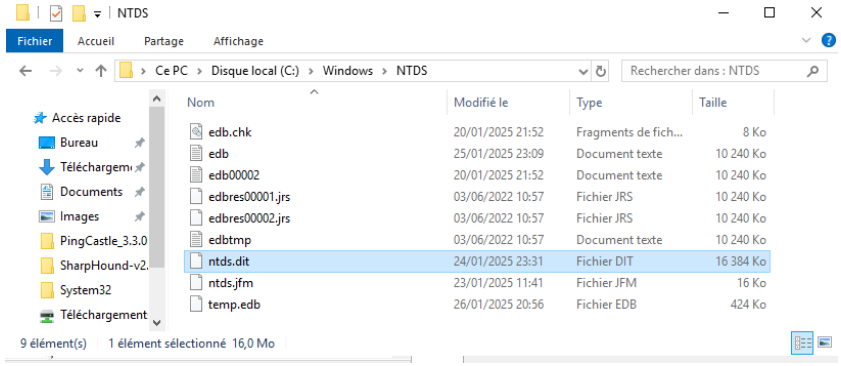
Introduction Active Directory

Qu'est-ce qu'Active Directory ?

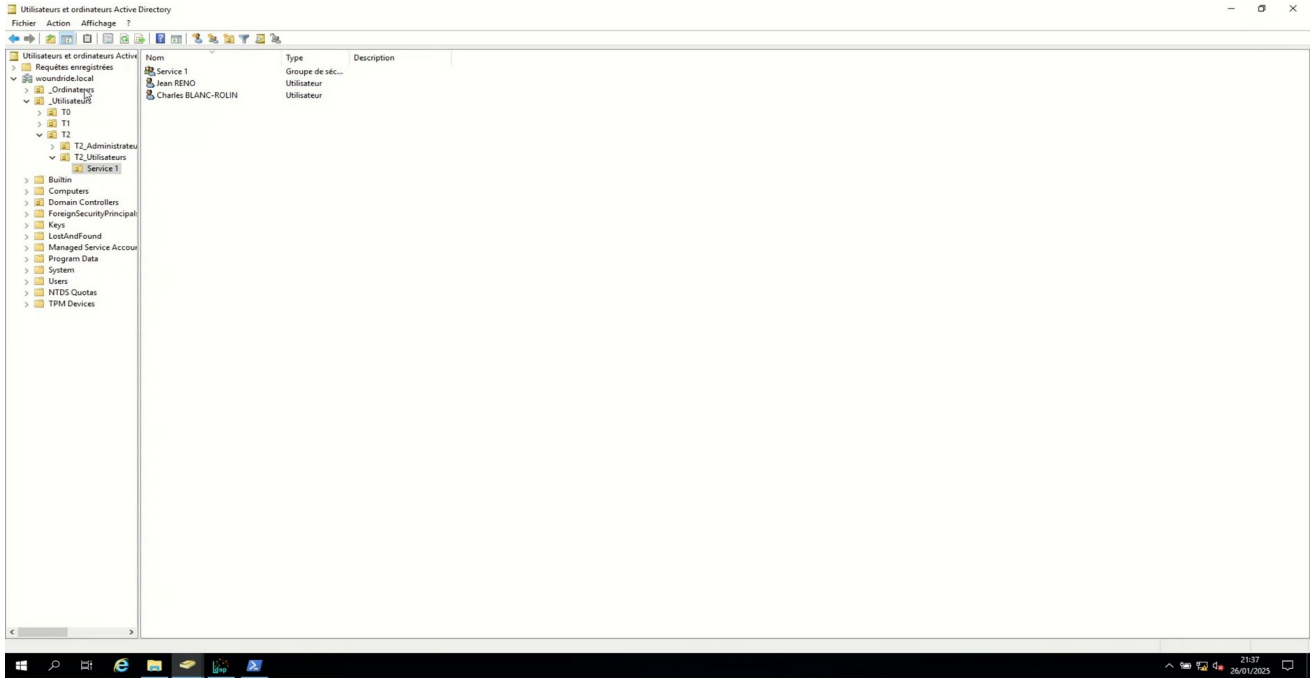
Définition :

- Service d'annuaire développé par Microsoft, souvent appelé AD
- Implémentation du protocole LDAP (Lightweight Directory Access Protocol) par Microsoft
- Disponible depuis 1999 avec l'arrivée de Windows 2000
- Initialement baptisé NTDS (New Technology Directory Service) par Microsoft, sa base de données porte toujours ce nom (ntds.dit)



LDAP n'est pas réservé à Windows

Interrogation d'un AD via LDAP depuis Linux :



Qu'est-ce qu'Active Directory ?

Objectifs :

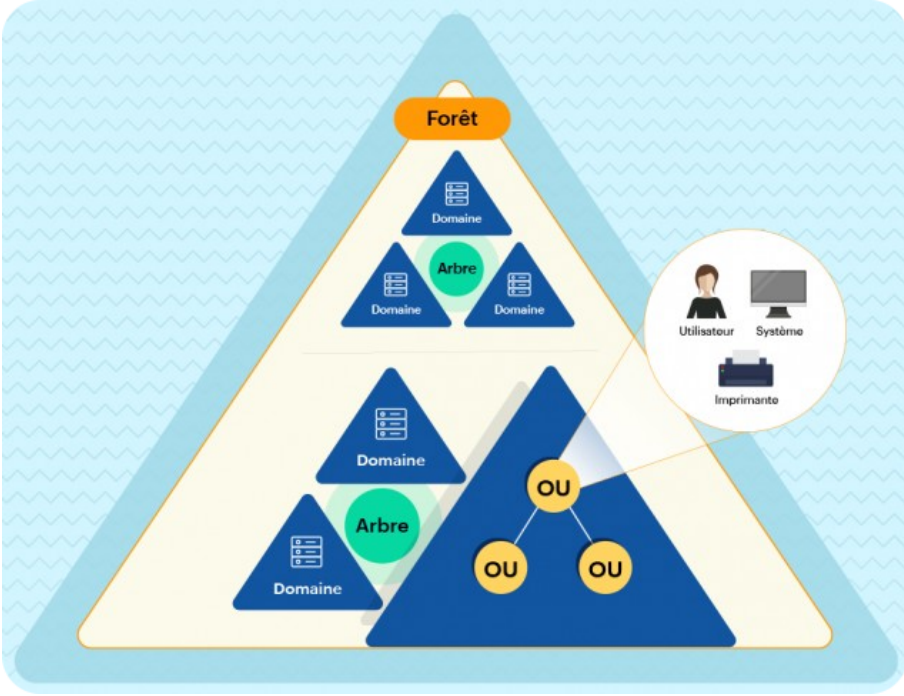
- Fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs (Windows, Linux ou macOS)
- Permettre une administration centralisée des utilisateurs et des machines répertoriés dans l'annuaire
- Configurer des groupes d'utilisateurs ou de machines Windows en masse grâce à l'application de « stratégies de groupe » (objets dans l'AD). On parle généralement de GPO (Group Policy Objects)
- Attribuer des droits à une ressource sur une autre ressource (droit d'un utilisateur sur un ordinateur, un partage de fichiers, une imprimante...)

