TUTOS-INFO
L'informatique par l'exemple

TUTORIEL

WINDOWS 2025

Configurer le rôle AD/DS

SOMMAIRE

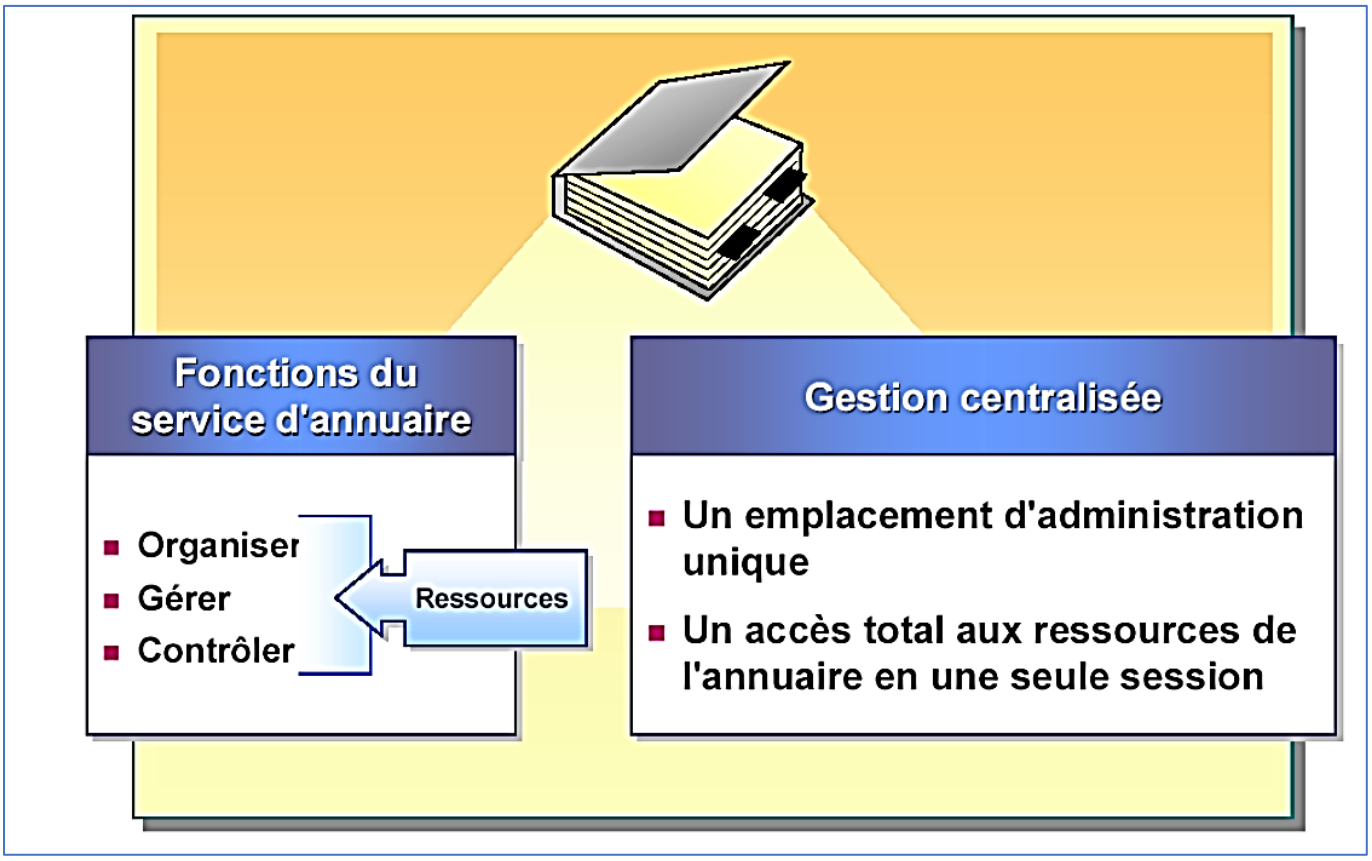
CONFIRME
DIFFICULTE

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE (version 8.3). Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © Virtualbox ou © VMWare Player et **suppose que vous avez réalisé le tutoriel n° 1** (installation et préparation du serveur Windows Server 2025).

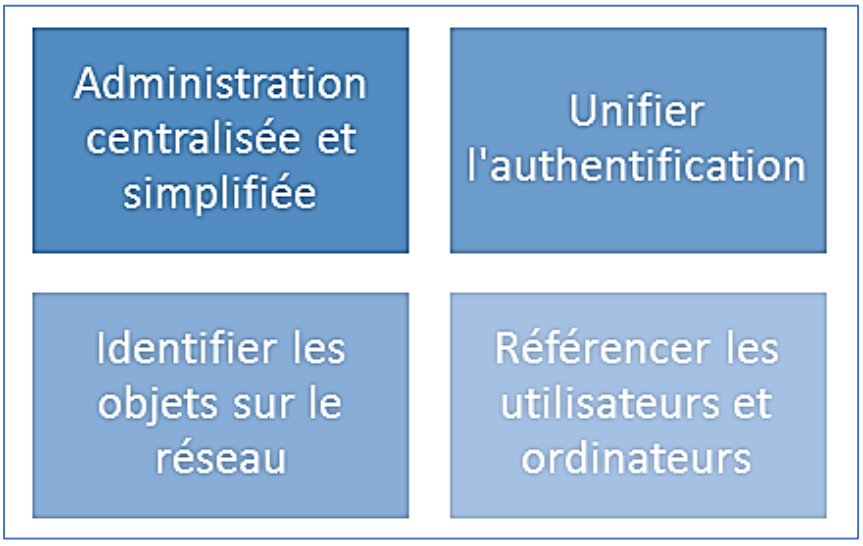
1 – QU'EST-CE QUE L'ACTIVE DIRECTORY ?

L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents **objets**, de différents types (utilisateurs, ordinateurs, etc.).

L'objectif étant de centraliser deux fonctionnalités essentielles : l'**identification** et l'**authentification** au sein d'un système d'information :



Pour résumer, l'Active Directory, c'est :

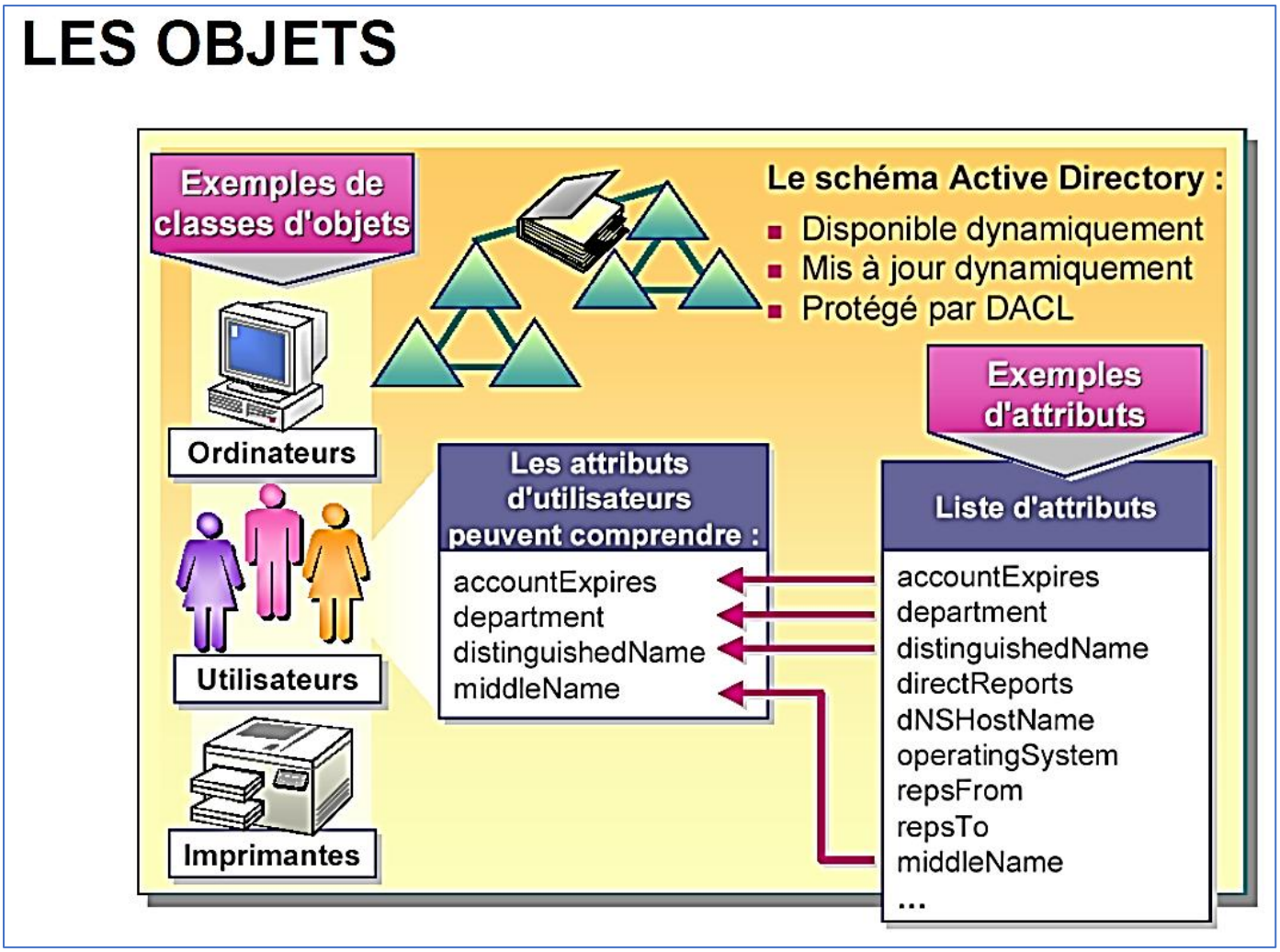


2 - LA STRUCTURE DE L'ACTIVE DIRECTORY

A. Les classes et les attributs

Au sein de l'annuaire Active Directory, il y a différents types **d'objets** tels que : les ***utilisateurs***, les ***ordinateurs***, les ***serveurs***, les ***unités d'organisation*** ou encore les ***groupes***. En fait, ces objets correspondent à d**es classes**, c'est-à-dire **des objets disposant des mêmes attributs**.

De ce fait, un objet ordinateur sera une instance d'un objet de la classe « **Ordinateur** » avec des valeurs spécifiques à l'objet concerné.



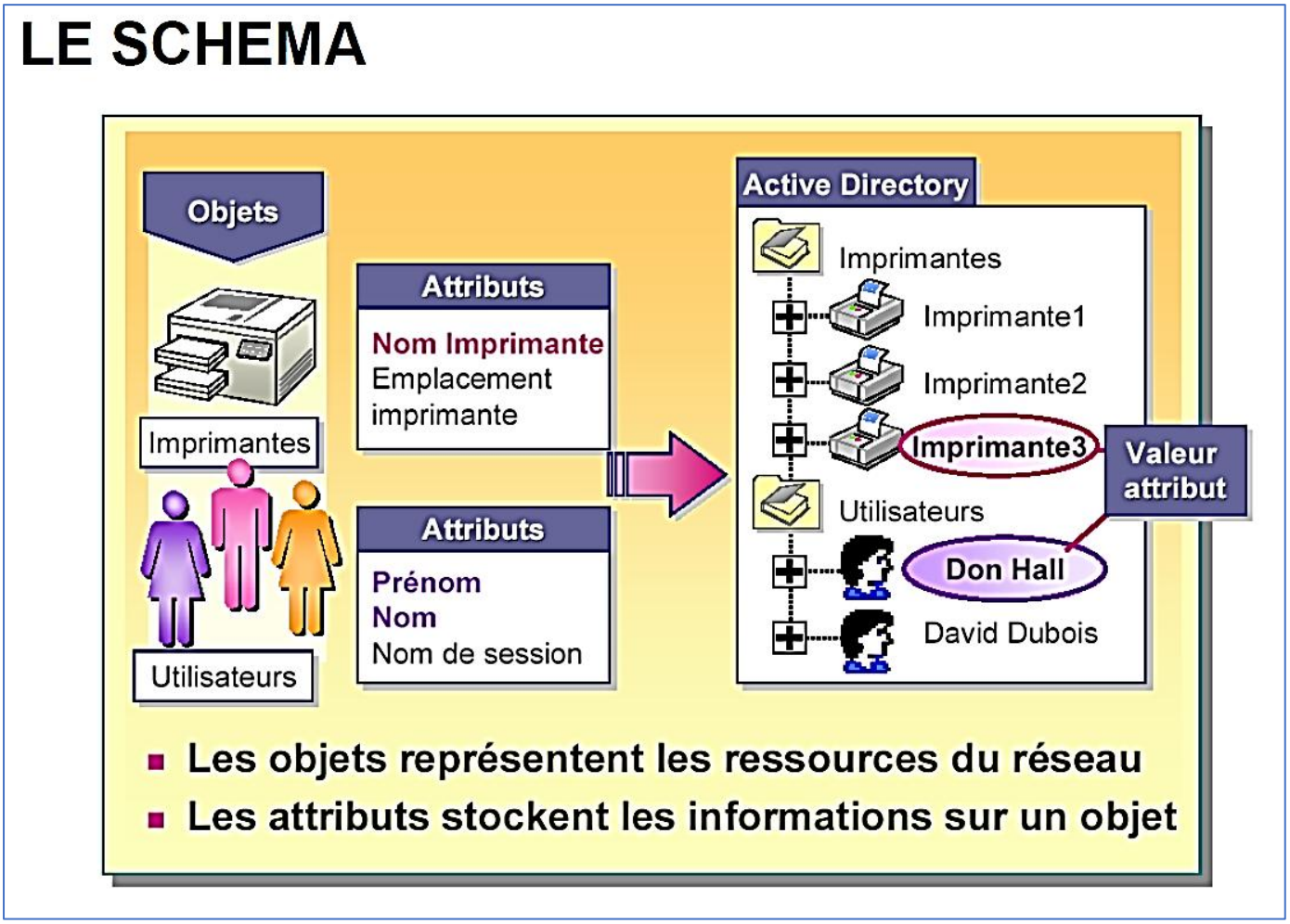
Par ailleurs, les **unités d'organisation (appelées « OU »)** sont des **containers d'objets afin de faciliter l'organisation de l'annuaire** et **permettre une organisation avec plusieurs niveaux**.

Sans les unités d'organisations, l'annuaire ne pourrait pas être trié correctement et l'administration serait moins efficace.

On peut comparer les unités d'organisations à des dossiers qui permettent de ranger les objets à l'intérieur.

B. Le schéma

Par défaut, tout annuaire Active Directory dispose de classes prédéfinies ayant chacune une liste d'attributs bien spécifique, et propre à tout annuaire, cela est défini grâce à **un schéma**.



Le schéma contient la définition de toutes les classes et de tous les attributs disponibles et autorisés au sein de votre annuaire. Il est à noter que le schéma est évolutif, le modèle de base n'est pas figé et peut évoluer selon vos besoins.

Par exemple, l'application de messagerie Microsoft Exchange effectue des modifications au schéma lors de son installation.

3 – NOTION DE GROUPE DE TRAVAIL ET DE DOMAINE

Du groupe de travail au domaine

Pour rappel, toutes les machines sous Windows sont par défaut intégrées dans un groupe de travail nommé « ***WORKGROUP*** ». Cela permet de mettre en relation des machines d'un même groupe de travail, notamment pour le partage de fichiers, mais **il n'y a pas de notions d'annuaire, ni de centralisation** avec ce mode de fonctionnement.

A. Modèle « Groupe de travail »

Une base d'utilisateurs par machine : appelée « base SAM », cette base est unique sur chaque machine et non partagée. Ainsi, chaque machine contient sa propre base d'utilisateurs.

