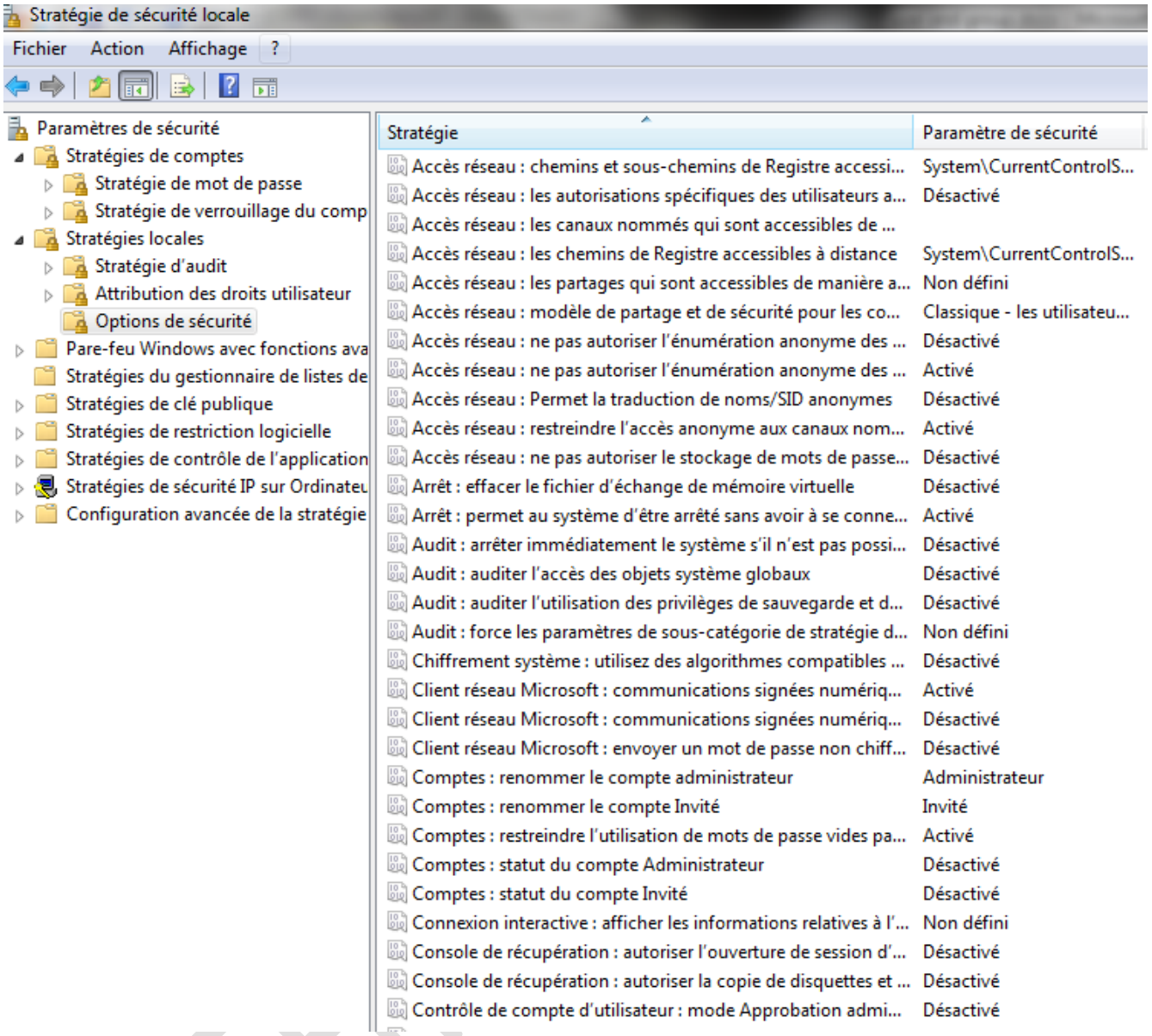
Ajouté dans Windows Vista, UAC a donc été présenté comme *la* solution pour la sécurité de l'utilisateur contre lui-même. Malheureusement, ses fenêtres de confirmation intempestives gênaient les utilisateurs qui ont pris pour habitude de désactiver complètement cette fonctionnalité. Elle perdait ainsi tout son intérêt.
Afin de persister dans cette solution, Windows 7 propose un compromis en proposant à l'utilisateur de définir le niveau d'alerte qu'il souhaite recevoir, sans pour autant avoir à désactiver cette sécurité complémentaire.
Si les fenêtres de confirmation vous gênent et que vous êtes sûr de vos actions, vous pouvez ainsi réduire le nombre des confirmations nécessaires.
Pour configurer les paramètres de contrôle de compte d'utilisateur, vous devez :
1 Ouvrir le Panneau de Configuration et cliquer sur Comptes et protection utilisateur.
2 Cliquer sur Comptes utilisateur, puis sur Modifier les paramètres de contrôle de compte utilisateur.