Forêts, arbres et domaines

L'arborescence de l'Active Directory :

- Forêt : plus haut niveau hiérarchique d'administration de l'AD, il est composé d'arbres
- Arbre : contient l'ensemble des sous-domaines d'un domaine principal. Exemple sousdomaine1.domaine.local, sousdomaine2.domaine.local sont les sous-domaines de l'arbre domaine.local
- Domaine : contient un ensemble d'objets administrés de manière centralisée

Un héritage des annuaires X.500



Les contrôleurs de domaine

Notions de contrôleurs :

- Le service d'annuaire Active Directory peut être mis en œuvre sur serveur Windows, il devient alors « contrôleur de domaine », en anglais « domain controler », communément appelé « DC »

- Le contrôleur de domaine principal est le premier contrôleur initialement installé, mais ce rôle peut être transféré sur un autre serveur, notamment dans le cadre d'une migration / montée de version

- Le(s) contrôleur(s) secondaire(s) permettent d'assurer une redondance en cas de panne, ou proposer le service au plus proche d'un réseau d'ordinateurs sur un site distant par exemple

- Les contrôleurs synchronises entre eux le contenu de la base de données de l'annuaire (fichier C:\Windows\System32\NTDS.dit)

- Pour des raisons de sécurité, des contrôleurs en « lecture seule » (appelés RODC), permettant uniquement à des utilisateurs de se connecter facilement sur un site distant peuvent être déployés

- Les 2 principaux rôles d'un contrôleur de domaine :
  - Traiter les demandes d'authentifications
  - Veiller à l'application des stratégies de groupe

Les services présentés par un contrôleur de domaine

```
charles@machine: ~
charles@machine:~$ sudo ntpdate 192.168.46.2
2025-01-30 22:07:48.955532 (+0100) -0.004602 +/- 0.000314 192.168.46.2 s1 no-leap
charles@machine:~$
```

Le service NTP sur le port 123/UDP

Port(s) client(s)	Port serveur	Service
49152-65535/UDP	123/UDP	W32Time
49152-65535/TCP	135/TCP	Mappeur de point de terminaison RPC
49152-65535/TCP	464/TCP/UDP	Modification de mot de passe Kerberos
49152-65535/TCP	49152-65535/TCP	RPC pour LSA, SAM, NetLogon (*)
49152-65535/TCP/UDP	389/TCP/UDP	LDAP
49152-65535/TCP	636/TCP	LDAP SSL
49152-65535/TCP	3268/TCP	LDAP GC
49152-65535/TCP	3269/TCP	LDAP GC SSL
53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
49152-65535/TCP	49152-65535/TCP	FRS RPC (*)
49152-65535/TCP/UDP	88/TCP/UDP	Kerberos
49152-65535/TCP/UDP	445/TCP	SMB (**)
49152-65535/TCP	49152-65535/TCP	DFSR RPC (*)

```
charles@machine:~$ sudo nmap -T4 -p- -n 192.168.46.2
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-29 23:23 CET
Nmap scan report for 192.168.46.2
Host is up (0.00016s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5357/tcp  open  wsdapi
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49668/tcp open  unknown
49671/tcp open  unknown
49672/tcp open  unknown
49675/tcp open  unknown
49680/tcp open  unknown
49704/tcp open  unknown
49966/tcp open  unknown
50964/tcp open  unknown
```

Le service LDAP (Lightweight Directory Access Protocol)

En synthèse :

- Service principal permettant la mise en place d'un annuaire Active Directory

- Les 4 ports utilisés par le service :
  - 389/tcp : LDAP
  - 636/tcp : LDAPS
  - 3268/tcp : LDAP Global Catalog
  - 3269/tcp : LDAPS Global Catalog

- Le service LDAP est le second service contacté par une machine Windows rattaché à un domaine Active Directory lors du démarrage. Il lui permet :
  - De récupérer les informations du domaine
  - De récupérer la liste des GPOs à appliquer depuis l'UO racine (DC=woundride,DC=local) jusqu'à l'UO de destination

Le service LDAP : informations « publiques »

De nombreuses informations (présentes à la racine dite « RootDSE » sont accessibles sans authentification :

```
charles@machine:~$ sudo nmap -T4 -p 389 -n 192.168.46.2 --script ldap-rootdse
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-29 23:08 CET
Nmap scan report for 192.168.46.2
Host is up (0.00024s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=woundride,DC=local
|       ldapServiceName: woundride.local:w2019-dc01$@WOUNDRIDE.LOCAL
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=woundride,DC=local
|       serverName: CN=W2019-DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=woundride,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=woundride,DC=local
|       namingContexts: DC=woundride,DC=local
|       namingContexts: CN=Configuration,DC=woundride,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=woundride,DC=local
|       namingContexts: DC=DomainDnsZones,DC=woundride,DC=local
|       namingContexts: DC=ForestDnsZones,DC=woundride,DC=local
|       isSynchronized: TRUE
|       highestCommittedUSN: 69753
|       dsServiceName: CN=NTDS Settings,CN=W2019-DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=woundride,DC=local
|       dnsHostName: W2019-DC01.woundride.local
|       defaultNamingContext: DC=woundride,DC=local
|       currentTime: 20250129220830.0Z
|_      configurationNamingContext: CN=Configuration,DC=woundride,DC=local
MAC Address: 08:00:27:3F:FA:8E (Oracle VirtualBox virtual NIC)
Service Info: Host: W2019-DC01; OS: Windows

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
charles@machine:~$
```

```
File  Edit  View  Search  Terminal  Help
┌──[root@parrot]─[/home/user]
└─#ldapsearch -LLL -x -H ldap://192.168.46.2:389 -b '' -s base '*'
dn:
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
rootDomainNamingContext: DC=woundride,DC=local
ldapServiceName: woundride.local:w2019-dc01$@WOUNDRIDE.LOCAL
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=woundride,DC=loc
 al
serverName: CN=W2019-DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Co
 nfiguration,DC=woundride,DC=local
schemaNamingContext: CN=Schema,CN=Configuration,DC=woundride,DC=local
namingContexts: DC=woundride,DC=local
namingContexts: CN=Configuration,DC=woundride,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=woundride,DC=local
namingContexts: DC=DomainDnsZones,DC=woundride,DC=local
namingContexts: DC=ForestDnsZones,DC=woundride,DC=local
isSynchronized: TRUE
highestCommittedUSN: 69750
dsServiceName: CN=NTDS Settings,CN=W2019-DC01,CN=Servers,CN=Default-First-Site
 -Name,CN=Sites,CN=Configuration,DC=woundride,DC=local
dnsHostName: W2019-DC01.woundride.local
defaultNamingContext: DC=woundride,DC=local
currentTime: 20250129214759.0Z
configurationNamingContext: CN=Configuration,DC=woundride,DC=local
```

