5.2 Promotion du DC « LABSRV02 »

Depuis Windows Server 2016, le mode Core est en fait le mode « **MSI : Minimal Server Interface** » de Windows Server 2012.

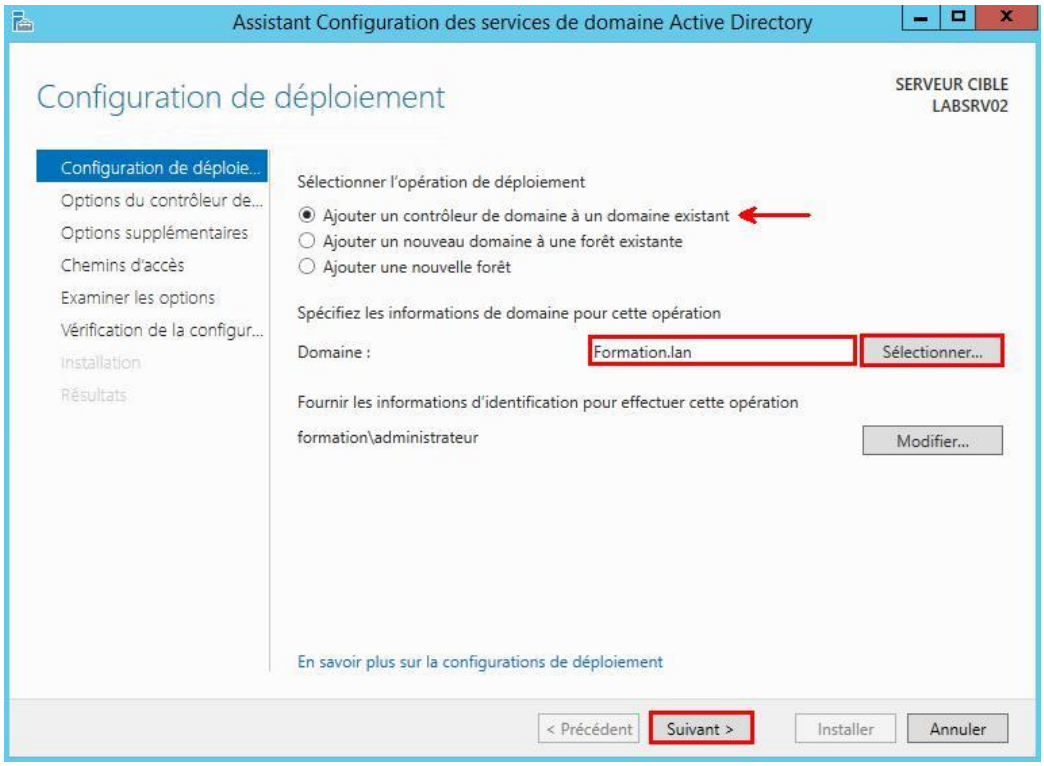
Ce mode représente une couche graphique regroupant tous les outils de gestion ainsi que certains outils du Panneau de Configuration.

Avec SCONFIG, rajoutez « **LABSRV02** » dans le domaine,
Redémarrez la machine pour finir

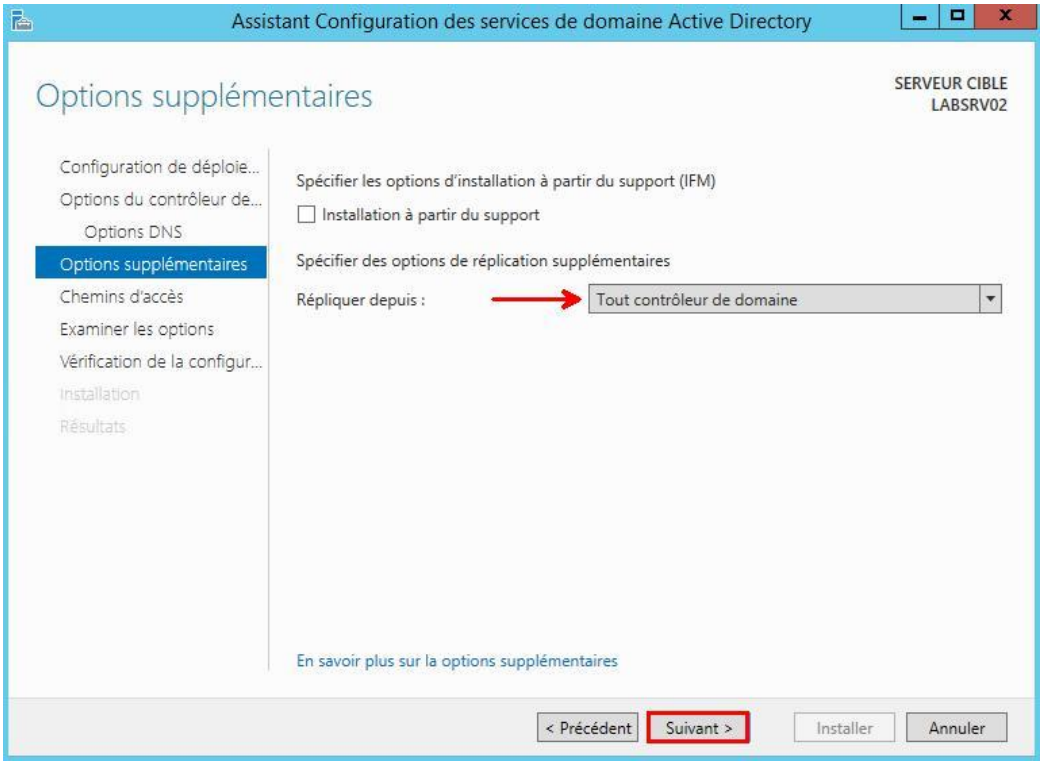
- Ouvrez le « Gestionnaire de Serveur » depuis « **LABSRV01** »

- Répétez dans LABSRV02 les mêmes actions effectuées lors du déploiement des services AD DS sur le premier serveur « **LABSRV01** »

- Quand l'assistant de promotion de DC s'ouvre, sélectionnez « **Ajouter un contrôleur de domaine à un domaine existant** » et cliquez sur « **sélectionner** » pour renseigner les identifiants du domaine et le domaine « **Formation.lan** », cliquez ensuite sur « **Suivant** » :



- Si le domaine sélectionné (formation.lan dans notre cas) est géré par plusieurs DCs, vous pouvez sélectionner un DC spécifique depuis la liste déroulante, le but ici est de préciser la source de récupération d'une copie de la base de données Active Directory ainsi que les zones DNS. Dans notre cas, un seul DC existe « **LABSRV01** », vous pouvez laisser la valeur « **Tout contrôleur de domaine** » comme source de réplication :



- Les étapes suivantes sont similaires à celles détaillées lors de la première promotion du DC « **LABSRV01** »
- Après déploiement du 2ème DC « **LABSRV02** », un redémarrage est requis
- Ouvrez une Session à l'aide du compte Administrateur du domaine Formation.lan après redémarrage et vérifiez que l'authentification fonctionne correctement.

5.3 Création des objets Active Directory

Après déploiement de notre infrastructure Active Directory, certains outils de gestion et de déploiement d'Active Directory sont installés automatiquement et disponibles depuis le dossier « **Outils d'Administration** » ou depuis l'interface Moderne (Interface UI).

Nous allons utiliser certains de ces outils pour créer la structure des OUs ainsi que les différents objets AD comme les comptes utilisateurs, ordinateurs, groupes pour organiser et gérer d'une manière efficace l'accès aux ressources de notre annuaire Active Directory.