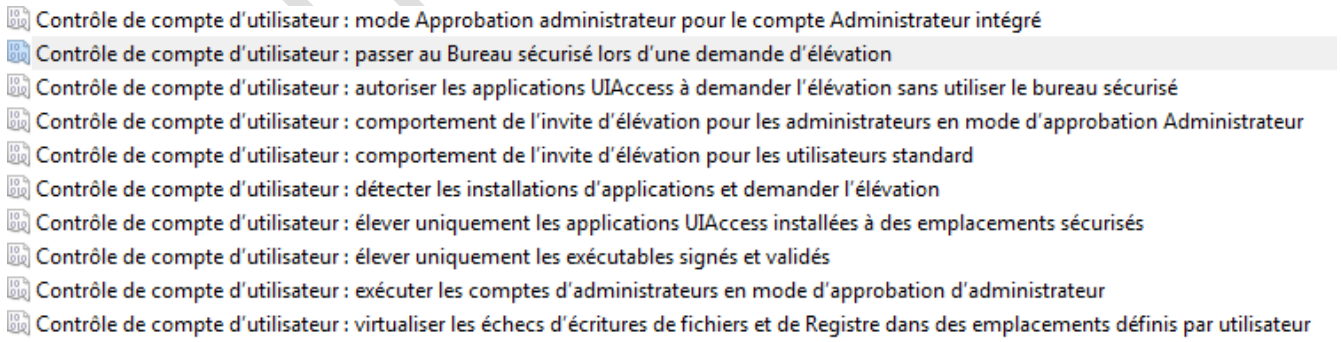
Une interface très simple vous permet alors de définir l'un des quatre niveaux disponibles, allant d'une sécurité maximale avec confirmation à chaque opération système jusqu'à la désactivation complète des alertes.

✓ CONFIGURATION AVANCÉE

Pour paramétrer plus précisément le contrôle utilisateur, vous pouvez utiliser les stratégies de sécurité locales.
1 - Ouvrez la console de gestion des stratégies de sécurité « gpedit.msc ».
2 - Dépliez l'arbre latéral en choisissant
Stratégie Ordinateur local>Configuration ordinateur>Paramètres Windows>Paramètres de sécurité.
3 - Cliquez ensuite sur *Stratégies locales>Options de sécurité*.



Dix stratégies sont alors à votre disposition afin de répondre à des cas d'utilisation du contrôle utilisateur.



Pour comprendre ces stratégies, il faut savoir que les droits utilisateur sont stockés dans un jeton, mais que vous démarrez toujours une session avec les droits minimaux, y compris si vous êtes administrateur de la machine. Les droits complémentaires ne vous sont octroyés qu'à la demande.

✓ Mode Approbation administrateur pour le compte Administrateur intégré

Si cette stratégie est désactivée, l'administrateur utilise toujours un jeton complet ne nécessitant jamais d'élévation de droits.

✓ Passer au Bureau sécurisé lors d'une demande d'élévation

Lorsque cette stratégie est activée, un rideau noir semi-transparent s'affiche au moment de la demande d'élévation de privilèges pour montrer de façon explicite qu'aucune opération n'est possible tant que la fenêtre d'élévation est ouverte.

