Table des matières

1 Historique

De nos jours, la méthode traditionnelle qui consiste à utiliser l'adresse MAC comme identifiant unique de l'ordinateur ne fonctionne plus. Pourquoi ? Parce que chaque ordinateur peut facilement avoir plusieurs adresses MAC grâce à la présence de multiples cartes réseau. Par exemple, presque tous les ordinateurs portables sont équipés d'un Ethernet, d'un adaptateur réseau Wi-Fi et d'un Bluetooth. L'adresse MAC change rapidement à chaque fois que votre ordinateur se connecte d'un réseau câblé à un réseau sans fil. De plus, l'adresse MAC peut être modifiée assez facilement sur une machine physique et très simplement sur une machine virtuelle. Bref, la MAC adresse ne peut plus servir à identifier formellement une machine.

2 UUID

L'UUID pour Universally Unique IDentifier (UUID), littéralement « identifiant universel unique » est une chaine de 32 caractères. L'UUID n'a pas de garantie d'unicité totale ; il faut donc comprendre « unique » au sens de « unicité très probable ». Même si deux UUID identiques peuvent exister dans le monde, la probabilité qu'ils soient en relation est très faible.

Initialement, la génération de l'UUID reposait sur l'adresse MAC. Mais de nouveaux standards ont été mis en place afin de générer un UUID « aussi unique que possible ». En outre, des mécanismes de HASH empêchent de retrouver toute information exploitable utilisée lors de la génération de l'UUID. L'UUID peut par exemple être généré sur base d'un HASH de la MAC adresse, de l'heure et de la date ainsi que de différents numéros de série issus des composants de la machine : carte mère, disque dur, processeur, carte graphique, version du système d'exploitation, etc.

3 Lire l'UUID

La commande « WMIC » permet de trouver toutes les informations système d'une machine Windows.

```
wmic csproduct get UUID : Affiche l'UUID de l'ordinateur
```

```
wmic bios get name,serialnumber,version : Affiche des infos du BIOS
```

D'autres exemples de WMIC :

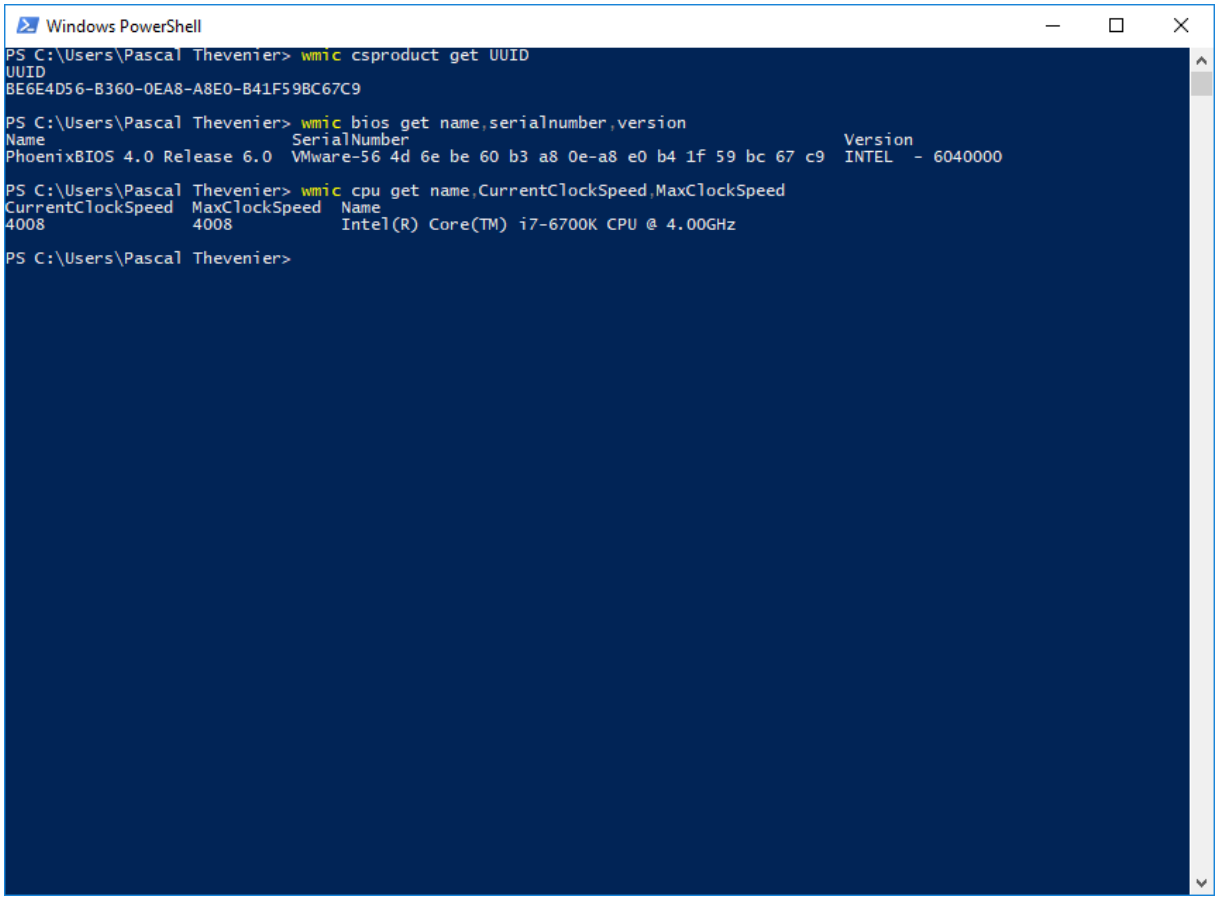
```
wmic csproduct get name,identifyingnumber,uuid
```

```
wmic cpu get name,CurrentClockSpeed,MaxClockSpeed
```

```
wmic cpu get name,CurrentClockSpeed,MaxClockSpeed /every:1
```