Ce modèle devient très vite inadapté notamment pour la gestion des comptes utilisateurs en nombre. En effet, **chaque utilisateur devra disposer d'un compte sur chaque machine si l'on souhaite mettre en place une authentification**. Par exemple, une salle avec 10 machines nécessitera de créer le compte de l'utilisateur sur chacune des 10 machines si l'on veut qu'il conserve à chaque fois le même identifiant et le même mot de passe ! Donc pour 10 utilisateurs, il faudra créer 10 utilisateurs par machine x 10 soit 100 manipulations !

B. Modèle « Domaine »

Base d'utilisateurs, de groupes et d'ordinateurs centralisée. Un seul compte utilisateur est nécessaire pour accéder à l'ensemble des machines du domaine.

L'annuaire contient toutes les informations relatives aux objets, tout est centralisé sur le contrôleur de domaine, il n'y a pas d'éparpillement sur les machines au niveau des comptes utilisateurs.

Ouverture de session unique par utilisateur, notamment pour l'accès aux ressources situées sur un autre ordinateur ou serveur.

Chaque contrôleur de domaine contient une copie de l'annuaire, qui est maintenue à jour et qui permet d'assurer la disponibilité du service et des données qu'il contient. Les contrôleurs de domaine se répliquent entre eux pour assurer cela.

Administration et gestion de la sécurité complètement centralisée avec mise en place de « stratégies »

4 – LA NOTION DE CONTRÔLEUR DE DOMAINE

Qu'est-ce qu'un contrôleur de domaine ?

Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine.

De ce fait, il devra vérifier les identifications des objets, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe ou encore stocker une copie de l'annuaire Active Directory.

Un contrôleur de domaine est indispensable au bon fonctionnement du domaine, si l'on éteint le contrôleur de domaine ou qu'il est corrompu, le domaine devient inutilisable.

De plus, lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez également le premier domaine, la première forêt, ainsi que le premier site.

Le fichier de base de données NTDS.dit

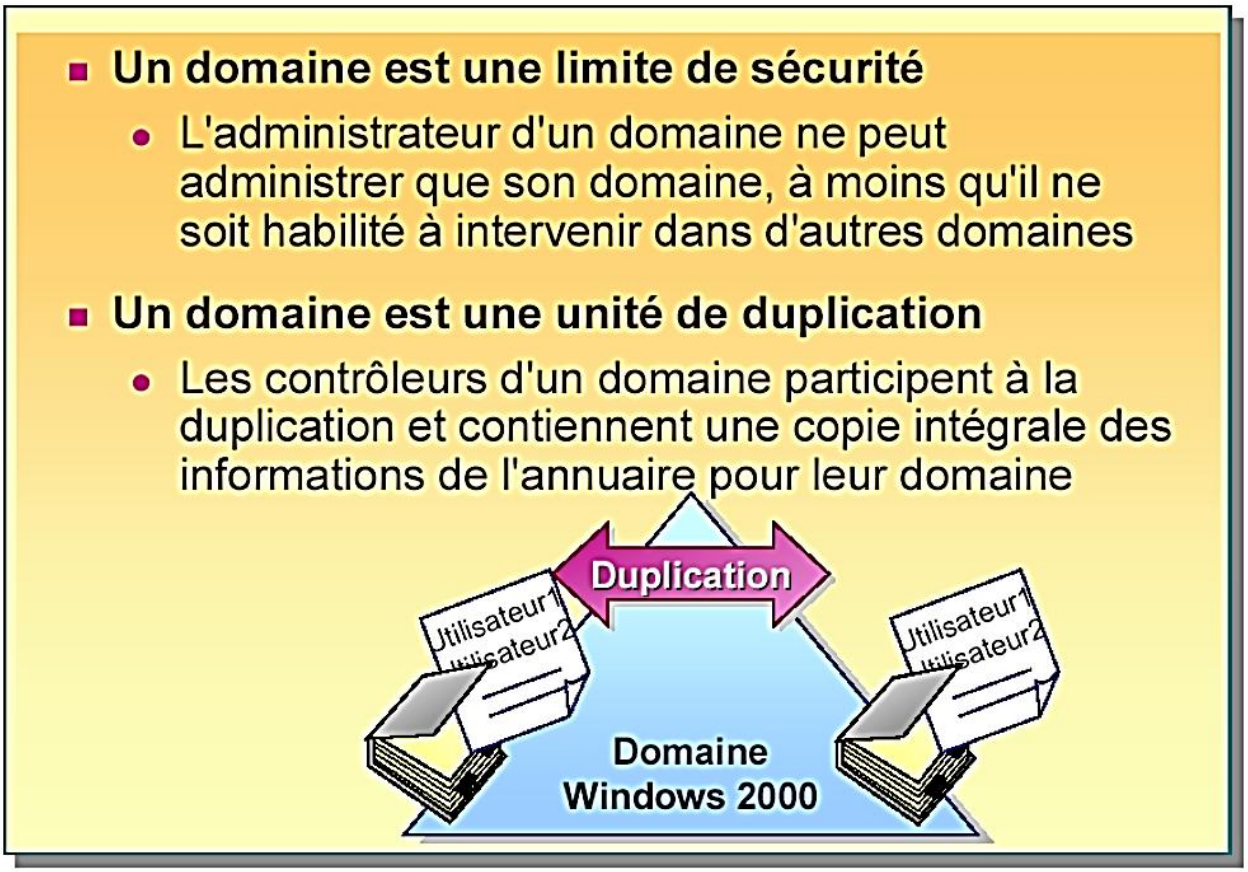
Sur chaque contrôleur de domaine, on trouve une copie de la base de données de l'annuaire Active Directory. Cette copie est symbolisée par un fichier « **NTDS.dit** » qui contient l'ensemble des données de l'annuaire.

La réplication des contrôleurs de domaine

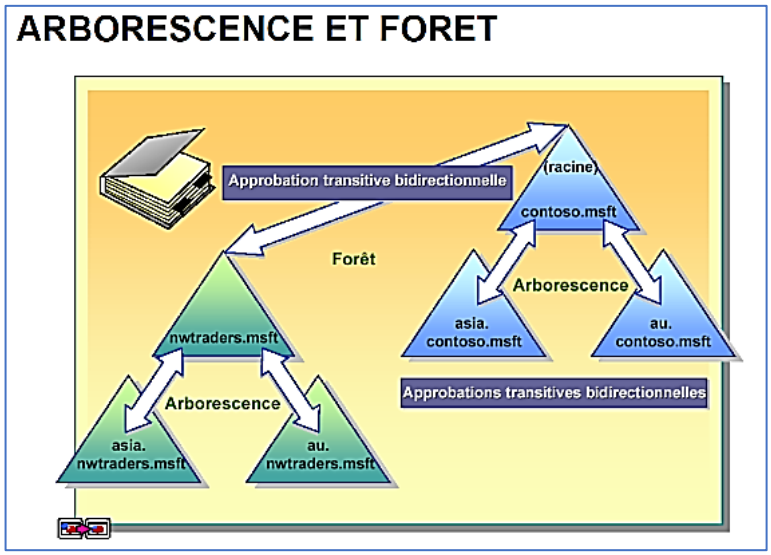
Afin d'assurer une haute disponibilité et d'éviter tout problème, il est vivement recommandé d'avoir **au minimum deux contrôleurs de domaine** pour assurer la disponibilité et la continuité de service des services d'annuaire.

De plus, cela permet d'assurer la pérennité de la base d'annuaire qui est très précieuse. À partir du moment où une entreprise crée un domaine, même si ce domaine est unique, il est important de mettre en place au minimum deux contrôleurs de domaine.

DOMAINE



Notion d'arbre et de forêt



Au sein du domaine schématisé par des triangles généralement, on retrouvera **tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes** : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc...

De nombreuses entreprises ont plusieurs succursales, ce qui implique plusieurs sites sur différents emplacements géographiques. Selon l'importance de ces sites, on pourra envisager de créer un sous-domaine au domaine principal, voir même plusieurs sous-domaines selon le nombre de succursales.

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.**

Une **forêt** est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.

Mais alors qu'apporte la création d'une forêt ?

- Tous les arbres d'une forêt partagent un schéma d'annuaire commun

- Tous les domaines d'une forêt partagent un « catalogue global commun ».

- Les domaines d'une forêt fonctionnent de façon indépendante, mais la forêt facilite les communications entre les domaines, c'est-à-dire dans toute l'architecture.7

- Création de relations entre les différents domaines de la forêt

- Simplification de l'administration et flexibilité. Un utilisateur d'un domaine pourra accéder à des ressources situées dans un autre domaine ou se connecter sur une machine du domaine si les autorisations le permettent.

Notion de niveau fonctionnel

Le niveau fonctionnel est une notion également à connaître lors de la mise en œuvre d'une infrastructure Active Directory. À la création d'un domaine, un niveau fonctionnel est défini et il correspond généralement à la version du système d'exploitation serveur depuis lequel on crée le domaine.

Par exemple, si l'on effectue la création du domaine depuis un serveur sous Windows Server 2025, le niveau fonctionnel sera « *Windows Server 2025* ». Dans un environnement existant, on est souvent amené à faire évoluer notre infrastructure, notamment les systèmes d'exploitation, ce qui implique le déclenchement d'un processus de migration. Une étape incontournable lors de la migration d'un Active Directory vers une version plus récente et le changement du niveau fonctionnel. Ainsi, il est important de savoir à quoi il correspond et les conséquences de l'augmentation du niveau.

Plus le niveau fonctionnel est haut, plus vous pourrez bénéficier des dernières nouveautés liées à l'Active Directory et à sa structure. Par exemple, **si le niveau fonctionnel est « Windows Server 2008 », vous ne pourrez pas ajouter un nouveau contrôleur de domaine sous Windows Server 2012 et les versions plus récentes.**

À l'inverse, si le niveau fonctionnel est « *Windows Server 2025* », **il sera impossible d'intégrer de nouveaux contrôleurs de domaine qui utilisent un système d'exploitation plus ancien que Windows Server 2025.**

De plus, vous ne pouvez pas avoir un niveau fonctionnel plus haut que la version de votre contrôleur de domaine le plus récent.

Il est impossible de passer à un niveau inférieur. Par exemple, on peut passer du niveau « *Windows Server 2022* » à « *Windows Server 2025* », mais pas l'inverse. Il existe toutefois une exception, il est possible rétrograder le niveau fonctionnel de Windows Server 2008 R2 à Windows Server 2008.

5 – LA NOTION DE PROTOCOLE LDAP

Qu'est-ce que le 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.
Il existe une déclinaison du protocole LDAP appelée LDAPS (*LDAP over SSL*) est qui apporte une couche de sécurité supplémentaire avec du chiffrement (**port 636**).

Que contient l'annuaire LDAP ?

L'annuaire LDAP correspond directement à l'Active Directory. Il contient un ensemble d'unités d'organisation qui forment l'arborescence générale. Ensuite, on trouve tous les différents types d'objets classiques : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, serveurs et imprimantes.

Pour chaque classe d'objets, il stocke les attributs correspondants et les différentes valeurs de ces attributs pour chaque instance d'un objet. Par exemple, il va stocker toutes les informations relatives à un utilisateur (nom, prénom, description, mot de passe, adresse e-mail, etc...).

Comment est structuré l'annuaire LDAP ?

Un annuaire est un ensemble d'entrées, ces entrées étant elles-mêmes constituées de plusieurs attributs. De son côté, **un attribut est bien spécifique et dispose d'un nom qui lui est propre, d'un type et d'une ou plusieurs valeurs.**

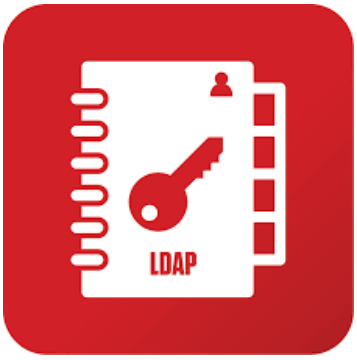
Chaque entrée dispose d'un identifiant unique qui permet de l'identifier rapidement, de la même manière que l'on utilise les identifiants (clé primaire) dans les bases de données pour identifier rapidement une ligne.

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, **et il se compose du nom de domaine auquel appartient l'objet ainsi que du chemin complet pour accéder à cet objet dans l'annuaire** (le chemin à suivre dans l'arborescence d'unités d'organisation pour arriver jusqu'à cet objet).

Par exemple, un objet « *utilisateur* » nommé « *prof* », du domaine « laboprof.sio » et étant stocké dans une unité d'organisation (OU) nommée « *btssio* » donnera en « langage » LDAP : **cn=prof,ou=btssio,dc=laboprof,dc=sio**

Dans un chemin LDAP vers un objet, on trouve toujours la présence du domaine sous la forme : « *dc=laboprof,dc=sio* » (ne pas mettre d'espace).

À quel moment a-t-on besoin d'utiliser le protocole LDAP ?



Le protocole LDAP permet de créer des liaisons entre une application et l'annuaire des utilisateurs.

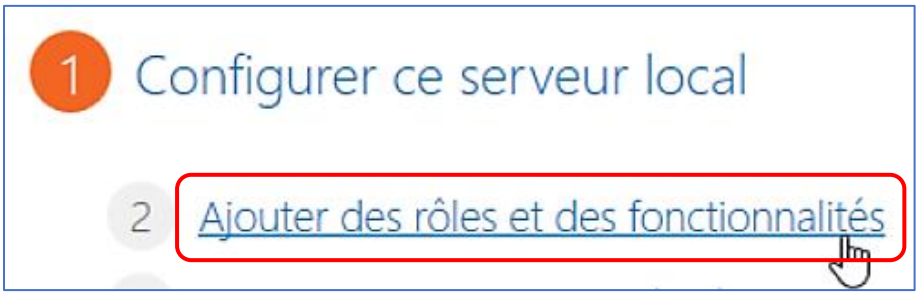
Prenons pour exemple un helpdesk de type GLPI. Lorsque les utilisateurs du domaine souhaitent se connecter à l'interface GLPI pour saisir un ticket de maintenance, il est souhaitable que l'identifiant de connexion et le mot de passe soient les mêmes que ceux utiliser pour la connexion au domaine. On évite ainsi les erreurs et une accumulation d'identifiants avec des mots de passe nombreux.

Le protocole LDAP permet donc d'effectuer une liaison entre GLPI et l'Active Directory de manière à **importer les utilisateurs de l'annuaire AD** dans l'application GLPI.

