Chapitre 13
La gestion des utilisateurs

1. Introduction

Les ressources contenues dans l'Active Directory sont accessibles à travers un certain nombre de règles propres à chacune. Un utilisateur Active Directory peut avoir accès ou non à ces ressources en fonction de ces règles mais aussi de logiques inhérentes au fonctionnement de l'infrastructure concernée. L'élément le plus important ici est qu'avant d'avoir accès aux différentes ressources d'une infrastructure Active Directory, un utilisateur doit pouvoir être clairement authentifié en son sein.

Nous comprenons donc que la notion de compte d'utilisateur est très importante dans le fonctionnement même du service d'annuaire Active Directory. Ce chapitre nous aidera à mieux comprendre cette notion de compte d'utilisateur. Nous y apprendrons ce que recouvre ce concept ainsi que les différents types d'opérations qui lui sont liés avec Windows PowerShell.

2. Qu'est-ce qu'un compte d'utilisateur Active Directory ?

Un compte d'utilisateur Active Directory représente la plupart du temps une entité physique (personne). Deux principes fondamentaux se dégagent de cette notion :

1. Un compte d'utilisateur identifie formellement l'entité physique dont il est question : ce principe permet un processus d'authentification dans une infrastructure Active Directory. Idéalement, un compte d'utilisateur unique ne devrait pas être utilisé par plusieurs personnes.

2. Un compte d'utilisateur autorise ou non l'accès à des ressources : grâce à des systèmes de permissions reliés aux ressources d'une infrastructure Active Directory, un compte d'utilisateur, en fonction de ses permissions, pourra ou non accéder à ces ressources.

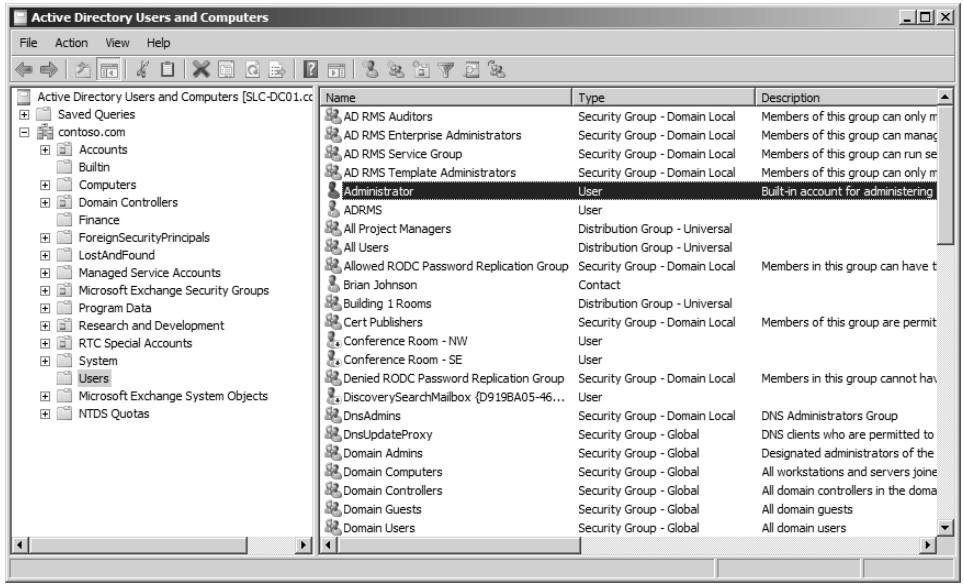
Il existe trois comptes par défaut, lors de la création d'un domaine Active Directory :

1. Le compte « *Administrateur* » : ce compte dispose d'un contrôle total du point de vue de la gestion d'un domaine Active Directory. Avec ce compte, des permissions peuvent être appliquées à d'autres comptes d'utilisateurs. Il représente le compte d'administration par excellence et doit être utilisé avec prudence.
2. Le compte « *Invité* » : ce compte est utilisé lorsqu'une personne n'a pas de compte de domaine, ou que le compte de domaine est désactivé mais pas supprimé.
3. Le compte « *HelpAssistant* » : ce compte est utilisé pour établir des sessions d'assistance à distance. Sa création est automatique lorsqu'une session d'assistance à distance est demandée. Il en est de même pour sa destruction, notamment lorsqu'une ou des demandes d'assistance à distance n'ont plus lieu d'être.

