Contrôleur de domaine

Alexandre LOPEZ

Active Directory

- L'Active Directory constitue un annuaire LDAP dédié aux systèmes d'exploitation Windows.
- Il regroupe divers types d'objets tels que des utilisateurs, des ordinateurs, etc.
- Son but principal est de centraliser deux fonctions cruciales : l'identification et l'authentification au sein d'un système d'information.

Active Directory

- Les intérêts de l'AD :
  - Administration centralisée et simplifiée
  - Unifier l'authentification
  - Identifier les objets sur le réseau
  - Référencer les utilisateurs et ordinateurs

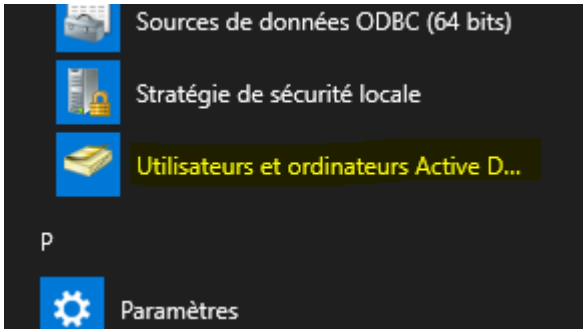
Administrer Active Directory

- Lors de l'installation du rôle de serveur AD DS, un service Windows nommé **Services de domaine Active Directory** est créé avec un type de démarrage automatique.

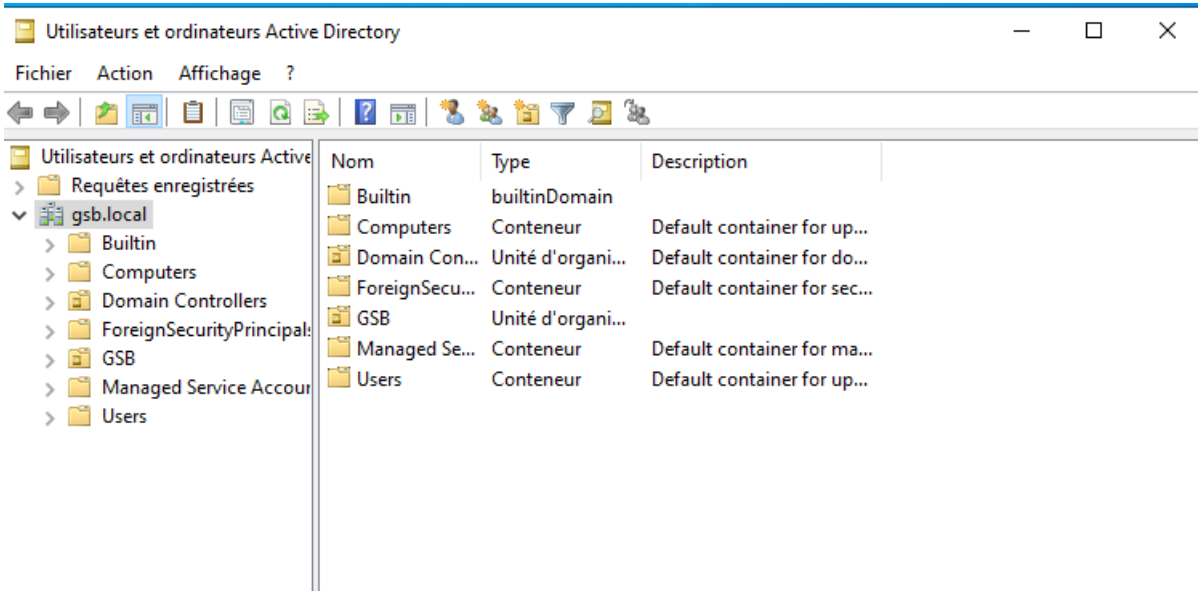
Nom	Description	État
Spouleur d'impression	Ce service met en sp...	En cours d
Services Web Active Directory	Ce service fournit un...	En cours d
Services de domaine Active Directory	Service de contrôleu...	En cours d
Services de chiffrement	Fournit trois services...	En cours d

Administrer Active Directory

- Après l'installation du rôle AD DS, vous avez une icône **Utilisateurs et ordinateurs Active Directory.** A cet endroit vous pourrez gérer votre AD.



Administrer Active Directory



Administrer Active Directory

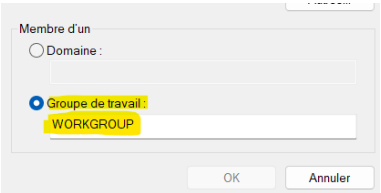
- Autre possibilité, le rôle de serveur Active Directory via une console nommée Centre d'administration Active Directory (Active Directory Administrative Center. Cette console est accessible via les outils du Gestionnaire de serveur.

© 2018 Microsoft Corporation. Tous droits réservés.

Administrer Active Directory

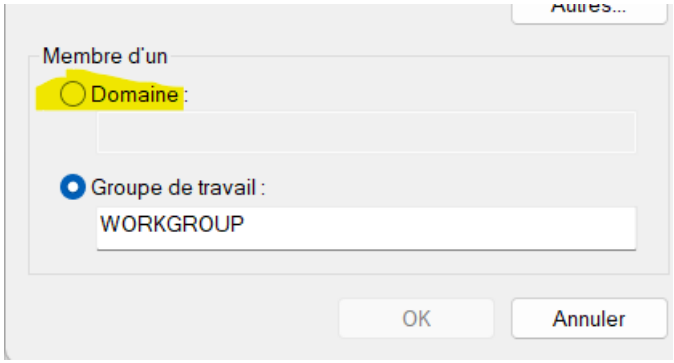
Groupe de travail

- **Fonctionnement peer-to-peer**
- **Une base d'utilisateurs par machine** : « base SAM », cette base est unique sur chaque machine et non partagée, les utilisateurs sont donc en local sur la machine.
- Plus adapté à un environnement d'entreprise, pas d'administration centralisée
- Simplicité pour la mise en place



