



Active Directory

Le 08/02/2021

PARIS Jean

MAILLARD Rémy

Sommaire

Explication

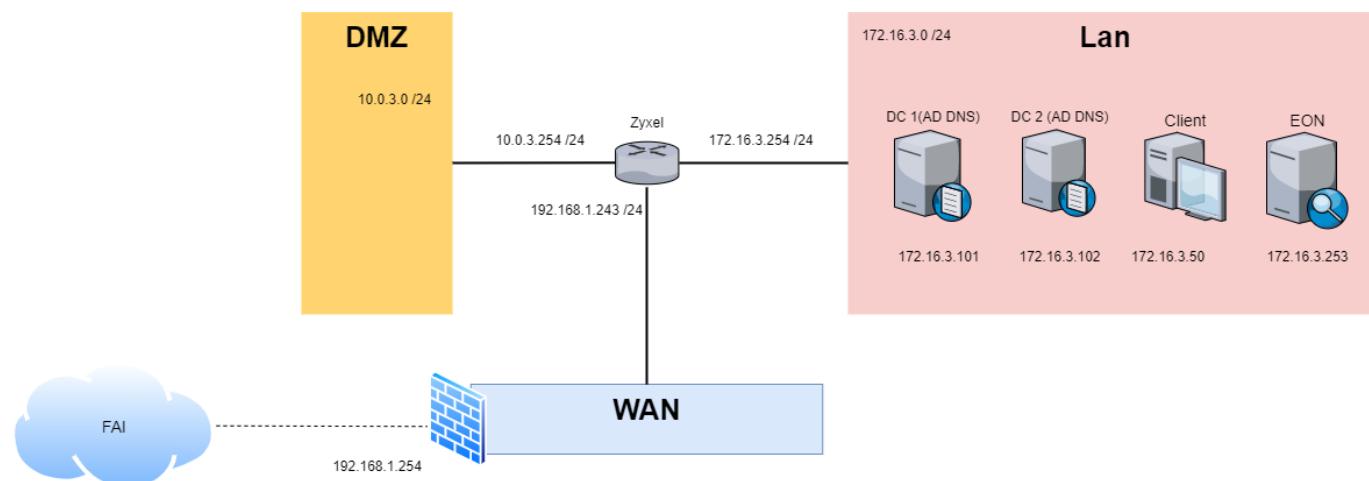
Test



Table des matières

Visio de l'infrastructure (mission 3)	2
I] Active Directory :	3
Le rôle d'un AD :	3
II] Installation et création de la forêt	3
Installation :	3
Configuration :	4
Les groupes et users :	5
Les profils (Itinérants)	7
Les types de profils :	7
1]Création du fichier partagé sur le SDF :	8
2] Configuration du chemin du profil :	9
Test profil :	10
Redondance de l'AD :	11
Stratégies de groupes (GPO) :	12
III] Tests	17

Visio de l'infrastructure (mission 3)





I] Active Directory :

Le rôle d'un AD :

Un active directory est un service s'appuyant sur un annuaire LDAP, permettant de faire de la gestion de session, de mettre en place de la sécurité et d'appliquer des stratégies de groupes (GPO) sur des UO (Unité d'Organisation). Il en existe une infinité comme la stratégie de mot de passe, stratégie de fond d'écran

II] Installation et création de la forêt

Installation :

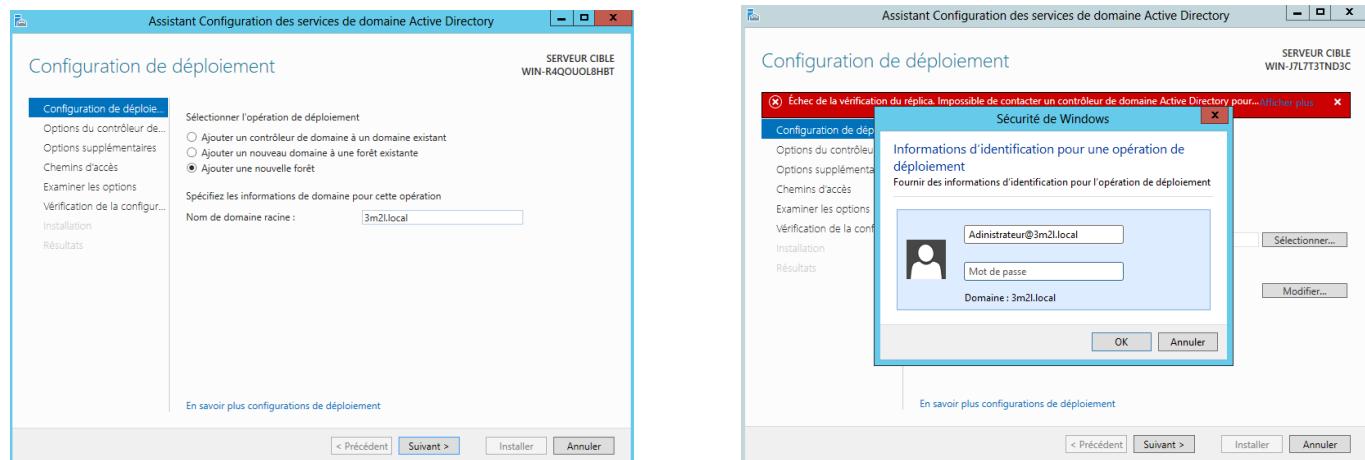
Tuto expliquant l'installation du service AD sur un Windows server :