✓ Autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé

Le Bureau sécurisé est l'écran noir s'affichant au moment de la demande d'élévation. Cette stratégie permet, lorsqu'elle est activée, de ne pas bloquer le fonctionnement des applications ayant besoin d'accéder à des composants de l'interface

✓ Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur

Cette stratégie concerne l'élévation de privilèges pour un utilisateur qui est déjà administrateur.
Trois options sont disponibles :
• Aucune invitation : l'élévation se fait en mode silencieux et sans demande particulière.
• Demande de consentement : l'administrateur doit confirmer l'élévation de privilèges.
• Demande d'informations d'identification : le mode le plus sécurisé, qui demande, à chaque action sensible, l'identifiant et le mot de passe administrateur.

✓ Comportement de l'invite d'élévation pour les utilisateurs standards

Lorsque le paramètre de cette stratégie est positionné sur Demande d'informations d'authentification, une fenêtre d'authentification (identifiant/mot de passe) s'affiche. Si le paramètre Aucune invite est activé, l'utilisateur doit choisir à chaque exécution l'option Exécuter en tant qu'administrateur.

✓ Détecter les installations d'applications et demander l'élévation

Lorsque cette stratégie est activée, le système tente de détecter soit par le nom de l'exécutable, soit par son manifeste, si ce dernier requiert une élévation de droits. Dans le cas où cela est nécessaire pour le bon fonctionnement de l'application, une demande d'élévation est alors proposée à l'utilisateur.

✓ Élever uniquement les applications UIAccess installées à des emplacements sécurisés

Cette stratégie limite l'accord de droits UIAccess (accès aux interfaces) aux applications installées dans le répertoire Programmes (%ProgramFiles%) et Windows (%Windir%). Dans le cas où un applicatif UIAccess est démarré depuis un autre emplacement, il obtiendra les droits de la personne qui l'exécute (niveau asInvoker).

✓ Élever uniquement les exécutables signés et validés

Lorsque cette stratégie est activée, seuls les fichiers exécutables signés peuvent s'exécuter. Elle se base sur une vérification de signature utilisant une PKI (Public Key Infrastructure) pour chaque exécutable nécessitant une élévation de privilèges. L'administrateur peut définir la liste des applications autorisées via le magasin d'éditeurs approuvés des ordinateurs locaux.

✓ Exécuter les comptes administrateur en mode d'approbation d'administrateur

Lorsque cette stratégie est désactivée, le contrôle utilisateur est quasiment éteint. Les comptes ayant des droits administrateur ne reçoivent plus de demandes d'élévation de privilèges. Le centre de sécurité indique d'ailleurs que le système est potentiellement faillible si jamais une application malintentionnée est exécutée sous la session du compte administrateur. Celle-ci pourra alors agir à sa guise sans qu'aucun contrôle ne soit disponible.

VII. PRÉSENTATION DES GROUPES

Un groupe est un ensemble de comptes utilisateurs. L'utilisation des groupes simplifie les tâches d'administration en vous permettant d'attribuer des autorisations et des droits à un groupe d'utilisateurs plutôt qu'à chaque compte individuellement.
Les autorisations ou permissions abordées dans le chapitre « Sécurité des fichiers et partage des ressources » permettent de définir un type d'accès relatif aux tâches que les utilisateurs peuvent effectuer sur une ressource (dossier, fichier, imprimante etc…).
Les utilisateurs peuvent être membre de plusieurs groupes, certains groupes (notamment les groupes systèmes) peuvent être membres d'autres groupes.

Microsoft Windows 7 propose deux types différents de groupes :