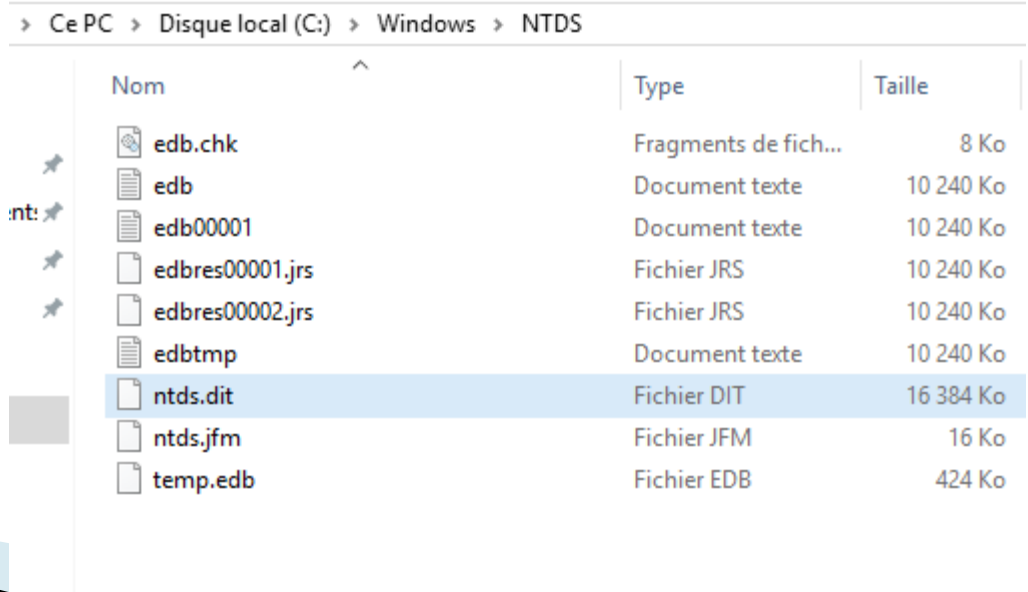
Domaine

- **Fonctionnement client/serveur**
- **Base d'utilisateurs, de groupes et d'ordinateurs centralisée.** Un compte utilisateur a la possibilité d'accéder à l'ensemble des machines du domaine
- **Administration et gestion de la sécurité centralisée.**



Gestion du service d'annuaire

- La base de données Active Directory est contenue dans un fichier situé par défaut à l'emplacement suivant : **%SYSTEMROOT%\NTDS\ntds.dit**
- **NTDS correspond à l'ancien nom de l'AD** « *NT Directory Services* »

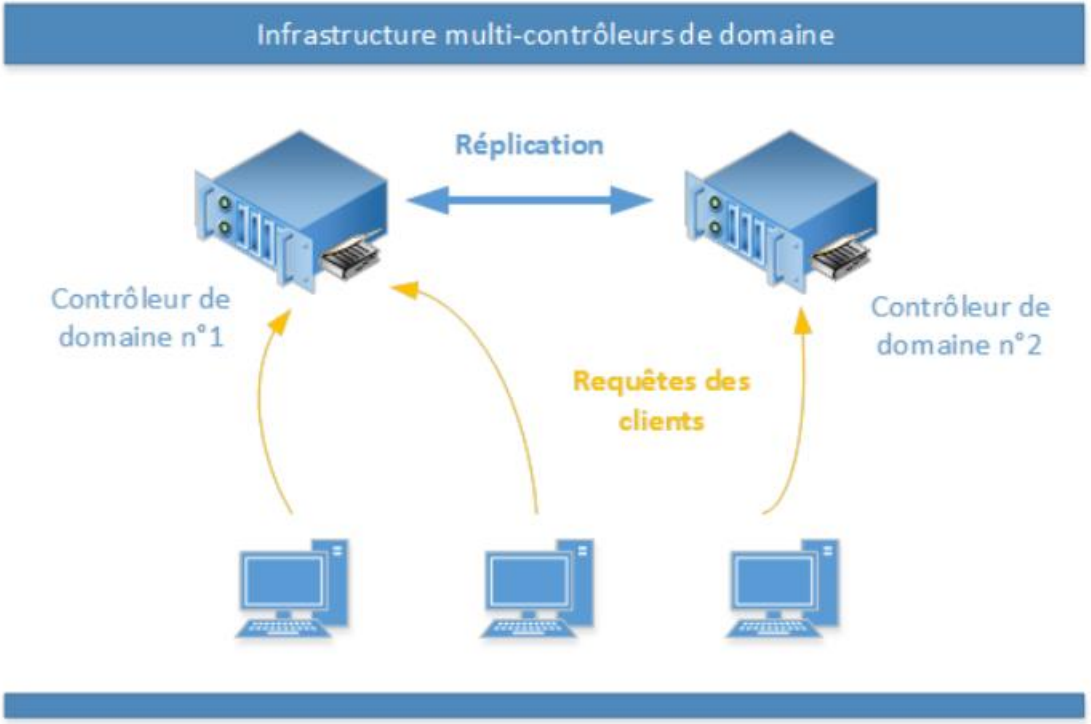


Redondance

- Dans le cadre de la haute disponibilité, il est préférable d'avoir deux contrôleurs de domaine en redondance.

- les DC répliquent les informations entre eux à intervalle régulier, afin de disposer d'un annuaire Active Directory identique. Sur les objets, un numéro de version est géré par les DC, ce qui lui permet de savoir s'il est à jour ou non par rapport à la version la plus récente de l'annuaire.

Redondance


Infrastructure multi-contrôleurs de domaine
Réplication
Contrôleur de domaine n°1
Contrôleur de domaine n°2
Requêtes des clients

Domaine

- Le schéma d'architecture Active Directory représente les domaines sous la forme suivante

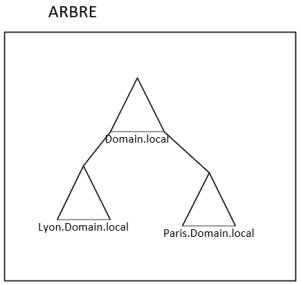
- Un domaine regroupe des unités d'organisations qui vont contenir des objets (ordinateurs, ordinateurs, groupes, GPO, …)