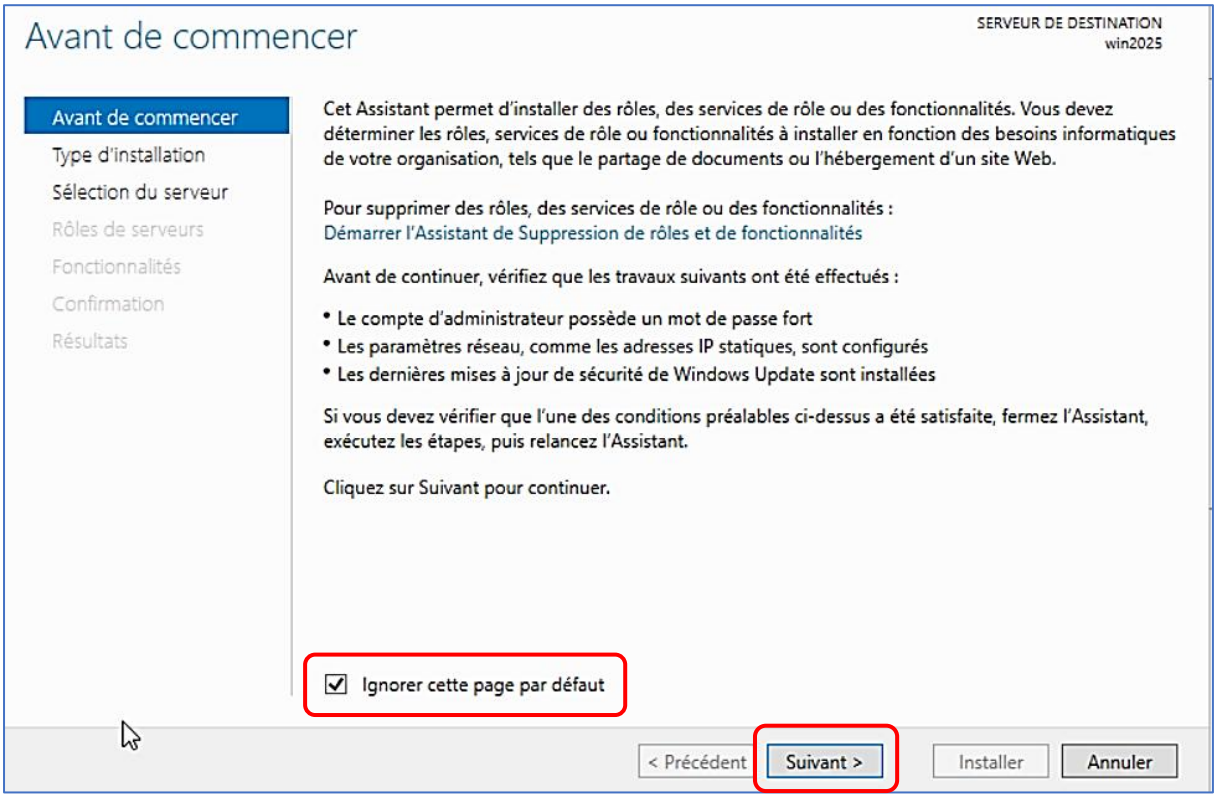
Ainsi, les utilisateurs ne seront pas à créer dans l'application puisqu'ils existent déjà dans l'annuaire et l'authentification de ces derniers restera identique à celle du domaine.

6 – INSTALLER ET CONFIGURER LE RÔLE AD/DS

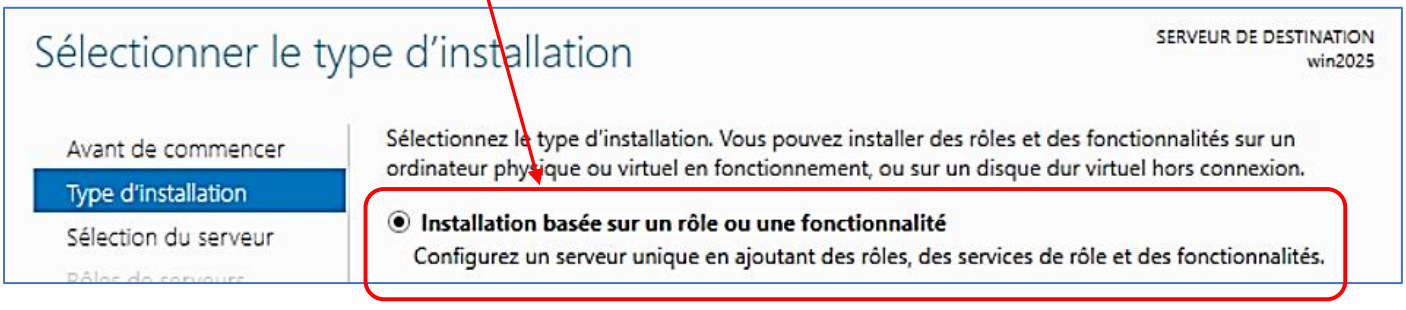
- Ouvrez une session administrateur sur votre serveur Windows 2025
- Dans le tableau de bord du gestionnaire de serveur, cliquez le lien « **Ajouter des rôles et des fonctionnalités** » :



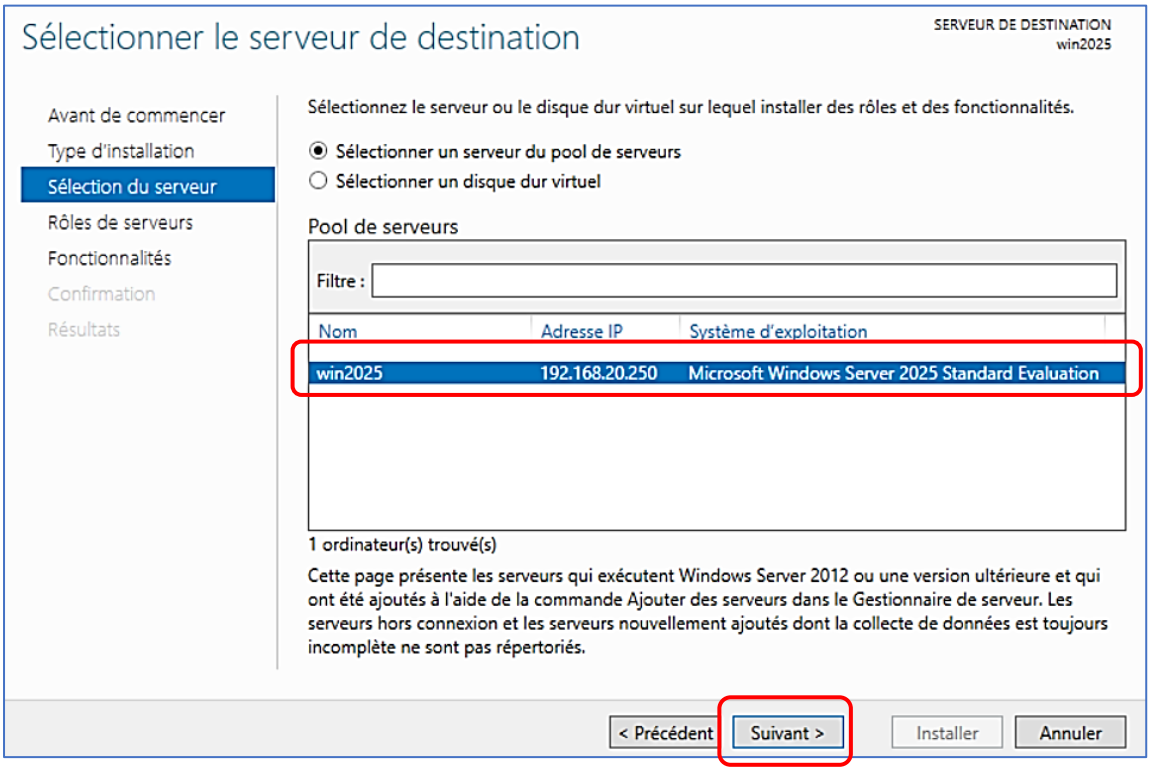
- Vous pouvez cliquer la case « **Ignorer cette page par défaut** » et cliquez le bouton « **Suivant** » (page de présentation sur l'installation des rôles et des services) :



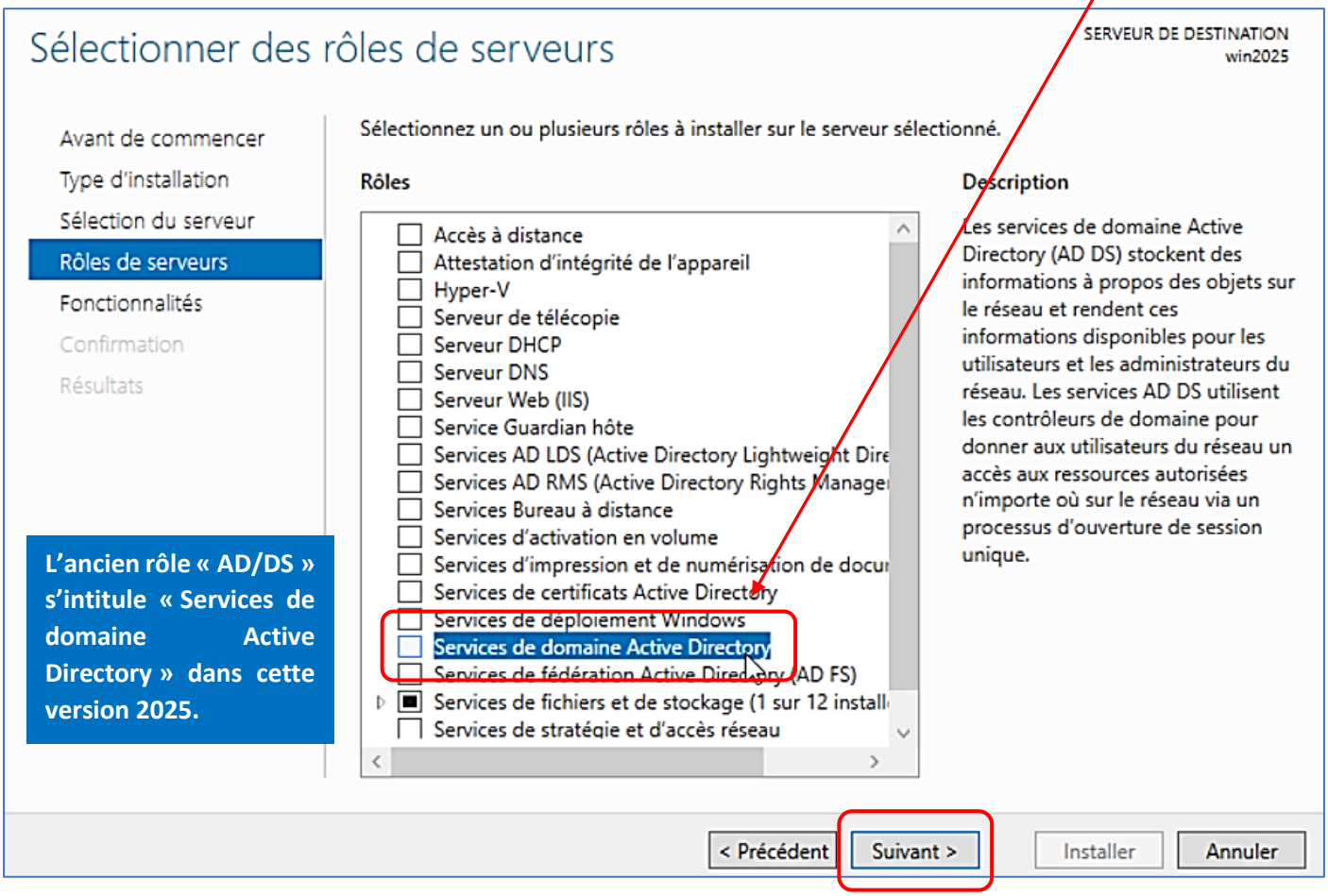
- Vérifiez que l'option « **Installation basée sur un rôle ou une fonctionnalité** » est bien cochée et cliquez le bouton « **Suivant** » :



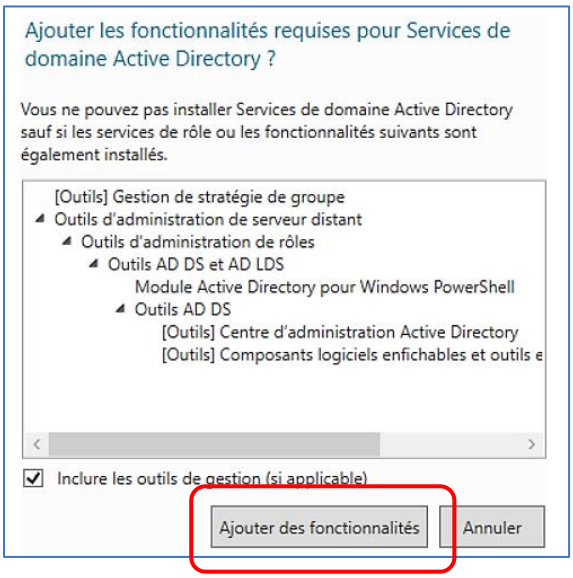
- Sélectionnez le serveur sur lequel vous souhaitez installer le rôle AD/DS et cliquez le bouton « **Suivant** » :



- Sélectionnez le rôle « **AD/DS** » qui est répertorié dans la liste sous le nom « **Services de domaine Active Directory** » :

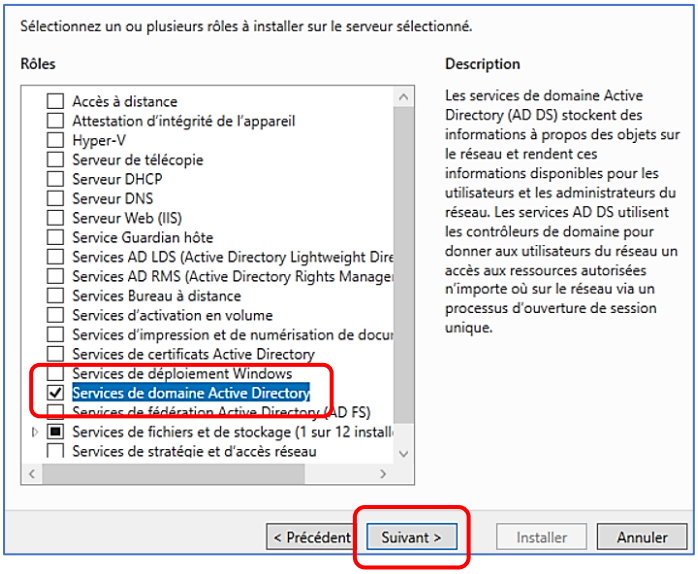


- Après avoir cliqué la case « **Services de domaine Active Directory** », une fenêtre s'affiche ; cliquez sur le bouton « **Ajouter des fonctionnalités** » :

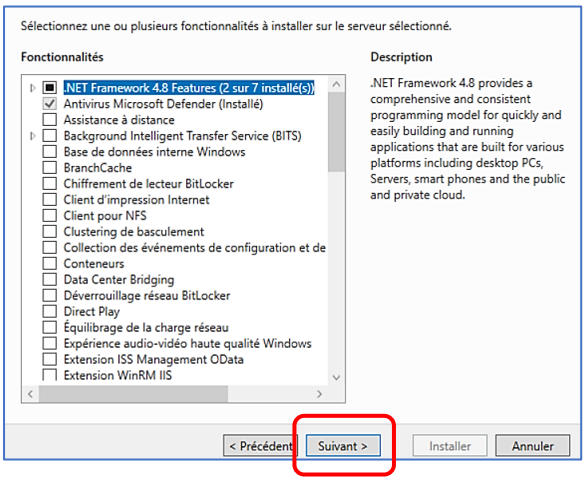


On laisse, ici, les fonctionnalités par défaut liées au rôle « AD/DS » que nous souhaitons ajouter.

