Notion de SID

(Security Identifier)

- Un SID est une valeur numérique de longueur variable constituée
  - `S-V-I-XXX-XXX-XXX`
    - `S` = La chaîne de caractères est un SID
    - `V` = numéro de version du format (1)
    - `I` = entier identifiant la source du SID
    - `XXX-XXX`... chaîne de longueur variable de sous-autorités ou d'identifiants relatifs (RID)

- Exemple SID d'un Administrateur :
  - `S-1-5-21-7623811015-3361044348-030300820-500`
  - `5` = SECURITY_NT_AUTHORITY
  - `21` = sous-autorité
  - `7623811015-3361044348-030300820` = identifiant de l'ordinateur ou du domaine
  - 500 = RID (Relative Identifiers) de l'administrateur
    - > 500 et < 1000 : builtin; > 1000 : users ou groupes non natifs;
      500 = administrateur ; 501 = guest

Notion de SID

(Security Identifier)

- Pour visualiser les SIDs
  - `psgetsid.exe`
    - http://www.microsoft.com/sysinternals
  - `wmic useraccount get name,sid`

```
Name                SID
Administrateur      S-1-5-21-1343024091-842925246-839522115-500
ASPNET              S-1-5-21-1343024091-842925246-839522115-1004
BvSsh_VirtualUsers  S-1-5-21-1343024091-842925246-839522115-1005
HelpAssistant       S-1-5-21-1343024091-842925246-839522115-1000
Invité              S-1-5-21-1343024091-842925246-839522115-501
john                S-1-5-21-1343024091-842925246-839522115-1003
SUPPORT_388945a0    S-1-5-21-1343024091-842925246-839522115-1002
```

- Les “well known” : communs à tous les systèmes
  - S-1-3-0 : creator owner
  - S-1-5-10 : self
  - S-1-5-21 : domain user
  - S-1-5-18 : local system account
  - S-1-5-19 : NT authority : local service