Arbre

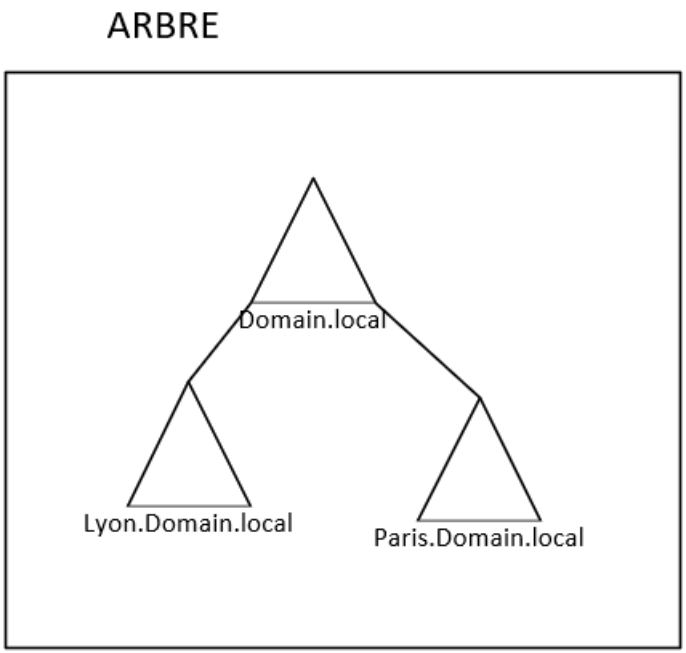
- Lorsqu'un domaine principal contient plusieurs sous-domaines on parle alors d'arbre, où chaque sous-domaine au domaine racine représente une branche de l'arbre

- **Un arbre est un regroupement hiérarchique de plusieurs domaines.**

- **Chaque domaine peut être considéré comme une branche**

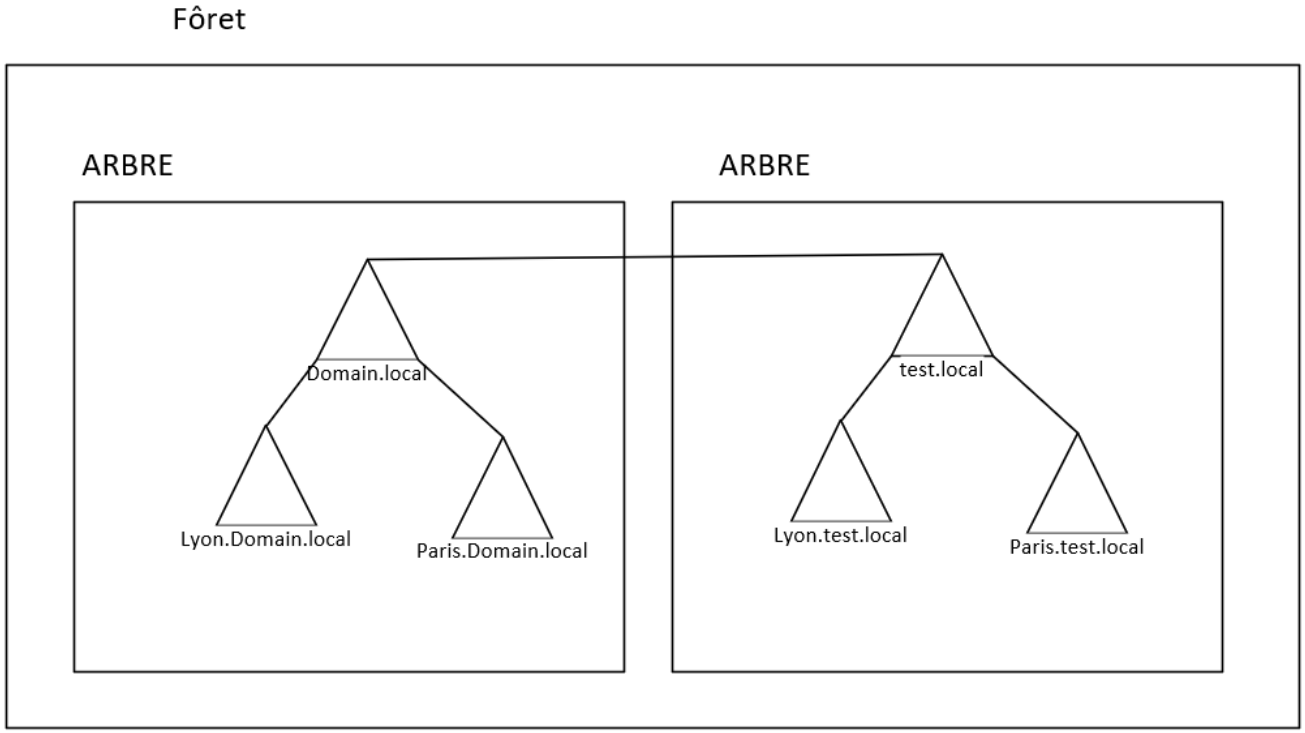


Arbre Active Directory



Forêt Active Directory

- Une forêt regroupe une ou plusieurs arborescences de domaine, c'est-à-dire un ou plusieurs arbres



Protocole LDAP

- Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole qui permet de gérer des annuaires, notamment grâce à des requêtes d'interrogations et de modification de la base d'informations. En fait, l'Active Directory est un annuaire LDAP.

- Les communications LDAP s'effectuent sur le port 389, en TCP, du contrôleur de domaine cible.

Structure du LDAP

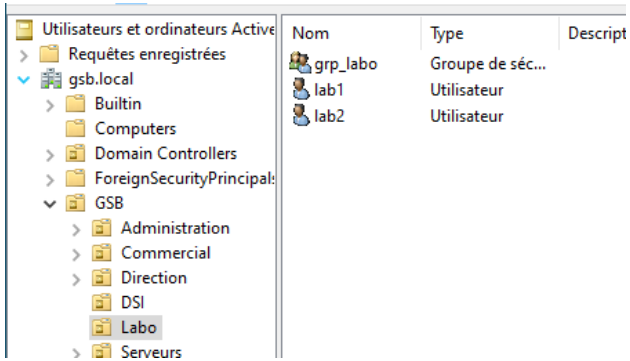
- Chaque objet dispose d'un identifiant unique.

- L'identifiant unique d'un objet est appelé GUID qui est « **l'identificateur unique global** ». Par ailleurs, un nom unique (DN – *Distinguished Name*) est attribué à chaque objet.

