Sommaire

Prérequis minimum

- Pour l'installation d'un , les prérequis sont les mêmes que pour l'installation de Windows Serveur 2016.
- Cependant, attention à prendre en compte la taille de votre domaine, ainsi que le nombre d'utilisateur ou d'ordinateur qui viendront s'ajouter sur ADDS.)

- CPU : Minimum: 1.4 GHz 64-bit
- Mémoire vive : 2048Mo (512Mo en version core)
- 32Go d'espace disque
- Une connexion réseau

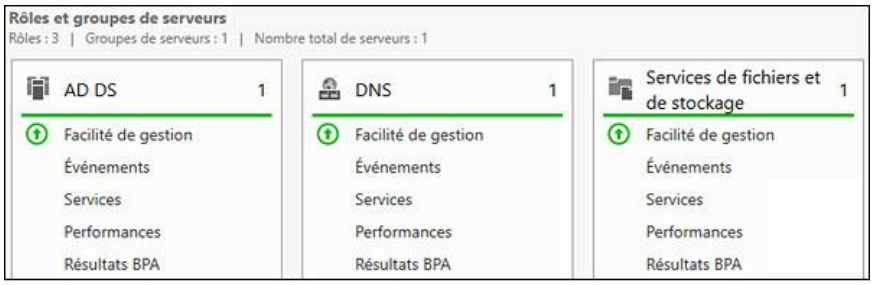
Installer Active Directory sur Windows Server 2016

- Cette opération consiste à transformer un simple système en serveur de domaine Active Directory pour qu'il devienne le premier contrôleur de domaine (DC)

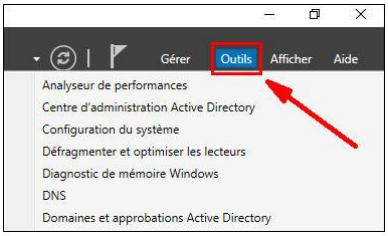
1. **ouvrir une session en Administrateur local** ou avec un compte qui fait partie des administrateurs locaux du serveur.
2. Dans le **Gestionnaire de serveur** « **Ajouter des rôles et des fonctionnalités** » .
3. Choisir « **Installation basée sur un rôle ou une fonctionnalité** » .
4. Choisir la bonne machine dans le pool de serveurs.
5. Cocher le rôle « **Services AD DS** » pour Active Directory Domain Services.
6. Valider aussi l'**ajout de rôles et de fonctionnalités complémentaires**, requises pour l'installation de ADDS.
7. L'écran suivant permet d'ajouter des fonctionnalités, cliquer sur **Suivant**.
8. Vérifier le résumé de l'installation et cliquer sur « **Installer** » pour démarrer l'opération.
9. En laissant l'écran ouvert, à la fin du processus, on peut lire « Configuration requise. Installation réussie sur SERVEUR » et surtout la ligne « **Promouvoir ce serveur en contrôleur de domaine** » : c'est sur cette phrase qu'il faut cliquer pour convertir le serveur en contrôleur de domaine du réseau.

Installer Active Directory sur Windows Server 2016

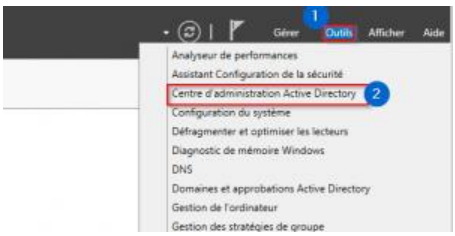
- La connexion à Windows doit maintenant se faire sur le domaine pour utiliser le compte Administrateur du domaine. Utiliser le mot de passe du compte Administrateur créé lors de l'installation de Windows Server 2016.



Outils d'administration



Centre d'administration (ADAC)

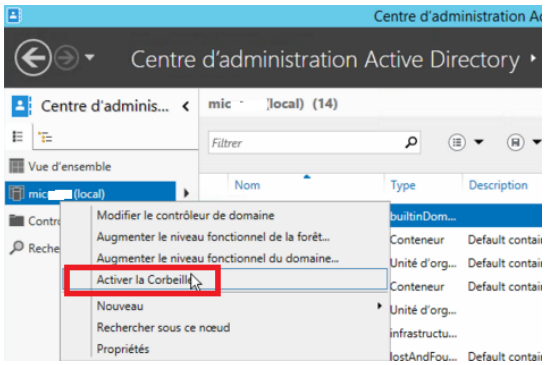


- Corbeille ActiveDirectory
- Stratégie de mot de passe affinée
- Visionneuse de l'historique de PowerShell de Windows