Dans le cadre de notre LAB, nous aurons besoin des objets AD suivants :

- Compte utilisateur :
  - Il s'agit d'un compte standard qui sera utilisé pour s'authentifier sur le domaine « **FORMATION.LAN** » depuis la machine cliente du réseau « **LABWin10** » le compte sera « **UtilisateurSTD** »
- Groupe de sécurité :
  - Nous allons utiliser deux types de groupes de sécurité :
    - Groupe « **ADMINs** » : ce groupe regroupera les comptes utilisateurs « **Admins du Domaine** » ayant des privilèges et droits de modification au niveau du domaine « **FORMATION.LAN** » et des différentes machines (Serveur et poste de travail) du réseau
    - Groupe « **STANDARDs** » : ce groupe regroupera les comptes « **Standard du domaine** » pour l'authentification sur le domaine « **FORMATION.LAN** » et l'accès aux ressources du réseau
- UO (Unité d'Organisation) :
  - Les UO (ou en anglais : Organizational Unit) vont être créées et utilisées pour organiser les différents objets AD à créer
    - E.i : OU « **Serveurs** » pour stocker et organiser les Serveurs | OU « **Utilisateurs** » pour stocker et organiser les utilisateurs (**UtilisateurSTD**) et les groupes (**ADMINs & STANDARDs** » …| OU « **Ordinateurs** » pour stocker et organiser les ordinateur

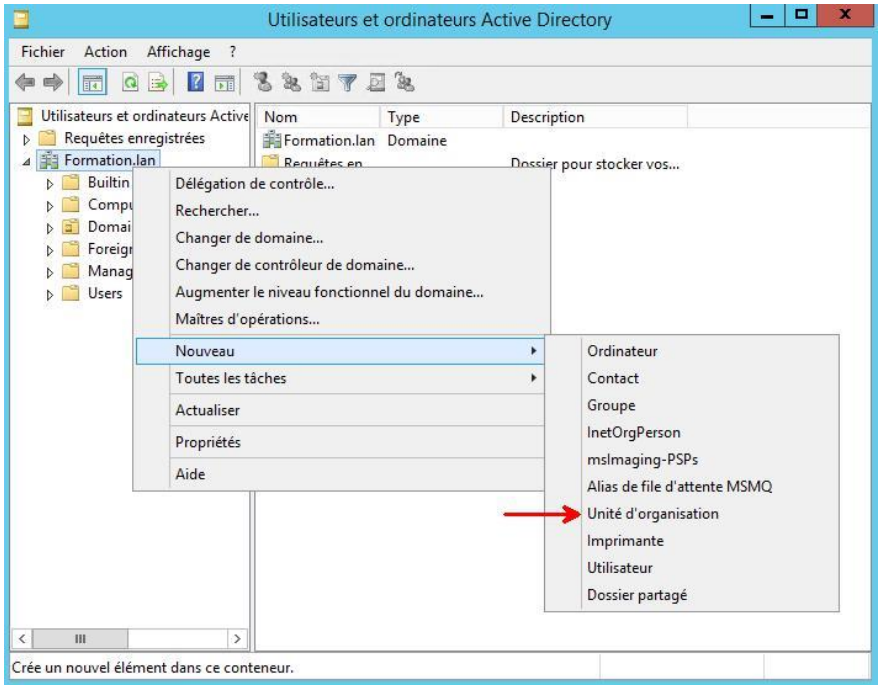
La création des objets cités ci-dessus peut se faire via différents outils (Graphiques et en Ligne de commande), notamment :

- DSA.msc (console « Utilisateurs & Ordinateurs Active Directory »)
- DSAC.exe (console « Centre d'Administration d'Active Directory »)
- DSAdd (outil en Ligne de commande de création d'objet AD)

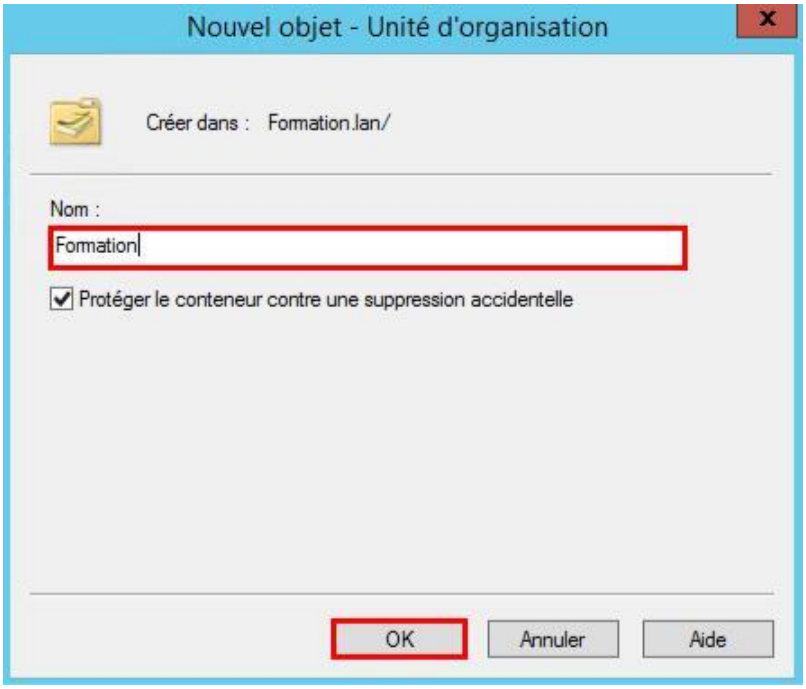
- Module PowerShell « ActiveDirectory » : module regroupant des Cmd-lets permettant de créer des objets AD : New-ADObjet | New-ADGroup | New-ADComputer…

Nous allons créer l'unité d'organisation 'mère' nommée « **Formation** », celle-ci regroupera les objets Active Directory qui seront créés par la suite.

Depuis le menu « **Outils** », ouvrez la console « **Utilisateurs & Ordinateurs Active Directory** », faites un clic droit sur le domaine « **Formation.lan** », sélectionnez « **Nouveau** » et ensuite « **Unité d'organisation** »

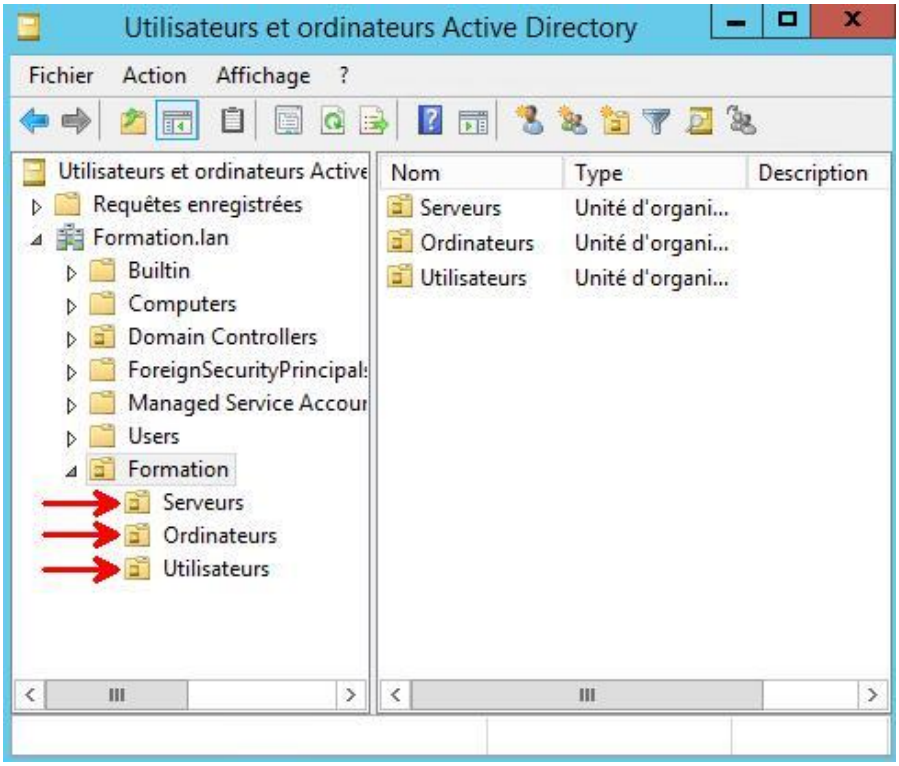


Renseignez le Nom « **Formation** » et cliquez « **OK** »