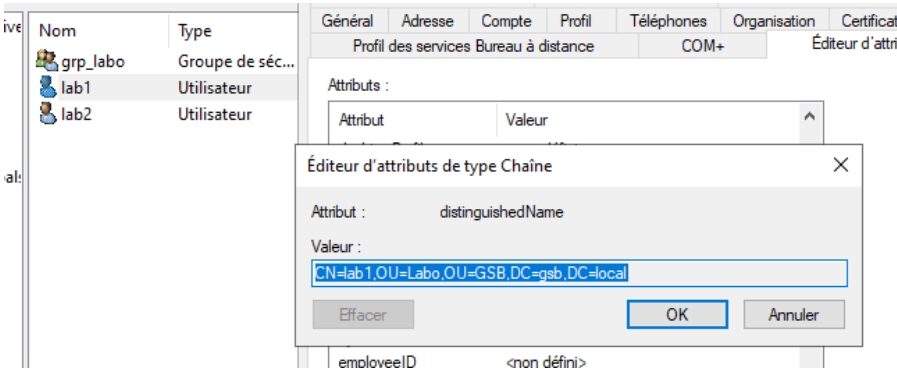
objectCat...	CN=Person,CN=Schema,CN=Configuration,DC=gsb,DC=
objectClass	top; person; organizationalPerson; user
objectGUID	c48817fc-520a-4760-855b-be5bf0d3e18a
objectSid	S-1-5-21-3303348701-2880797340-798786356-1115
objectVer...	<non défini>

Structure du LDAP

- Exemple pour accéder à l'utilisateur « lab1 » via le DN



- Le DN sera le suivant



Les objets Active Directory

- Unités d'organisations
  Organizational Unit
- Utilisateurs
  User
- Groupes
  Group
- GPO
- Imprimantes
- Contacts
- Ordinateurs
- …

SID

- SID (Security Identifier), identifiant de sécurité unique associé à chaque objet relatif à la sécurité (utilisateurs, groupes, ordinateurs, services, etc...) sur une machine Windows. Dans l'annuaire Active Directory, chaque objet est également associé à un SID unique.

SID

- Exemple SID

objectGUID	c4881fc-520a-4760-855b-be5bf0d3e18a
objectSid	S-1-5-21-3303348701-2880797340-798786356-1115
objectVer	<non défini>

- Composition du SID

- **S-1** : préfixe commun des SID
- **-5** : autorité d'identification, ici **Autorite NT**
- **-21** : autorité secondaire
- **-1990400566-1867844161-3796721076** : identifiant du domaine ou de l'ordinateur (valeur unique sur chaque machine)
- **-500** : **RID** pour **Relative ID** ou identificateur **relatif de l'objet.** Entre deux utilisateurs locaux d'une même machine, il n'y a que le RID qui sera différent dans le SID.

DNS

- L'Active Directory a besoin du DNS pour pouvoir fonctionner, celui-ci sera un DNS privé qui aura la possibilité de faire les résolutions DNS de vos machines.

- Lorsque vous installez le rôle Active Directory vous devez aussi installer le rôle DNS.

Kerberos

- Kerberos est un protocole d'authentification réseau qui vise à fournir une sécurité robuste.
- Chaque contrôleur de domaine dispose d'un service de distribution de clés de sécurité, appelé « **Centre de distribution de clés (KDC)** ».
- Le principal avantage de Kerberos est qu'il permet une authentification unique (Single Sign-On – SSO), ce qui signifie que les utilisateurs n'ont besoin de s'authentifier qu'une seule fois pour accéder à plusieurs services au sein du même domaine de sécurité.

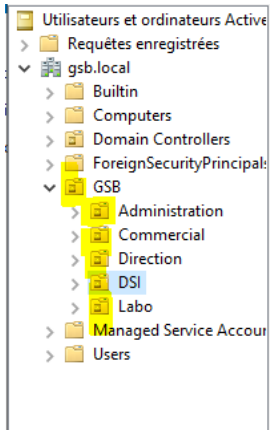
En résumé

- LDAP : Gestion de l'annuaire
- Kerberos : Authentification et gestion des sessions
- DNS : Communication et gestion des noms

Ces trois protocoles sont indispensables au bon fonctionnement de l'AD

Gestion des unités d'organisation

- Afin d'organiser une infrastructure Active Directory, l'ensemble des objets d'un domaine est stocké dans un conteneur appelé **unité d'organisation** (OU pour Organizational Unit). Une unité d'organisation permet d'organiser l'ensemble des objets :



Gestion des unités d'organisation

- **Ajouter une OU avec PowerShell**

- Ouvrez le Gestionnaire de serveur puis Outils et Module Active Directory pour Windows PowerShell.

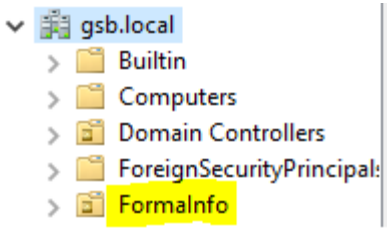
- Entrer la commande suivante :

- New-ADOrganizationalUnit -Name NouvelleOU -Path "OU=NomOUDéjàExistante,DC=Domaine,DC=TLD" -ProtectedFromAccidentalDeletion:$true

Ajouter une OU avec PowerShell

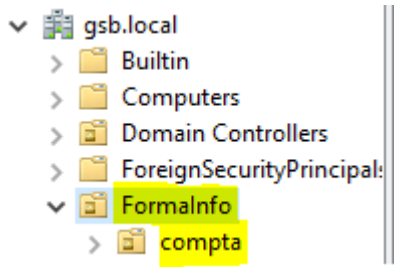
- Création de l'OU à la racine

```
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name FormaInfo -path "DC=gsb,DC=local" -ProtectedFromAccidentalDel
etion:$true
```