<https://techexpert.tips/fr/windows-fr/installation-dactive-directory-sur-windows-server/#:~:text=Ouvrez%20l'application%20Server%20Manager,le%20bouton%20Ajouter%20des%20fonctionnalit%C3%A9s.>



Configuration :

Pour la mise en place de l'Active Directory nous devons créer une nouvelle forêt car il n'y en a pas encore d'existante. On indique le domaine racine c'est-à-dire sur quel domaine la forêt va s'appuyer : le domaine 3m2l.local



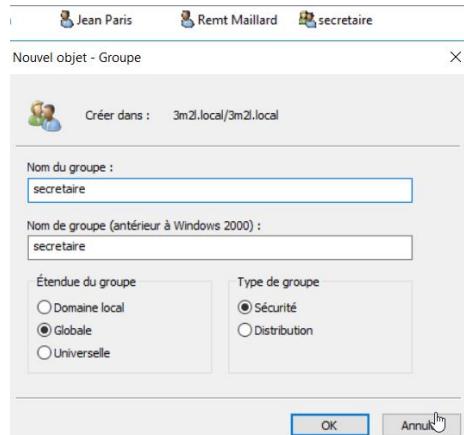
Afin de rallier notre AD au domaine nous devons avoir l'autorisation d'un Domain Controller, c'est celui qui dispose des droits d'entrée dans le domaine. Administrateur@3m2l.local mdp : Admin123\$



Les groupes et users :

Afin de gérer nos utilisateurs il faut déjà les créer et les renseigner dans des groupes pour faciliter la compréhension et gérer les droits plus facilement : on définit les droits à un groupe et non à chaque user. Dans notre cas nous allons créer des groupes par secteur dans l'entreprise.

ex : secrétaire, commercial, technicien ...

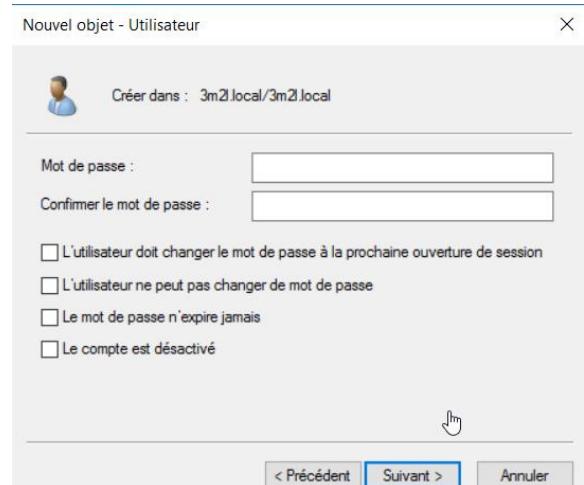
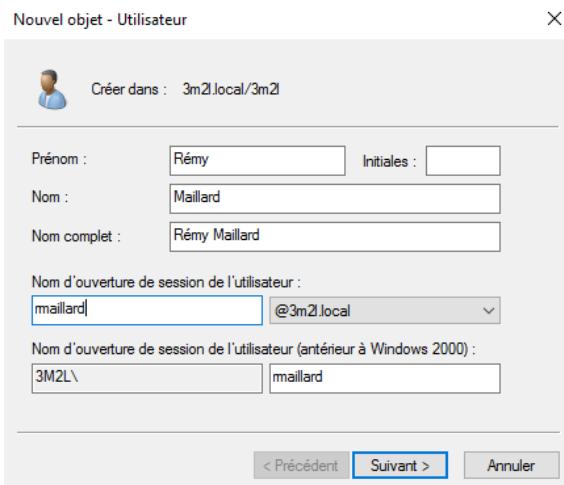


Le groupe « secrétaire » maintenant présent nous allons créer nos users (nouveau > utilisateurs).

Comme dans notre architecture nous créons que quelques utilisateurs, nous faisons le tout à la main mais à savoir que dans un contexte d'entreprise comportant un grand nombre d'employés, il est plus intéressant d'automatiser la création de ces utilisateurs à l'aide d'un scrypt PowerShell comme nous avons fait en début d'année.

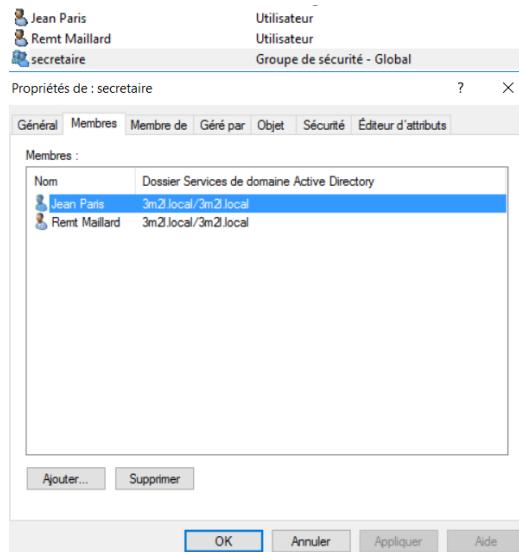
Un exemple d'utilisateur créé :

Le mot de passe des users sera « Admin123\$ » afin de le retenir plus facilement. Il est également possible de définir une stratégie de mot de passe directement depuis la création du user.