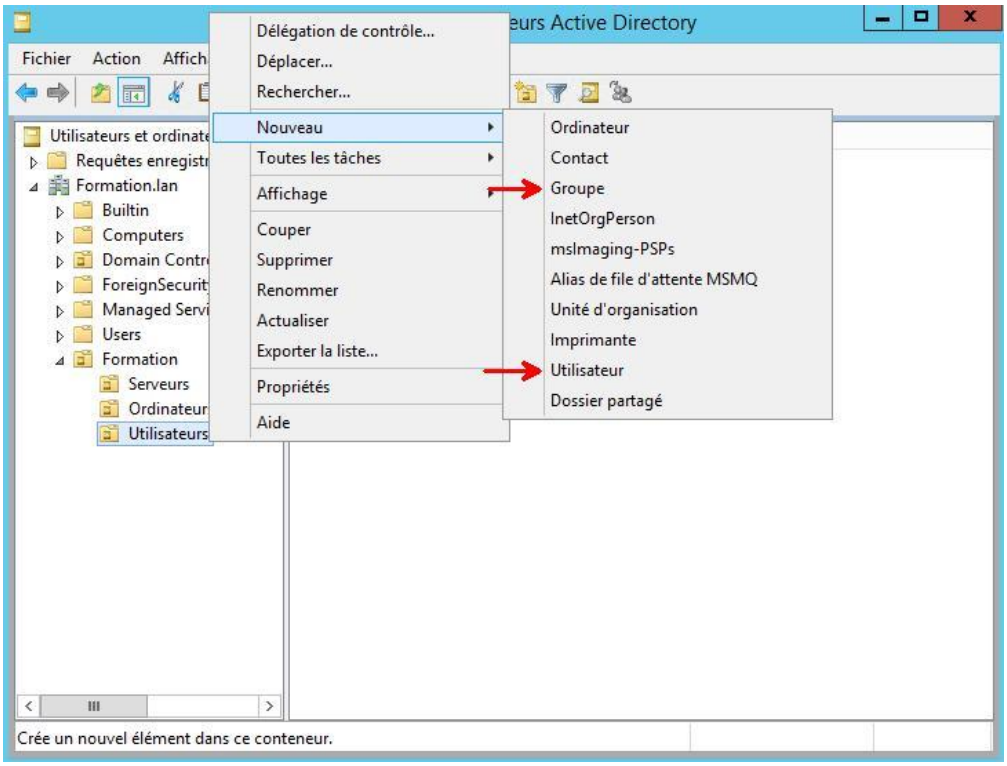
Faites un clic-droit sur l'OU créée « **Formation** » et répétez les mêmes actions effectuées précédemment pour créer les deux sous-OU suivantes :

- **Serveurs**
- **Ordinateurs**
- **Utilisateurs**

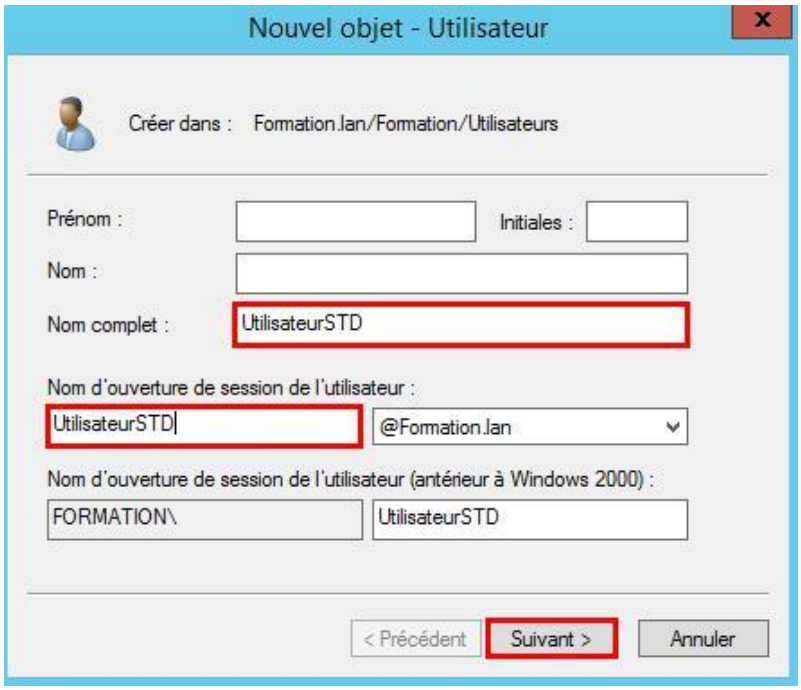


Nous allons maintenant créer l'utilisateur « **UtilisateurSTD** » ainsi que les deux groupes « **ADMINs** » et « **STANDARDs** »

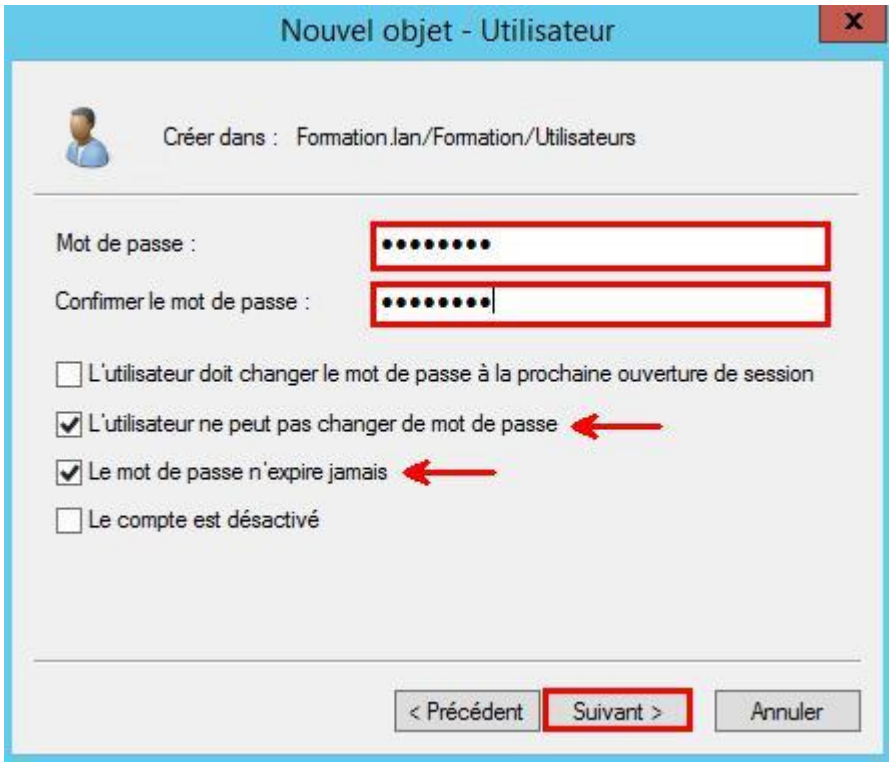
Faites cette fois un clic-droit sur l'OU « **Utilisateurs** » et sélectionnez « **Nouveau** » puis « **Utilisateur** » ou « **Groupe** »



Renseignez les informations suivantes et cliquez sur « **Suivant** »

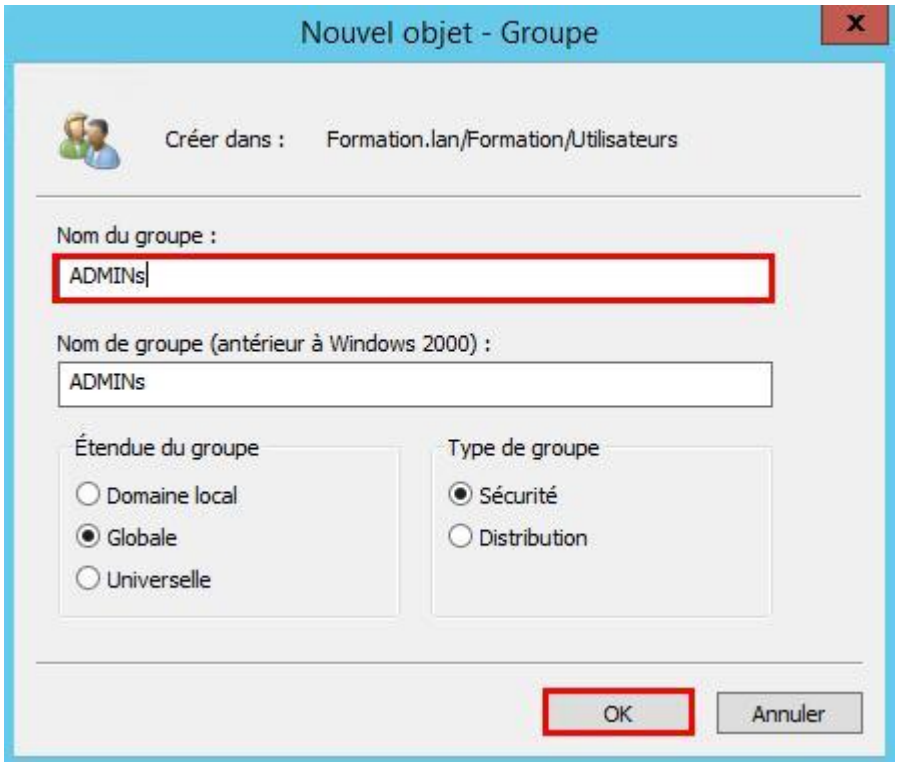


Renseignez le mot de passe, décochez « **L'utilisateur doit changer de mot de passe …** » et cochez « **l'utilisateur ne peut … passe** », « **le mot … n'expire jamais** » et cliquez sur « **Suivant** » pour continuer