Une partie des informations est tronquée ici

Le service LDAP : exemples d'informations accessibles à tout utilisateur

Les ordinateurs du domaine, leurs systèmes et versions précises

```
charles@machine:~$ ldapsearch -LLL -H ldap://192.168.46.2:389 -b "DC=woundride,DC=
local" -D "CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilis
ateurs,DC=woundride,DC=local" '(&(objectClass=computer))' operatingSystem operatin
gSystemVersion -W
Enter LDAP Password:
dn: CN=W2019-DC01,OU=T0_DC,OU=T0,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows Server 2019 Standard
operatingSystemVersion: 10.0 (17763)

dn: CN=PC01,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Professionnel
operatingSystemVersion: 10.0 (19044)

dn: CN=PC03,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 7 Professionnel
operatingSystemVersion: 6.1 (7601)

dn: CN=PC02,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Professionnel
operatingSystemVersion: 10.0 (17134)

dn: CN=PC04,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Enterprise
operatingSystemVersion: 10.0 (18362)

dn: CN=PC05,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Entreprise LTSC
operatingSystemVersion: 10.0 (17763)

dn: CN=PC06,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Entreprise LTSC
operatingSystemVersion: 10.0 (17763)

dn: CN=PC07,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 7 Professionnel
operatingSystemVersion: 6.1 (7601)

dn: CN=PC08,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Professionnel
operatingSystemVersion: 10.0 (17134)

dn: CN=PC09,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
operatingSystem: Windows 10 Enterprise
operatingSystemVersion: 10.0 (18362)
```

Les utilisateurs membres du groupe « Admins du domaine »

```
charles@machine:~$ ldapsearch -LLL -H ldap://192.168.46.2:389 -b "DC=woundride,DC=lo
cal" -D "CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateu
rs,DC=woundride,DC=local" -x "cn=Admins du domaine" member -W
Enter LDAP Password:
dn: CN=Admins du domaine,OU=T0_Administrateurs,OU=T0,OU=_Utilisateurs,DC=wound
 ride,DC=local
member: CN=[Admin T0] Charles BLANC-ROLIN,OU=T0_Administrateurs,OU=T0,OU=_Util
 isateurs,DC=woundride,DC=local
member: CN=Administrateur,OU=T0_Administrateurs,OU=T0,OU=_Utilisateurs,DC=woun
 dride,DC=local

# refldap://ForestDnsZones.woundride.local/DC=ForestDnsZones,DC=woundride,DC=lo
 cal

# refldap://DomainDnsZones.woundride.local/DC=DomainDnsZones,DC=woundride,DC=lo
 cal

# refldap://woundride.local/CN=Configuration,DC=woundride,DC=local
```

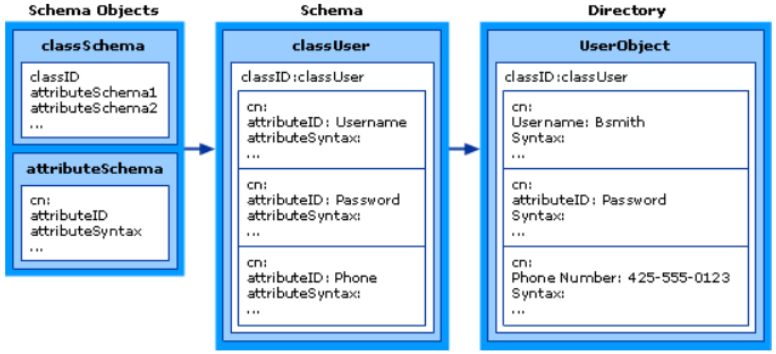
L'identifiant de session d'un compte utilisateur (sAMAccountName)

```
charles@machine:~$ ldapsearch -LLL -H ldap://192.168.46.2:389 -b "DC=woundride,DC=lo
cal" -D "CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateu
rs,DC=woundride,DC=local" -x "cn=[Admin T0] Charles BLANC-ROLIN" samaccountname -W
Enter LDAP Password:
dn: CN=[Admin T0] Charles BLANC-ROLIN,OU=T0_Administrateurs,OU=T0,OU=_Utilisat
 eurs,DC=woundride,DC=local
sAMAccountName: admin_t0_cbr
```

Schéma, classes et objets

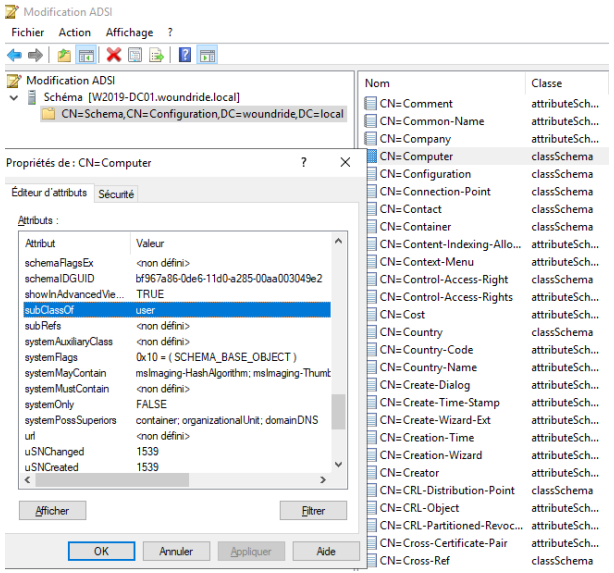
Le schéma :

- Contient l'ensemble de classes



Les classes :

- Définissent les différents types d'objets (Utilisateur, ordinateur etc..)
- Chaque classe possède des attributs
- Un système d'héritage des classes existe, exemple la classe « Computer » hérite de la classe « User »



Les objets :

- Chaque objet est unique
- Il est identifié par un DN (Distinguished Name)
- Il dispose aussi d'un GUID (Globally Unique Identifier)
- Chaque objet possède des attributs (dont DN et GUID)

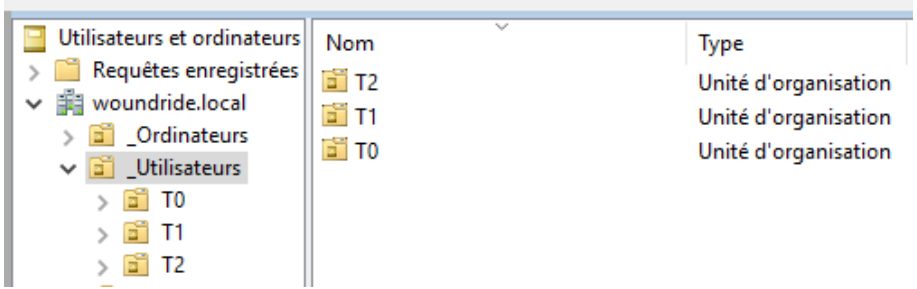
DN = chemin complet depuis la racine du domaine

CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woundride,DC=local

Les objets

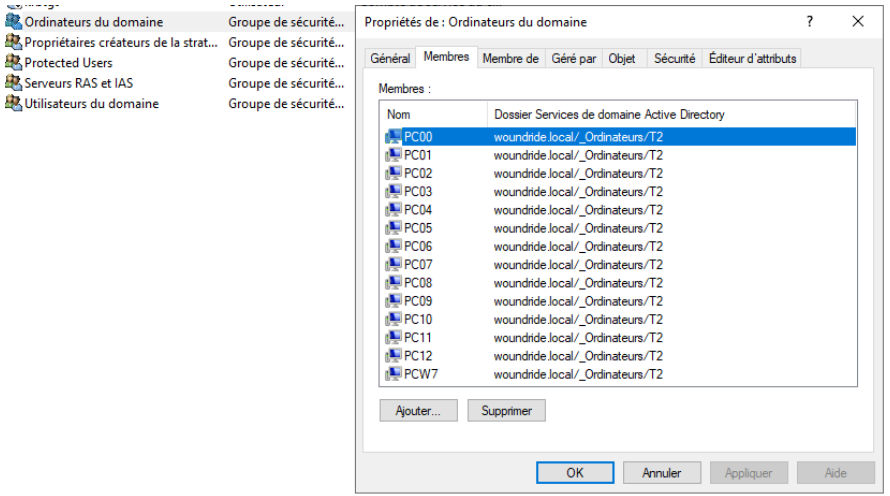
Unité d'Organisation (UO / Organizational Unit / OU) :