- La fenêtre d'ajout de rôles s'affiche à nouveau et le rôle « **Services de domaine Active Directory** » doit être coché ; cliquez le bouton « **Suivant** » :

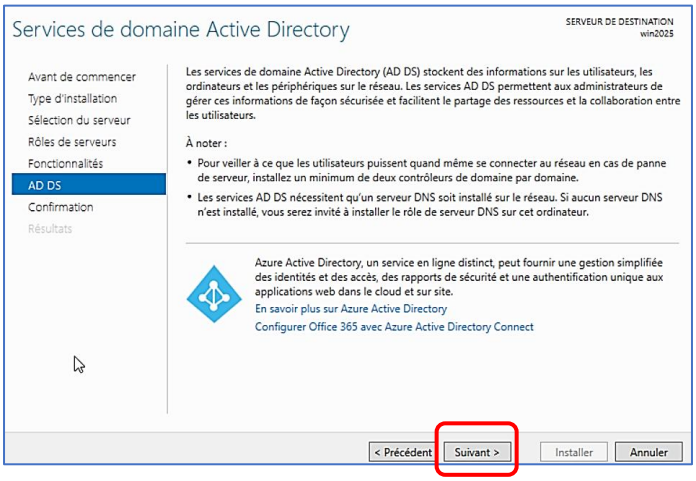


- Laissez les fonctionnalités par défaut activées et cliquez le bouton « **Suivant** » :



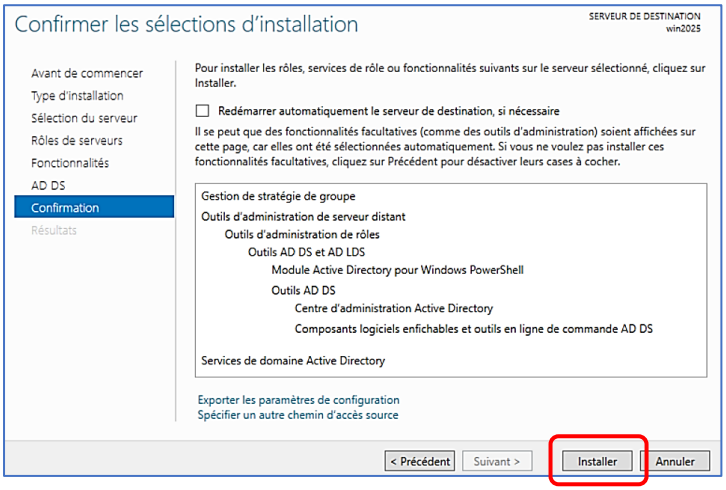
On laisse, ici, les fonctionnalités par défaut liées au rôle « AD/DS » que nous souhaitons ajouter.

- Nous n'utilisons pas les services cloud Azure ici ; cliquez le bouton « **Suivant** » :



Nous n'utilisons pas, ici, les services Azure (cloud) de Microsoft.

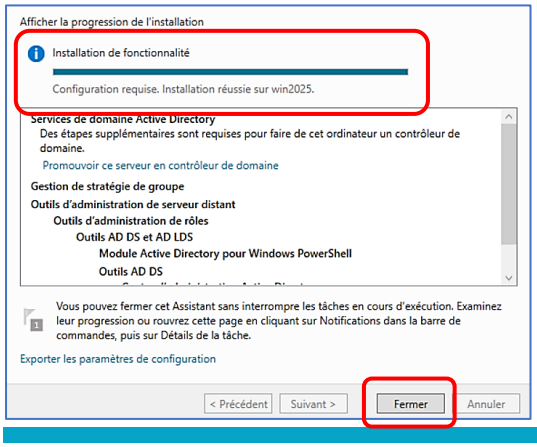
- Cliquez le bouton « **Installer** » pour lancer l'installation du rôle et patientez :



On lance l'installation du rôle AD/DS une fois l'ensemble des paramètres validés.

Une barre de progression affiche l'état de l'installation ; patientez quelques minutes :

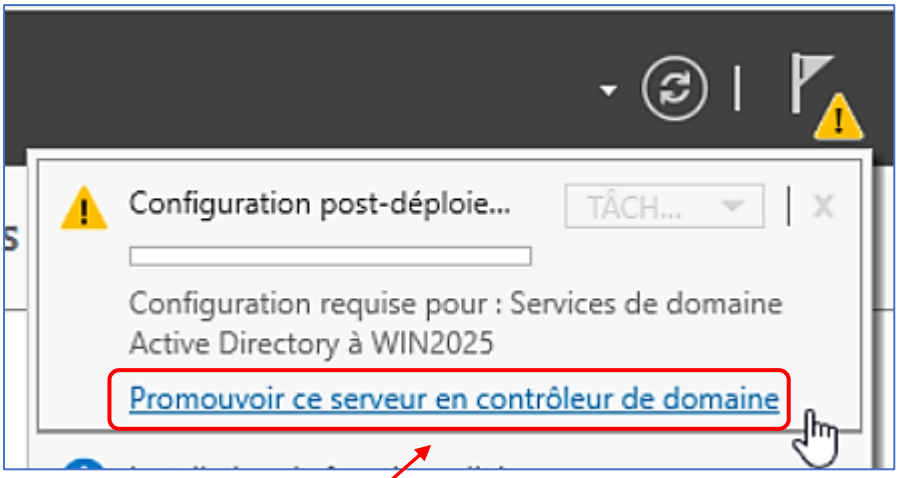
Une fois le rôle installé, vous obtenez la fenêtre ci-dessous ; cliquez le bouton « **Fermer** » :



Patientez pendant l'installation du rôle jusqu'à l'affichage du message de réussite.

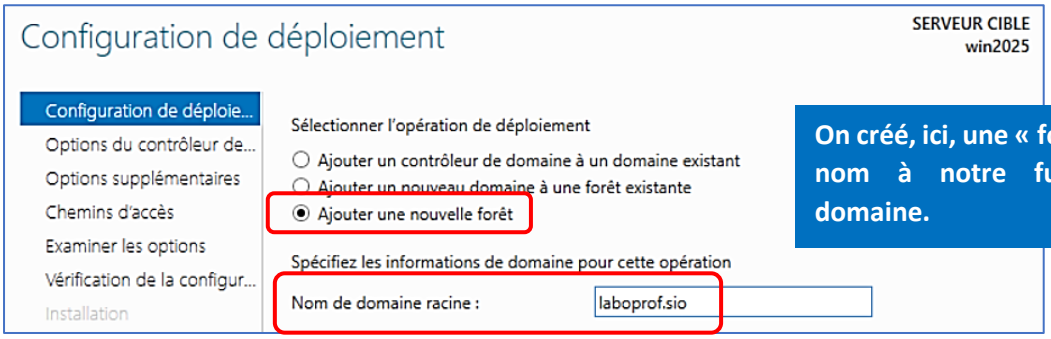
L'écran d'accueil du gestionnaire de tableau affiche un avertissement (triangle jaune) dans la partie haute :

- Cliquez le triangle jaune pour afficher la fenêtre ci-dessous :



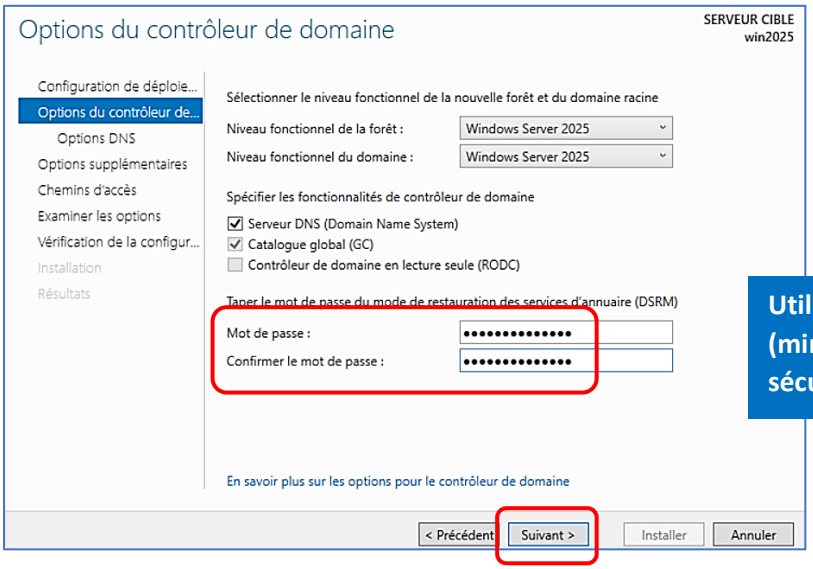
Une fois le rôle AD/DS installé, il faut « promouvoir » notre serveur au rang de contrôleur de domaine en cliquant le lien bleu qui est affiché dans le gestionnaire de serveur.

- Cliquez le lien « **Promouvoir ce serveur en contrôleur de domaine** » ; une fenêtre s'affiche
- Cliquez « **Ajouter une nouvelle forêt** » et saisissez le nom du domaine souhaité
- Cliquez le bouton « **Suivant** » :



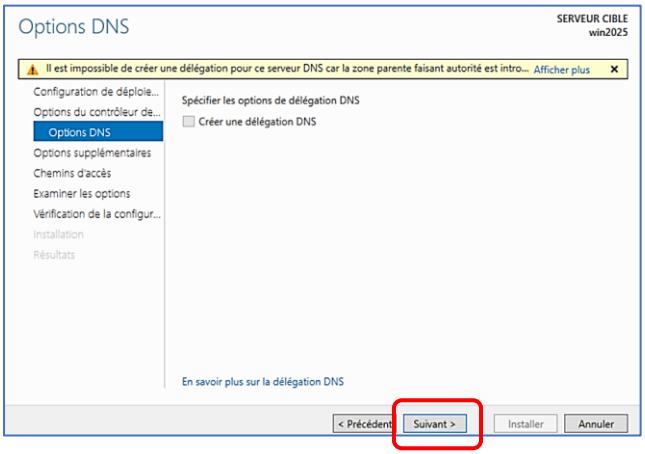
On créé, ici, une « forêt » et on donne un nom à notre futur contrôleur de domaine.

- Saisissez un mot de passe pour la restauration éventuelle des services d'annuaire et cliquez « **Suivant** » :



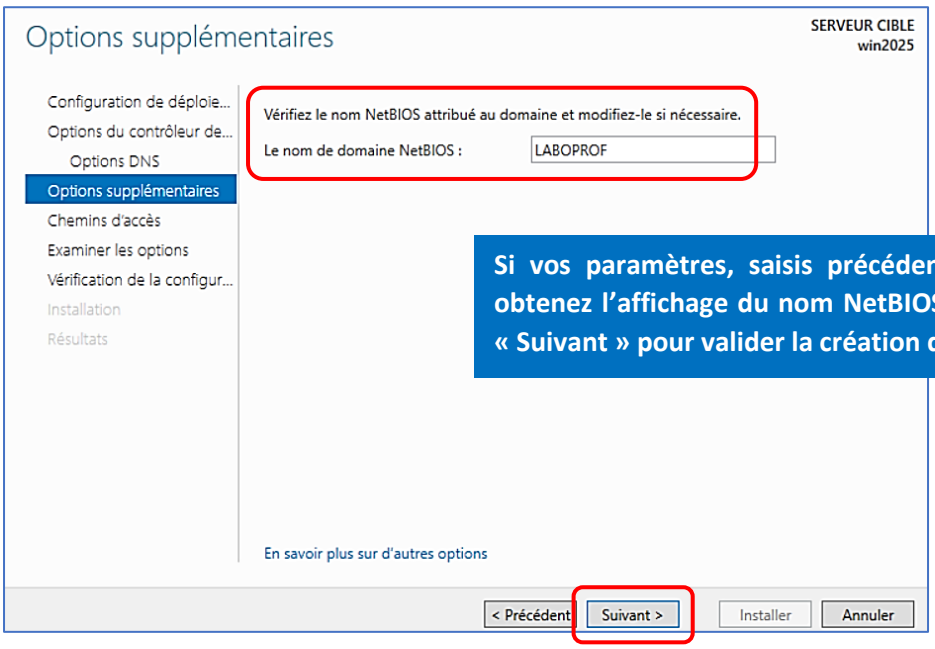
Utilisez des mots de passe forts (minimum 12 caractères) pour assurer la sécurité de votre contrôleur.

- Nous n'avons pas besoin, ici, de créer une délégation DNS ; cliquez le bouton « **Suivant** » :



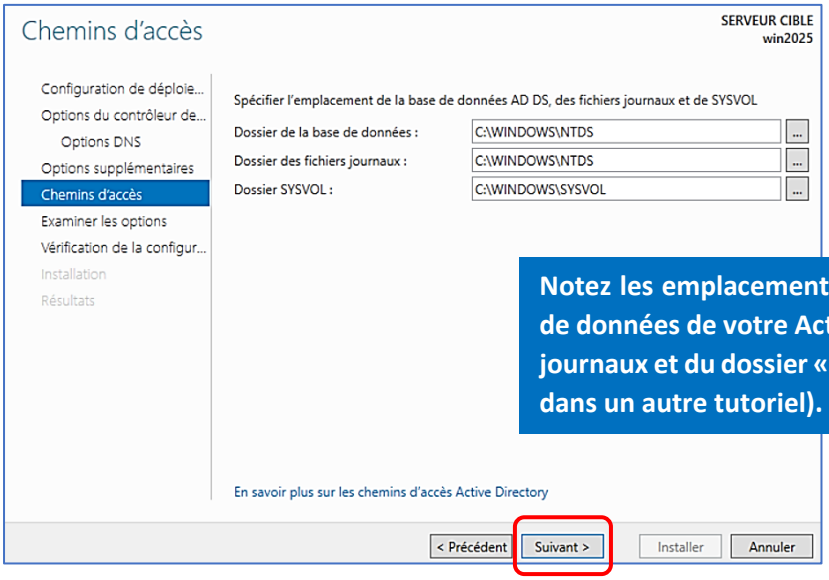
Il n'y a pas lieu, pour le moment, de créer une délégation DNS ici. Cliquez directement « Suivant » pour poursuivre.

- Patientez quelques instants ; le nom du domaine doit s'afficher ; cliquez le bouton « **Suivant** » :



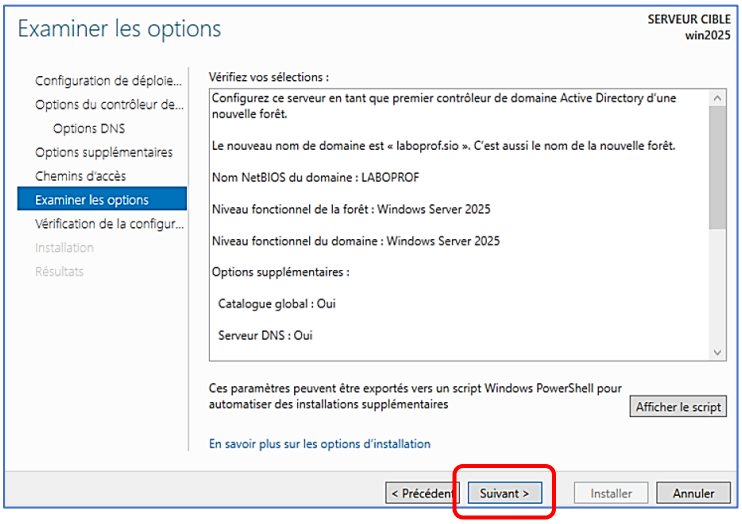
Si vos paramètres, saisis précédemment, sont corrects, vous obtenez l'affichage du nom NetBIOS de votre domaine. Cliquez « Suivant » pour valider la création du contrôleur de domaine.