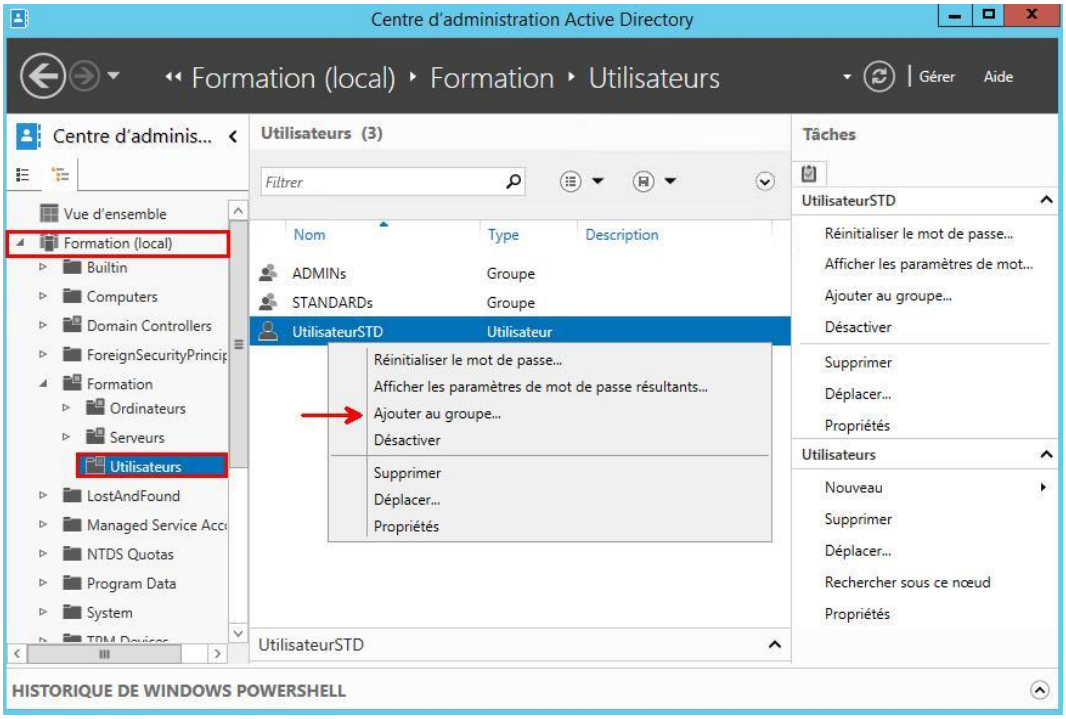
Vérifiez les informations et cliquez sur « **Terminer** »

Quant aux groupes de sécurité, renseignez le Nom « **ADMINs** » et cliquez sur « **OK** », répéter la même opération pour le groupe « **STANDARDs** »



Nous allons maintenant ajouter l'utilisateur « **UtilisateurSTD** » au groupe « **STANDARDs** »

Depuis le menu « **Outils** », ouvrez le « **Centre d'Administration Active Directory** », naviguez jusqu'à l'utilisateur « **UtilisateurSTD** », faites un clic droit et cliquez sur « **Ajouter au groupe** »



Tapez « **Standards** » et cliquez sur « **Vérifier les noms** », cliquez ensuite sur « **OK** » pour confirmer l'ajout.

Dans l'exemple suivant, nous allons ajouter le groupe « **Admins du domaine** » au groupe « **ADMINs** » à l'aide de l'outil en ligne de commande « **DSMod.exe** »

Ouvrez l'invite de commande en tant qu'administrateur et tapez la commande suivante :

DSMod group "cn=Admins du domaine,cn=Users,dc=formation,dc=lan" -addmbr "cn=ADMINs,ou=Utilisateurs,ou=Formation,dc=formation,dc=lan"

5.4 Découverte de l'outil « Centre d'Administration Active Directory »

Le Centre d'administration Active Directory repose sur la technologie de l'interface de ligne de commande Windows PowerShell. Il procure une gestion améliorée des données Active Directory et une riche interface utilisateur graphique.

Vous pouvez utiliser le Centre d'administration Active Directory pour effectuer des tâches courantes de gestion des objets Active Directory par le biais d'une navigation pilotée par les données et orientée vers les tâches.

Les tâches suivantes peuvent être réalisées via le Centre d'Administration Active Directory :

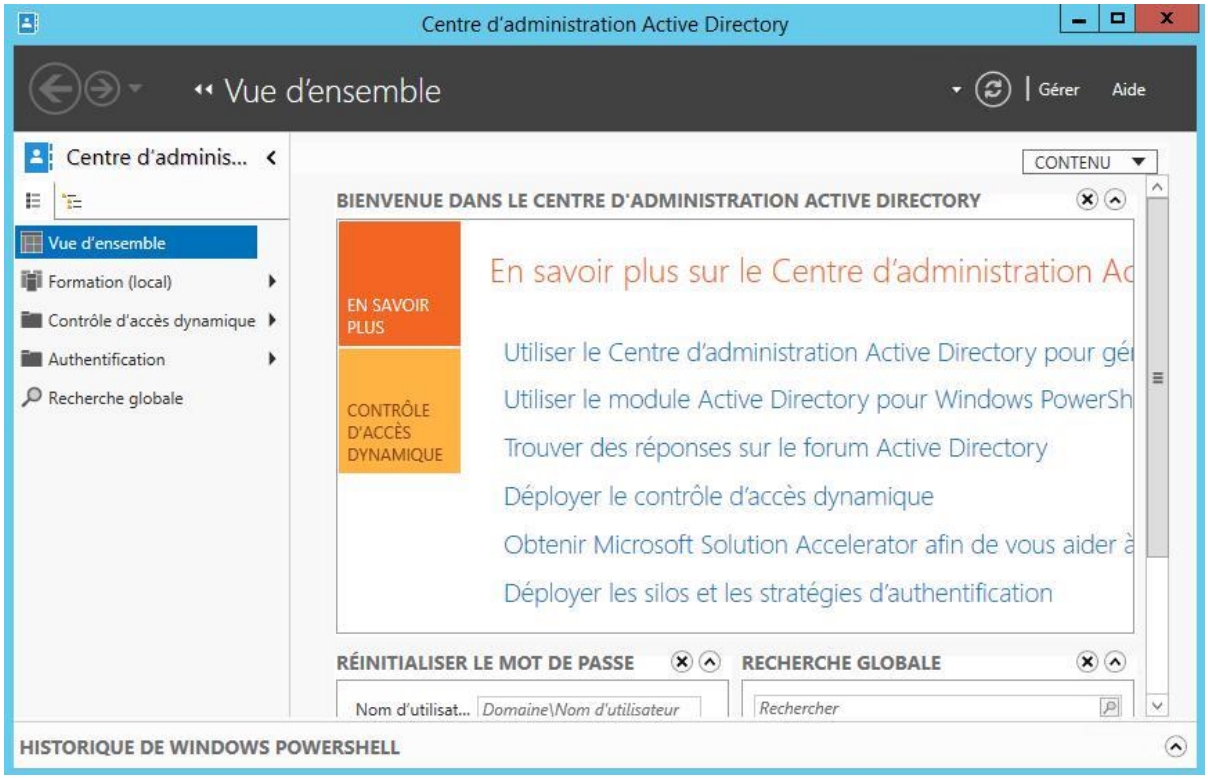
- Gestion des utilisateurs

- Gestion des groupes
- Gestion des ordinateurs
- Gestion des domaines et des contrôleurs de domaine
- Gestion des unités d'organisation
- Localisation des objets Active Directory

L'outil Centre d'Administration Active Directory peut être lancé via deux méthodes :

- Depuis le Menu « **Outils** » du Gestionnaire de Serveur
- Depuis le Menu « **Exécuter** » > **DSAC.exe**