- Objet conteneur de la norme LDAP
- Utilisé pour hiérarchiser l'annuaire (à voir comme un dossier / répertoire)
- Permet une délégation et un héritage (pour les « sous UO ») des autorisations
- Permet d'appliquer des stratégies de groupes à l'ensemble de ses objets



Les objets

Les groupes :



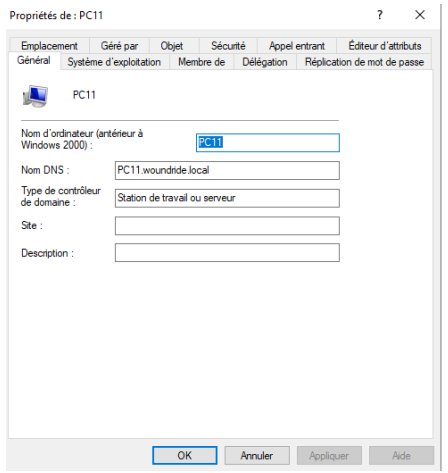
- Peuvent contenir plusieurs objets :
  - D'autres groupes
  - Des comptes d'ordinateurs
  - Des comptes utilisateurs
  - Des imprimantes
  - ...

- Permet de simplifier l'administration en appliquant des droits sur des ressources ou des paramètres de configuration 1 seule fois pour tous les objets du groupe

Les objets

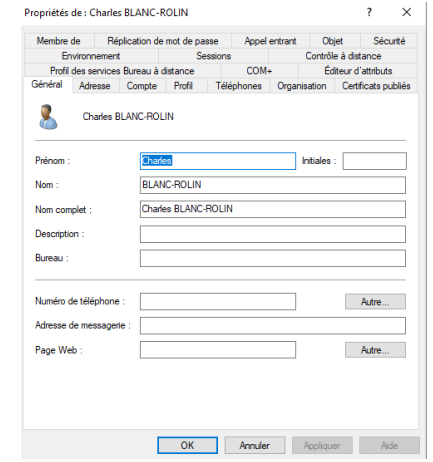
Compte d'ordinateur :

- Permet la connexion d'une machine à l'annuaire AD
- Placé dans une UO, il hérite des autorisations et des stratégies



Compte utilisateur :

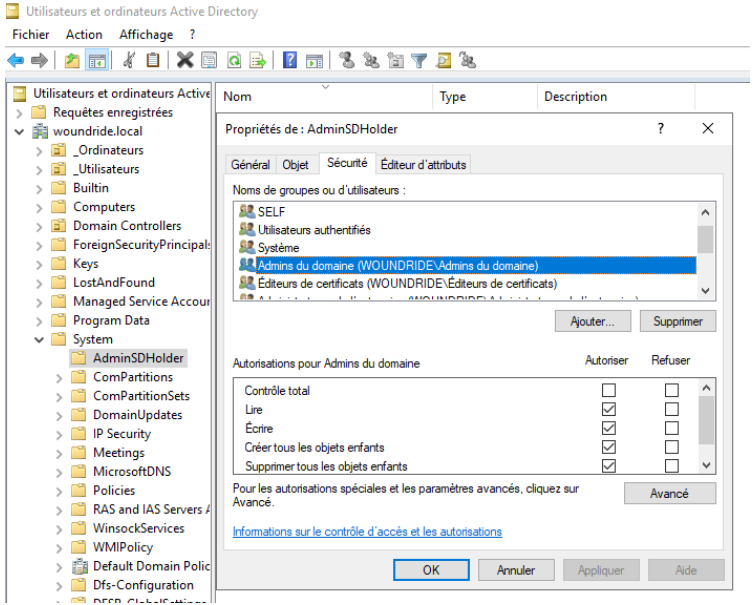
- Permet la connexion d'un utilisateur aux ressources de l'AD (suivant ses autorisations)
- Placé dans une UO, il hérite des autorisations et des stratégies



Les objets

Les conteneurs « système » sans objets :

- Utilisés comme modèles pour l'application de privilèges, comme AdminSDHolder par exemple



Les objets

Les groupes et comptes protégés :

- Disposent de privilèges élevés, permettant « d'administrer » l'AD
- Chaque compte membre d'un groupe protégé hérite de ses privilèges sur l'AD
- Le groupe protégé le plus connu est généralement le groupe « Admins du domaine »

Windows Server 2003 R2 RTM	Windows Server 2003 SP1	Windows Server 2012, Windows Server 2008 R2 Windows Server 2008	Windows Server 2016
Opérateurs de compte	Opérateurs de compte	Opérateurs de compte	Opérateurs de compte
Administrateur	Administrateur	Administrateur	Administrateur
Administrateurs	Administrateurs	Administrateurs	Administrateurs
Opérateurs de sauvegarde	Opérateurs de sauvegarde	Opérateurs de sauvegarde	Opérateurs de sauvegarde
Éditeurs de certificats			
Administrateurs du domaine	Administrateurs du domaine	Administrateurs du domaine	Administrateurs du domaine
Contrôleurs de domaine	Contrôleurs de domaine	Contrôleurs de domaine	Contrôleurs de domaine
Administrateurs de l'entreprise	Administrateurs de l'entreprise	Administrateurs de l'entreprise	Administrateurs de l'entreprise
Krbtgt	Krbtgt	Krbtgt	Krbtgt
Opérateurs d'impression	Opérateurs d'impression	Opérateurs d'impression	Opérateurs d'impression
		Contrôleurs de domaine en lecture seule	Contrôleurs de domaine en lecture seule
Duplicateur	Duplicateur	Duplicateur	Duplicateur
Administrateurs du schéma	Administrateurs du schéma	Administrateurs du schéma	Administrateurs du schéma
Opérateurs de serveur	Opérateurs de serveur	Opérateurs de serveur	Opérateurs de serveur

Source : Microsoft

Security IDentifier (SID) = identifiant unique de sécurité d'un objet du domaine

Structure des SID :

S-R-X-Y1-Y2-Yn-1-Yn

S-1-5-21-3332904308-1614487934-3407257785-1121

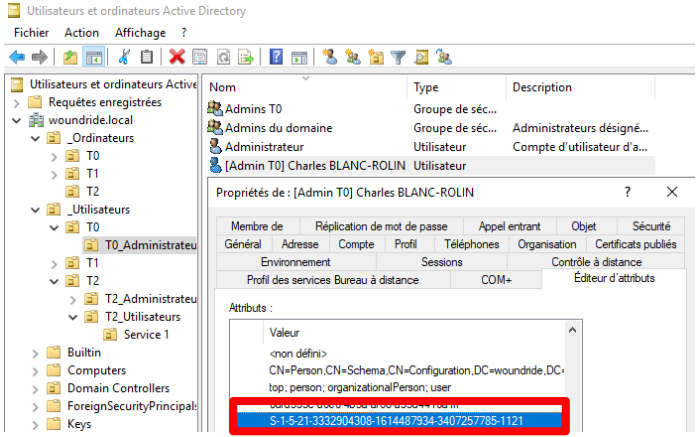
- **S** : indique que la chaîne est un SID
- **R** : niveau de révision (1 seule révision à ce jour, vaut toujours 1)
- **X** : autorité de délivrance (5 pour l'autorité NT, 12 pour Azure AD)
- **Y1-Y2-Yn-1** : identifiant du domaine
- **Yn** : identifiant relatif ou RID (Relative Identifier)

Windows Service
S-1-5-80-859482183-879914841-863379149-1145462774-2388618682

Azure Active Directory User
S-1-12-1-1414772360-7548652109-3974151294-7485145544

Active Directory User
S-1-5-21-415289841-218583201-7485910196-84512

Windows Logon ID
S-1-5-5-0-137426688



Quelques exemples de SID / RID intéressants :

- Un SID est généralement unique (grâce à l'identifiant de domaine unique), contrairement à un RID qui est unique seulement sur un domaine.

