ESTRUCTURA DEL SID

(SECURITY IDENTIFIER)

Què és el SID

És el codi que identifica cada objecte AD.

Com és identificador ⇨ és únic a nivell del bosc

Estructura:

SID = ID de domini + RID

Exemple:

S-1-5-21-3548378443-52182257-1425571249-1003

Estructura

SID d'usuari o d'equip:

$$SID_{usuari} = \underline{ID\ de\ domini\ } + RID$$

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

S: indica que la cadena és un SID

1: nivell de revisió (1 Byte)

Estructura

SID d'usuari o d'equip:

$$SID_{usuari} = \underline{\text{ID de domini}} + \text{RID}$$

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

A: valor de l'autoritat de l'identificador

0 = autoritat nul·la (Null Authority)
1 = autoritat mundial (World Authority)
2 = autoritat local (Local Authority)
3 = autoritat de creator (Creator Authority)
4 = autoritat no-única (Non-unique Authority)
5 = autoritat NT (NT Authority)
9 = administrador de recursos de l'autoritat (Resource Manager A.)

Estructura

SID d'usuari o d'equip :

$$SID_{usuari} = \underline{ID\ de\ domini\ } + RID$$

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

Algunes combinacions de A + zz indiquen que es tracta d'un grup:

S-1-0-0	nadie
S-1-1-0	**todos** (des de XP SP2 todos no inclou els anònims)
S-1-2-0	local (tots els usuaris que han iniciat sessió en local)
S-1-2-1	consola (tots els usuaris que han iniciat sessió en la consola física) (desde W7 i S2008 R2)
S-1-3-0	**creator owner**
S-1-3-1	Creator group

Estructura

SID d'usuari o d'equip :

SID_{usuari} = ID de domini + RID

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

zz: tipus d'usuari (4 bytes):

18=SYSTEM
19=Local Service -> "SERVICIO LOCAL"
20="network service" -> "Servicio de red"
21=usuari connectat (el més freqüent)

Estructura

SID d'usuari o d'equip :

SID_{usuari} = ID de domini + RID

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

xxxxxx-xxxxxx-xxxxxx: identificador del domini o de la màquina local

Aquest codi el genera el **Domain Name Master** (un dels rols dels controladors de domini) i és diferent per cada domini del nostre bosc.

Format: 4Bytes-4Bytes-4Bytes

Estructura

SID d'usuari o d'equip :

SID_{usuari} = ID de domini + RID

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

yyyy: RID (Relative ID). El codi de l'usuari dins del domini determinat.
Aquest número de sèrie el dóna el rol de **RID Master**.

Format: 4Bytes

Estructura

SID d'usuari o d'equip :

SID_{usuari} = ID de domini + RID

S-1-A-zz-xxxxxx-xxxxxx-xxxxxx-yyyy

yyyy: RID (Relative ID)

Valors predeterminats:

500= administrador local
501=invitado local
512=administrador de dominio
513=usuarios del dominio
514=invitado del dominio
....
>1000= els usuaris creats

Identificar els SID dels usuaris

Saber el SID del nostre usuari:

whoami /all>resultat.txt

O també **Whoami /user**

Per veure tots els que s'han connectat al PC:

En el registre:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\ProfileList

Per saber quin és cada usuari:

Consultar la clau **ProfileImagePath**

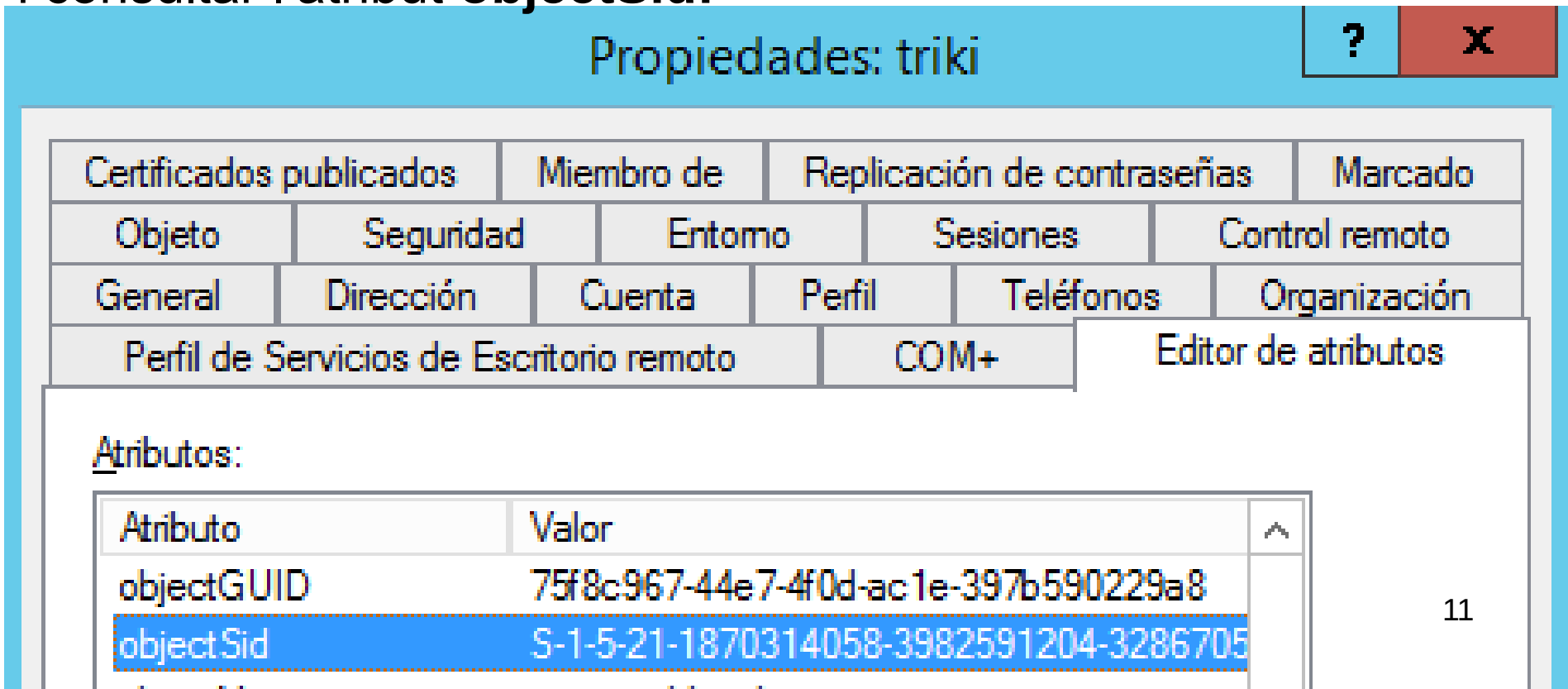
Identificar els SID

Per veure un usuari determinat del domini:

Usuarios y equipos de AD -> **Ver\Características avanzadas**

Sobre l'usuari que volem: **propiedades\Editor de atributos**

i consultar l'atribut **objectSid:**



Identificar els SID

Millor encara: **Get-ADComputer –Filter ***

```
PS C:\Users\Administrador> Get-ADComputer -Filter *


DistinguishedName : CN=SERVER-PRI,OU=Domain Controllers,DC=rpla,DC=local
DNSHostName       : SERVER-PRI.rpla.local
Enabled           : True
Name              : SERVER-PRI
ObjectClass       : computer
ObjectGUID        : 688eb9a9-7834-4f0c-be43-de8f5b3ecefe
SamAccountName    : SERVER-PRI$
SID               : S-1-5-21-1870314058-3982591204-3286705234-1001
UserPrincipalName :

DistinguishedName : CN=W8-1,CN=Computers,DC=rpla,DC=local
DNSHostName       : w8-1.rpla.local
Enabled           : True
Name              : W8-1
ObjectClass       : computer
ObjectGUID        : 63ce4e46-66ab-429f-b967-679a87a0072e
SamAccountName    : W8-1$
SID               : S-1-5-21-1870314058-3982591204-3286705234-1104
UserPrincipalName :
```

Identificar els SID

Millor encara: **Get-ADUser –Filter ***

```
PS C:\Users\Administrador> Get-ADUser -Filter *


DistinguishedName : CN=Administrador,CN=Users,DC=rpla,DC=local
Enabled           : True
GivenName         :
Name              : Administrador
ObjectClass       : user
ObjectGUID        : acc5cba1-a76d-45ae-9e01-576c37a267f9
SamAccountName    : Administrador
SID               : S-1-5-21-1870314058-3982591204-3286705234-500
Surname           :
UserPrincipalName :

DistinguishedName : CN=espinete,CN=Users,DC=rpla,DC=local
Enabled           : True
GivenName         : espinete
Name              : espinete
ObjectClass       : user
ObjectGUID        : 70ac4dfb-1593-4146-b49d-aeaa0359830d
SamAccountName    : espinete
SID               : S-1-5-21-1870314058-3982591204-3286705234-1105
Surname           :
UserPrincipalName : espinete@rpla.local
```