- Laissez les chemins par défaut et cliquez le bouton « **Suivant** » :

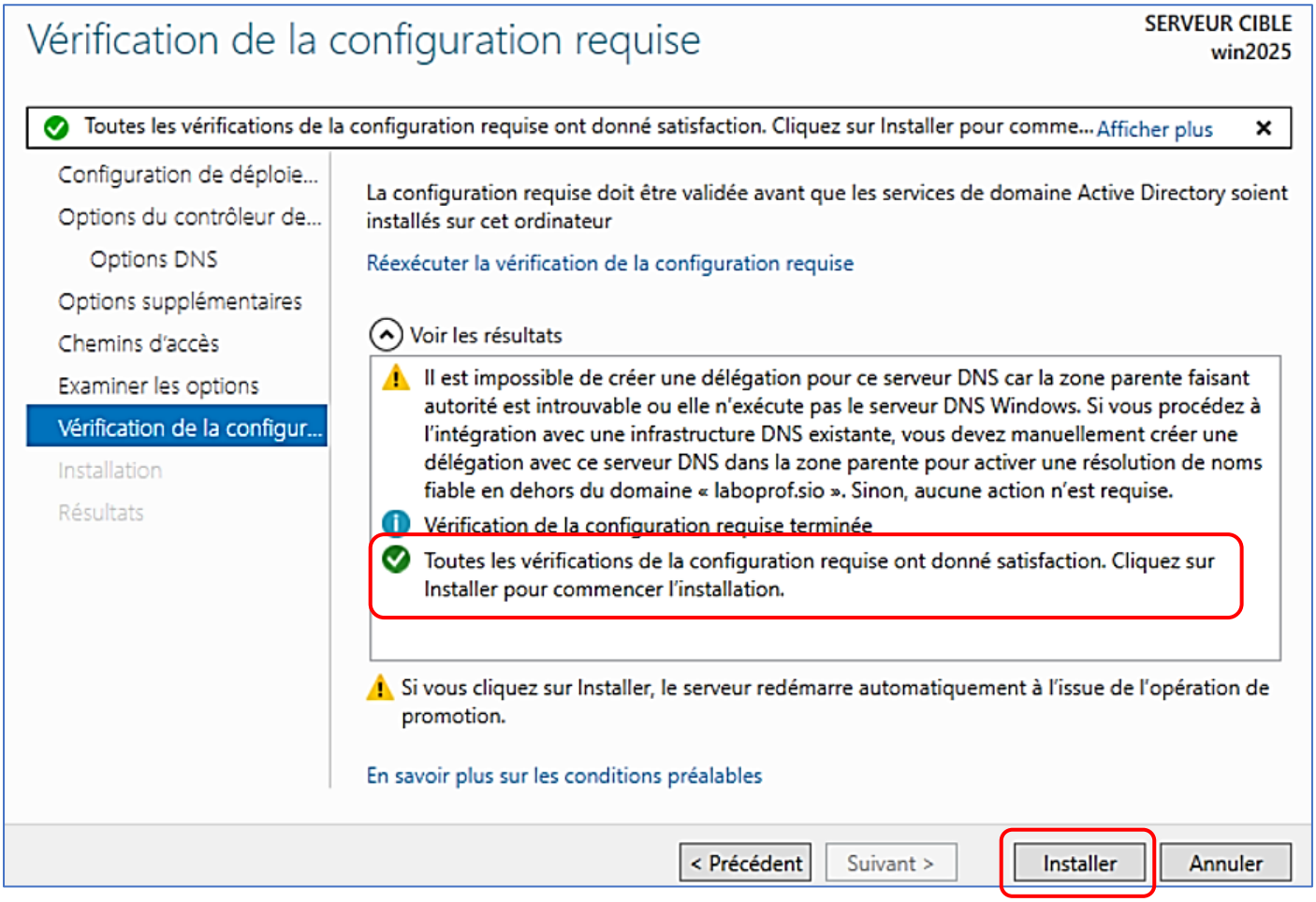


Notez les emplacements par défaut du dossier de la base de données de votre Active Directory ainsi que des fichiers journaux et du dossier « SYSVOL » (nous verrons son utilité dans un autre tutoriel).

- Examinez les options saisies et, si tout est correct, cliquez le bouton « **Suivant** » :

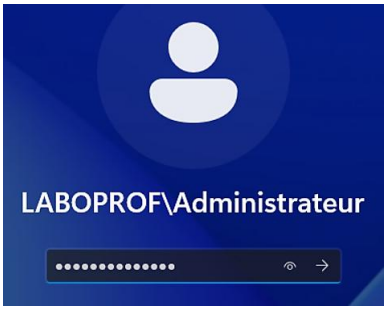


- Lancez la procédure d'installation du rôle en cliquant le bouton « **Installer** » :



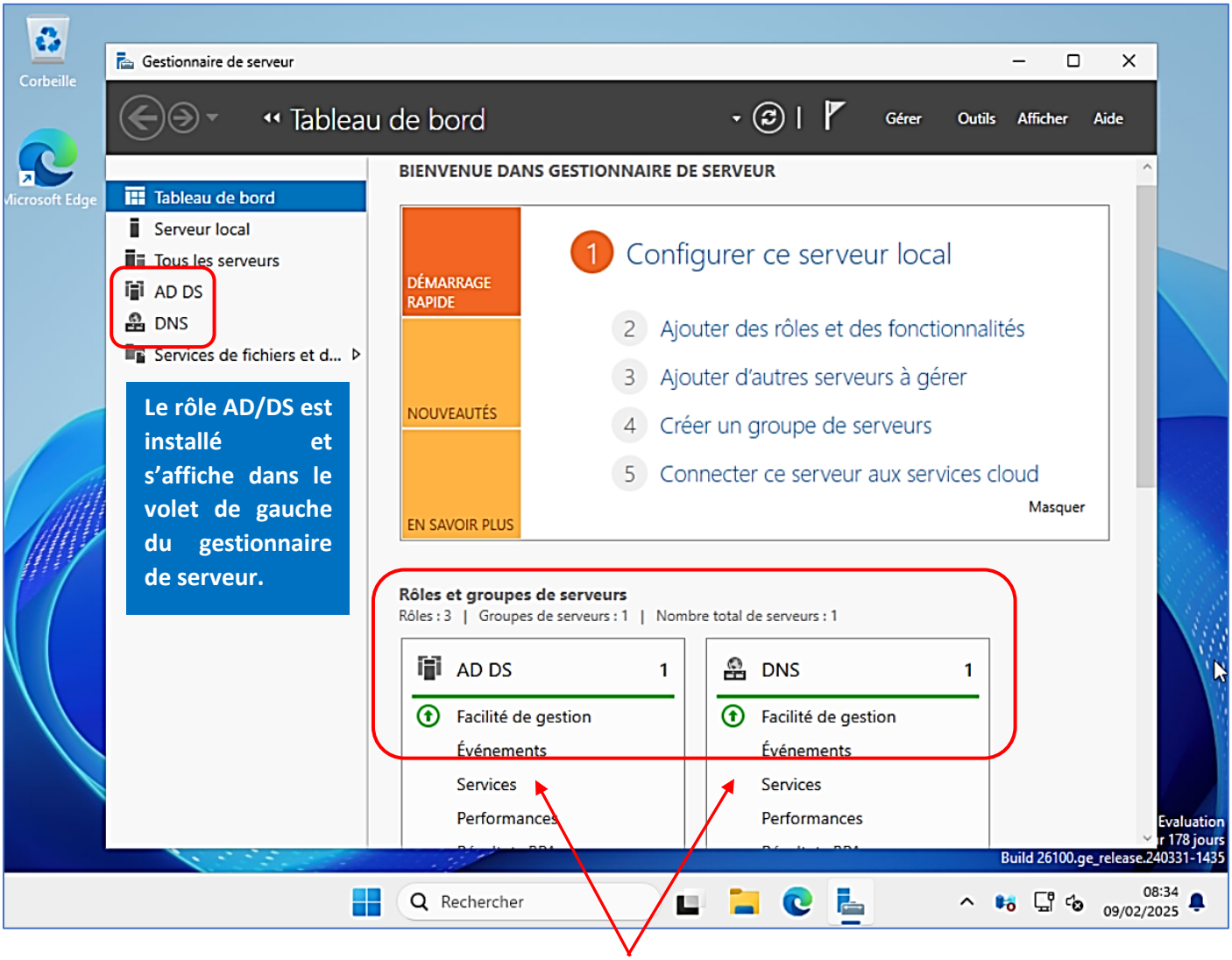
Il faut maintenant patienter plusieurs minutes le temps que le rôle soit complètement installé. La machine va redémarrer automatiquement une fois le processus terminé (le processus peut être long) :

Le serveur redémarre et affiche cette fenêtre d'ouverture de session ; saisissez le mot de passe de l'administrateur tel que vous l'avez défini lors de l'installation du serveur (tutoriel 1) :



Au redémarrage du serveur, la session administrateur s'affiche : saisissez le mot de passe défini lors de l'installation de Windows Server 2025 pour ouvrir la session.

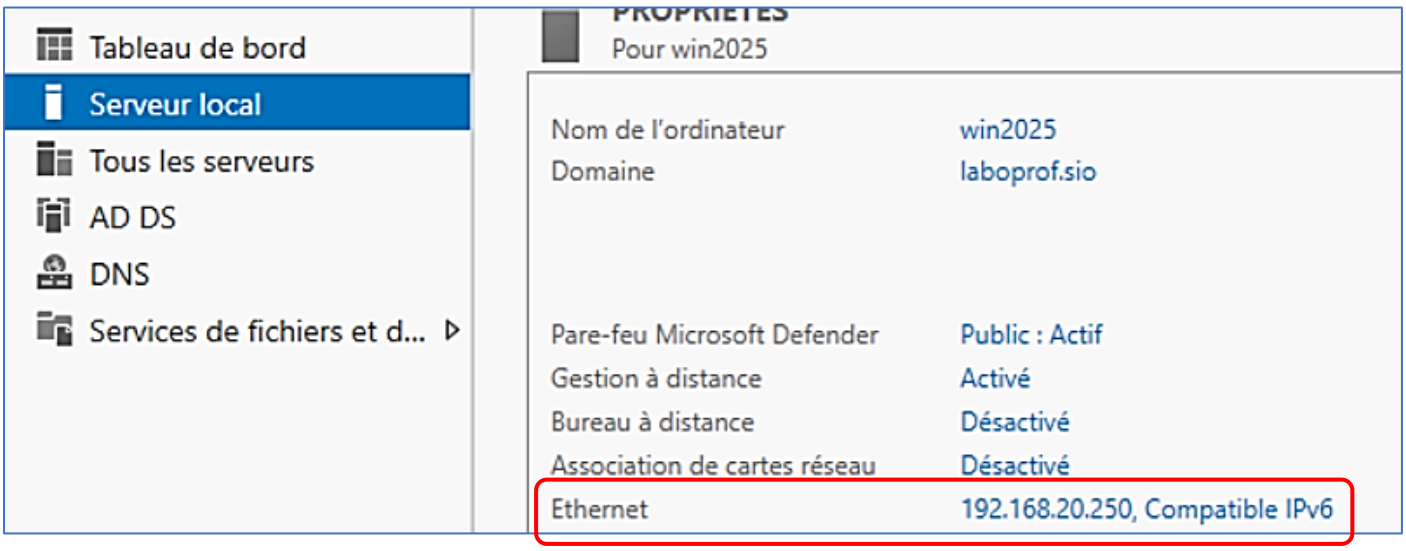
L'écran d'accueil de votre serveur affiche le gestionnaire de serveur (tableau de bord). On peut voir que les rôles « AD/DS » et « DNS » sont maintenant installés et configurés (volet de gauche) :



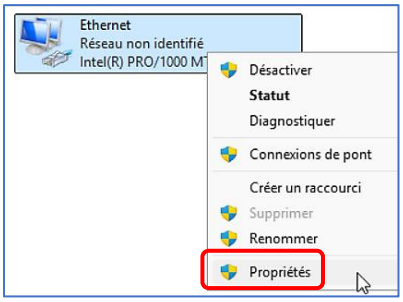
Le gestionnaire de serveur affiche, également, l'état des services (voir ci-dessus) en vert une fois que ces derniers sont initialisés (en fonction des ressources de votre hyperviseur, l'état « vert » ne sera peut-être pas immédiat).

Le menu « **Outils** » sera le menu qui sera principalement utilisé par la suite.

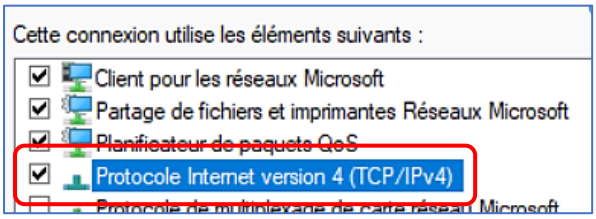
Une fois le rôle AD/DS installé, on va vérifier le paramétrage IP en cliquant sur « **Serveur local** » (volet de gauche) et sur le lien « **Ethernet** » avec l'adresse IP configurée lors de l'installation (tutoriel 1) :



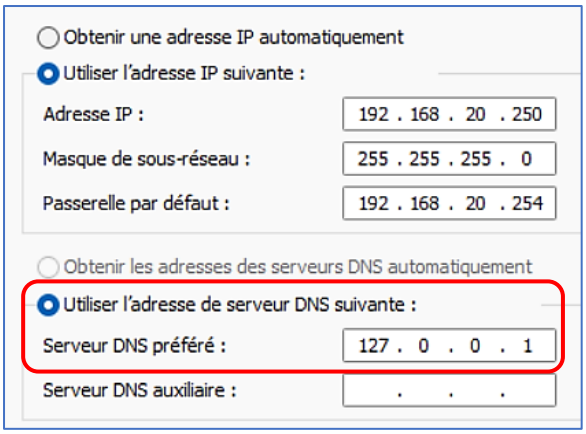
- Faites un clic droit sur l'icône « **Ethernet** » et cliquez « **Propriétés** » :



- Double-cliquez sur l'option « **Protocole Internet version 4 (TCP/IPv4)** » :

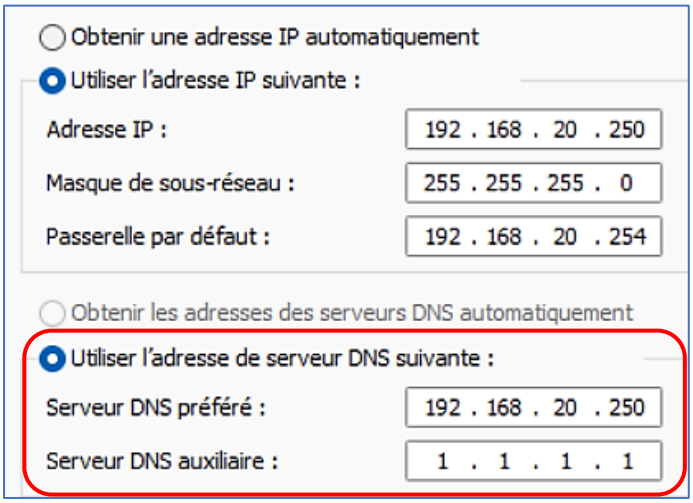


On constate que le serveur DNS a été configuré sur l'adresse « localhost », à savoir 127.0.0.1. Nous vous recommandons de la modifier car cela peut engendrer des erreurs par la suite :



Par défaut, lors de l'ajout du rôle AD/DS, Windows a modifié l'adresse IP du serveur DNS préféré en indiquant l'adresse « localhost » de type 127.0.0.1

- Remplacez l'adresse localhost 127.0.0.1 par l'adresse IP de votre serveur et validez la modification :



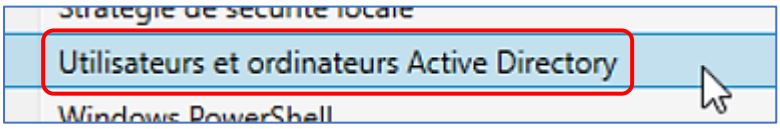
Nous vous recommandons de modifier l'adresse IP « localhost » par celle exacte de votre serveur pour éviter tous problèmes de connexion par la suite (notamment lors de l'intégration des machines clientes à votre domaine).

7 – CREER UNE UNITE D'ORGANISATION DANS L'ACTIVE DIRECTORY

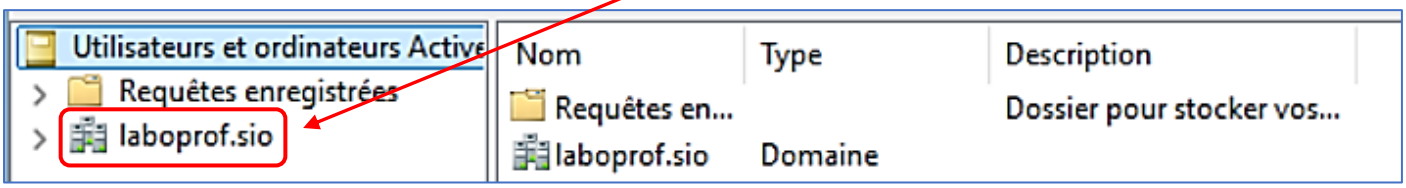
Les **unités d'organisation (appelées « OU »)** sont des **containers d'objets afin de faciliter l'organisation de l'annuaire** et **permettre une organisation avec plusieurs niveaux**. Sans les unités d'organisations, l'annuaire ne pourrait pas être trié correctement et l'administration serait moins efficace.