Windows 2016 server : Active directory

Gestion de la corbeille

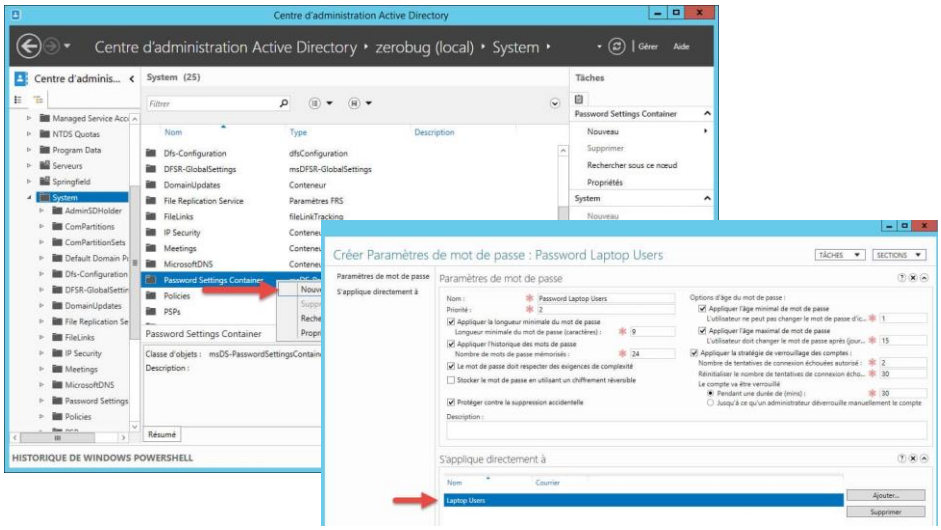
- Pour activer la corbeille le niveau fonctionnel de votre Active Directory doit être au minimum à Windows Server 2008 R2.
- L'activation de la corbeille est irrémédiable
- Après avoir activé la corbeille pensez à sauvegarder votre Active Directory car les sauvegardes précédentes ne sont plus utilisables
- La taille de la base Active Directory va grandir plus vite



Windows 2016 server : Active directory

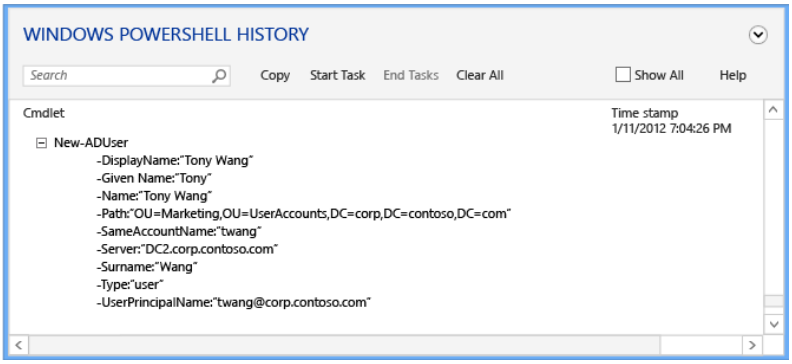
Stratégie de mot de passe affinée

- pour spécifier plusieurs stratégies de mot de passe et appliquer des restrictions de mot de passe et des stratégies de verrouillage de compte différentes à des ensembles différents d'utilisateurs au sein d'un même domaine.



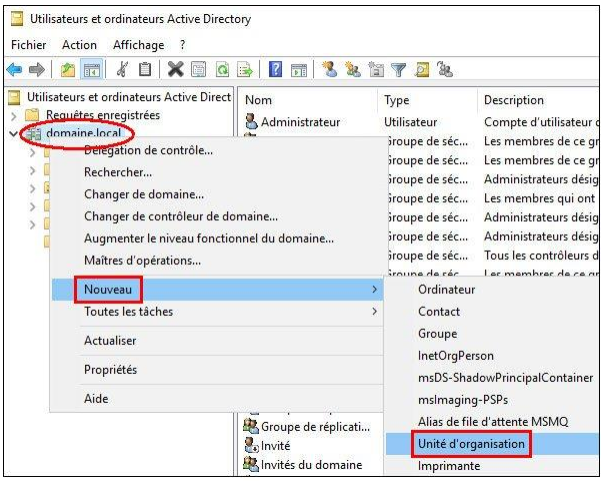
Visionneuse de l'historique de PowerShell

- Le centre d'administration Active Directory fournit désormais un historique complet de toutes les applets de commande Windows PowerShell qu'il s'exécute et leurs arguments et leurs valeurs.
- Vous pouvez copier l'historique de l'applet de commande ailleurs pour étude ou modification et réutilisation.
- Vous pouvez créer des tâche pour isoler des tâches du centre d'administration
- Vous pouvez filtrer l'historique pour trouver des points d'intérêt.