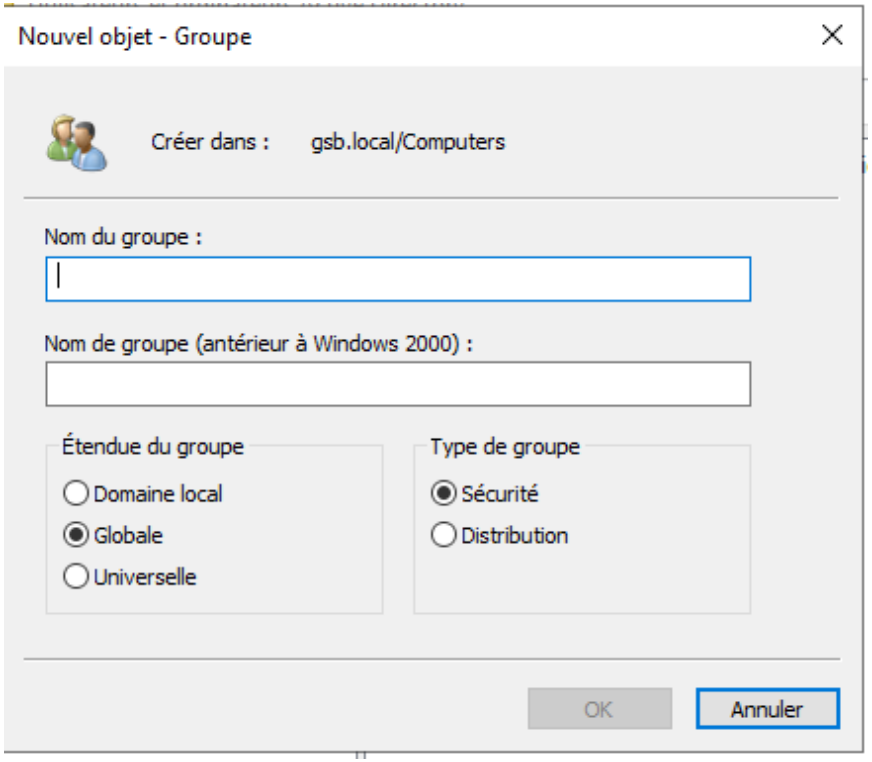
- Création de l'OU dans une OU

```
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name compta -path "OU=FormaInfo,DC=gsb,DC=local" -ProtectedFromAcc
identalDeletion:$true
PS C:\Users\Administrateur>
```



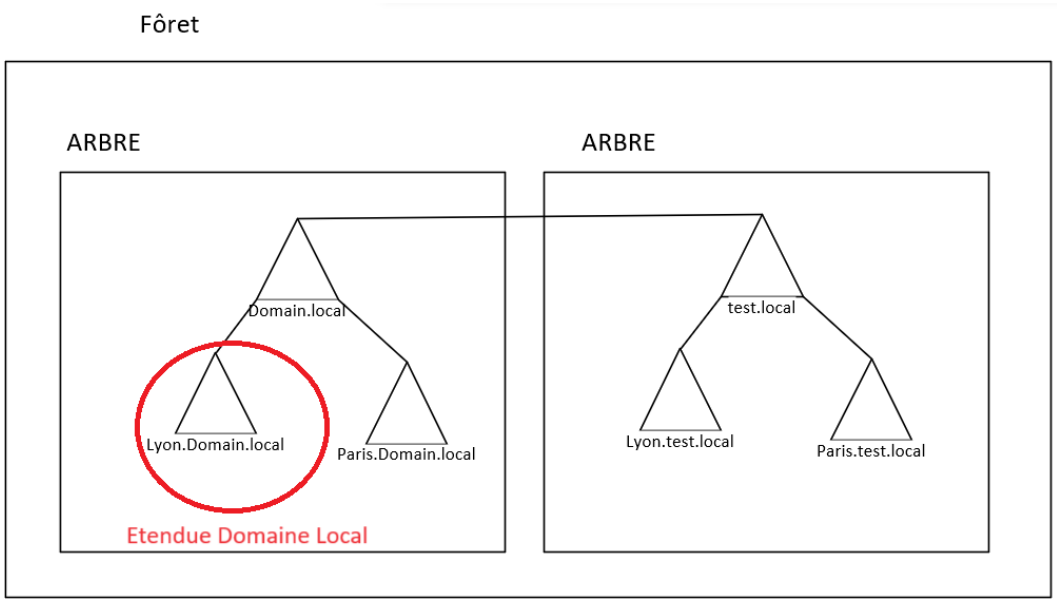
Les groupes

- Permettent le groupement d'un ensemble d'utilisateurs et/ou d'ordinateurs entre autres



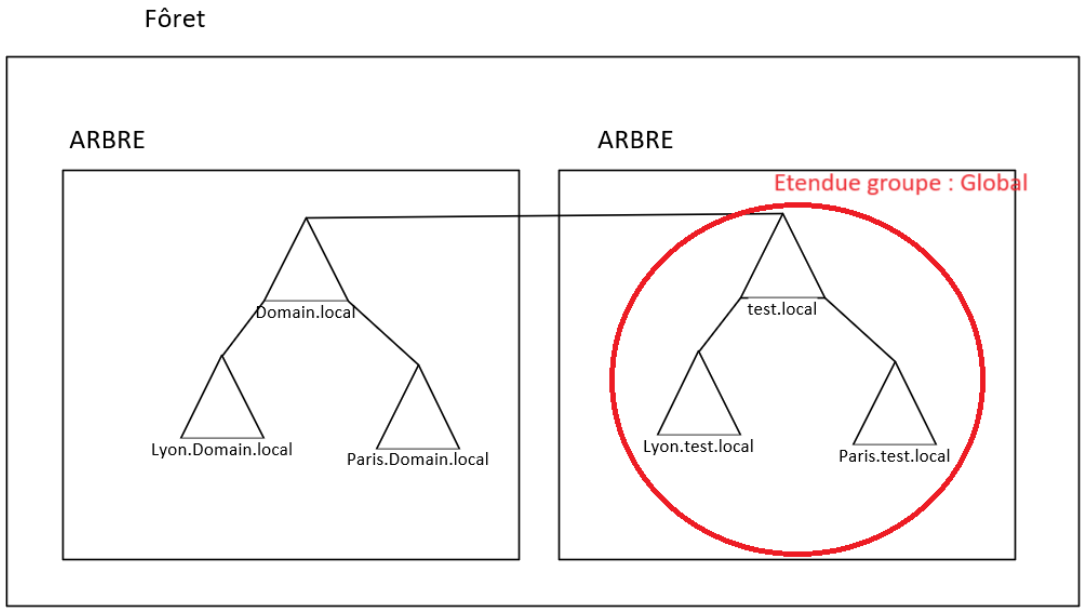
L'étendue du groupe

- **Domaine local** : Un groupe de domaine local est utilisé pour regrouper des utilisateurs, des ordinateurs et d'autres groupes au sein d'un seul domaine spécifique. Il peut donc être utilisé uniquement dans le domaine dans lequel il est créé.