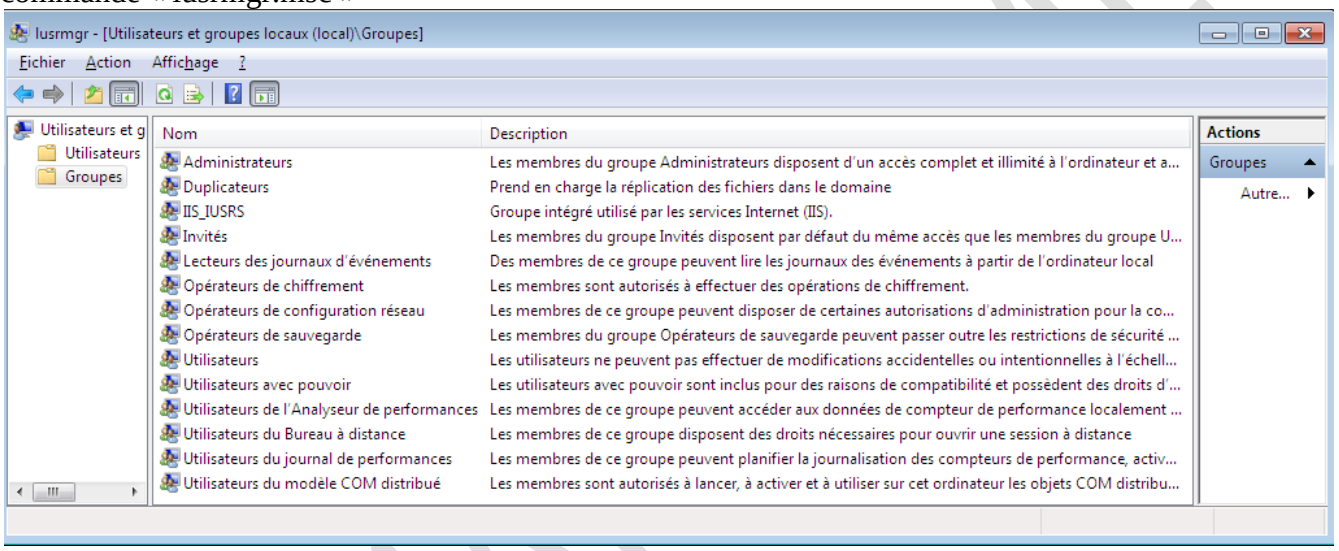
- ✓ des groupes prédéfinis ;
- ✓ des groupes locaux.

GROUPES PRÉDÉFINIS

Les groupes prédéfinis sont créés automatiquement lors de l'installation de Windows 7. Ils ne peuvent en aucun cas être supprimés.
Il existe deux groupes prédéfinis : les groupes locaux et les groupes spéciaux.

GROUPES LOCAUX PRÉDÉFINIS

Les groupes locaux prédéfinis permettent de définir des niveaux d'accès et d'habilitation pour les comptes utilisateurs.
La liste des groupes locaux prédéfinis est accessible depuis la console « lusrmgr » ou en exécutant la commande « lusrmgr.msc »



GROUPES LOCAUX

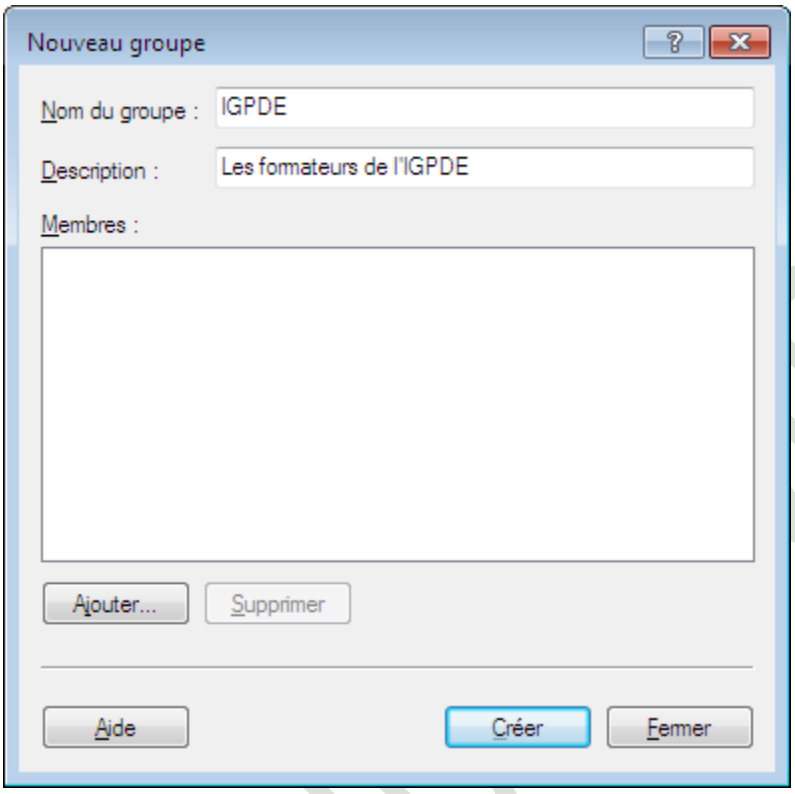
Un groupe local est un ensemble de comptes utilisateurs créés sur un ordinateur et possédant des besoins identiques en termes d'administration.
Les permissions et droits assignés à un groupe sont répercutés sur tous les utilisateurs de ce groupe.
Dans la base de données locale de sécurité de l'ordinateur, Windows 7 ne peut créer qu'un seul type de groupe : les groupes locaux.
Les groupes locaux sont utilisés exclusivement sur l'ordinateur à partir duquel ils ont été créés.
Les règles d'appartenance aux groupes locaux sont les suivantes :