Créer les comptes utilisateurs du domaine

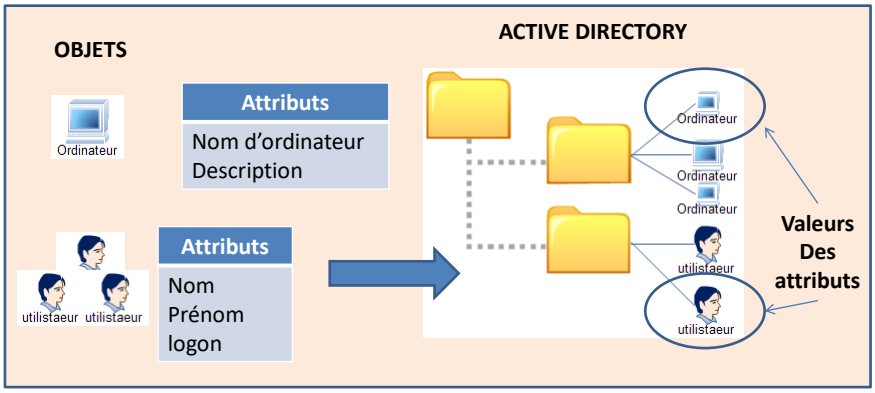
- clic droit sur le nom du domaine, Nouveau, Unité d'organisation.



Windows 2016 server : Active directory

Les comptes utilisateurs : définition

- **Authentifie l'identité d'un utilisateur.**
- **Autorise ou refuse l'accès aux ressources de domaine.**



Windows 2016 server : Active directory

Utilisateur local et de domaine

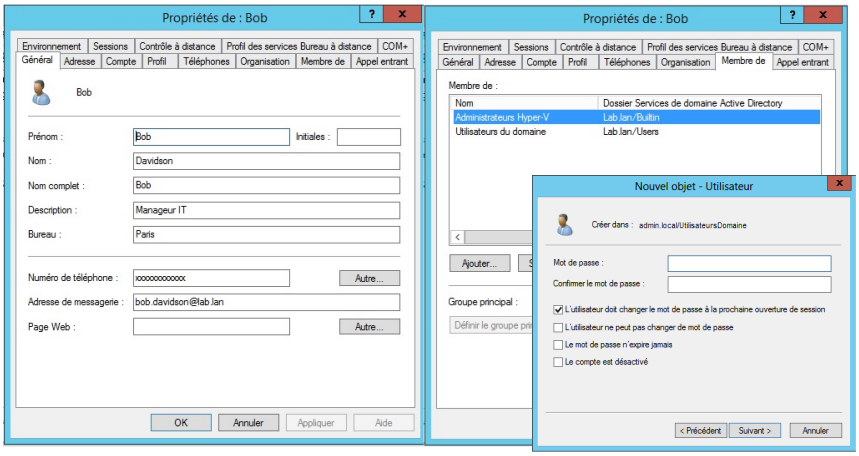
- **Les utilisateurs : types de comptes**

- **utilisateur local** :
  - permet d'ouvrir une session localement
  - et d'accéder uniquement aux ressources de l'ordinateur
- stockés dans la SAM locale
- fichier chargé au démarrage de la machine

- **utilisateur de domaine Active Directory** :
- Sur un contrôleur de domaine les comptes sont stockés
- dans le fichier NTDS.DIT

Les comptes utilisateurs : création

- Autoriser ou refuser l'autorisation
- Accordez l'accès à des processus et des services
- Gérer l'accès aux ressources



Les profils

Stocke tout un ensemble de paramètres et de données

- Le bureau
- Les paramètres d'affichage
- Les raccourcis
- Le paramétrage d'Internet Explorer.
- Les fichiers temporaires.
- Les répertoires utilisateurs
- Etc…

- Lorsque l'utilisateur se logue
- son profil est chargé
- il retrouve son environnement