On peut comparer les unités d'organisations à des dossiers qui permettent de ranger les objets à l'intérieur.

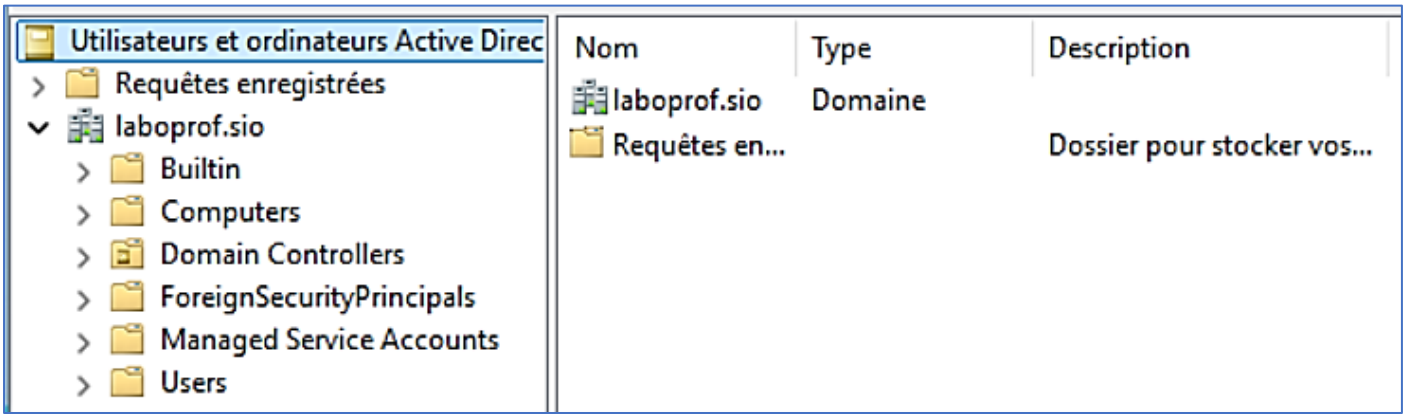
- Dans le gestionnaire de serveur, cliquez le menu « **Outils** » et « **Utilisateurs et ordinateurs Active Directory** » :



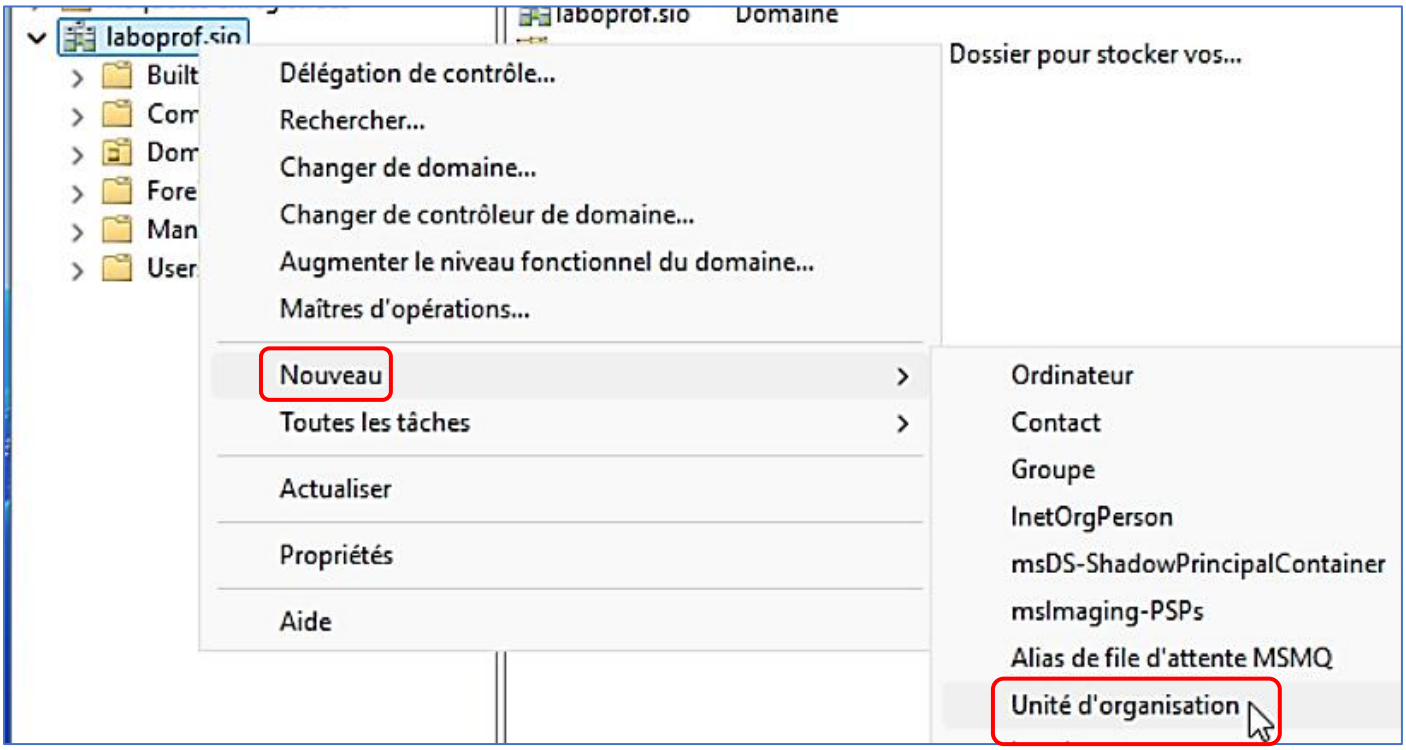
Une fenêtre s'affiche avec le nom de votre contrôleur de domaine (« laboprof.sio » dans notre cas) :



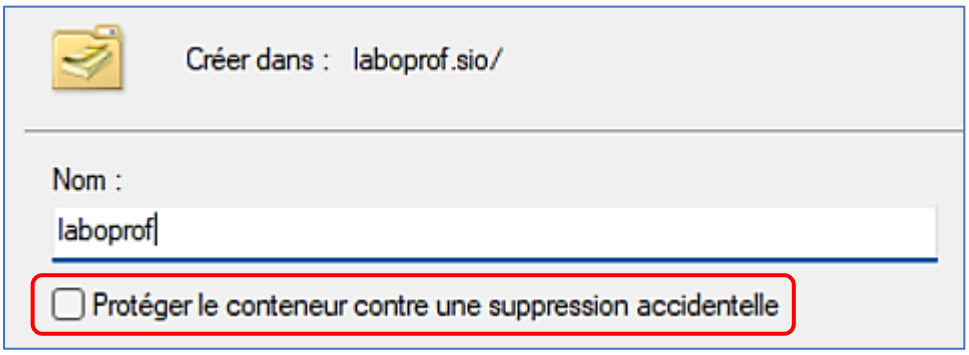
- Cliquez sur « **>** » pour déployer l'arborescence de votre Active Directory :



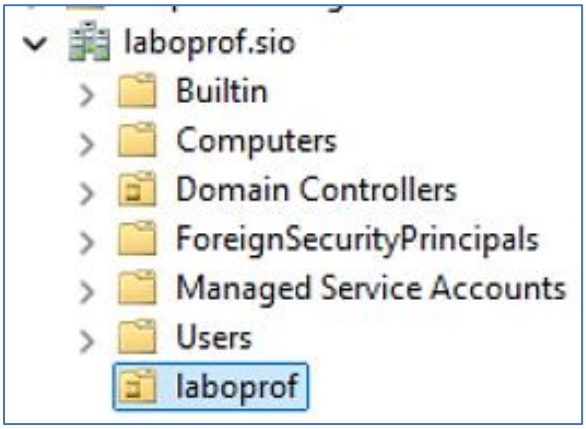
- Faites un clic droit sur le nom de votre contrôleur de domaine et cliquez « **Nouveau** » - « **Unité d'organisation** » :



- Une fenêtre s'affiche ; saisissez le nom de votre unité d'organisation (ici, nous avons repris le nom de notre domaine**). Attention, si vous voulez conserver la possibilité de supprimer l'unité d'organisation par la suite, il faut décocher la case** « **Protéger le conteneur contre une suppression accidentelle** ». Validez la création de votre unité d'organisation en cliquant le bouton « **OK** » :



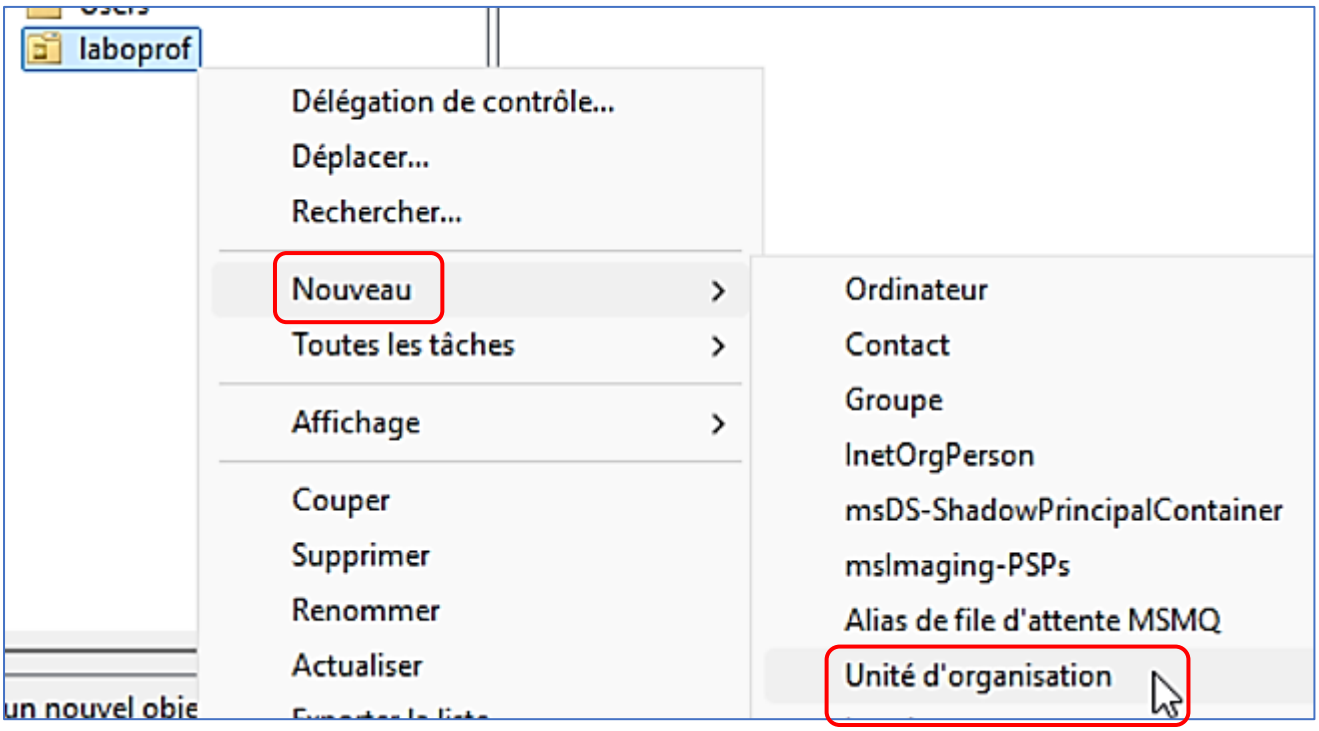
L'unité d'organisation apparaît maintenant dans votre Active Directory sous cette forme :



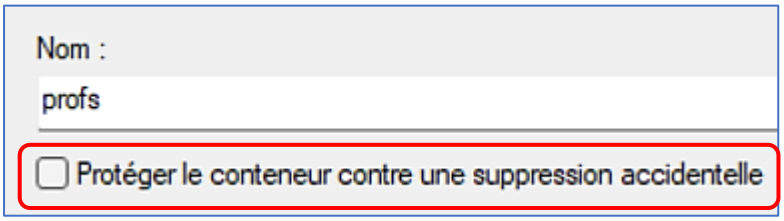
Ici, nous avons créé une unité d'organisation « générale » portant le nom de « LABOPROF ». La OU est symbolisé par un petit symbole. La OU « LABOPROF » sera la OU principale qui contiendra d'autres unités d'organisation permettant d'organiser et de structurer l'Active Directory en fonction de l'organisation (on peut penser aux différents services de l'entreprise par exemple).

Nous allons créer, dans l'unité d'organisation générale, deux autres unités d'organisation que nous nommerons « profs » et « élèves ». Pour cela, effectuez les manipulations suivantes :

- **Faites un clic droit sur l'unité d'organisation créée précédemment** et cliquez « **Nouveau** » - « **Unité d'organisation** » :

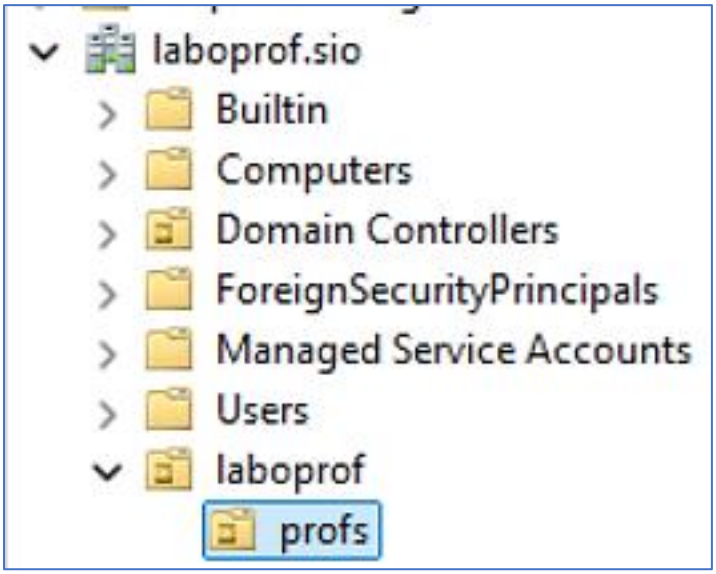


- Créez la OU « **profs** » et validez en cliquant le bouton « **OK** » :

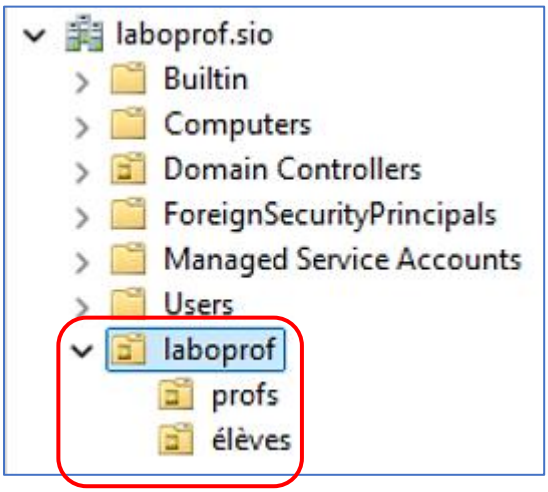


Attention, par défaut la case « Protéger le conteneur… » est cochée. Cela signifie que vous ne pourrez pas supprimer l'unité d'organisation par la suite si vous laissez la case activée (à voir en fonction de votre stratégie de sécurité). Ici, nous l'avons décochée car nous sommes dans un environnement de laboratoire.