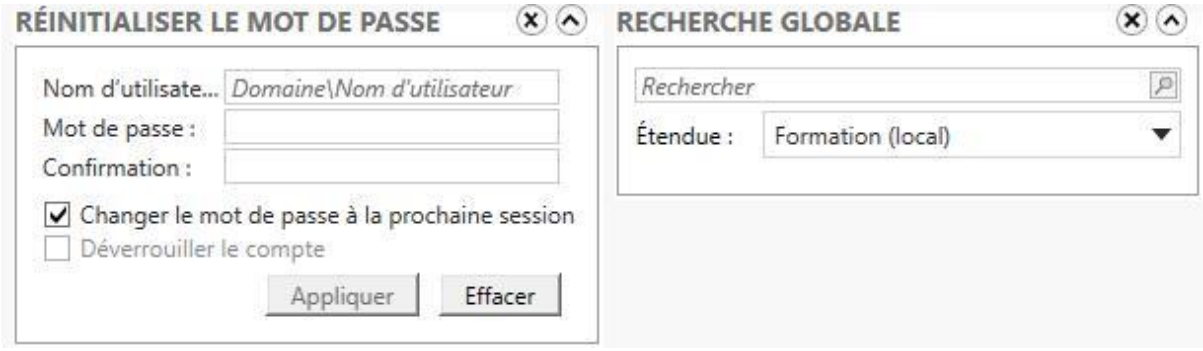
Une fois lancé, l'outil Centre d'Administration Active Directory ressemble à l'image ci-après :



Le volet « **Vue d'ensemble** » regroupe plusieurs informations et liens utiles qui vous permettent de prendre en main l'outil.

Il suffit de cliquer sur les liens pour en savoir plus.

De plus, des options de réinitialisation et de recherche sont disponibles depuis ce volet, vous pouvez en effet, réinitialiser le mot de passe d'un utilisateur donné depuis la partie « **REINITIALISER LE MOT DE PASSE** » ou localiser des objets Active Directory en utilisant les champs de la partie « **RECHERCHE GLOBALE** » :



Le volet gauche, regroupe les différentes catégories liées à Active Directory, notamment :

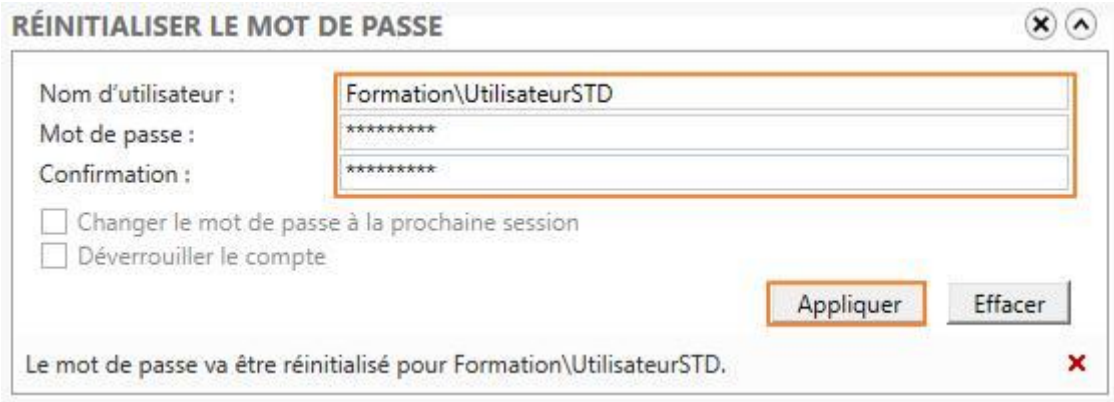
DomaineAD (local) (Formation (local) dans notre cas) : détaille la structure des OU et sous OU et présente l'ensemble des objets AD créés, la structure est similaire de celle affichée depuis l'outil DSA.msc (Utilisateurs et Ordinateurs Active Directory)

Contrôle d'accès dynamique (DAC) : volet permettant de créer et configurer des listes de contrôles d'accès et de configurer les différentes options de sécurité associées.

Authentification : ce volet vous permet de créer et configurer des stratégies d'authentification Active Directory

Recherche Globale : outil de recherche qui vous permet de rechercher et localiser rapidement des objets Active Directory

Dans l'exemple suivant, nous allons réinitialiser le mot de passe de l'utilisateur « UtilisateurSTD » depuis le volet « **Vue d'Ensemble** » :

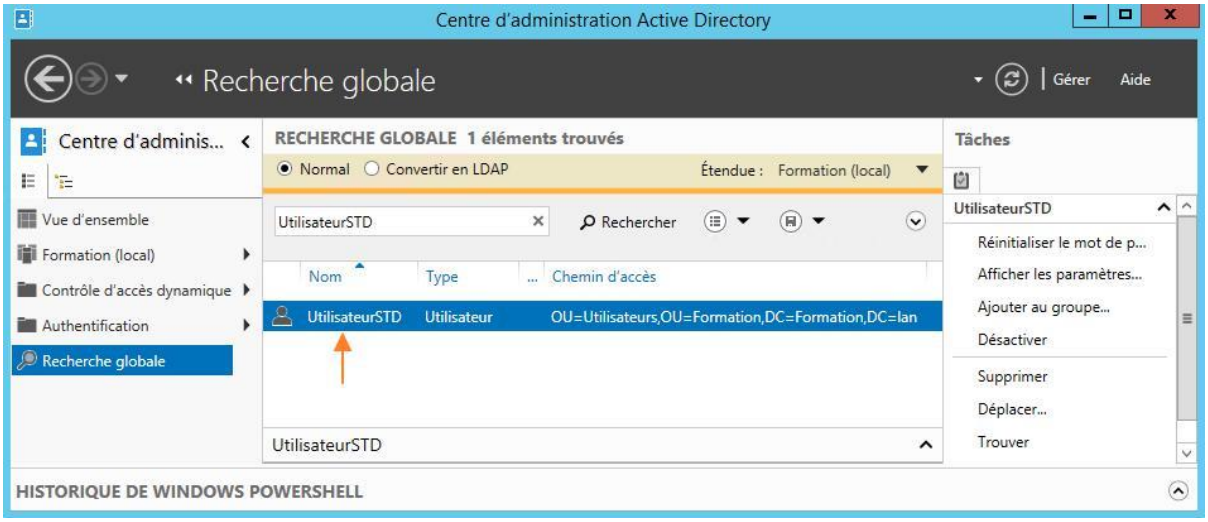


Après avoir cliqué sur « **Appliquer** », un message apparait vous confirmant la prise en compte de l'opération.

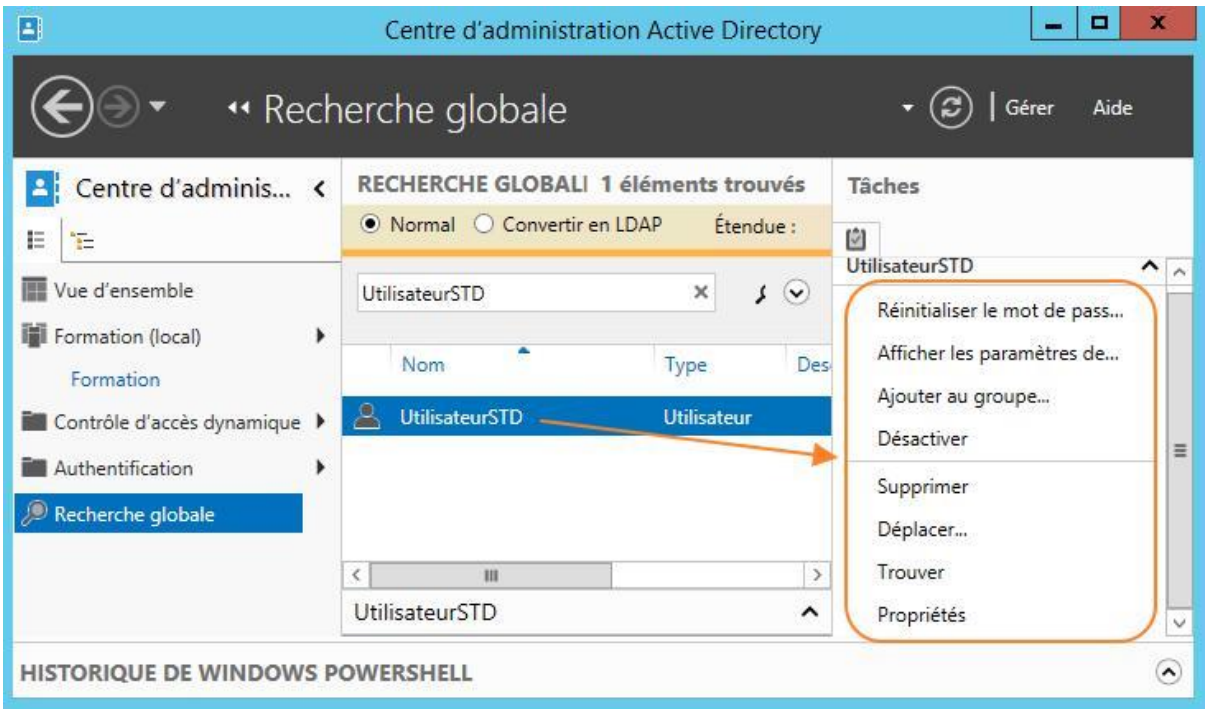
Nous allons cette fois-ci essayer de localiser le compte utilisateur « UtilisateurSTD » via les options de recherches globales.