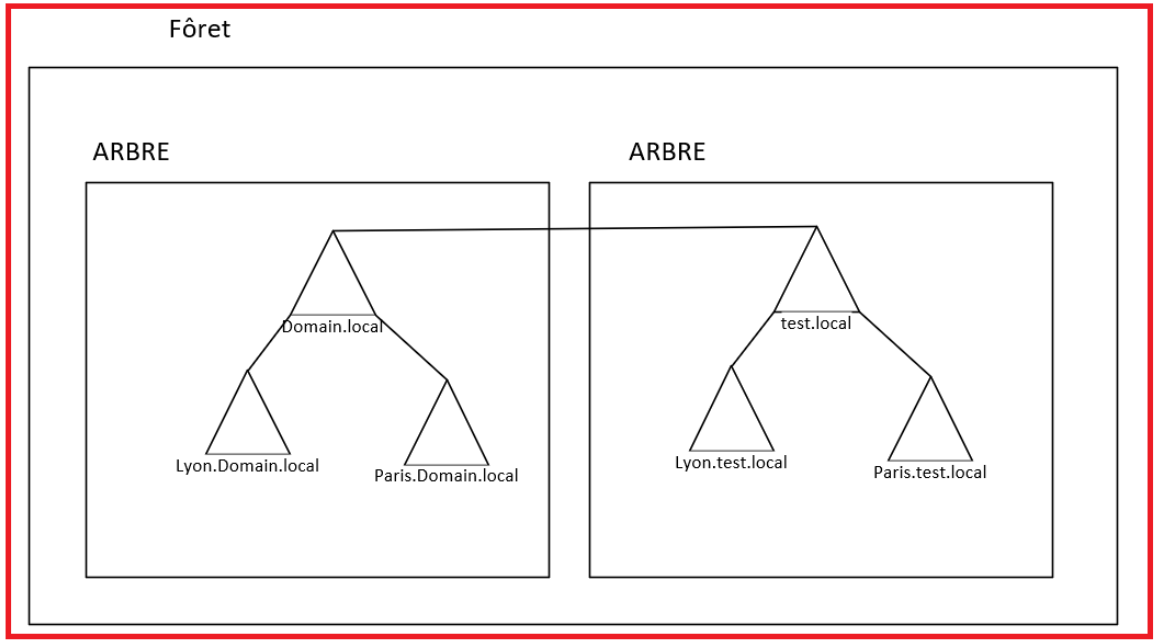
L'étendue du groupe

- **Global**: Un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base.



L'étendue du groupe

- **<u>Universelle</u>**: Un groupe universel est également utilisé pour regrouper des utilisateurs, des ordinateurs et d'autres groupes à travers plusieurs domaines au sein d'une forêt Active Directory.



Etendue de groupe : Universelle

Type de groupe

- **Sécurité** : Un groupe de sécurité est principalement utilisé pour gérer l'accès aux ressources.

- **Diffusion** : Un groupe de diffusion est utilisé pour envoyer des messages à un ensemble de destinataires sans nécessiter de contrôle d'accès aux ressources.

Gestion des comptes d'utilisateurs

- Le système Windows Server gère plusieurs types de comptes d'utilisateurs :

- **Les comptes d'utilisateurs locaux**
- **Les comptes d'utilisateurs du domaine**
- **Les comptes de service et comptes virtuels**

Les comptes d’utilisateurs locaux

- Les comptes d’utilisateurs locaux permettent d’accéder aux ressources locales d’un serveur tandis que les comptes d’utilisateurs du domaine permettent d’accéder aux ressources du domaine complet.

Les comptes d’utilisateurs du domaine

- Si un serveur Windows Server fait office de contrôleur de domaine, ce dernier ne prend plus en charge les comptes d’utilisateurs locaux, qui ne sont supportés que par les serveurs membres du domaine.

Les comptes de service et comptes virtuels

- Le contexte de sécurité détermine la capacité du service à accéder aux ressources locales et réseau. Les systèmes d'exploitation Windows dépendent des services permettant d'exécuter diverses fonctionnalités. Ces services peuvent être configurés par le biais des applications, du composant logiciel enfichable Services ou du gestionnaire des tâches, ou à l'aide de Windows PowerShell.

Les comptes de service et comptes virtuels

- Les comptes de services sont des comptes de domaine avec les avantages ci-dessous :

- Gestion de mots de passe automatisés.
- Gestion du SPN Simplifié, incluant la délégation de gestion à d'autres administrateurs.

- Les comptes virtuels sont des comptes locaux avec les avantages ci-dessous :

- Pas de gestion de mots de passe.
- La capacité d'accéder au réseau avec l'identité de l'ordinateur.

Un **SPN** est le nom par lequel un client identifie de manière unique une instance d'un service

Création d'un compte utilisateur

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active
- Requêtes enregistrées
- formainfo.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal
  - Managed Service Accour
  - Users

Nom	Type	Description
Administrat...	Utilisateur	Compte d'utilisateur d'a...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Administrateurs désigné...
Admins du ...	Groupe de séc...	Administrateurs désigné...
Contrôleurs ...	Groupe de séc...	Tous les contrôleurs de ...
	Groupe de séc...	Les membres de ce grou...
	Groupe de séc...	Les membres de ce grou...
Protected Us...		
Serveurs RA...		

Délégation de contrôle...
Rechercher...
Nouveau
Toutes les tâches
Affichage
Actualiser
Exporter la liste...
Propriétés
Aide

Ordinateur
Contact
Groupe
InetOrgPerson
msDS-KeyCredential
msDS-ResourceProperty List
msDS-ShadowPrincipalContainer
msImaging-PSPs
Alias de file d'attente MSMQ
Imprimante
Utilisateur

Créer un nouvel objet...