- ✓ Les groupes locaux contiennent uniquement les comptes utilisateurs et les groupes prédéfinis système.
- ✓ Les groupes locaux ne peuvent être membres d'aucun autre groupe.

CRÉATION D'UN GROUPE LOCAL

La création d'un groupe local s'effectue à partir du composant logiciel enfichable *Utilisateurs et groupes locaux* accessible depuis la console Gestion de l'ordinateur.
Pour créer un groupe local :
1. Ouvrez Gestion de l'ordinateur depuis Outils d'administration du menu Programmes.
2. Dans la partie gauche Arbre, sélectionnez Groupes du composant Utilisateurs et groupes locaux.
3. Activez le menu Action ou le menu contextuel (clic droit) du dossier « Groupes » ou le menu contextuel (clic droit) dans la partie droite de la fenêtre.
4. Sélectionnez Nouvel groupe.

5. Complétez les rubriques de la boîte de dialogue Nouveau groupe.
6. Ajoutez ou supprimez des membres.
7. Cliquez sur le bouton « Créer ».



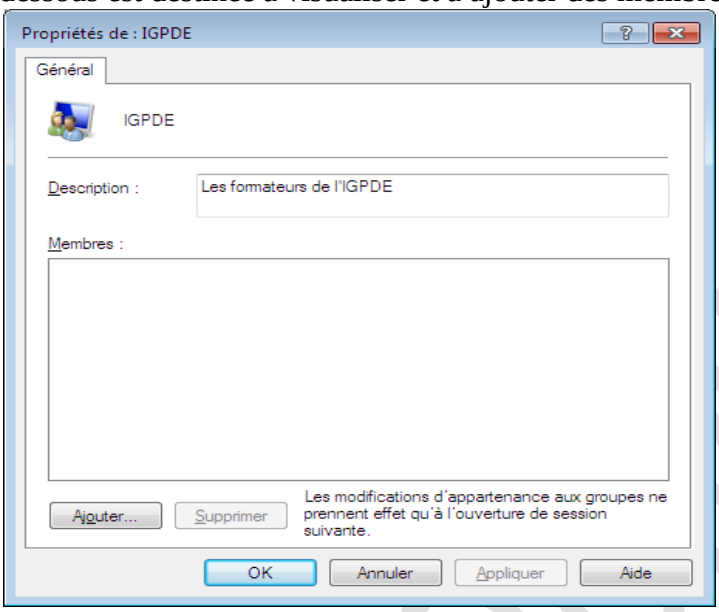
Rubrique	Description
Nom de groupe	Nom **unique** du groupe local. Ce nom doit être **différent** de tout autre nom de groupe ou nom d'utilisateur contenu dans la base de données locale de sécurité de l'ordinateur. Il peut contenir jusqu'à **256 caractères**. Cette zone est **obligatoire.**
Description	Zone permettant la saisie d'un texte descriptif sur le groupe local.
Ajouter	Permet d'ajouter un utilisateur dans la liste des membres du groupe local.
Supprimer	Permet de supprimer l'utilisateur sélectionné dans la liste des membres du groupe local.
Créer	Valide la création d'un nouveau groupe.
Fermer	Ferme la boite de dialogue Nouveau groupe mais ne valide pas la création en cours d'un nouveau groupe.

CONFIGURATION D'UN GROUPE LOCAL

Le menu contextuel du groupe local permet d'accéder à sa configuration.