Saisissez donc UtilisateurSTD sur le champ « **Rechercher** » et cliquez ensuite sur la touche « **Entrée** » du clavier pour valider votre recherche.

Notez que vous êtes automatiquement redirigé sur le volet « **Recherche globale** » et l'objet AD recherché est donc listé sur le volet du milieu.

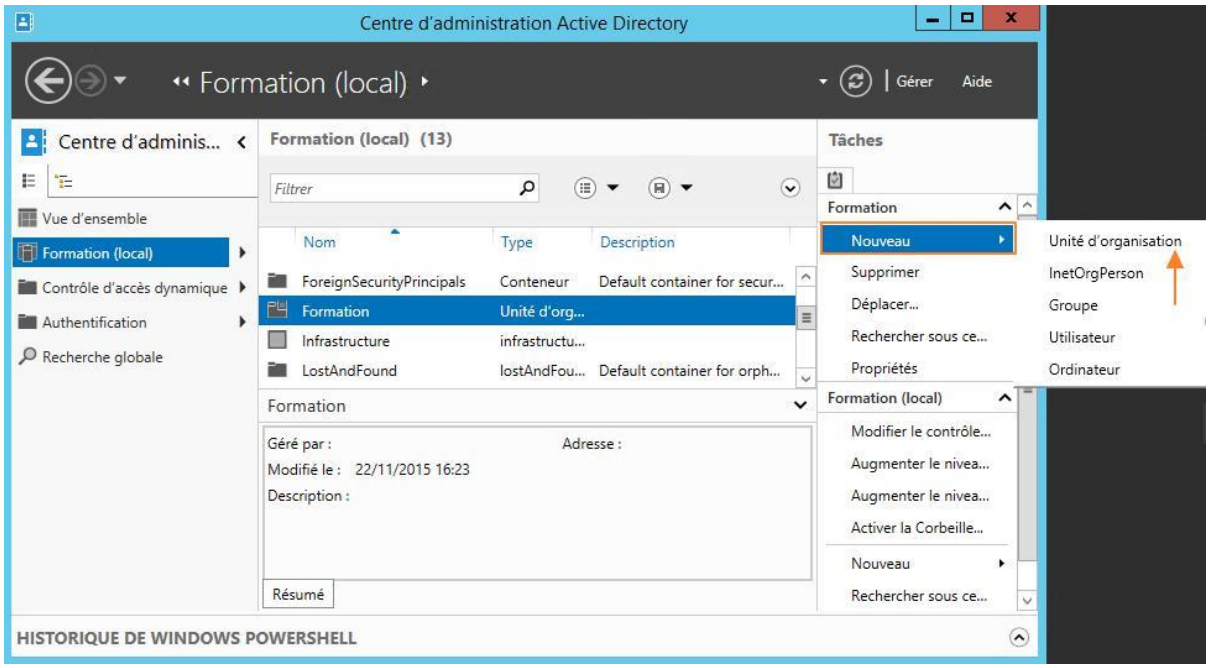


Le volet droit (**Tâches**) regroupe toutes les opérations que vous pouvez retrouver sur le menu contextuel obtenu via le clic-droit de la souris, comme illustré dans l'image ci-dessus, vous pouvez réinitialiser le mot de passe du compte utilisateur recherché et localisé, afficher ses paramètres, l'ajouter à un groupe de sécurité particulier, désactiver le compte, le supprimer ou encore le déplacer vers une autre OU ou sous OU.

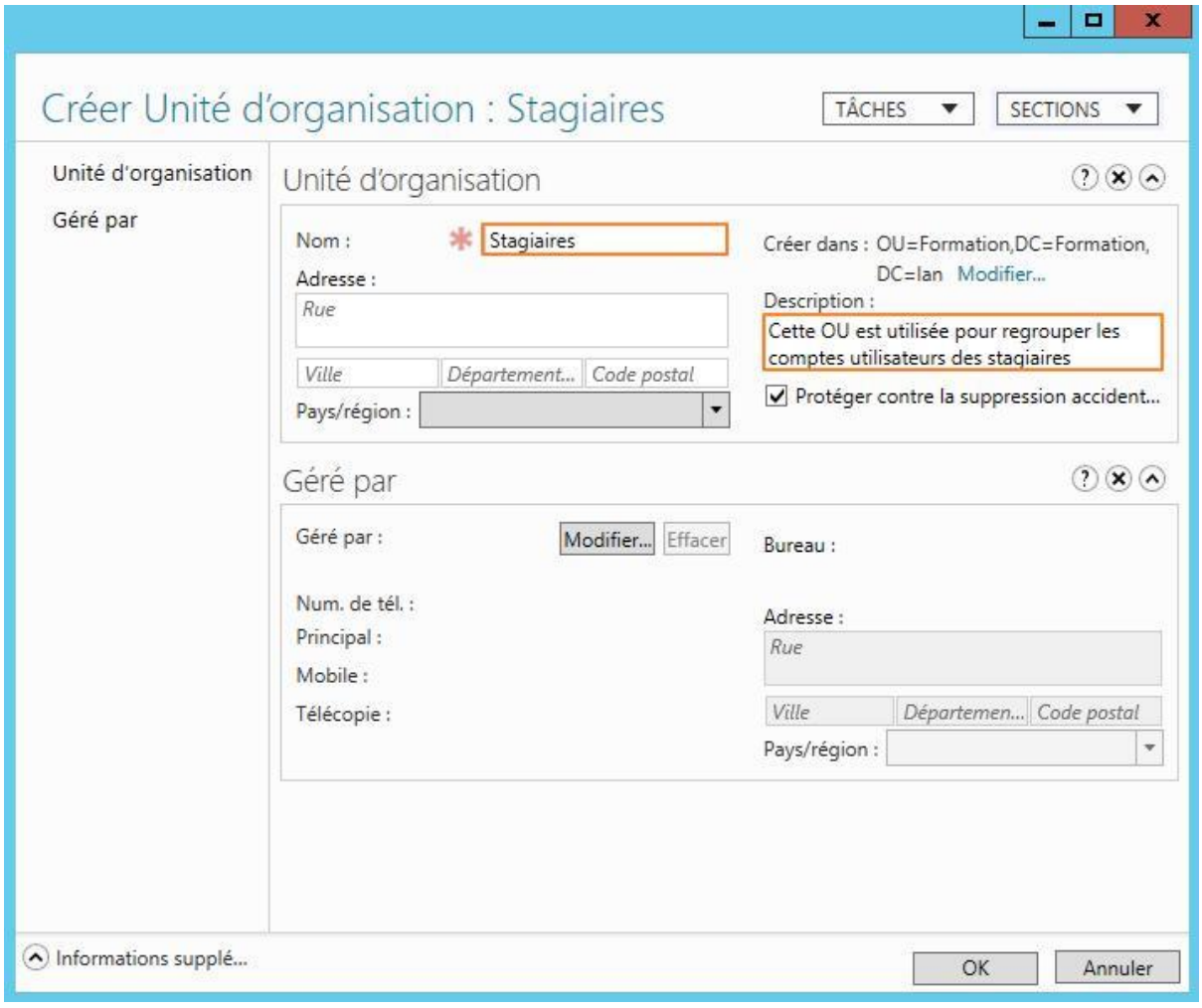


Nous allons maintenant utiliser le centre d'Administration AD pour créer une nouvelle OU pour regrouper les comptes utilisateurs des stagiaires.