Les profils itinérants et les profils obligatoires

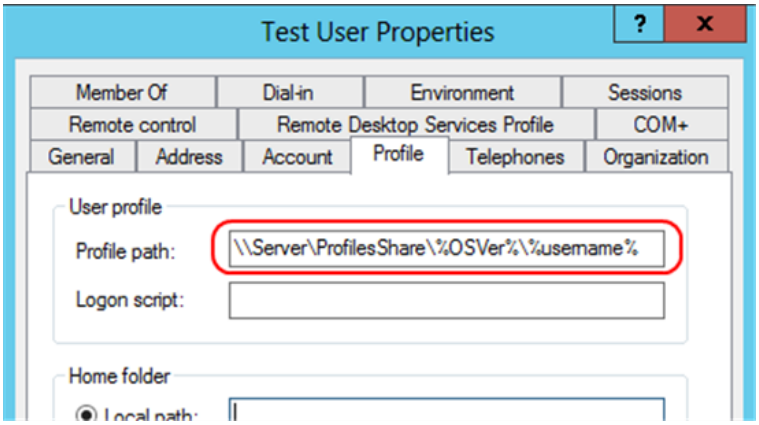
Les profils itinérants (Roaming) **:**

- stockés sur un partage réseau
- défini au niveau du domaine Active Directory

Les profils obligatoires (Mandatory)**:**

- profils en lecture seule
- Pendant sa session, l'utilisateur pourra cependant modifier son environnement mais ses changements ne seront pas sauvegardés.

Paramétrage d'un profil



Privilèges d'exécution

Au login l'utilisateur se voit attribué un jeton d'authentification (token) contenant :

- l'identifiant de sécurité (SID)
- le ou les SID des groupes auxquels appartient cet utilisateur
- un SID de session (logon SID) qui sert à identifier la session de l'utilisateur
- la liste des privilèges de l'utilisateur
- l'identification de la source du jeton (Session Manager, LAN Manager, RPC Server, ...)

Droit et privilège

- Un **droit** est appliqué à un objet d'une arborescence
(fichier, répertoire, clé de registre... lecture, d'écriture, d'exécution,,,)

- Un **privilège** concerne une opération spécifique possible sur le noyau ou le système.

Comptes de groupes : présentation

Groupe : objets d'annuaire
- ensemble de comptes d'utilisateurs et d'ordinateurs
- de contacts
- et d'autres groupes
- qui peuvent être gérés comme une seule unité

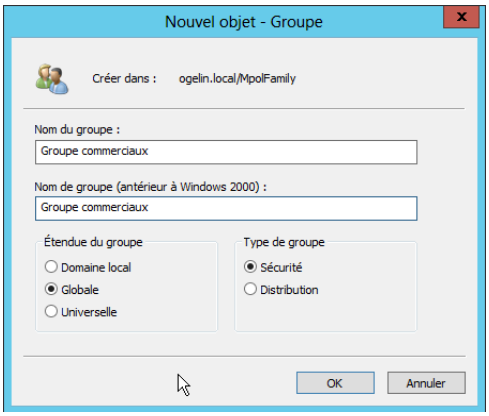
Comptes de groupes : présentation (suite)

- **Présentation des comptes de groupes**

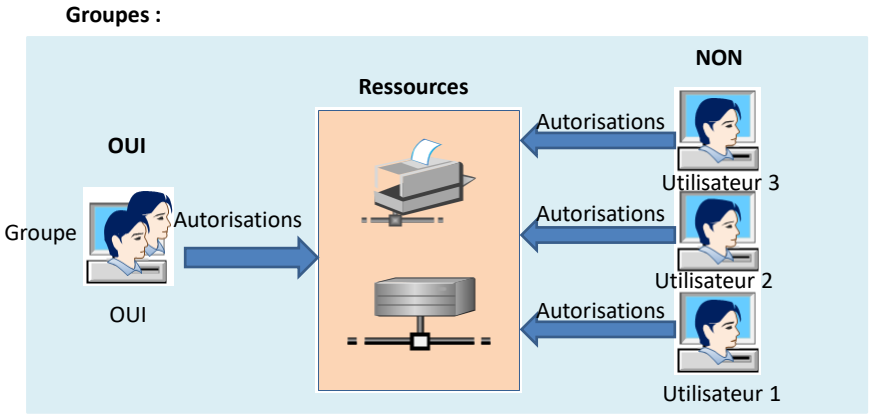
- **groupes de sécurité** créés automatiquement lorsque à la création un domaine Active Directory (ex Admins)
- Un jeu de droits d'utilisateur qui autorise les membres d'un groupe à effectuer des actions spécifiques dans un domaine est affecté automatiquement à de nombreux groupes par défaut
- Leur étendue de groupe et type de groupe ne peuvent pas être modifiés

Les types de groupes

- les groupes de distribution : pour créer des listes de distribution électronique
- les groupes de sécurité : pour affecter des autorisations à des ressources partagées



Le Centre d'administration Active Directory



- **le groupe de sécurité** : Ce type permet de gérer la sécurité pour l'accès et l'utilisation des ressources de votre réseau.
- **le groupe de distribution**. Ce type permet simplement de gérer des listes de distribution d'e-mails dans un serveur de messagerie.