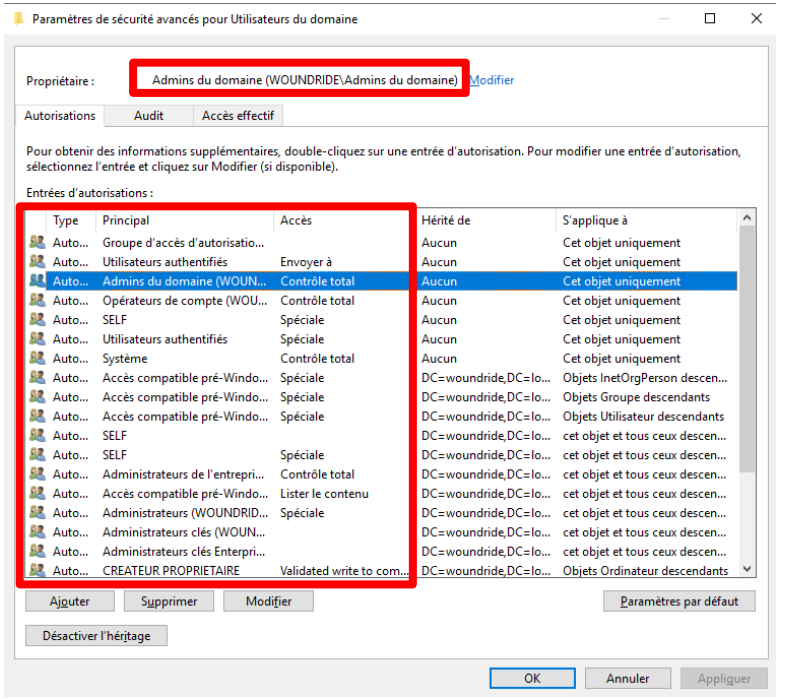
- S-1-5-21-3332904308-1614487934-3407257785-**512** (groupe « Admins du domaine »)
- S-1-5-21-3332904308-1614487934-3407257785-**500** (compte « Administrateur » du domaine)
- S-1-5-21-3332904308-1614487934-3407257785-**501** (compte « Invité »)
- S-1-5-21-3332904308-1614487934-3407257785-**502** (compte « krbtgt »)
- S-1-5-21-3332904308-1614487934-3407257785-**513** (groupe « Utilisateurs du domaine »)
- S-1-5-21-3332904308-1614487934-3407257785-**515** (groupe « Ordinateurs du domaine »)
- S-1-5-21-3332904308-1614487934-3407257785-**516** (groupe « Contrôleurs de domaine »)
- S-1-1-0 (groupe « Tout le monde »)
- S-1-5 (Autorité NT)
- S-1-12 (Autorité Azure AD)
- S-1-5-32-**544** (groupe « Administrateurs » > groupe local répliqué entre les DC)

Tout RID inférieur à 1000 est un objet présent par défaut dans tout AD (tout RID > 1000 = objet créé)

Les descripteurs de sécurité

Un descripteur de sécurité contient les informations de sécurité associées à un objet « sécurisable » :

- Chaque objet contenu dans l'AD est « sécurisable » (Securable Object)
- L'accès à ces objets est donc paramétrable
- Un descripteur de sécurité se compose d'une structure SECURITY_DESCRIPTOR et de ses informations de sécurité associées :
  - SID du propriétaire de l'objet
  - Une liste de contrôle d'accès (ACL* pour Access Control List en anglais)
  - Liste qui contient des entrées (ACEs pour Access Control Entries en anglais)



ACL pour le groupe « Utilisateurs du domaine »

*on parle aussi de DACL (Discretionnary Access Control List) et de SACL (System Access Control List)

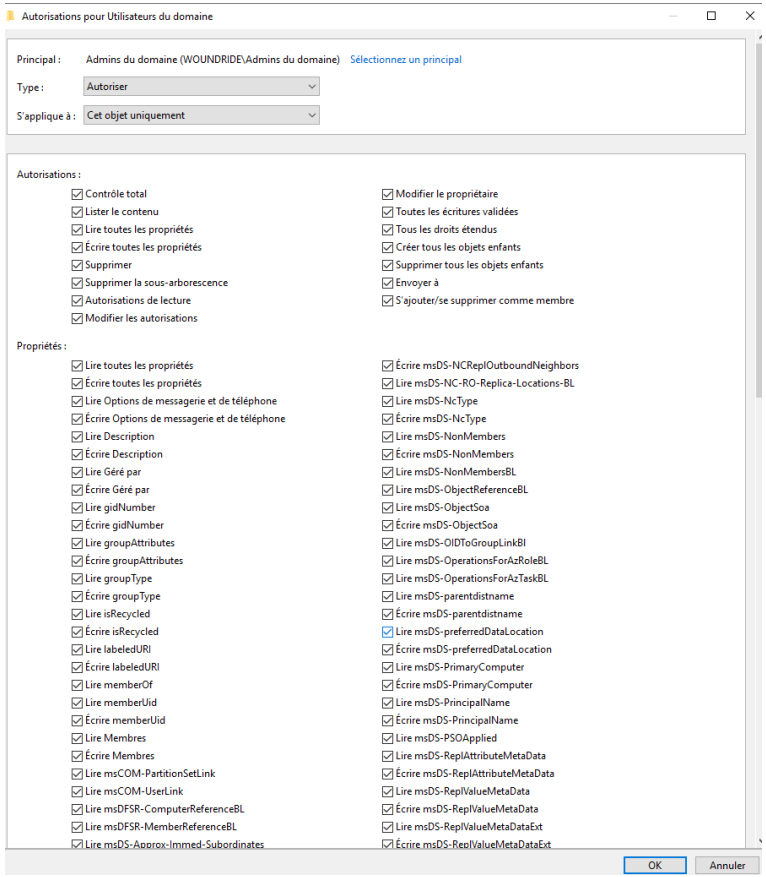
Les listes de contrôle

Une ACE spécifie les droits d'accès autorisés ou refusés à des utilisateurs ou groupes sur un objet (appelé dans ce cas « Security Principal »)

- Exemples de permissions :
  - Droits génériques : GENERIC_READ, GENERIC_WRITE, GENERIC_EXECUTE, GENERIC_ALL
  - Droits standards : DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER
  - Droits spécifiques : dépend de la classe de l'objet