En outre, des options liées à la notion de compte d'utilisateur Active Directory précisent davantage comment il doit être utilisé. Parmi celles-ci :

– « *L'utilisateur doit changer de mot de passe à la prochaine ouverture de session* » : indique qu'un utilisateur doit changer de mot de passe lors de la prochaine ouverture de session. C'est une manière de forcer un utilisateur à modifier une information de compte d'utilisateur.
– « *L'utilisateur ne peut pas changer de mot de passe* » : empêche l'utilisateur de changer de mot de passe.
– « *Le mot de passe n'expire jamais* » : indique que le mot de passe de compte d'utilisateur ne peut pas expirer.
– « *Le compte est désactivé* » : ce type de compte sert de modèle pour d'autres créations de comptes. Ainsi cette option empêche un utilisateur de se connecter avec le compte d'utilisateur concerné.

Un compte d'utilisateur Active Directory est créé à l'aide de tous ces éléments ; les administrateurs d'une infrastructure Active Directory considèrent l'ensemble de ces points en fonction du contexte dans lequel ils s'inscrivent. En effet, dans le cas contraire, cela conduirait invariablement à des complications dont l'analyse sera difficile dans le cas d'une infrastructure complexe.



Le conteneur `Users` (ou `Utilisateurs`) dans la console MMC « Active Directory Users and Computers » est disposé par défaut lors de la création d'un domaine Active Directory.

3. Obtenir des informations à propos des comptes d'utilisateurs

Nous savons à présent ce que recouvre la notion de compte d'utilisateur Active Directory. En ce qui concerne la structure d'un objet représentant un compte d'utilisateur, le premier constat est qu'elle est riche en informations essentielles pour les informaticiens ayant pour charge de gérer tout ou partie d'une infrastructure Active Directory. Windows PowerShell rend possible la découverte de ces informations de manière très aisée : la cmdlet `Get-ADUser` est redoutablement efficace pour lister un objet représentant un compte d'utilisateur (cela est évidemment aussi le cas pour lister plusieurs objets), et donc pour obtenir toutes les informations qui lui sont liées.

3.1 La cmdlet Get-ADUser

`Get-ADUser` cherche au sein d'un annuaire Active Directory un objet dont la particularité est d'être un compte d'utilisateur. Un compte d'utilisateur peut notamment être identifié par son nom, son nom unique (`DistinguishedName`) ou son identificateur de sécurité (`SID`). Pour atteindre le ou les objets concernés, la cmdlet `Get-ADUser` fonctionne avec des paramètres puissants que l'on peut retrouver dans d'autres contextes :

Le paramètre **-Filter**

Spécifie une requête basée sur des expressions Windows PowerShell et listant le ou les objets Active Directory recherchés.

Le paramètre **-Identity**

Spécifie un objet Active Directory représentant un compte d'utilisateur.

Le paramètre **-LDAPFilter**

Spécifie une requête LDAP servant à filtrer le ou les objets collectés.

Le paramètre **-Partition**

Spécifie une partition Active Directory où la requête sera effectuée.

Le paramètre **-SearchBase**

Indique un chemin d'accès Active Directory où la requête sera effectuée.

Le paramètre **-SearchScope**

Spécifie la portée qu'une requête pourra avoir. Les valeurs possibles sont : `Base` (ou `0`), `OneLevel` (ou `1`) et `Subtree` (ou `2`). Si la valeur est `Base`, alors la requête est réalisée uniquement au niveau du chemin spécifié. Si la valeur est `OneLevel`, alors la requête est réalisée exclusivement au niveau des « enfants directs » du chemin spécifié. Enfin, si la valeur est `Subtree`, alors la requête sera réalisée au niveau du chemin spécifié et de tous ses enfants directs et indirects. La valeur par défaut est `Subtree`.

Le paramètre **-Server**

Indique l'instance des services de domaine Active Directory à laquelle se connecter.