Pour ce faire, sélectionnez l'OU « **Formation** », faites un clic-droit dessus et sélectionnez **Nouveau > Unité d'Organisation** ou utilisez le volet « **Tâches** » pour effectuer la même opération :



La boite de dialogue suivante apparaît, renseignez « **Stagiaires** » comme Nom d'OU et si nécessaire une description :

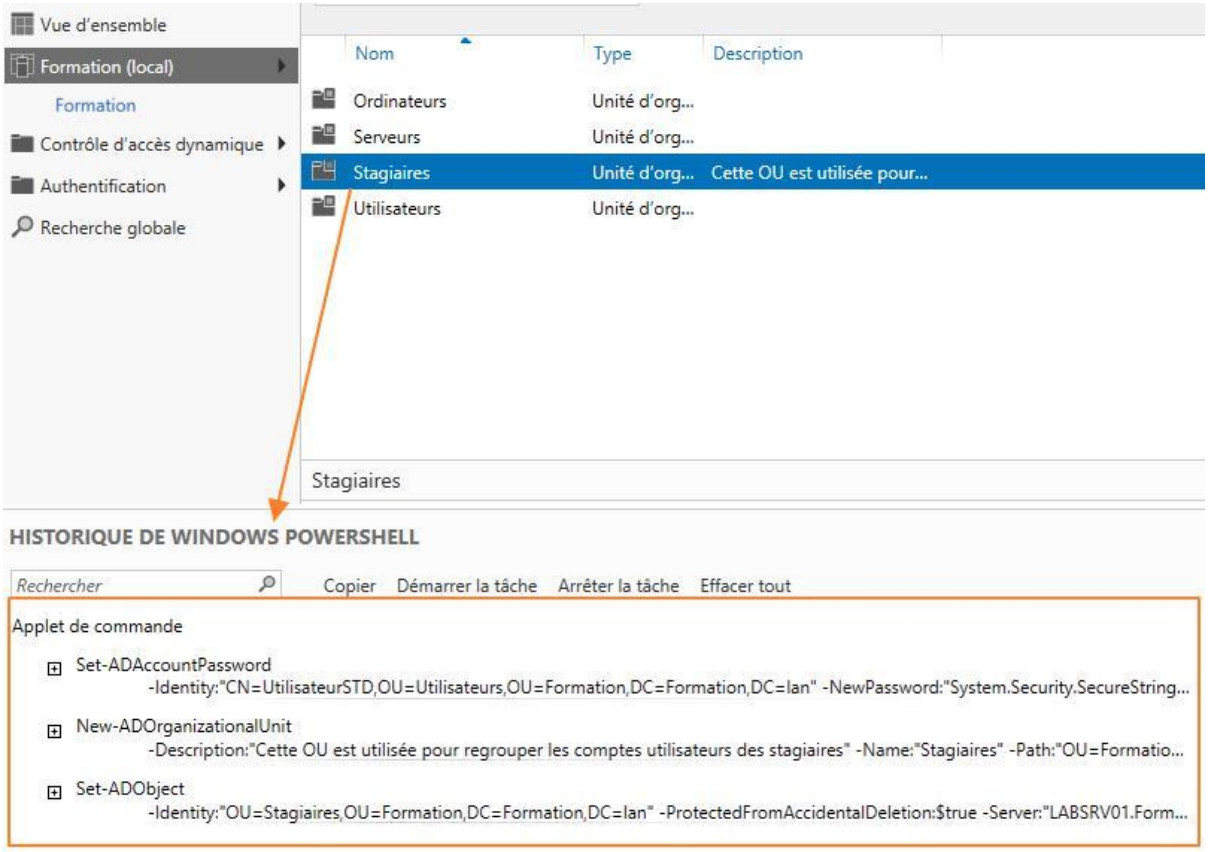


L’OU « Stagiaires » est donc créée sous l’OU « Formation ».

Enfin, le Centre d’Administration Active Directory inclut une fonctionnalité qui va surement vous intéresser, il s’agit de « **L’HISTORIQUE DE WINDOWS POWERSHELL** »

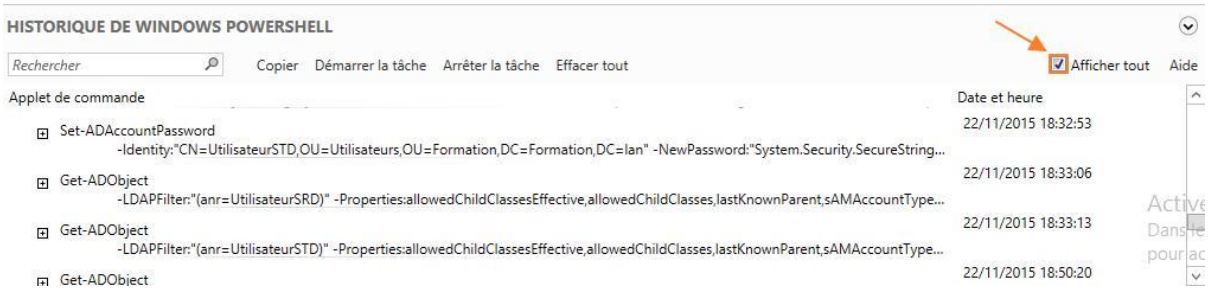
Cette fonctionnalité liste toutes les Cmd-let ayant été utilisées pour effectuer les tâches et opérations réalisées via les options graphiques.

Dans l’exemple suivant, la liste des Cmd-lets PowerShell (ainsi que leur paramètres associés) utilisées pour créer l’OU « Stagiaires » sont listées sur la partie « HISTORIQUE DE WINDOWS POWERSHELL », voir image ci-après :



De plus, le volet d’historique PowerShell peut vous être utile si vous désirez récupérer la liste des Cmd-lets utilisées pour chaque opération et les intégrer par la suite dans un script PowerShell pour automatiser toute tâche répétitive et fastidieuse.

L’Historique de Windows PowerShell inclut également une option « afficher tout », qui vous permet d’avoir plus de détails sur les commandes lancées à chaque opération, comme illustré dans l’image ci-après, il suffit de cliquer sur « **Afficher tout** » pour afficher la liste complète des Cmd-lets.



Essayez de créer un nouveau compte utilisateur et groupe de sécurité via les options graphiques du Centre d'Administration Active Directory et notez les Cmd-lets appelées et utilisées depuis le volet « HISTORIQUE DE WINDOWS POWERSHELL ».

5.5 Manipulation des profils utilisateurs

5.5.1 La redirection des profils (Profils itinérants)

La redirection de profils permet de répondre à la contrainte de l'accessibilité des données personnelle lorsque les utilisateurs utilisent l'ordinateur d'un collègue, ou change régulièrement de machine. Dans ce cas-là l'utilisateur n'a pas accès à ces données car elles sont stockées dans le C:\utilisateurs\<Nom Utilisateur> de l'ordinateur.

C'est dans cette optique que les profils itinérants peuvent être envisagés. Le fonctionnement est assez simple :

- Lors de l'ouverture de la session les données du profil de l'utilisateur sont téléchargées sur la machine
- Lors de la fermeture de la session les données sont envoyées au serveur pour être disponible à la prochaine ouverture de session.

Les profils itinérants permettent la mobilité des utilisateurs ainsi que la centralisation des données des profils Utilisateur.

Allez sur le « **LABSRV03** » pour créer un partage qui servira à stocker les données des profils des utilisateurs. Nommez ce dossier « **Profils_Itinerants** ».