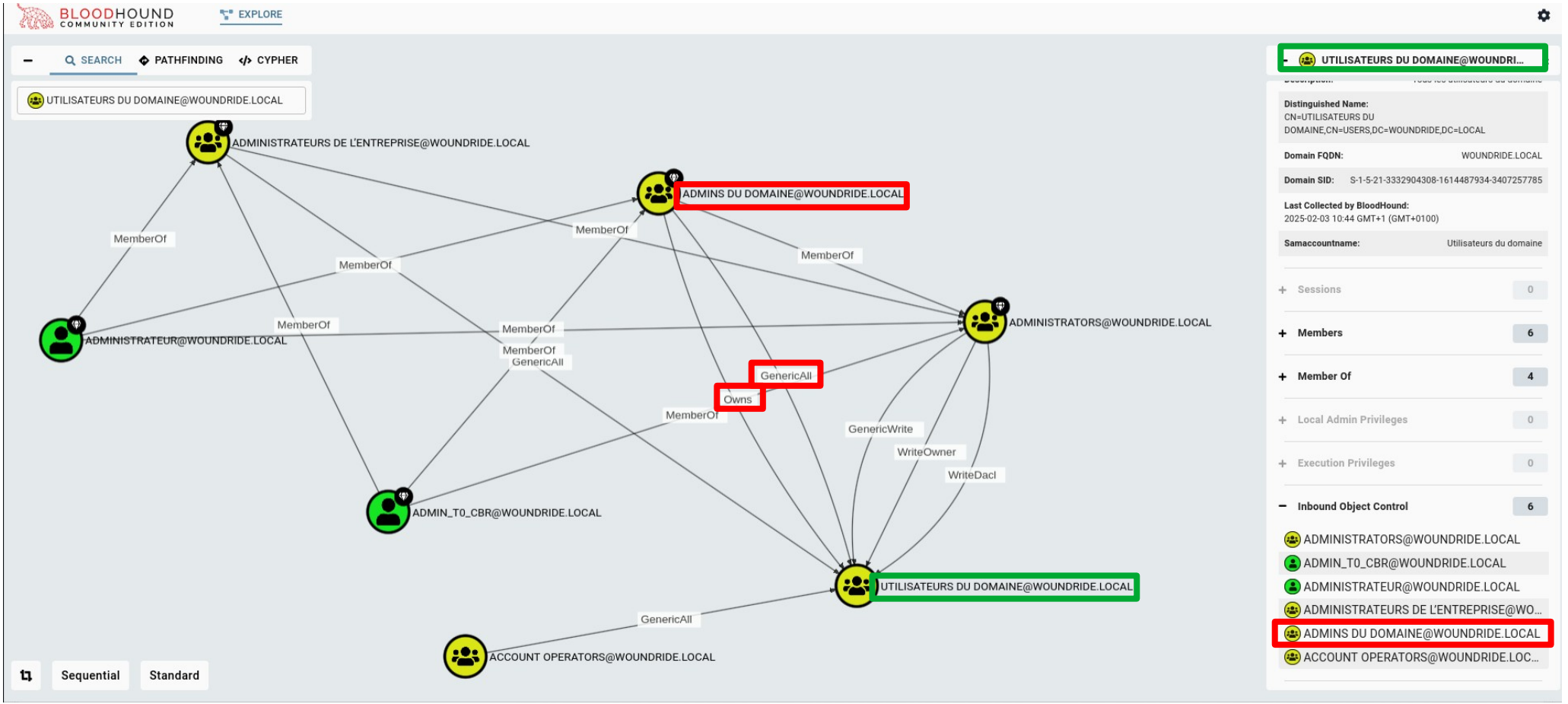
- Ces permissions peuvent être héritées d'autres objets :
  - UO(s) d'appartenance
  - Groupe(s) d'appartenance

- Le fait d'attribuer des droits d'administration spécifiques à certains comptes utilisateurs (administrateurs d'une partie spécifique de l'AD) est généralement appelée la « délégation de privilèges



ACE pour le groupe « Admins du domaine » sur le groupe « Utilisateurs du domaine »

Des privilèges pas toujours faciles à appréhender...



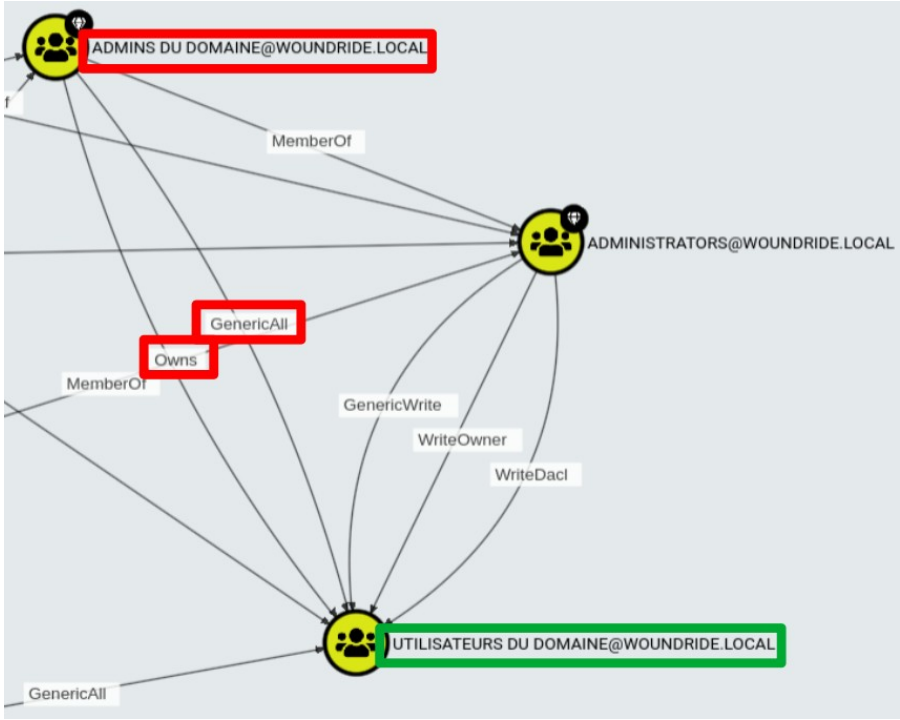
Vue graphique de l'ACL pour le groupe « Utilisateurs du domaine » avec BloodHound

Focus sur les droits

Exemples de droits :

- **WRITE_DAC** : permet d'ajouter une ACE dans la DACL de l'objet (droit possédé implicitement par le propriétaire de l'objet)
- **WRITE_OWNER** : permet de modifier le propriétaire de l'objet
- **GENERIC_WRITE** : permet toutes les écritures de propriétés
- **GENERIC_ALL** = GENERIC_WRITE + WRITE_DAC + WRITE_OWNER (contrôle total)

- **DS_WRITE_PROP** : permet l'écriture de toutes les propriétés de l'objet
- **DS_CONTROL_ACCESS** : permet tous les droits étendus