✓ AJOUTER AU GROUPE

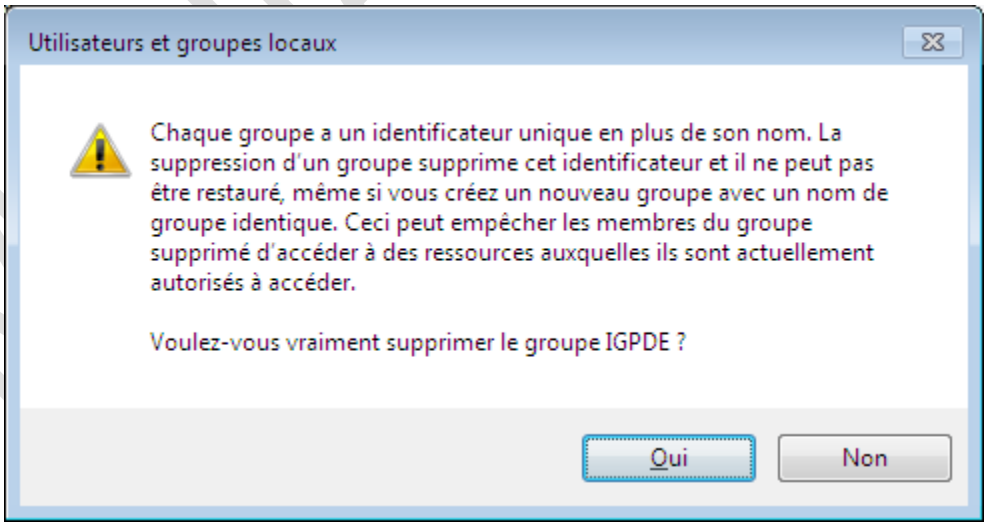
Vous pouvez ajouter des membres à un groupe local lors de la création du groupe ou ultérieurement.
La boîte de dialogue ci-dessous est destinée à visualiser et à ajouter des membres à un groupe local.



Le bouton **Ajouter** permet d'ajouter un ou plusieurs membres au groupe local.

✓ SUPPRIMER UN GROUPE LOCAL

Chaque groupe local créé est doté d'un identificateur unique et non réutilisable.
La suppression d'un groupe annule les autorisations et les droits associés, mais n'entraîne pas la suppression des membres de ce groupe.
Si vous supprimez un groupe, la création d'un nouveau groupe portant le même nom ne vous permettra pas de récupérer les informations et les propriétés qui lui étaient précédemment affectées, car il n'hérite pas de celles qui étaient attribuées à l'ancien.
Le message de confirmation de suppression d'un groupe local reprend les observations consignées ci-dessus.

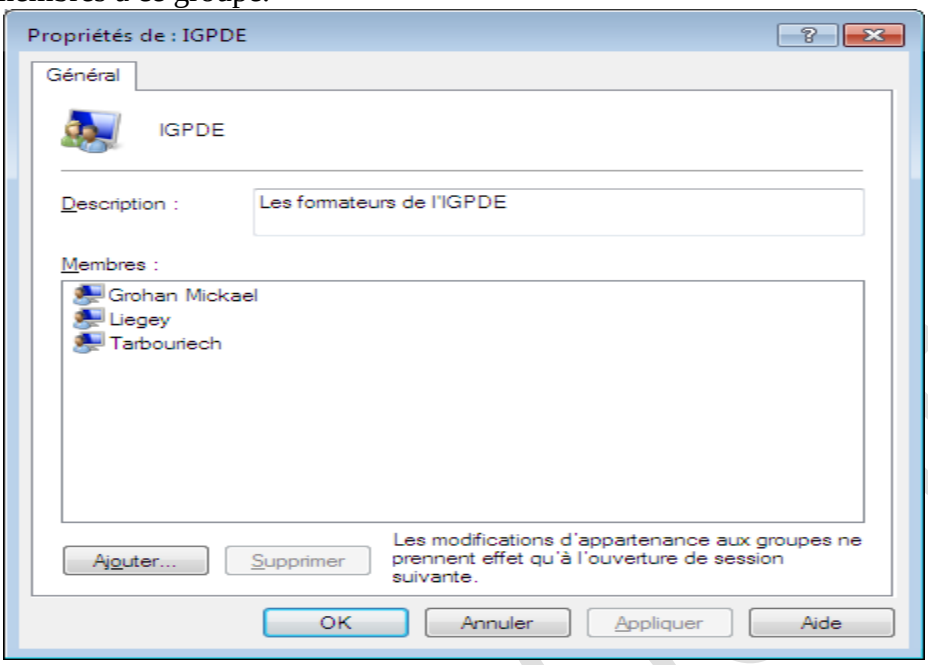


✓ RENOMMER UN GROUPE LOCAL

Lorsque vous renommer un groupe, vous ne perdez pas les informations, les autorisations et droits rattachés à ce groupe.