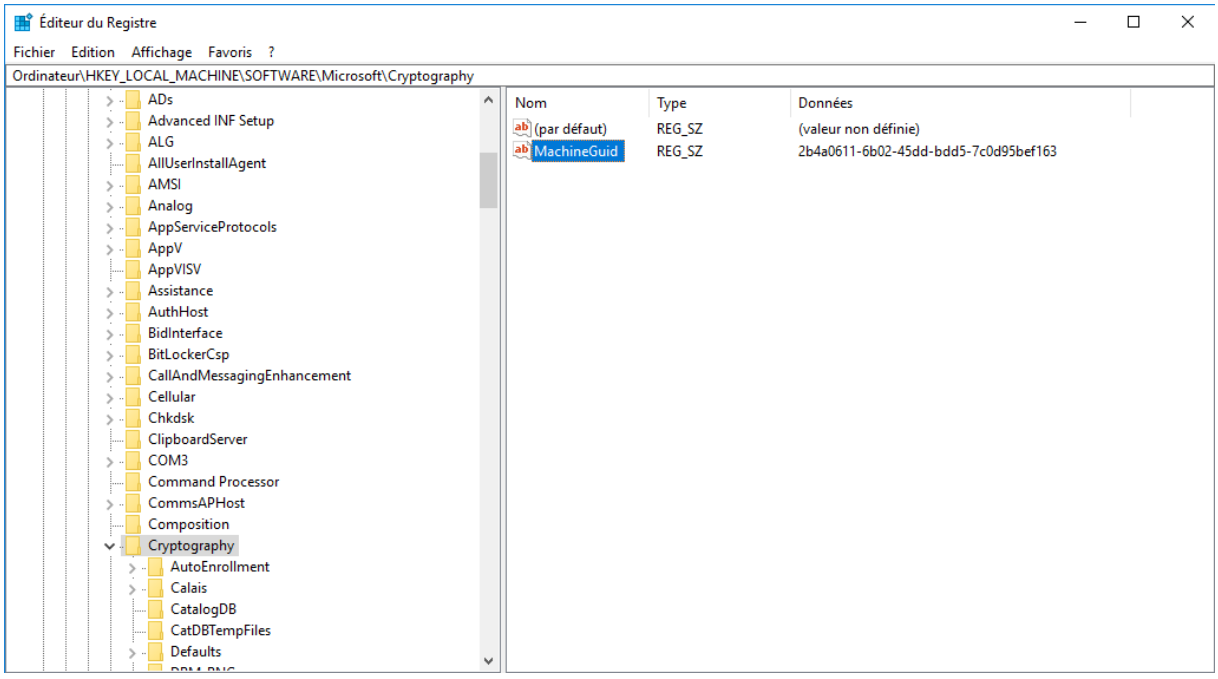
```
wmic diskdrive get SerialNumber
```

La capture suivante montre le résultat de plusieurs de ces commandes. Pour aller plus loin avec la commande WMIC : https://technet.microsoft.com/en-us/library/bb742610.aspx



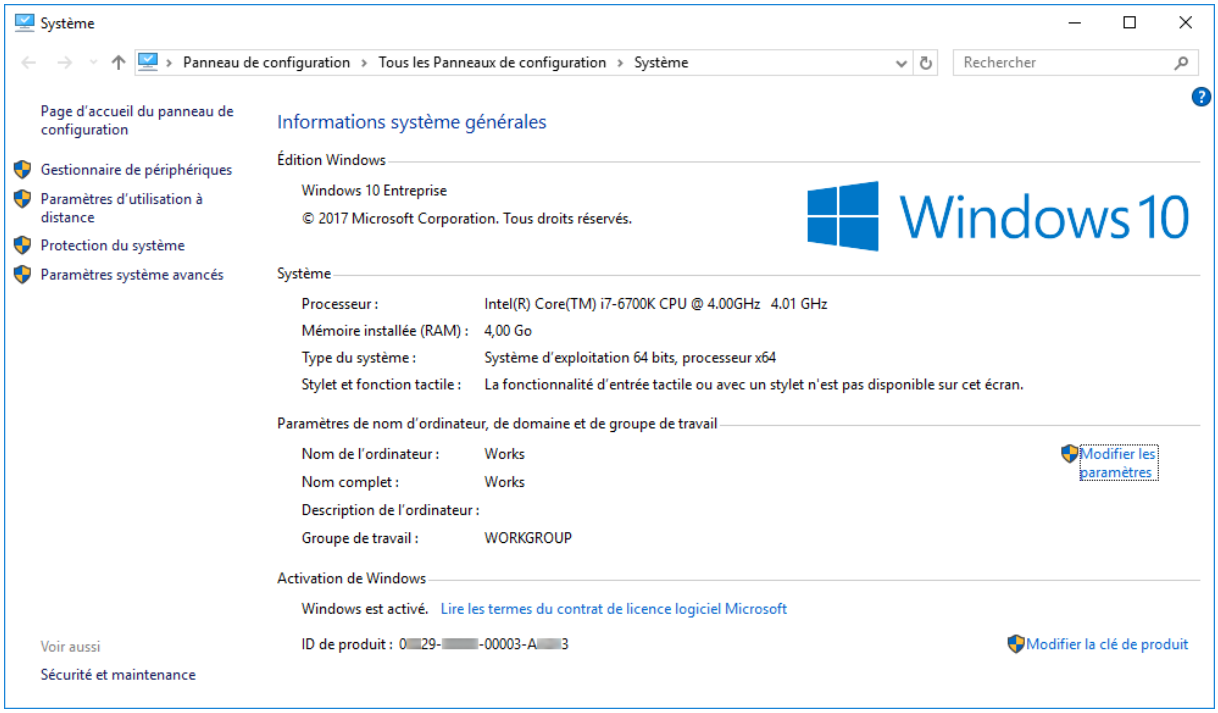
4 MachineGuid

D'autres identifiants « relativement » uniques existent dans Windows comme MachineGuid.