Une fois les users créés, il faut les placer dans les groupes. Afin de se faciliter la tâche il est plus intéressant de faire par le biais du « drag and drop » (glisser déposer) qu'on active dans « affichage » et en activant « utilisateurs, contacts et ordinateurs en tant que conteneurs ».



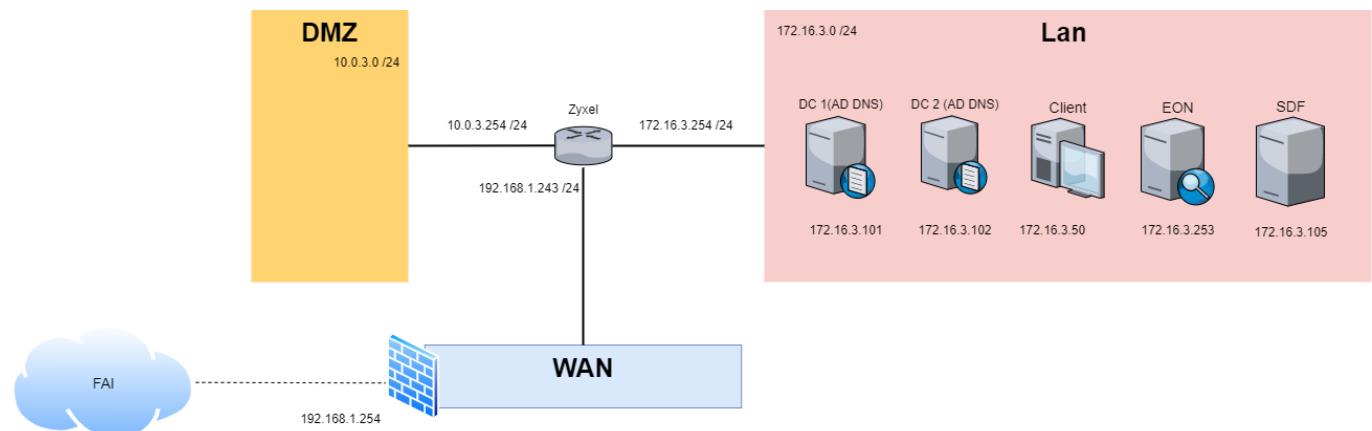
Les profils (Itinérants)

Les types de profils :

Il existe plusieurs types de profils :

- Profil **local** : chargé localement sur la machine
- Profil **itinérant** = stocké dans un fichier partagé sur un serveur (il y a une copie en local).
- Profil **temporaire** = lorsque le profil itinérant ne peut être chargé. Une fois la session fermée toutes les données seront supprimées.
- Profil **Obligatoire** = On définit un profil à l'utilisateur (par exemple si on met un fond d'écran et que l'on éteint l'ordinateur, il se rallumera avec un bureau vierge).

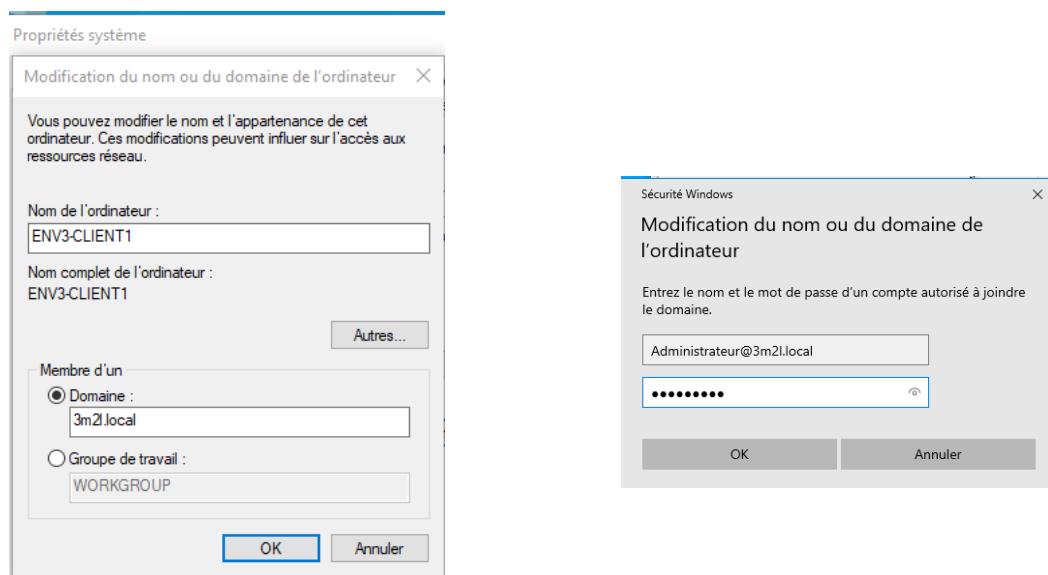
Pour mettre en place nos profils itinérants, on rajoute à notre infrastructure un Serveur De Fichier pour qu'il puisse stocker les profils.