✓ PROPRIÉTES D'UN GROUPE LOCAL

Les propriétés du groupe local permettent de modifier la description du groupe, d'ajouter ou de supprimer des membres à ce groupe.



Désactiver l'affichage du dernier utilisateur à l'écran d'accueil.

Stratégie de sécurité locale / paramètres de sécurité / Stratégie locales / Options de sécurité

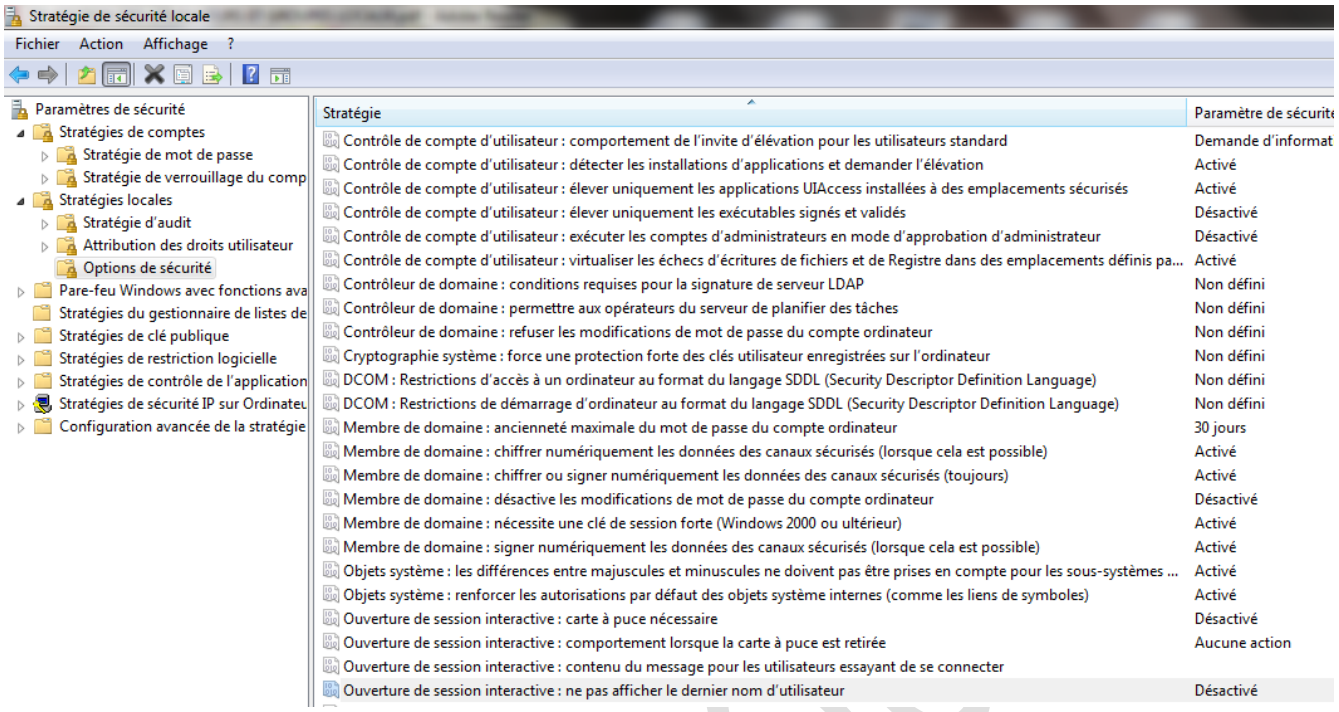
Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur

Ce paramètre de sécurité détermine si le nom du dernier utilisateur qui s'est connecté à l'ordinateur est affiché dans l'écran d'ouverture de session de Windows.