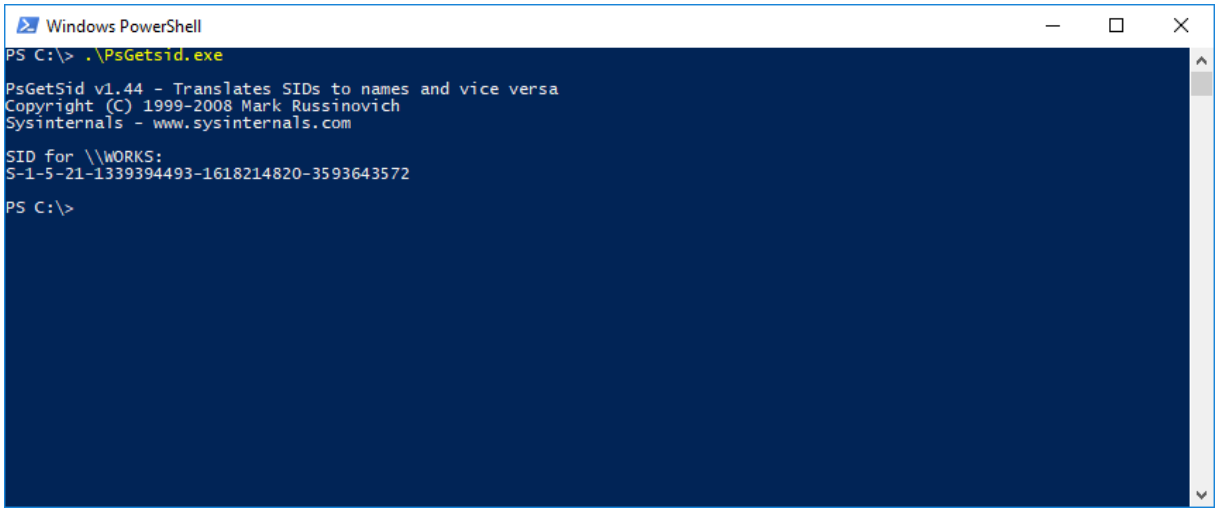
5 Windows Product ID

Ce numéro est n'est pas vraiment unique. Il est le même pour des activations en volume ou des versions « none genuine » de Windows ou encore quand aucun numéro de série n'est encodé.



6 SID

Au lieu d'utiliser des noms « unique », les systèmes d'exploitation Windows utilisent des SID (Security Identifiers). L'utilitaire PsGetsid de la suite PStools permet d'afficher le SID d'une machine.



Ce SID devrait en principe être « unique » mais il ne l'est pas non plus et des clones avec le même SID peuvent fonctionner en Workgroup et en domaine. Des failles de sécurité peuvent en découler.
https://blogs.technet.microsoft.com/markrussinovich/2009/11/03/the-machine-sid-duplication-myth-and-why-sysprep-matters/

Exemple d'un SID en détail : S-1-5-21-4064627337-2434140041-2375368561-1036.

- S : L'identificateur qui identifie la chaine de caractères comme un SID.
- 1 : Le « revision level » ou la version des spécifications du SID. Cette valeur est jusqu'à maintenant toujours de 1.
- 5 : L'« identifier authority value ». Il s'agit d'un identifiant prédéfini pour l'autorité de niveau supérieur ayant émis le SID. Il s'agit généralement de 5, qui représente SECURITY_NT_AUTHORITY.
- 21-4064627337-2434140041-2375368561 : Cette section est l'identifiant du domaine ou de l'ordinateur local (dans cet exemple, un identifiant de domaine). Il s'agit d'une chaîne de 48 bits identifiant l'autorité (l'ordinateur ou le domaine) qui a créé le SID.
- 1036 : Le Relative ID (RID) est la dernière partie du SID. Les objets créés par Windows lui-même ont un RID inférieur à 1000 (notamment le compte domain admin : 500). Les RID à partir de 1000 sont créés par la suite.

Script PowerShell pour compter les groupes et utilisateurs de l'AD :

```
$Groups = Get-ADGroup -Filter *
$Users = Get-ADuser -Filter *

Write-Host "Number of groups is " -nonewline; Write-Host $Groups.Count
Write-Host "Number of users is " -nonewline; Write-Host $Users.Count
```