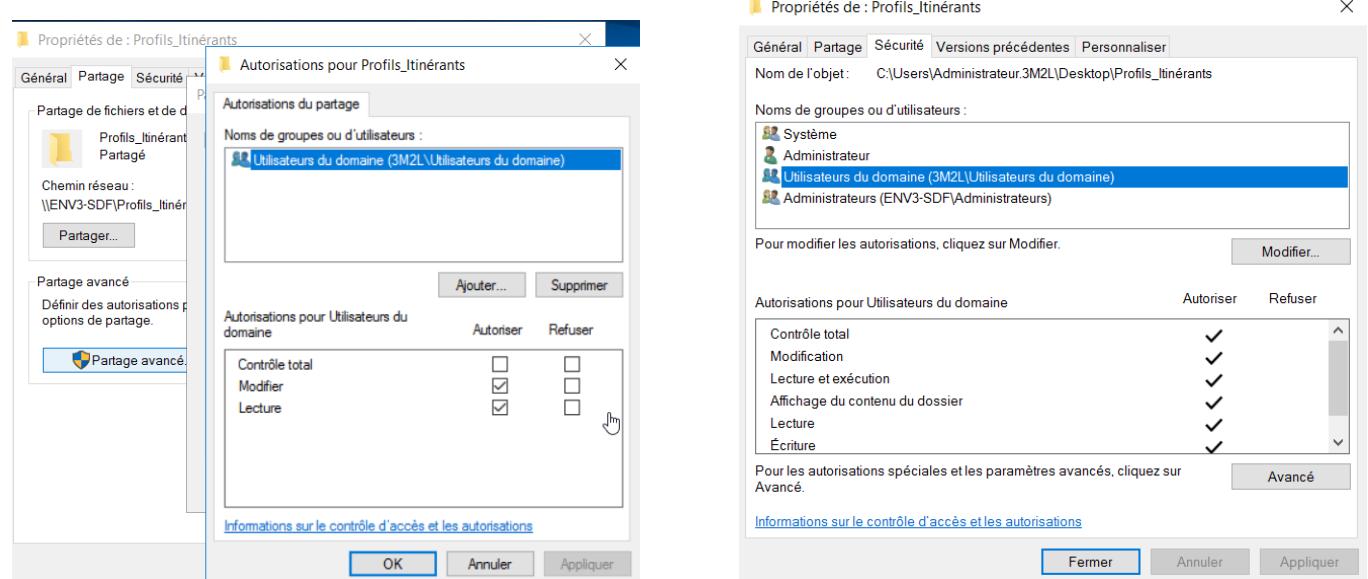


1]Création du fichier partagé sur le SDF :

La première étape est de mettre le serveur de fichier dans le domaine 3m2l.local pour qu'il puisse gérer la sécurité de partage et les droits d'écriture.



La 2^e étape est de mettre en place la sécurité. On autorise les utilisateurs du domaine à accéder au dossier partagé et on autorise également le fait qu'il puisse écrire dessus pour y mettre le contenu de leur profil.



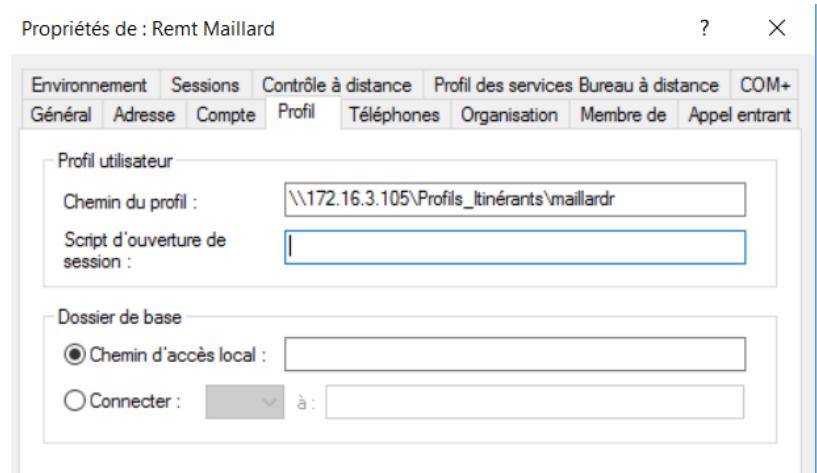


2] Configuration du chemin du profil :

Définir le chemin de profil permet de définir où sera stocké le contenu du profil. Ici on définit que le profil contenu dans le dossier maillardr sera stocké dans le dossier partagé « Profils_Itinérants » sur le serveur de fichier. Afin de ne pas rajouter à la main à chaque fois le nom du fichier qui devra être créé, on peut sélectionner tout nos users et dans le chemin du profil inscrire :

« \\172.16.3.105\Profils_Itinérants%\username% »