Si cette stratégie est activée, le nom du dernier utilisateur à avoir ouvert une session avec succès n'est pas affiché dans l'écran de connexion.

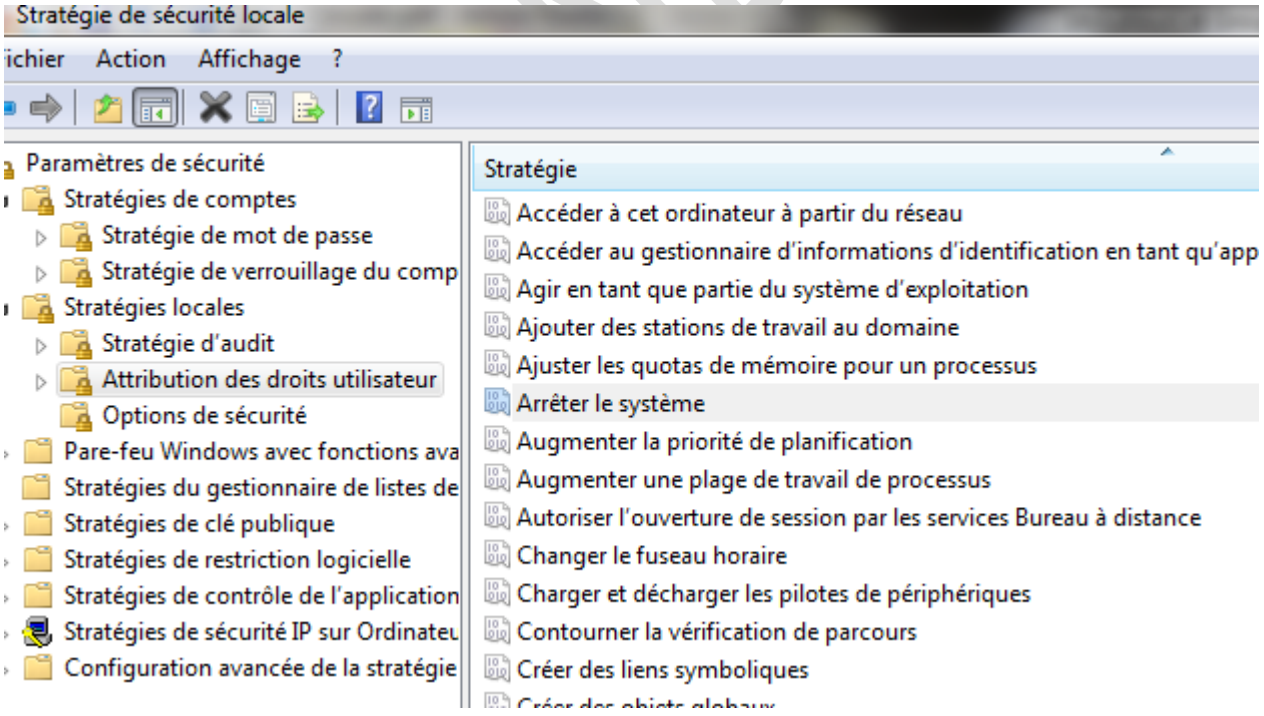
Si cette stratégie est désactivée, le nom du dernier utilisateur à avoir ouvert une session est affiché.

Valeur par défaut : Désactivé.



Seuls les membres du groupe G1 sont autorisés à éteindre la machine.

Stratégie de sécurité locale / paramètres de sécurité / Stratégie locales /Attribution des droits d'utilisateur/



Arrêter le système

Ce paramètre de sécurité détermine quels utilisateurs connectés localement à l'ordinateur peuvent arrêter le système d'exploitation à l'aide de la commande Arrêter. Une utilisation incorrecte de ce droit d'utilisateur peut entraîner un déni de service.

Valeur par défaut sur les stations de travail : Administrateurs, Opérateurs de sauvegarde, Utilisateurs.

Valeur par défaut sur les serveurs : Administrateurs, Opérateurs de sauvegarde.

Valeur par défaut sur les contrôleurs de domaine : Administrateurs, Opérateurs de sauvegarde, Opérateurs de serveur, Opérateurs d'impression.