Votre arborescence devrait ressembler à ceci :



- Répétez l'opération précédente pour créer la OU « élèves » afin d'obtenir ceci :

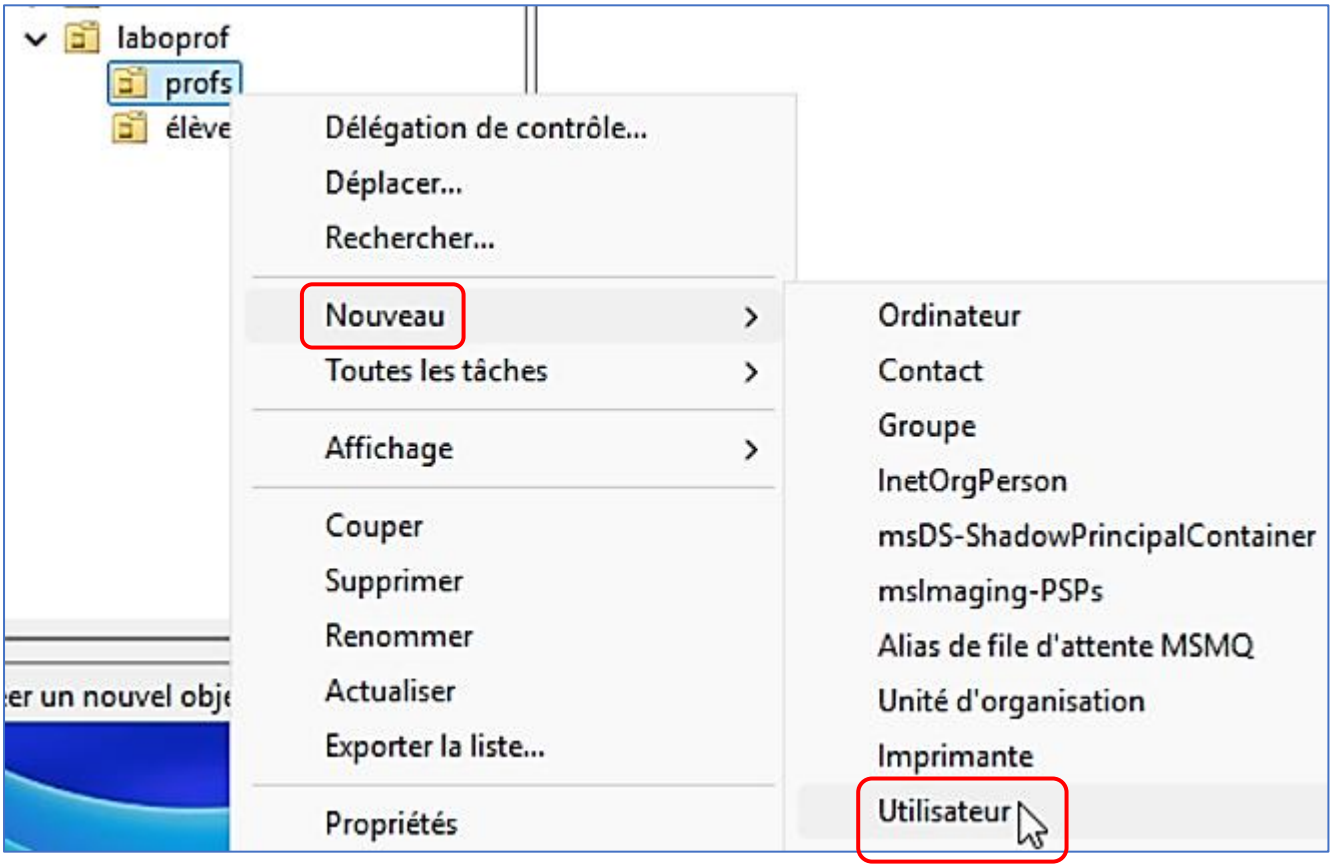


L'unité d'organisation générale « LABOPROF » comporte maintenant 2 autres unités d'organisation qui reflètent l'organisation interne de l'entreprise.

La structure de notre Active Directory est maintenant prête. Nous allons maintenant ajouter des utilisateurs à notre Active Directory.

8 – CREER DES UTILISATEURS ET DES GROUPES D'UTILISATEUR DANS L'ACTIVE DIRECTORY

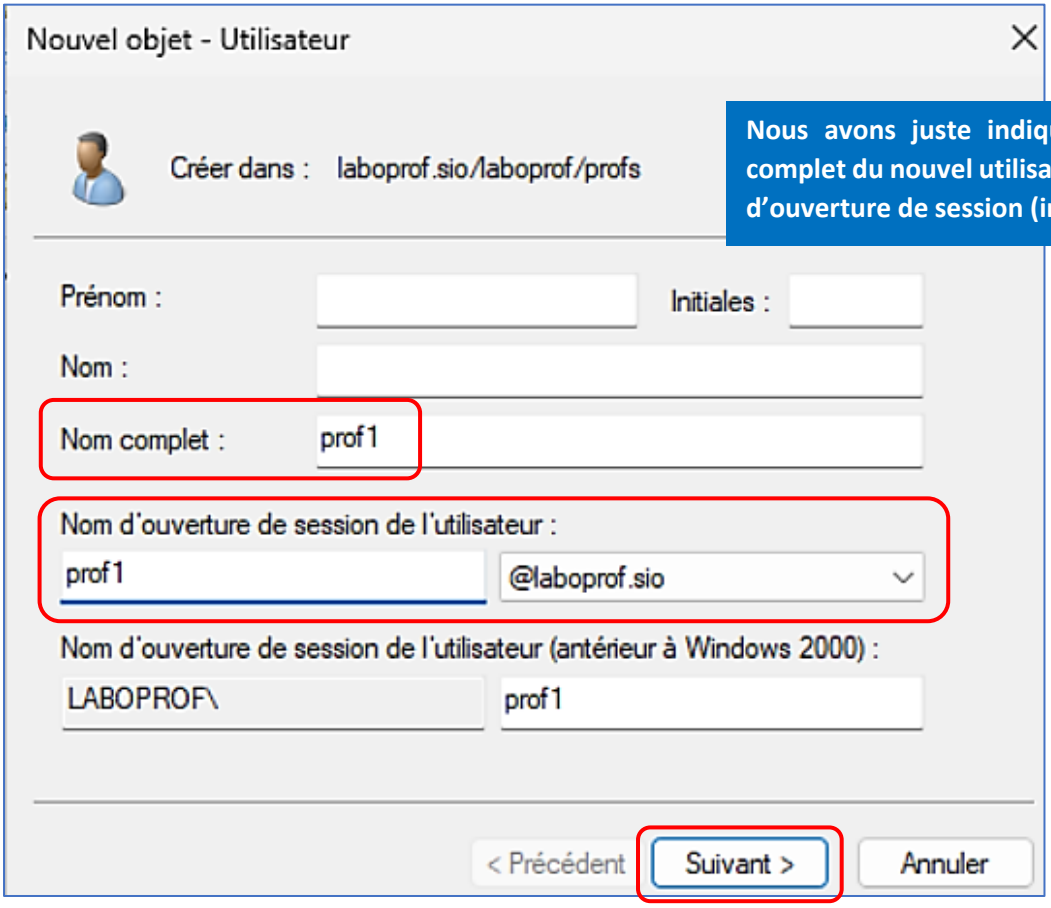
- Faites un clic droit sur la OU « profs » et créez un utilisateur en cliquant « **Nouveau** » - « **Utilisateur** » :



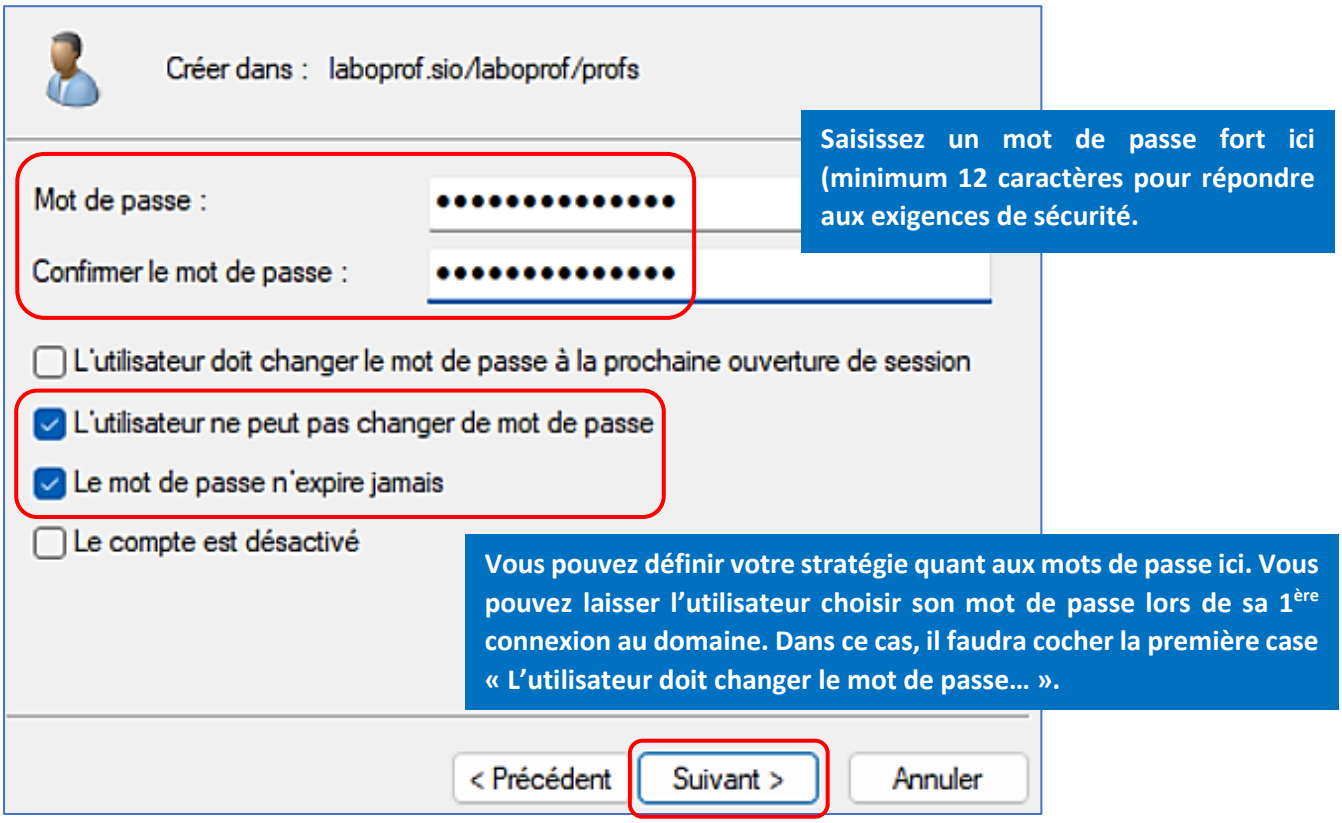
Remarque :

En faisant un clic droit sur la OU « profs », l'utilisateur sera automatiquement ajouté à la OU. Si vous faites un clic droit sur « Users », l'utilisateur ne sera pas ajouté à la OU « profs » et il faudra, par la suite, le déplacer dans la OU adéquate.

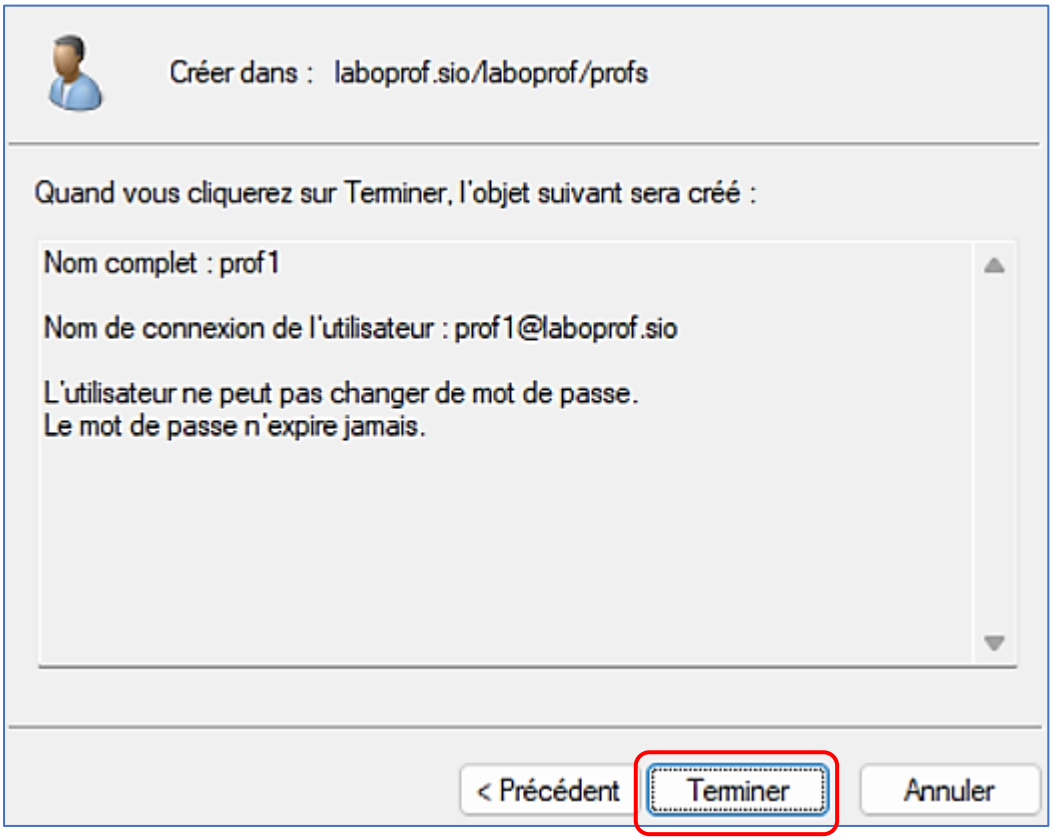
- Une fenêtre s'affiche ; complétez l'identifiant du nouvel utilisateur et cliquez « **Suivant** » :



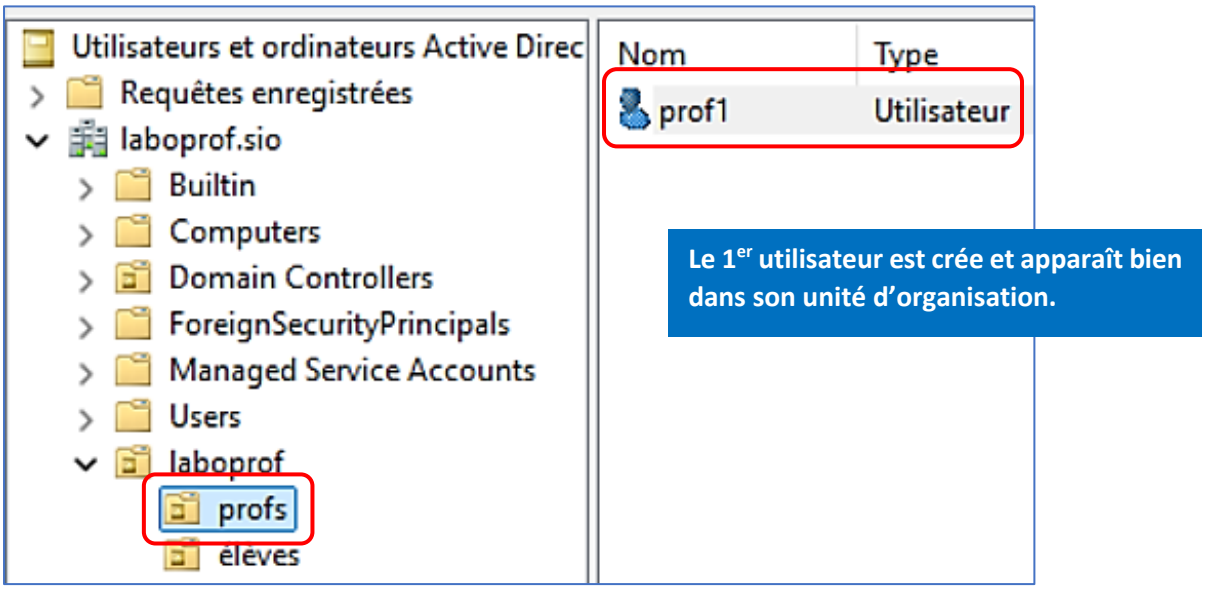
- Saisissez un mot de passe fort pour l'utilisateur et configurez les options en rapport avec le mot de passe de session de l'utilisateur selon votre politique de sécurité ; validez vos choix en cliquant « **Suivant** » :