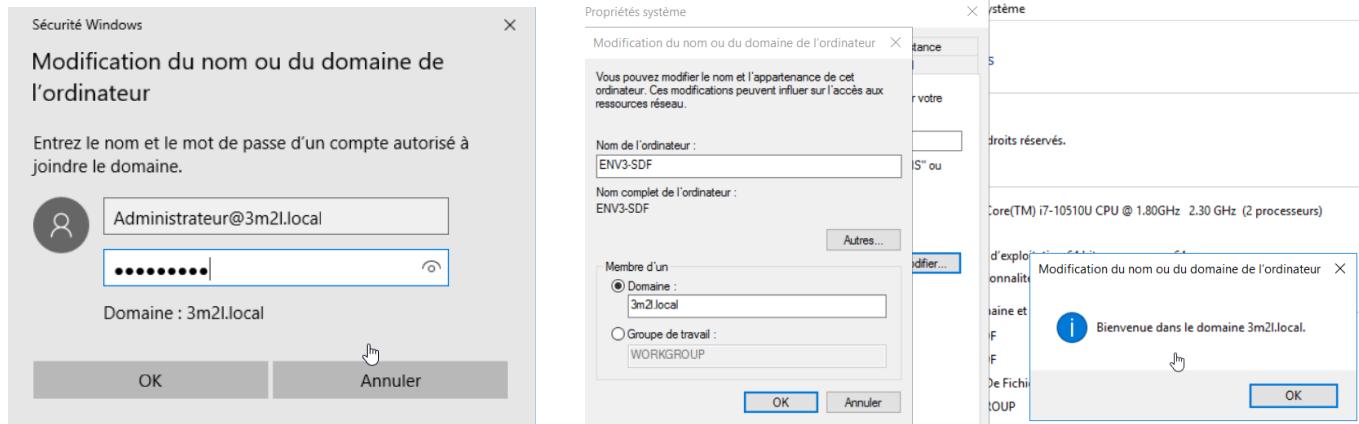
Ainsi le « %username% » remplacera automatiquement par le nom du profil correspondant.



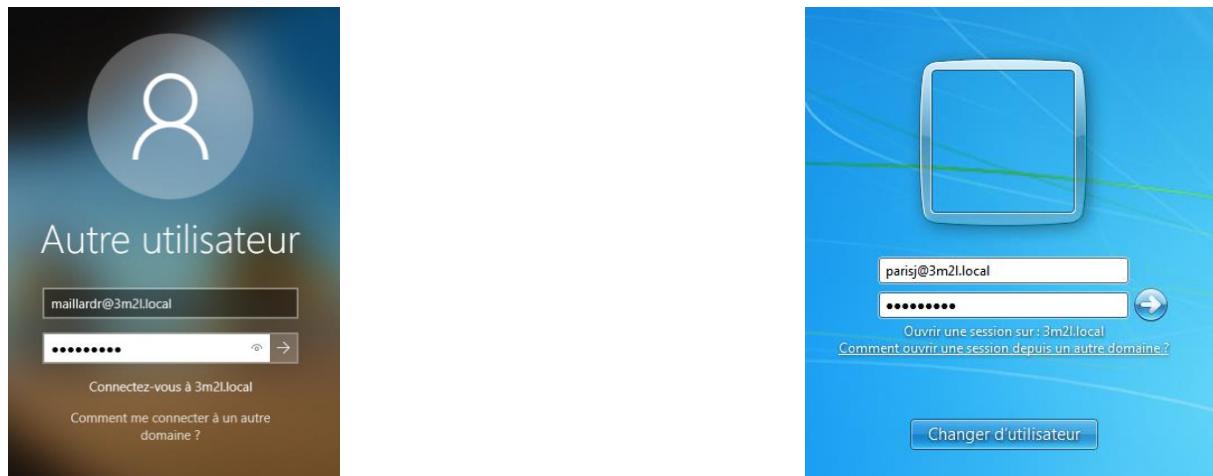


Test profil :

Afin de tester si notre profil arrive bien à charger il faut d'abord inscrire l'hôte dans le domaine pour qu'il comprenne qu'il doit charger le profil depuis le domaine et non en local.



Peut importe si le profil est chargé sur un Windows 10 ou Windows 7 le résultat doit être le même. Les Login et Mots de passes sont ceux que nous avons ajouté lors de la création des users.





Pour vérifier si le profil s'est bien chargé depuis le serveur de fichier, on doit voir le dossier du profil sur le dossier partagé. Le dossier du profil est créé lors de sa première connexion.

The screenshot shows a Windows File Explorer window with the title bar 'Profils_Itinérants'. The left sidebar has 'Accès rapide' with icons for Bureau, Téléchargements, Documents, Images, Ce PC, and Réseau. The main area shows a list of files and folders:

Nom	Modifié le	Type
maillardr.V6	20/03/2021 21:23	Dossier de fichiers
parisj.V2	20/03/2021 21:35	Dossier de fichiers

Redondance de l'AD :

Pour rajouter un nouveau Domain Controller il faut tout comme le serveur maître installer le service DNS en plus du service AD, celui-ci est indispensable car le service AD s'appuie sur le service DNS. Il faut donc d'abord redonner le DNS. Il est possible de configurer les 2 en même temps pour gagner du temps. Pour rajouter un domain controller il faut lors de la configuration indiquer vers quel domaine il va devoir s'appuyer, soit dans notre cas le domaine : 3m2l.local. Pour pouvoir y accéder il faut l'autorisation d'un utilisateur faisant autorité, pour cela on indique login et mot de passe du domain controller : Administrateur@3m2l.local mdp : Admin123\$

The image contains two side-by-side screenshots of the 'Assistant Configuration des services de domaine Active Directory' wizard.