Nouvel objet - Utilisateur

Créer dans : formainfo.local/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @formainfo.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : FORMAINFO\

< Précédent Suivant > Annuler

Création d'un compte utilisateur Powershell

- Il est necessaire d'ajouter le module
- Import-Module ActiveDirectory

- Pour voir les syntaxe existante :
- Get-Command New-ADUser -Syntax

```
PS C:\Users\Administrateur> Import-Module ActiveDirectory
PS C:\Users\Administrateur> Get-Command New-ADUser -syntax

New-ADUser [-Name] <string> [-WhatIf] [-Confirm] [-AccountExpirationDate <datetime>] [-AccountNotDelegated <bool>] [-Acc
ountPassword <securestring>] [-AllowReversiblePasswordEncryption <bool>] [-AuthenticationPolicy <ADAuthenticationPolicy>
] [-AuthenticationPolicySilo <ADAuthenticationPolicySilo>] [-AuthType <ADAuthType>] [-CannotChangePassword <bool>] [-Cer
tificates <X509Certificate[]>] [-ChangePasswordAtLogon <bool>] [-City <string>] [-Company <string>] [-CompoundIdentitySu
pported <bool>] [-Country <string>] [-Credential <pscredential>] [-Department <string>] [-Description <string>] [-Displa
yName <string>] [-Division <string>] [-EmailAddress <string>] [-EmployeeID <string>] [-EmployeeNumber <string>] [-Enable
d <bool>] [-Fax <string>] [-GivenName <string>] [-HomeDirectory <string>] [-HomeDrive <string>] [-HomePage <string>] [-H
omePhone <string>] [-Initials <string>] [-Instance <ADUser>] [-KerberosEncryptionType <ADKerberosEncryptionType>] [-Logo
nWorkstations <string>] [-Manager <ADUser>] [-MobilePhone <string>] [-Office <string>] [-OfficePhone <string>] [-Organiz
ation <string>] [-OtherAttributes <hashtable>] [-OtherName <string>] [-PassThru] [-PasswordNeverExpires <bool>] [-Passwo
rdNotRequired <bool>] [-Path <string>] [-POBox <string>] [-PostalCode <string>] [-PrincipalsAllowedToDelegateToAccount <
ADPrincipal[]>] [-ProfilePath <string>] [-SamAccountName <string>] [-ScriptPath <string>] [-Server <string>] [-ServicePr
incipalNames <string[]>] [-SmartcardLogonRequired <bool>] [-State <string>] [-StreetAddress <string>] [-Surname <string>
] [-Title <string>] [-TrustedForDelegation <bool>] [-Type <string>] [-UserPrincipalName <string>] [<CommonParameters>]

PS C:\Users\Administrateur>
```

Création d'un compte utilisateur Powershell

- Pour créer un utilisateur :
- New-ADUser NomUser

```
PS C:\Users\Administrateur> New-ADUser test
PS C:\Users\Administrateur> Get-ADuser -Filter * -Properties samAccountName | Select samAccountName

samAccountName
--------------
Administrateur
Invité
krbtgt
test
```

- Pour supprimer un utilisateur
- Remove-ADUser NomUtilisateur

```
PS C:\Users\Administrateur> Remove-ADUser test

Confirmer
Êtes-vous sûr de vouloir effectuer cette action ?
Opération « Remove » en cours sur la cible « CN=test,CN=Users,DC=formainfo,DC=local ».
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : O
PS C:\Users\Administrateur> Get-ADuser -Filter * -Properties samAccountName | Select samAccountName

samAccountName
--------------
Administrateur
Invité
krbtgt
```

Création d'un compte utilisateur Powershell

- Pour créer un compte en ajoutant des paramètres, exemple :

- **Nom** – test2
- **Nom du compte** – test2
- **Adresse du chemin** – "OU=Users,DC=formainfo,DC=local"
- **Saisie du mot de passe**
- **État** – Activé

Création d'un compte utilisateur Powershell

- New-ADUser -Name “test2" -SamAccountName "test2" -Path "DC=formainfo,DC=local »-AccountPassword(Read-Host -AsSecureString "Windows2019") -Enabled $true

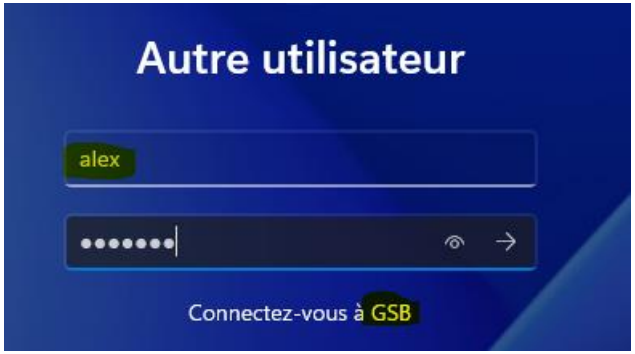
```
PS C:\Users\Administrateur> New-ADUser -Name "test2" -SamAccountName "test2" -Path "DC=formainfo,DC=local" -AccountPass
ord (Read-Host -AsSecureString "Windows2019") -Enable $true
Windows2019: ***********
PS C:\Users\Administrateur>
```

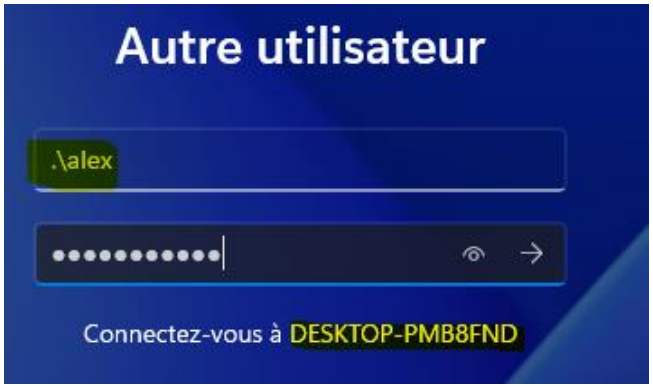
```
SamAccountName
--------------
Administrateur
Invité
krbtgt
test
test2

PS C:\Users\Administrateur
```

Accès compte local / domaine

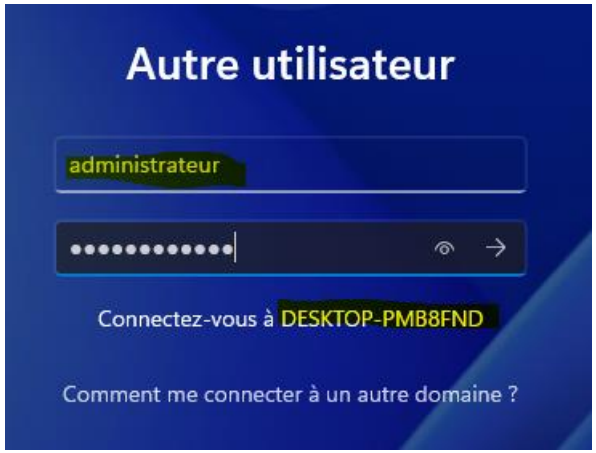
- Lorsque la machine est dans un domaine, par défaut la session va se connecter avec un utilisateur du domaine. Pour ouvrir une session avec un compte local, il suffit de mettre « .\ » ou « NomPC\ » pour se connecter en local sur la machine.