Emplacement de création des groupes

Dans AD DS, les groupes sont créés dans des domaines

un groupe est aussi caractérisé par son étendue. L'étendue d'un groupe détermine les informations suivantes :

- Le domaine à partir duquel les membres sont ajoutés
- Le domaine dans lequel les droits et les autorisations affectés au groupe sont valides

Trois étendues de groupe

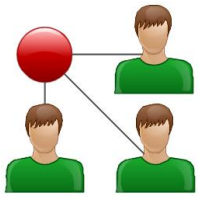
Les groupes sont caractérisés par une étendue
qui identifie le degré d'application du groupe dans la forêt ou l'arborescence de domaine

- **groupe global**
- **groupe de domaine local**
- **groupe universel**

Les Groupes de domaines locaux

permettent de définir et de gérer l'accès aux ressources dans un seul domaine

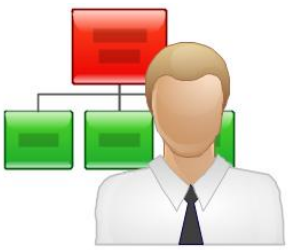
Ces groupes peuvent contenir les membres suivants :



- **Groupes à étendue globale**
- **Groupes à étendue universelle**
- **Comptes**
- **Autres groupes à étendue de domaine local**
- **Une combinaison des éléments ci-dessus**

Les Groupes de domaines locaux (suite)

- peuvent inclure d'autres groupes et comptes provenant uniquement du domaine où le groupe est défini.
- Les membres de ces groupes peuvent recevoir des autorisations
- dans n'importe quel domaine de la forêt.



- Pour gérer des objets d'annuaire qui nécessitent une maintenance quotidienne (comptes utilisateurs, imprimantes)
- Les groupes à étendue globale ne sont pas répliqués à l'extérieur de leur propre domaine

Les groupes universels

- peuvent inclure d'autres groupes et comptes provenant des domaines de la forêt ou de l'arborescence de domaine

- pour consolider les groupes qui s'étendent sur plusieurs domaines
- Tout changement apporté à l'appartenance de ce type de groupe entraîne la réplication de l'appartenance entière du groupe vers chaque catalogue global de la forêt

La création des objets avec Powershell

- Fichier CSV et un script pour alimenter un AD

```
Import-Module ActiveDirectory
$path = Split-Path -parent $MyInvocation.MyCommand.Definition
$ou = "OU=users,OU=demo,DC=demo1,DC=local"
$upnsuffix = "@test1.local"
$securepwd = ConvertTo-SecureString "Pass/123" -AsPlainText -Force
Import-Csv "$path\adusers.csv" | New-ADUser `
    -Name {$_.GivenName+" "+$_.Surname} -Path $ou `
    -DisplayName {$_.GivenName+" "+$_.Surname} `
    -UserPrincipalName {$_.SamAccountName+$upnsuffix} `
    -AccountPassword $securepwd -Enabled $true
```

Script utilisant Select-Object

```
Import-Module ActiveDirectory
$path = Split-Path -parent $MyInvocation.MyCommand.Definition
$ou = "OU=users,OU=demo,DC=demo1,DC=local"
$upnsuffix = "@demo1.local"
$securepwd = ConvertTo-SecureString "Pass/123" -AsPlainText -Force
Import-Csv "$path\adusers.csv" | Select-Object *,
    @{Name="Name"; Expression={$_.GivenName+" "+$_.Surname}},
    @{Name="Path"; Expression={$ou}},
    @{Name="DisplayName"; Expression={$_.GivenName+" "+$_.Surname}},
    @{Name="UserPrincipalName";
Expression={$_.SamAccountName+$upnsuffix}},
    @{Name="AccountPassword"; Expression={$securepwd}},
    @{Name="Enabled"; Expression={$true}} | New-ADUser
```