Pour les autorisations de partage : Donnez le droit « **Modifier** » aux « **Utilisateurs authentifié** » et supprimez le droit « **Tout le monde** »

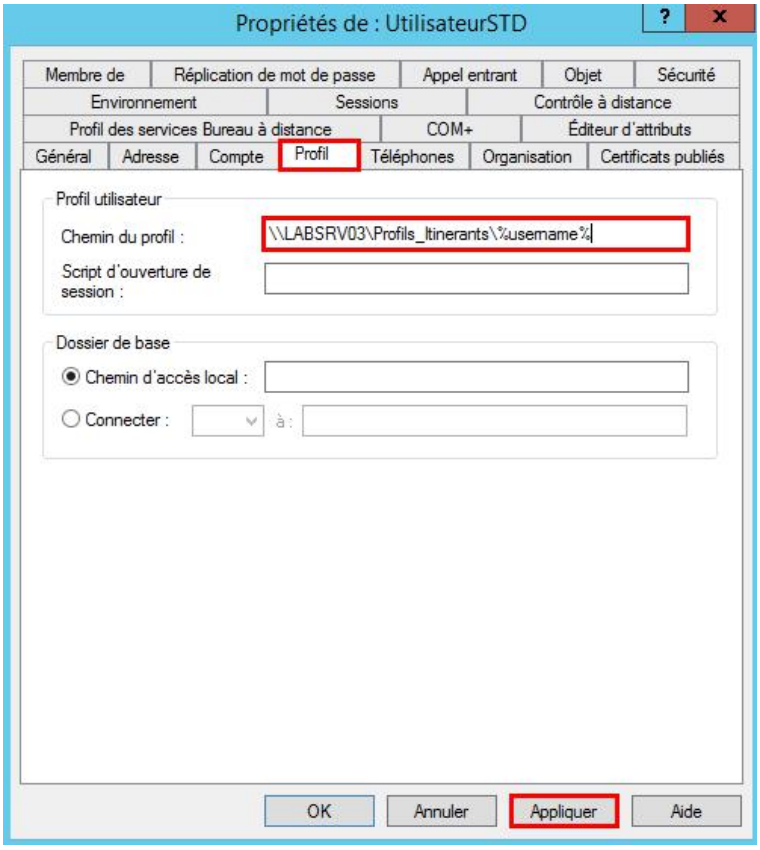
Pour les autorisations NTFS : Donner le droit « **Contrôle total** » aux « **Utilisateurs authentifié** »

Allez ensuite sur le serveur « **LABSRV01** » et ouvrez la console « **Utilisateur et ordinateur Active Directory** », allez dans l'OU « **Formation** » puis « **Utilisateurs** » et faites un clic droit « **Propriétés** » sur l'utilisateur « **UtilisateurSTD** »

Sur l'onglet « **Profils** » renseignez les informations suivante :

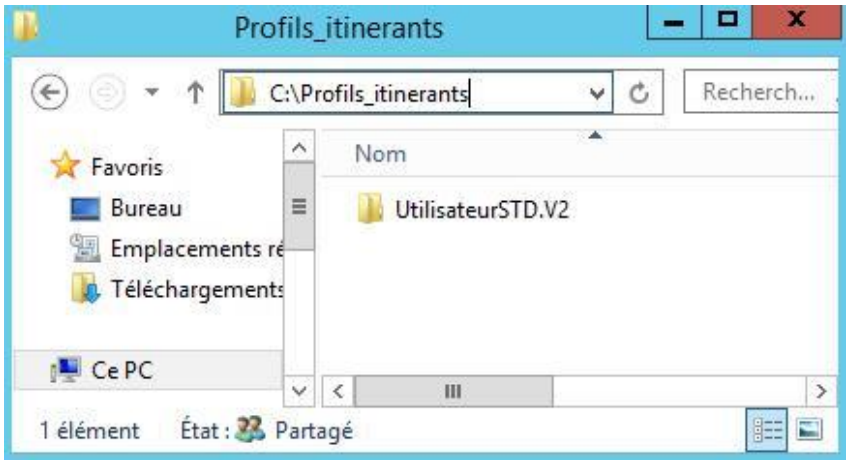
\\LABSRV03.formation.lan\ Profils_Itinerants\%username%

[redacted]	**L'utilisation de la variable est recommandée, de plus cela permet de sélectionner plusieurs utilisateurs en même temps pour renseigner le chemin.**

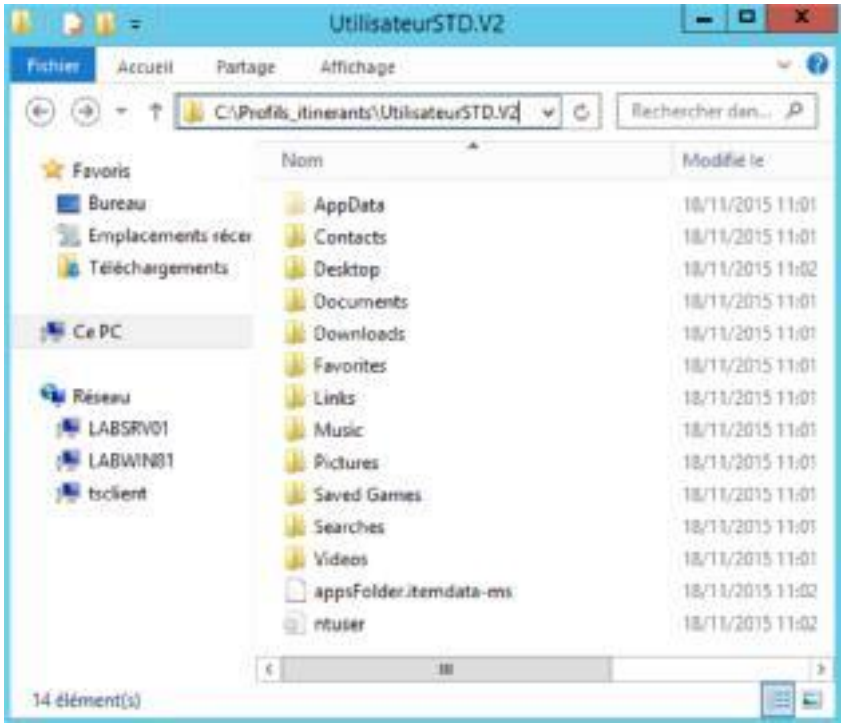


Allez sur la machine cliente « **LABWin10** » et connectez-vous avec le compte « **UtilisateurSTD** »

Allez ensuite sur le serveur « **LABSRV03** » et allez dans le dossier « **C:\Profils_Itinerants** » et constatez la création d'un dossier au nom de l'utilisateur « **UtilisateurSTD.V2** ».

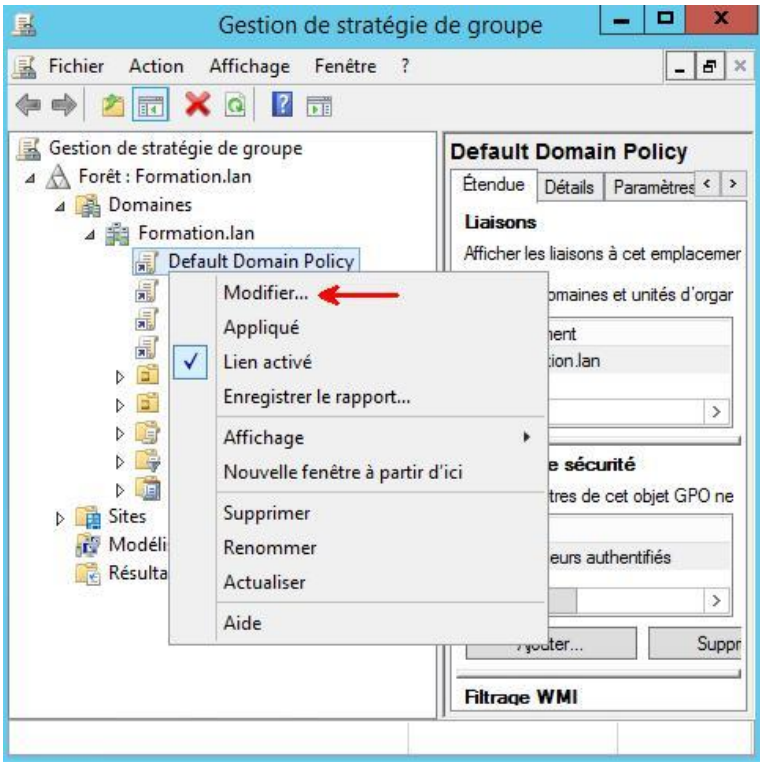


Voici la liste des dossiers contenu dans le profil itinérant de « **UtilisateurSTD** » il faudra vous rendre propriétaire du dossier pour y accéder.



Allez ensuite sur le serveur « **LABSRV01** » et dans « **Outils** » ouvrez « **Gestion des stratégies de groupe** » ou lancez depuis le menu « **Exécuter** » la commande « **GPMC.MSC** »

Prenez la GPO du domaine et faite un clic droit et « **Modifier** »



Allez dans : **Configuration utilisateur | Stratégies | Modèles d'administration | Système | Profils utilisateur**

4 GPO sous disponible :

- Connecter le répertoire de base à la racine du partage
- Spécifier les répertoires réseau à synchroniser seulement au moment de l'ouverture/fermeture de session
- Exclure des répertoires dans les profils itinérants
- Limiter la taille du profil

Configurer les GPO suivant vos besoins.

D'autre GPO sont disponible dans : **Configuration Ordinateur | Stratégies | Modèles d'administration | Système | Profils utilisateur**