Screenshot 1: Configuration de déploiement

This screen shows the 'Échec de la vérification' step. It displays a 'Informations d'identification pour une opération de déploiement' dialog box. The 'Fournir des informations d'identification pour l'opération de déploiement' section contains fields for 'Utilisateur' (Administrateur@3m2l.local) and 'Mot de passe' (Admin123\$). Below these fields is the text 'Domaine : 3m2l.local'. At the bottom are 'OK' and 'Annuler' buttons.

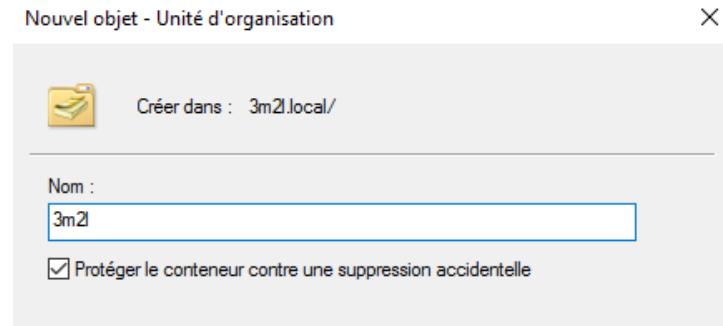
Screenshot 2: Sélectionner un domaine dans la forêt

This screen shows the 'Sélectionnez un domaine dans la forêt où le nouveau contrôleur de domaine résidera.' dialog box. It lists '3m2l.local' as the selected domain. At the bottom are 'OK' and 'Annuler' buttons.



Stratégies de groupes (GPO) :

Afin de mettre en place des GPOS, il faut commencer par créer nos UO (Unité d'Organisation) sur lesquelles va s'appuyer la GPO. / ! une GPO fait autorité sur une UO et non un groupe.



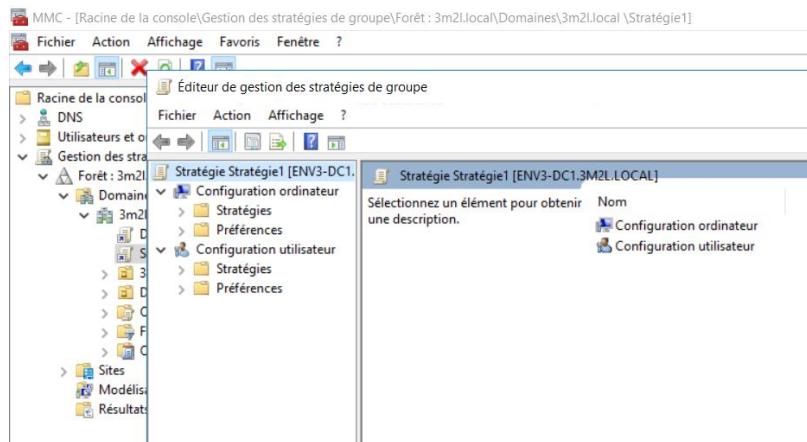
Une fois nos Unités d'organisations créées, nous devons créer notre GPO.

The screenshot shows the Windows Management Console (MMC) interface for managing Group Policy Objects (GPOs). The left pane lists various Active Directory components like DNS and User/Computer. The main pane is focused on the 'Gestion des stratégies de groupe' (Group Policy Management) under the 'Forêt : 3m2I.local' node. The 'Etat' tab is selected, providing real-time status for the domain's replication and SYSVOL (DFRS) services. A context menu is open over the '3m2I.local' domain node, offering options such as 'Créer un objet GPO dans ce domaine, et le lier ici...', 'Lier un objet de stratégie de groupe existant...', 'Bloquer l'héritage', 'Assistant Modélisation de stratégie de groupe...', 'Nouvelle unité d'organisation', 'Rechercher...', 'Modifier le contrôleur de domaine...', 'Supprimer', 'Utilisateurs et ordinateurs Active Directory...', 'Affichage', 'Nouvelle fenêtre à partir d'ici', 'Nouvelle vue de la liste des tâches...', 'Actualiser', 'Propriétés', and 'Aide'.



Il existe 2 types de GPO :

- Les stratégies d'ordinateurs : Se portent sur l'ordinateur peu importe l'utilisateur.
- Les stratégies d'utilisateurs : Se portent sur l'utilisateur peu importe l'ordinateur du domaine utilisé.
- On peut également voir des stratégies qui se portent sur les 2 objets présentés juste avant mais souvent on essaye de les dissocier au maximum



Pour notre part on va mettre en place une GPO consistant à charger des pages définies sur chrome au chargement de l'application. Pour cela il faut d'abord télécharger les modèles ADM ou ADMX qui permettent de définir les règles de Chrome. Une fois ajouté le modèle dans « ajouter ou supprimer un modèle », on peut retrouver les stratégies liées à chrome et les mettre en place.