Droits par défaut

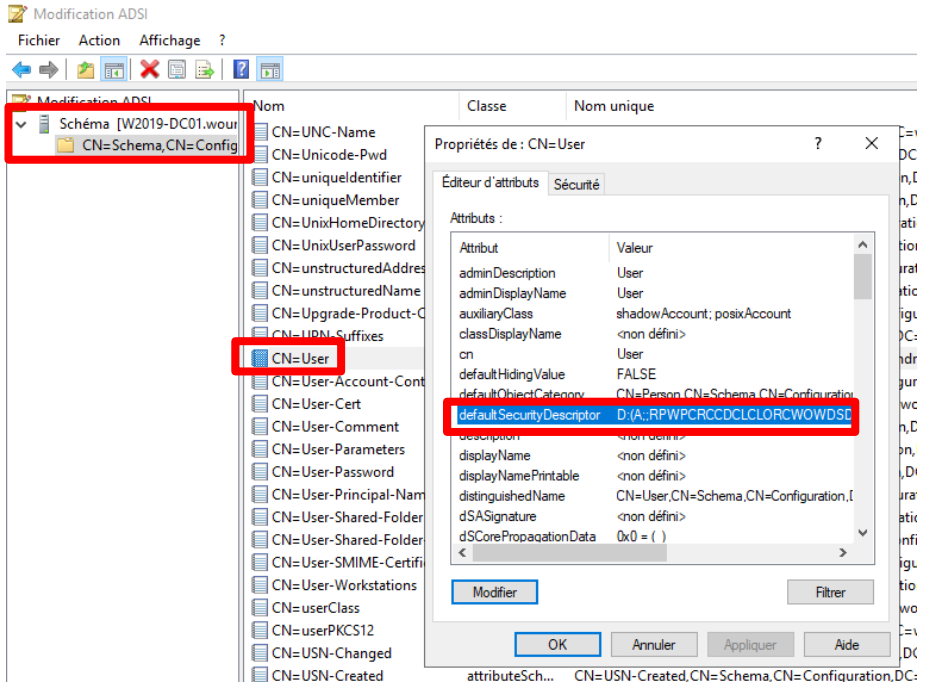
Les droits par défaut sont stockés :

- Au niveau du schéma, dans la « classe » d'un objet
- Via l'attribut « defaultSecurityDescriptor »

- Les droits par défaut peuvent être réappliqués (ainsi que ceux hérités de l'UO parente) à l'aide de la commande :

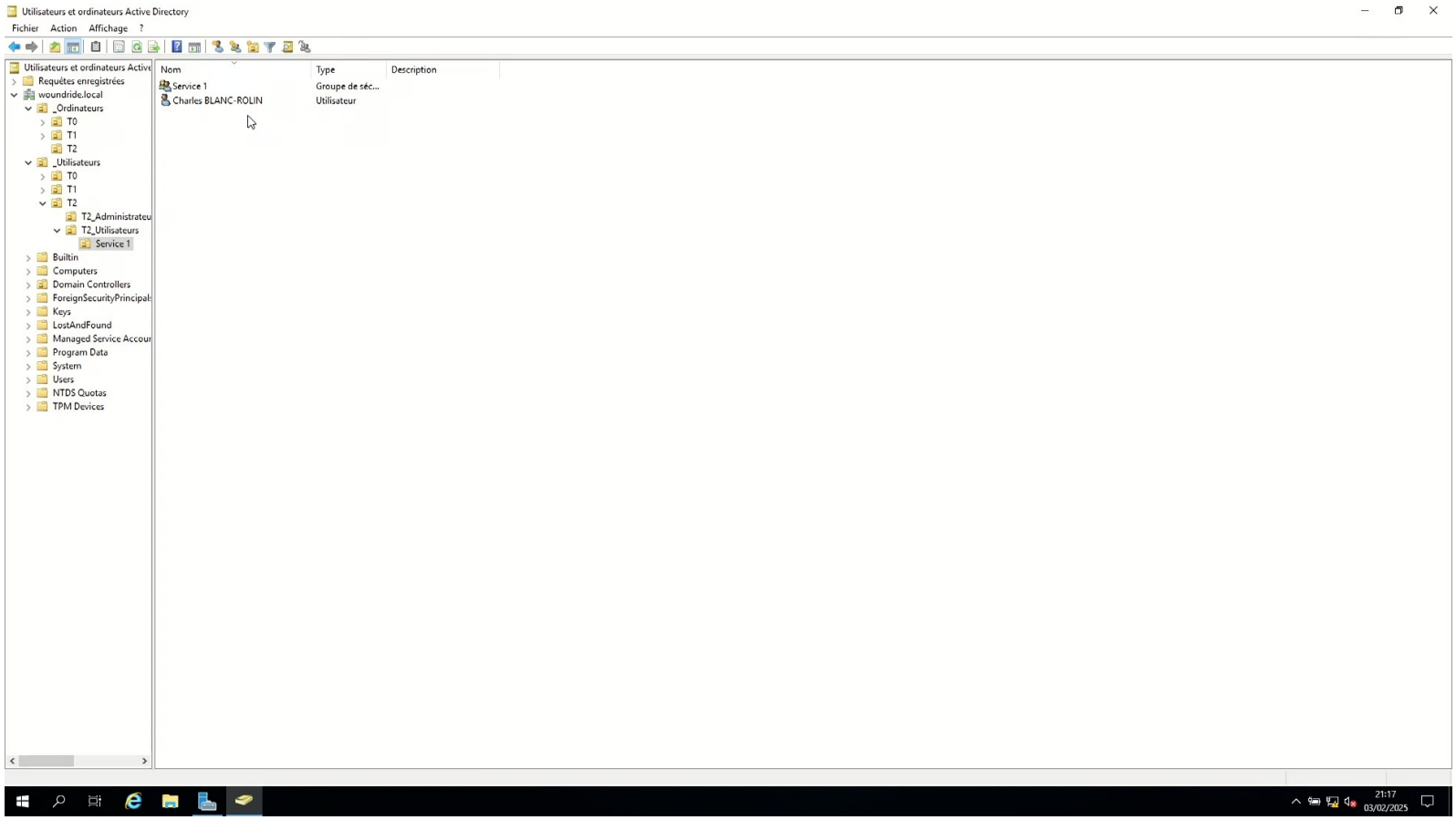
.\dsacls.exe "CN=Charles BLANC-ROLIN,OU=Service 1,OU=T2_Utilisateurs,OU=T2,OU=_Utilisateurs,DC=woundride,DC=local" /S /T

- Les arguments :
  - le DN (Distinguished Name) de l'objet à réinitialiser
  - /S : restaurer le descripteur de sécurité de l'objet à sa valeur par défaut
  - /T : restaurer également les descripteurs de sécurité des objets enfants (si applicable)



La classe « User » est accessible dans le Schéma via la console « adsiedit.msc »

Restaurer les droits par défaut



Les stratégies de groupe ou GPO (Group Policy Objects)

Elles permettent :