7 Sysprep

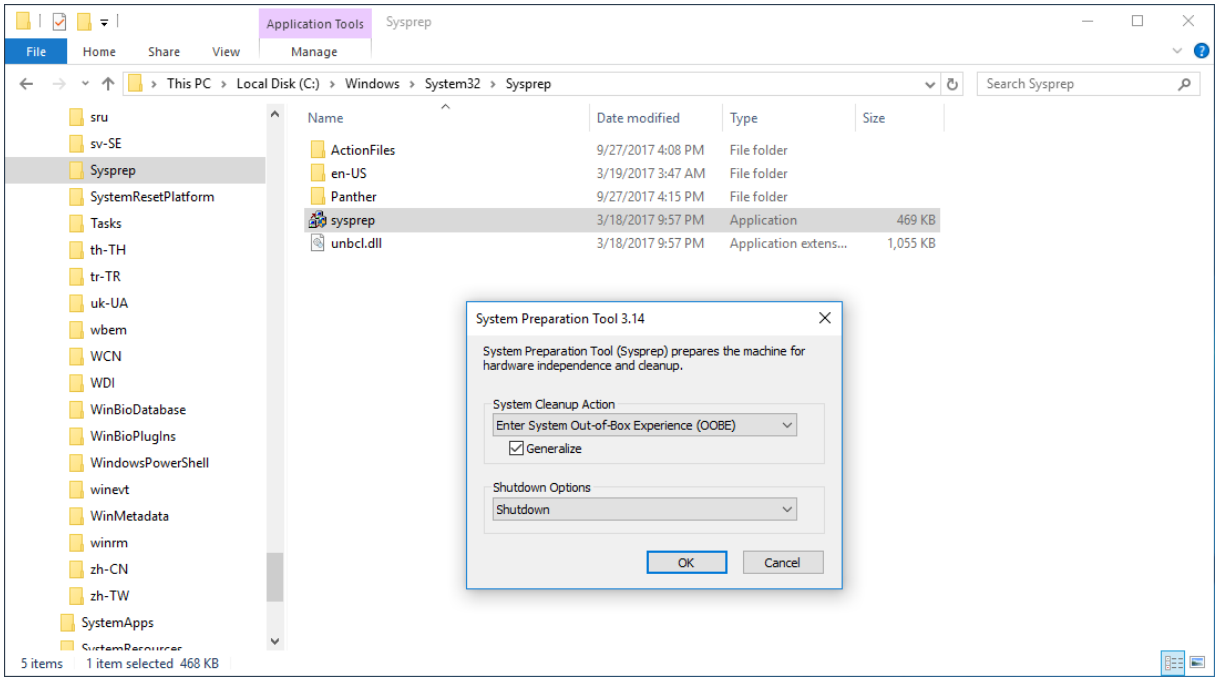
Lors du clonage d'une machine le SID et le MachineGuid ne changent pas. Un nouvel UUID est par contre généré automatiquement. Dans un domaine, tous les objets doivent être uniques. Sysprep permet de supprimer **toutes** les informations spécifiques générées lors de l'installation de Windows.

Dans le cadre de la préparation de base et la création de clones (liés), seule une partie des possibilités de Sysprep est utilisée : celle qui « neutralise » l'installation de Windows.

Extrait de https://technet.microsoft.com/fr-fr/library/cc721940(v=ws.10).aspx :

« L'outil Sysprep prépare une installation de Windows à la duplication, à l'audit et à la livraison au client. La duplication, également appelée acquisition d'images, permet de capturer une image système Windows personnalisée que vous êtes à même de réutiliser dans toute votre organisation. Grâce au mode Audit, vous pouvez ajouter des applications ou des pilotes de périphériques supplémentaires à une installation de Windows. Une fois les applications et pilotes installés, vous avez la possibilité de tester l'intégrité de l'installation de Windows. Sysprep permet également de préparer une image qui sera ensuite livrée à un client. Ainsi, lorsque le client démarre Windows, les écrans d'accueil de Windows s'affichent. »

Pour préparer une base Windows utilisable (sans futurs problèmes potentiels) pour la création de clones, il faut utiliser sysprep en mode OOBE (comme une nouvelle installation) avec l'option Generalize (pour supprime toutes les valeurs uniques), sélectionner Shutdown et valider.



Ensuite, il ne faut plus redémarrer ce Windows sinon de nouvelles valeurs uniques seront régénérées et il faudra passer par un nouveau sysprep.

Si deux ordinateurs ont le même RID dans un domaine, les problèmes seront directement présents…