<https://support.google.com/chrome/a/answer/187202?hl=fr#zippy=%2Cwindows>

Vous pouvez également télécharger les modèles séparément et consulter la documentation sur les règles commune à tous les systèmes d'exploitation ici : [fichier ZIP contenant les modèles et la documentation Google Chrome](#).

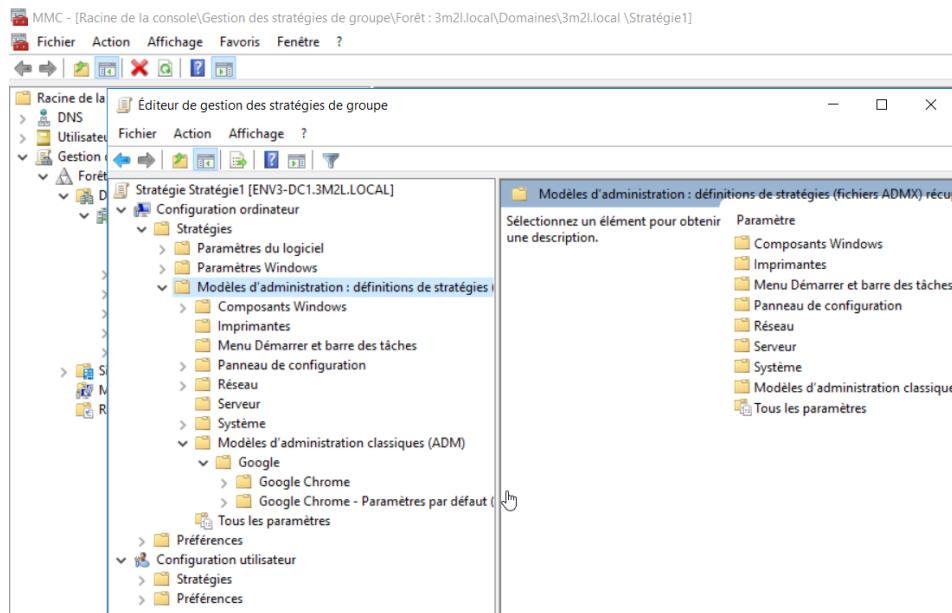
Étape 2 : Ouvrez le modèle ADM ou ADMX que vous avez téléchargé

1. Accédez à Démarrer > Exécuter : gredit.msc (ou exécutez gredit.msc sur votre terminal).
2. Accédez à Stratégie Ordinateur local > Configuration ordinateur > Modèles d'administration.
3. Cliquez avec le bouton droit de la souris sur Modèles d'administration, puis sélectionnez Ajout/Suppression de modèles.
4. Dans la boîte de dialogue qui s'affiche, ajoutez le modèle chrome.adm.
5. Une fois cette opération effectuée, le dossier "Google/Google Chrome" apparaît, s'il n'y figure pas déjà, dans la section "Modèles d'administration". Si vous avez ajouté le modèle ADM sous Windows 7 ou 10, il apparaît dans le dossier "Modèles d'administration classiques/Google/Google Chrome".

Étape 3 : Configurez les règles

Dans l'éditeur de stratégie de groupe, ouvrez le modèle que vous venez d'ajouter et modifiez les paramètres de configuration. Les règles généralement modifiées sont les suivantes :

- Set the home page (Définir la page d'accueil) : la page d'accueil est l'URL qui s'ouvre lorsqu'un utilisateur lance le navigateur Chrome ou clique sur le bouton



Pour notre stratégie nous allons activer les « actions au démarrage » et les « URL à ouvrir au démarrage ».

Démarrage, page d'accueil et page Nouvel onglet

Action au démarrage

Modifier le paramètre de stratégie

Paramètre

État

Afficher le bouton Accueil sur la barre d'outils Non configuré

Configurer l'URL de la page d'accueil Non configuré

Utiliser la page "Nouvel onglet" comme page d'accueil Non configuré

Action au démarrage Activé

URL à ouvrir au démarrage Non configuré

Action au démarrage

Non configuré Activé

Commentaire :

Pris en charge sur : Microsoft Windows 7 ou version ultérieure

Options :

Action au démarrage

Ouvrir une liste d'URL

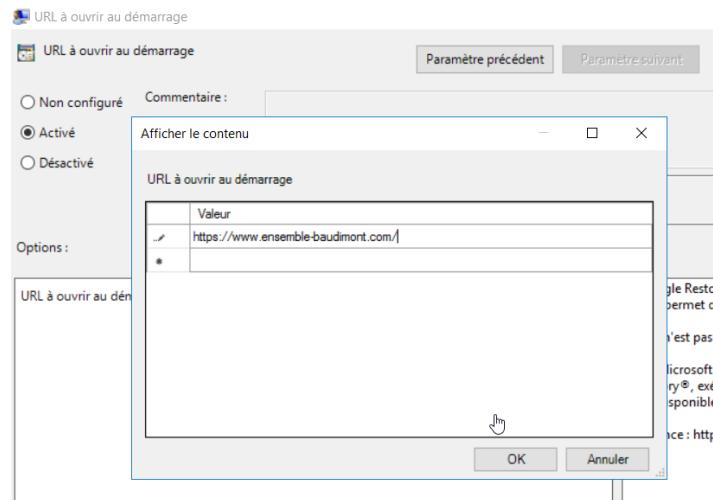
Aide :

Permet de définir le comportement du système au démarrage. Désactiver cette règle revient à ne pas la configurer, car le comportement de Google Chrome au démarrage doit être spécifié.