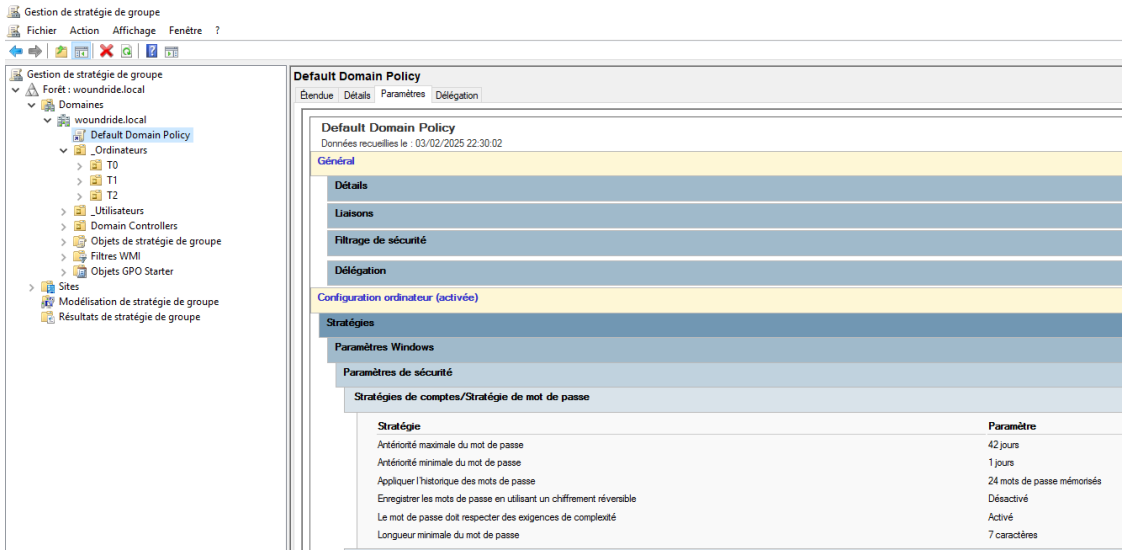
- D'appliquer sur des comptes utilisateurs ou d'ordinateurs différents paramètres
- De contrôler des clés de registre
- De contrôler des droits NTFS
- D'appliquer des politiques de sécurité et / ou de les auditer
- D'installer des logiciels
- D'exécuter des scripts
- D'installer des imprimantes
- De monter des lecteurs réseau

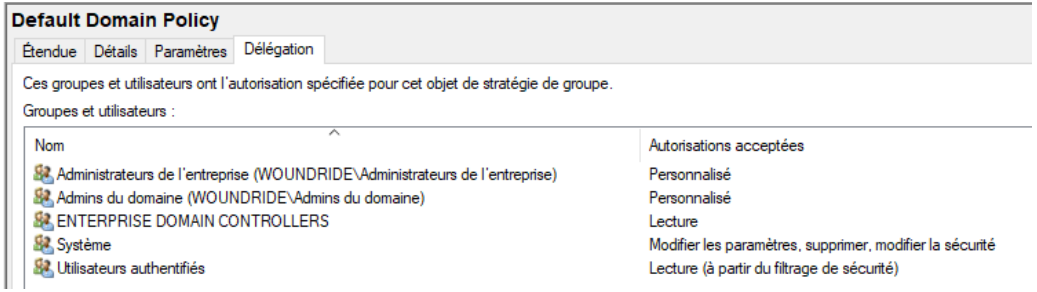
...

Les stratégies de groupe ou GPO (Group Policy Objects)

Grands principes :

- Elles disposent d'un identifiant unique GUID
- Leurs autorisations sont personnalisables
- Elles sont définies à l'aide de modèles d'administration basés sur un modèle XML (on parle de template ADMX)
- Elles s'appliquent au niveau du domaine ou de ses UO « filles »

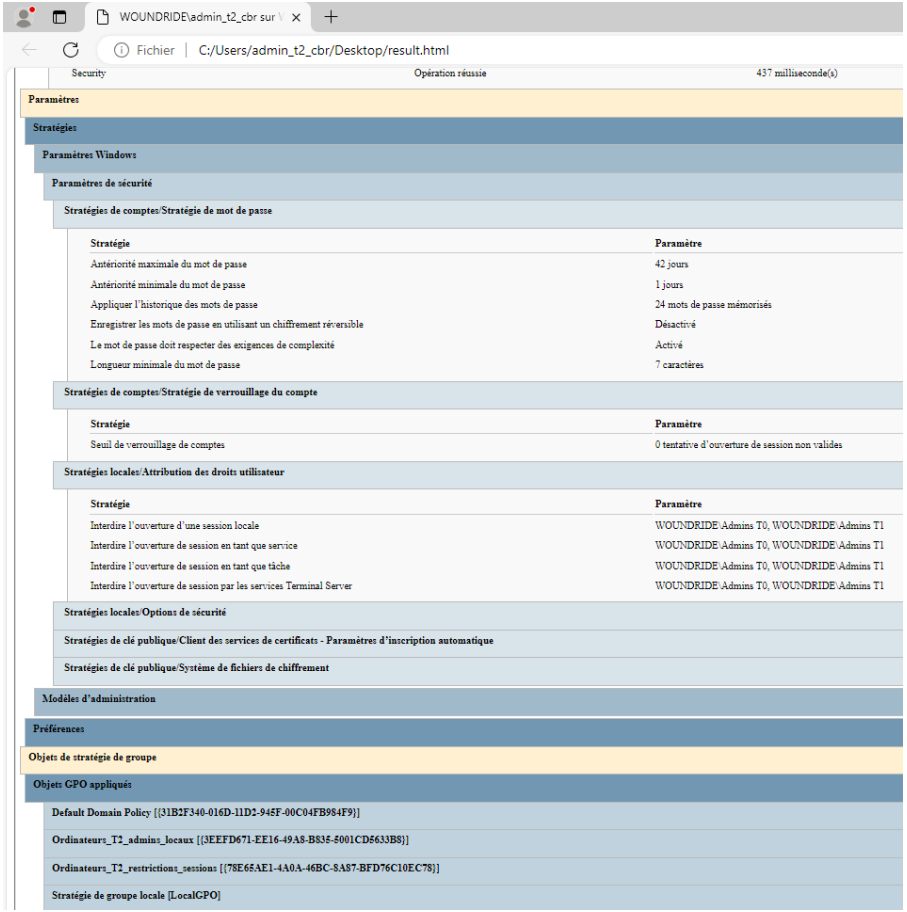


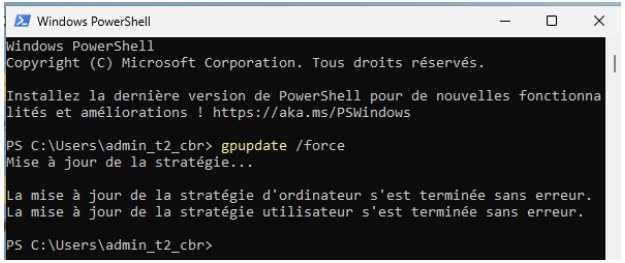


Récupération des GPO sur un poste

Grands principes :

- Les postes récupèrent les stratégies au démarrage + à intervalle aléatoire entre 1h et 2h par défaut)
- Il est possible d'exporter le contenu des GPO appliquées sur un ordinateur à l'aide de la commande :
  gpresult /H result.html
- Il esr possible de forcer l'application des stratégies depuis un ordinateur à l'aide de la commande :
  gpupdate /force





Ressources et outils utilisés

- Identificateurs de sécurité - SID (Microsoft) :
  https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/understand-security-identifiers
  https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dtyp/81d92bba-d22b-4a8c-908a-554ab29148ab

- Flux réseau AD (Microsoft) :
  https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/active-directory/config-firewall-for-ad-domains-and-trusts

- Descripteurs de sécurité (Microsoft) :
  https://learn.microsoft.com/fr-fr/windows/win32/secauthz/security-descriptors

- BloodHound (Specterops) :
  https://specterops.io/bloodhound-community-edition/