Le paramètre **-Credential**

Indique un compte d'utilisateur Active Directory ayant les privilèges nécessaires pour réaliser la requête.

Le paramètre **-Properties**

Indique une ou des propriétés à lister en plus des propriétés par défaut.

Il existe d'autres paramètres, mais ceux-ci sont les plus communément utilisés.

3.2 Get-ADUser en action

La première opération que nous allons accomplir pour illustrer la commande `Get-ADUser` consiste à lister les comptes d'utilisateurs dont les noms commencent par la lettre `C` (`-Filter`) et qui se situent au sein de l'unité d'organisation `Accounts` (`-SearchBase`) :

```
PS> Get-ADUser -Filter 'Name -like "C*"'
-SearchBase "OU=Accounts,DC=contoso,DC=com"


DistinguishedName : CN=Carlos Grilo,OU=Accounts,DC=contoso,DC=com
Enabled           : True
GivenName         : Carlos
Name              : Carlos Grilo
ObjectClass       : user
ObjectGUID        : 8689604e-7177-45b6-b0ef-44659300f793
SamAccountName    : CarlosG
SID               : S-1-5-21-2153971331-1430186003-2770964410-1142
Surname           : Grilo
UserPrincipalName : CarlosG@contoso.com

DistinguishedName : CN=Claire O'Donnell,OU=Accounts,DC=contoso,DC=com
Enabled           : True
GivenName         : Claire
Name              : Claire O'Donnell
ObjectClass       : user
ObjectGUID        : 1a338d23-2084-407a-94b1-44498be163e0
SamAccountName    : ClaireO
SID               : S-1-5-21-2153971331-1430186003-2770964410-1143
Surname           : O'Donnell
UserPrincipalName : ClaireO@contoso.com
```

Deux comptes d'utilisateurs correspondant à `Claire O'Donnell` et `Carlos Grilo` sont affichés ici. Cependant, les propriétés affichées ne sont qu'une partie de l'ensemble des propriétés inhérentes à ce type d'objet ; le paramètre `-Properties` nous aidera à en savoir plus à propos de ces structures :

```
PS> Get-ADUser -Filter 'Name -like "C*"'
-SearchBase "OU=Accounts,DC=contoso,DC=com" -Properties '*'


AccountExpirationDate              :
accountExpires                     : 9223372036854775807
AccountLockoutTime                 :
AccountNotDelegated                : False
AllowReversiblePasswordEncryption  : False
BadLogonCount                      : 0
```

```
badPasswordTime                 : 0
badPwdCount                     : 0
CannotChangePassword            : False
CanonicalName                   : contoso.com/Accounts/Carlos Grilo
Certificates                    : {}
City                            :
CN                              : Carlos Grilo
codePage                        : 0
Company                         :
Country                         :
countryCode                     : 0
Created                         : 26/07/2010 19:40:57
createTimeStamp                 : 26/07/2010 19:40:57
Deleted                         :
Department                      :
Description                     :
DisplayName                     : Carlos Grilo
DistinguishedName               : CN=Carlos Grilo,OU=Accounts,DC=con...
Division                        :
DoesNotRequirePreAuth           : False
dSCorePropagationData           : {05/08/2010 17:49:19, 05/08/2010
EmailAddress                    : CarlosG@contoso.com
EmployeeID                      :
EmployeeNumber                  :
Enabled                         : True
Fax                             :
GivenName                       : Carlos
HomeDirectory                   :
HomedirRequired                 : False
HomeDrive                       :
homeMDB                         : CN=MDB01,CN=Databases,CN=Exchange...
homeMTA                         : CN=Microsoft MTA,CN=SLC-DC01,CN=...
HomePage                        :
HomePhone                       :
Initials                        :
instanceType                    : 4
isDeleted                       :
LastBadPasswordAttempt          :
LastKnownParent                 :
lastLogoff                      : 0
lastLogon                       : 0
LastLogonDate                   :
legacyExchangeDN                : /o=First Organization/ou=Exchange...
LockedOut                       : False
logonCount                      : 0
LogonWorkstations               :
mail                            : CarlosG@contoso.com
mailNickname                    : CarlosGrilo
Manager                         :
```