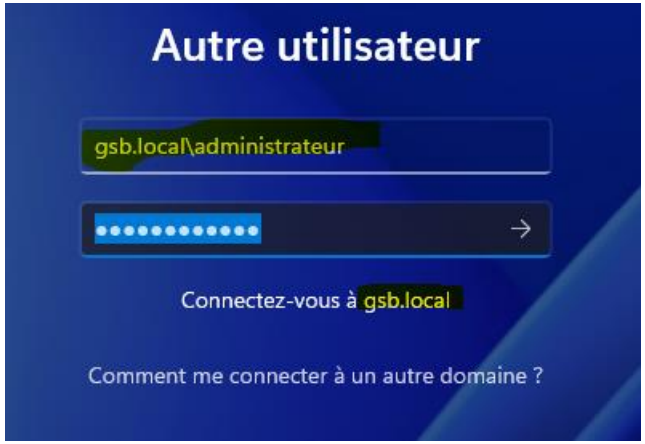




Accès compte local / domaine

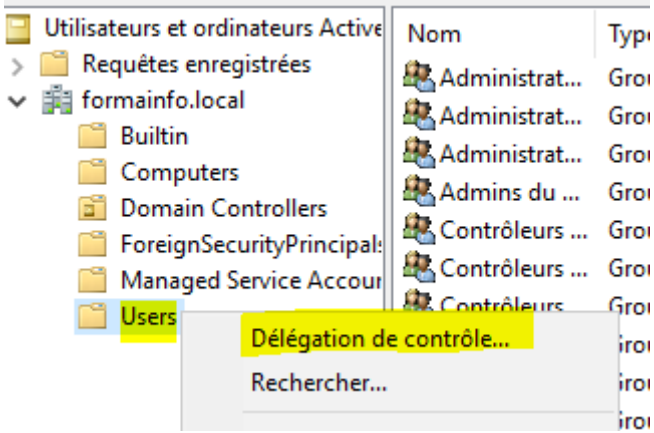
- Seul cas spécifique, lorsque vous souhaitez vous connecter avec un compte administrateur, celui-ci se connecte directement en local. Dans ce cas vous devez saisir le domaine complet.

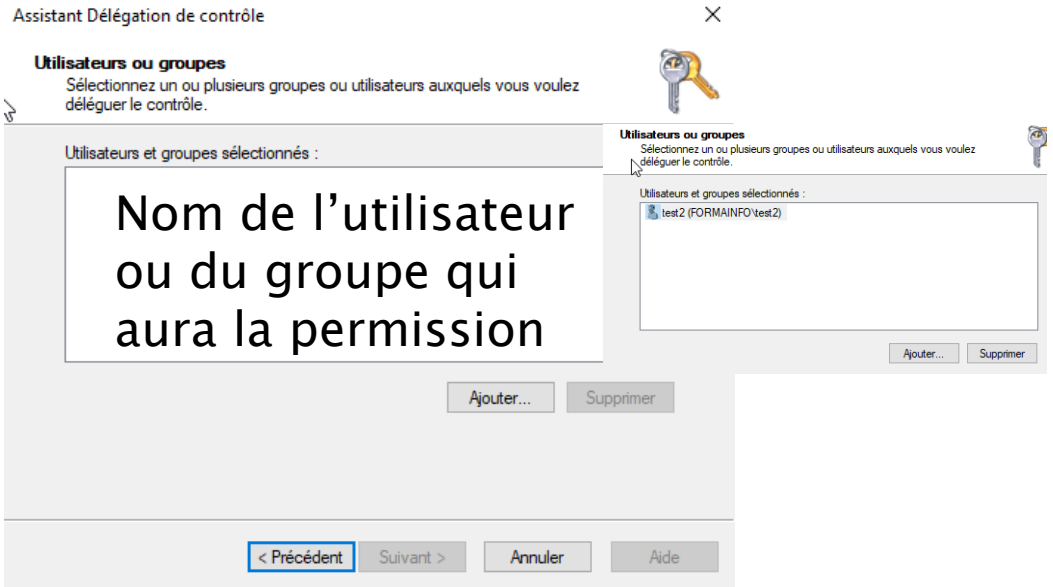
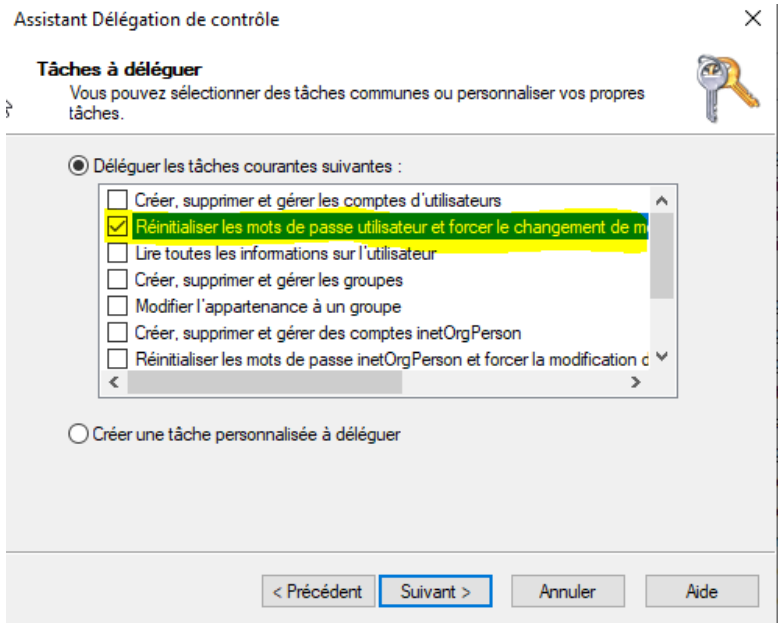




Délégation de la gestion des paramètres de mot de passe

- Il est possible de déléguer la gestion des paramètres de mot de passe à un utilisateur ou à un groupe d'utilisateur





Délégation de la gestion des paramètres de mot de passe