Si cette règle est configurée, les utilisateurs ne peuvent pas la modifier dans Google Chrome. Si elle n'est pas configurée, les utilisateurs peuvent la modifier dans Google Chrome.



On peut renseigner autant de pages à charger au démarrage que l'on veut. Dans notre exemple nous allons juste définir de charger la page de Baudimont.

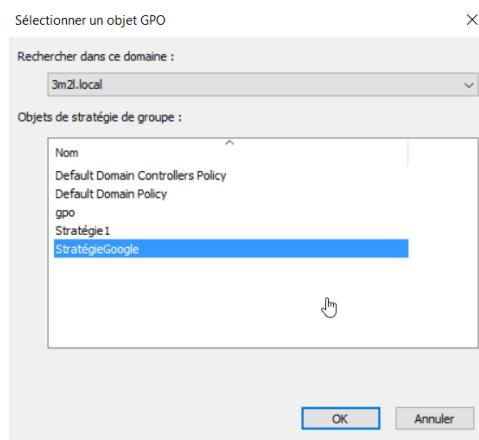


On peut voir ici l'état des stratégies afin de vérifier si les bonnes stratégies sont activées. Il en existe une infinité notamment avec google et autres applications. De ce fait il faut faire très attention avec les GPO que nous voulons mettre en place. Pour une compréhension plus simple et pour éviter toutes confusions il faut essayer de structurer au mieux notre plan de stratégie.

Paramètre	État
Afficher le bouton Accueil sur la barre d'outils	Non configuré
Configurer l'URL de la page d'accueil	Non configuré
Utiliser la page "Nouvel onglet" comme page d'accueil	Non configuré
Action au démarrage	Activé
URL à ouvrir au démarrage	Activé



Une fois notre stratégie configurée, nous devons la lier à l'objet sur lequel nous voulons faire autorité. Dans notre cas nous allons choisir notre OU qui contient notre domaine afin d'appliquer cette stratégie de pages qui se lancent à l'ouverture de chrome à l'ensemble des users du domaine.



MMC - [Racine de la console\Gestion des stratégies de groupe\Forêt : 3m2.local\Domaines\3m2.local\3m2.local\Secrétaire]

Fichier Action Affichage Favoris Fenêtre ?

Navigation icons: Back, Forward, Stop, Refresh, Home, Favorites, Help, Exit.

Ordre des liens	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO	Filtre
1	StratégieGoogle	Oui	Oui	Activé	Aucun

Racine de la console

- > DNS
- > Utilisateurs et ordinateurs Active Directory [ENV3-DC1]
- ✓ Gestion des stratégies de groupe
 - ✗ Forêt : 3m2.local
 - ✗ Domains
 - ✗ 3m2.local
 - ✗ Default Domain Policy
 - ✗ 3m2.local
 - ✗ StratégieGoogle
 - ✗ Secrétaire
 - > Domain Controllers
 - > Objets de stratégie de groupe
 - > Filtres WMI
 - > Objets GPO Starter
 - > Sites
 - ✗ Modélisation de stratégie de groupe
 - ✗ Résultats de stratégie de groupe



III] Tests

D'après le paramétrage par défaut, l'actualisation des GPO se fait toutes les 15 minutes. On peut choisir de changer cette variable afin d'éviter que tout le monde sur le réseau fasse la mise à jour en même temps. Dans ce cas nous pouvons forcer la mise à jour des GPO depuis le client pour éviter d'attendre ce laps de temps.

On utilise donc la commande « gpupdate/force » sur l'invite de commande powershell en mode administrateur. Ou encore « gpedit/force »

```
Sélection Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> gpupdate /force
Mise à jour de la stratégie...
```

Aussi, pour que nos GPO puissent se charger correctement nous devons vérifier que les dates et heures soient coordonnées.

The screenshot shows a web browser window with the following details:

- Title Bar:** Ensemble Baudimont
- Address Bar:** ensemble-baudimont.com
- Header:** Rechercher (Search), Contact | Actualités (Contact | News), Ecole Directe (School Direct)
- Logo:** Ensemble BAUDIMONT ARRAS
- Navigation:** Présentation, Nos établissements, Espace Entreprise
- Content Area:** A large image of three smiling people. Overlaid text reads: "Que chacun soit connu, reconnu, estimé et appelé à se dépasser" (Saint-Vincent de Paul).
- Call-to-Action:** Découvrez l'Ensemble Baudimont, <https://www.jpo-ensemble-baudimont.fr/>
- Cookie Consent Bar:** Nous utilisons des cookies pour vous garantir la meilleure expérience sur notre site. Si vous continuez à utiliser ce dernier, nous considérerons que vous acceptez l'utilisation des cookies. Ok
- Address Bar:** Taper ici pour rechercher
- System Icons:** Microsoft Store, Task View, File Explorer, Edge, Mail, Settings, Google Chrome.
- System Status:** 08:05, 02/04/2021