- Confirmez la création de votre utilisateur en cliquant « **Terminer** » :



Votre utilisateur a été créé directement dans l'unité d'organisation « profs » :

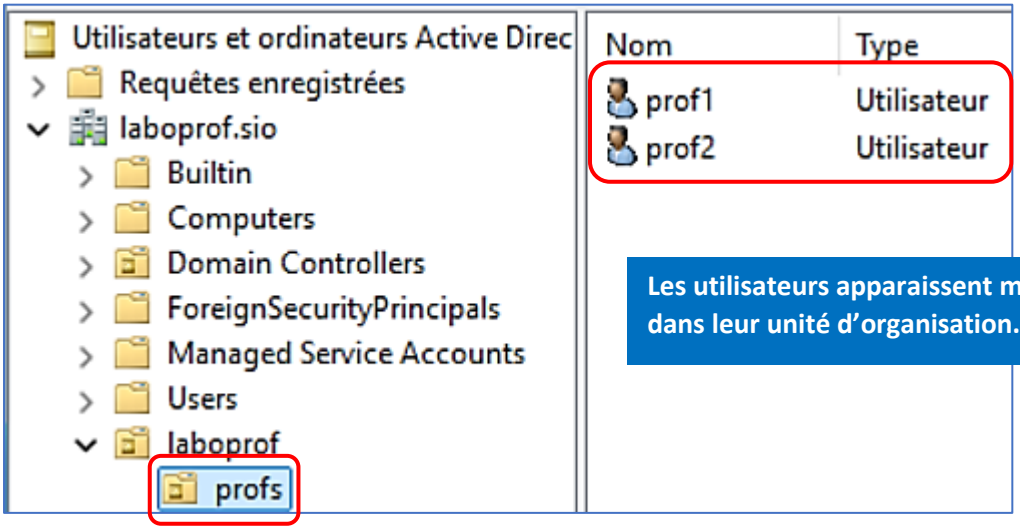


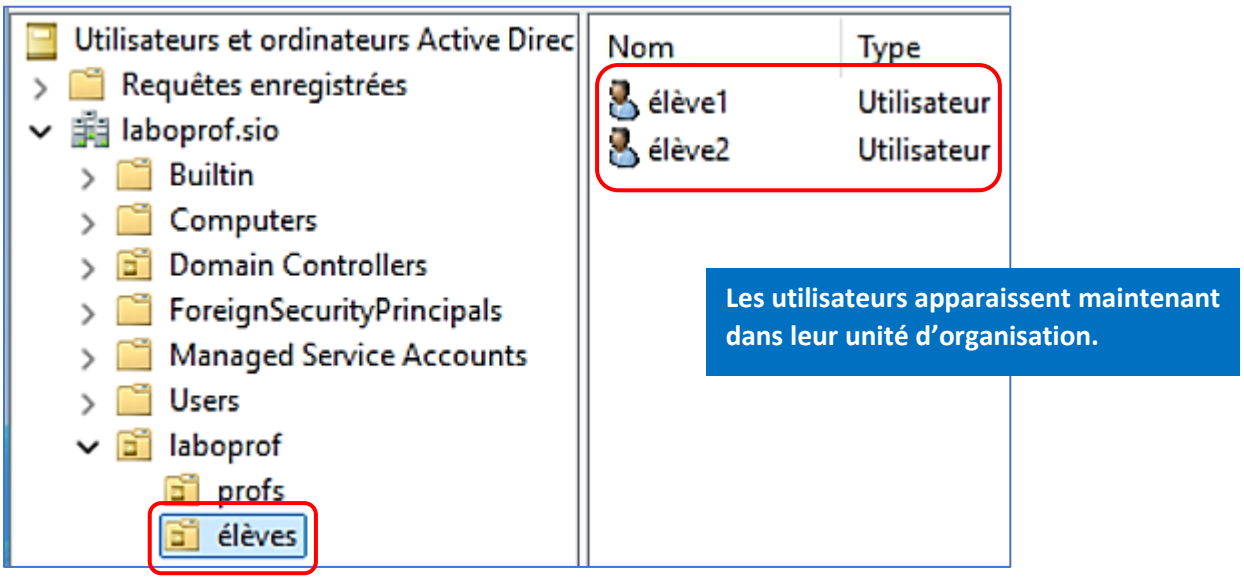
Répétez l'opération pour créer un autre utilisateur « prof2 » dans l'unité d'organisation « profs » et « élève1 », « élève2 » dans l'unité « élèves ».

Remarque :

Pour créer un autre utilisateur, vous pouvez faire un clic droit sur l'utilisateur « prof1 » et cliquer « **Copier** » (autre possibilité).

Votre Active Directory soit se présenter ainsi :

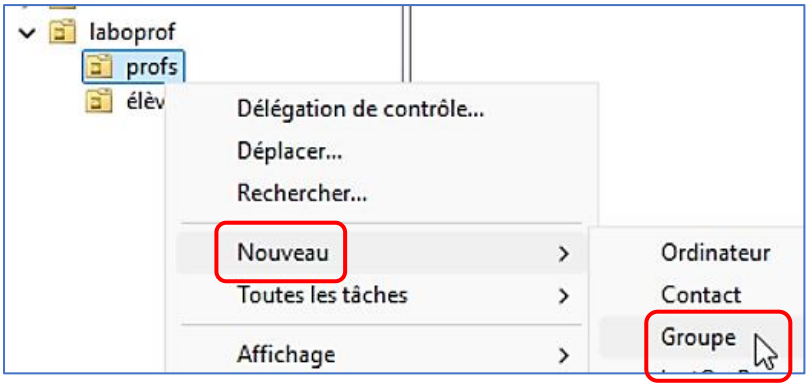




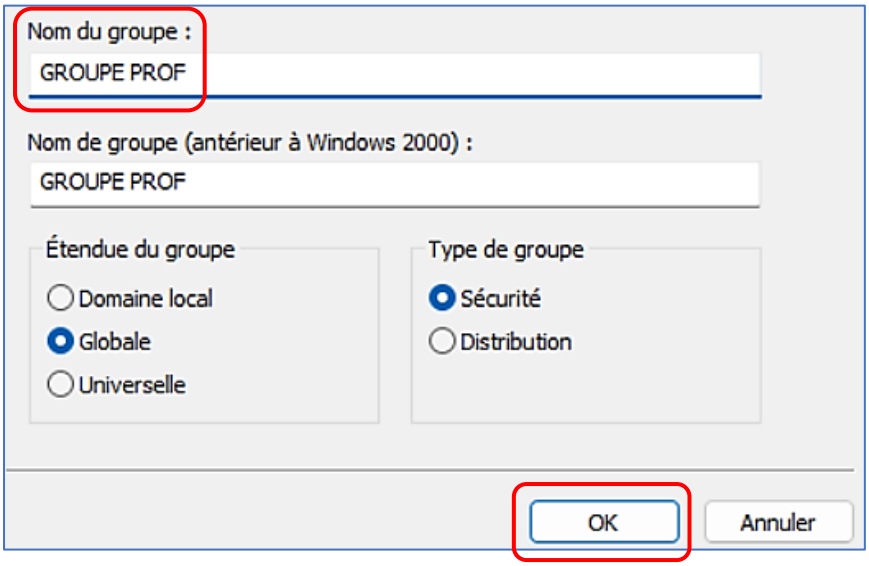
9 – CREER UN GROUPE D'UTILISATEUR DANS L'ACTIVE DIRECTORY

Il est intéressant de créer des « **groupes d'utilisateurs** » **car ils permettront une meilleure gestion des droits pour les utilisateurs membres du groupe**. Par exemple, dans un autre tutoriel, nous verrons comment partager des ressources (lecteurs réseau) et la gestion des groupes d'utilisateurs facilitera le partage des dossiers et la gestion des droits pour les membres du groupe.

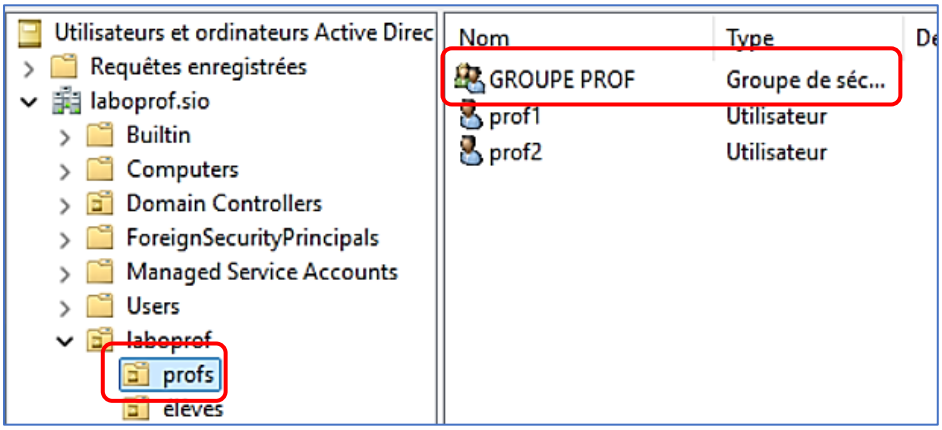
- Faites un clic droit sur la OU « **profs** » et cliquez « **Nouveau** » - « **Groupe** » :



- Saisissez un nom de groupe et cliquez le bouton « **OK** » :

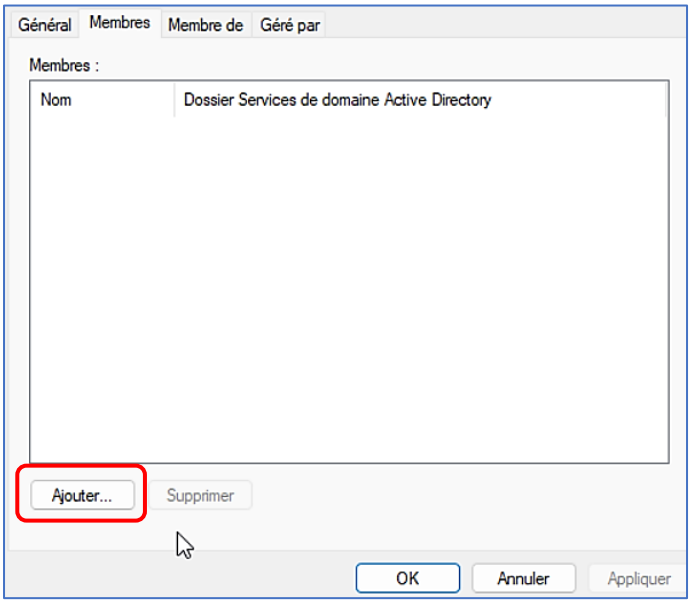


L'arborescence se présente ainsi :

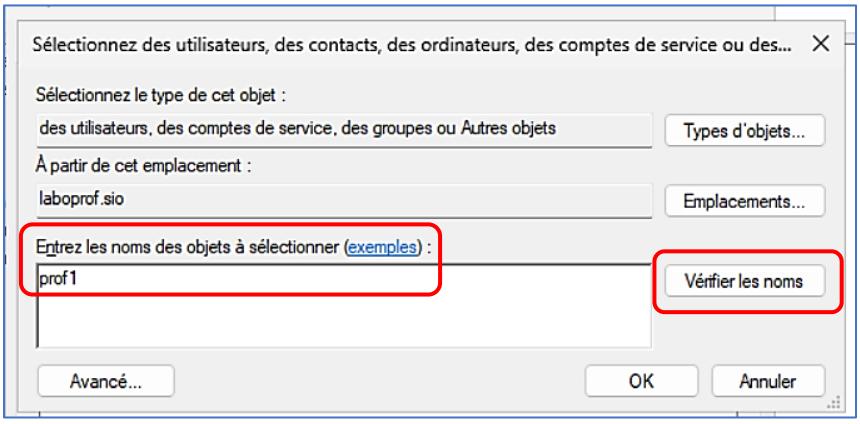


On ajoute, ensuite, les membres dans le groupe adéquat (les profs dans notre cas) :

- Double-cliquez sur le nom du groupe concerné : une fenêtre s'affiche ; cliquez « **Ajouter** » :

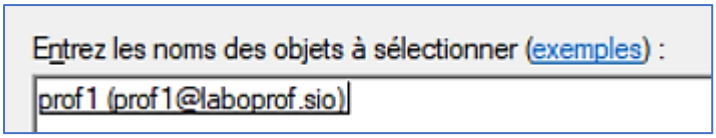


- Saisissez le nom des utilisateurs concernés, par exemple « prof1 » et cliquez le bouton « **Vérifier les noms** » :



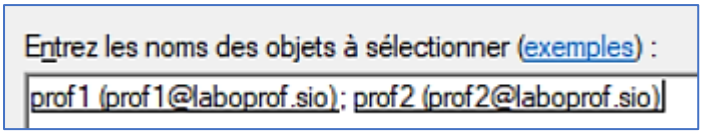
Vous pouvez aussi rechercher vos utilisateurs « manuellement » dans l'AD en cliquant le bouton « Avancé » et « Rechercher ».

Si l'utilisateur est localisé dans l'Active Directory, la fenêtre affiche ceci :

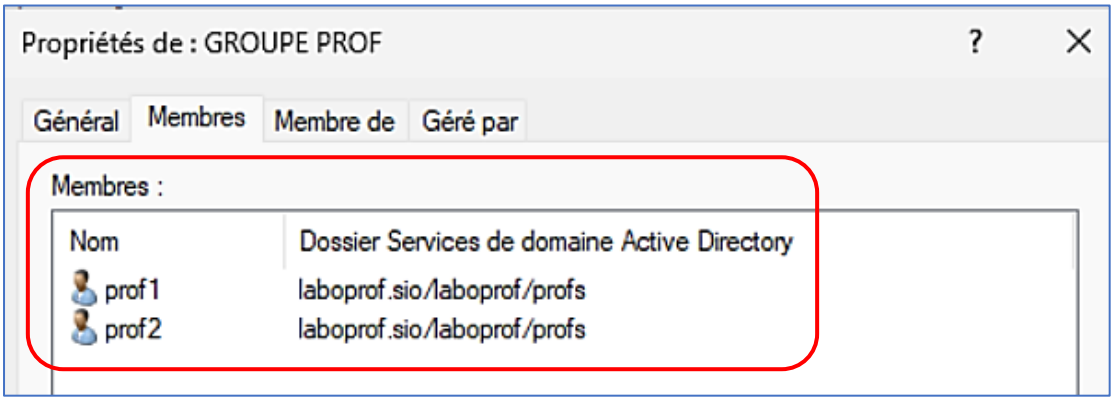


- Saisissez le nom de l'autre utilisateur à ajouter au groupe :

Si l'utilisateur est localisé dans l'Active Directory, la fenêtre affiche ceci :

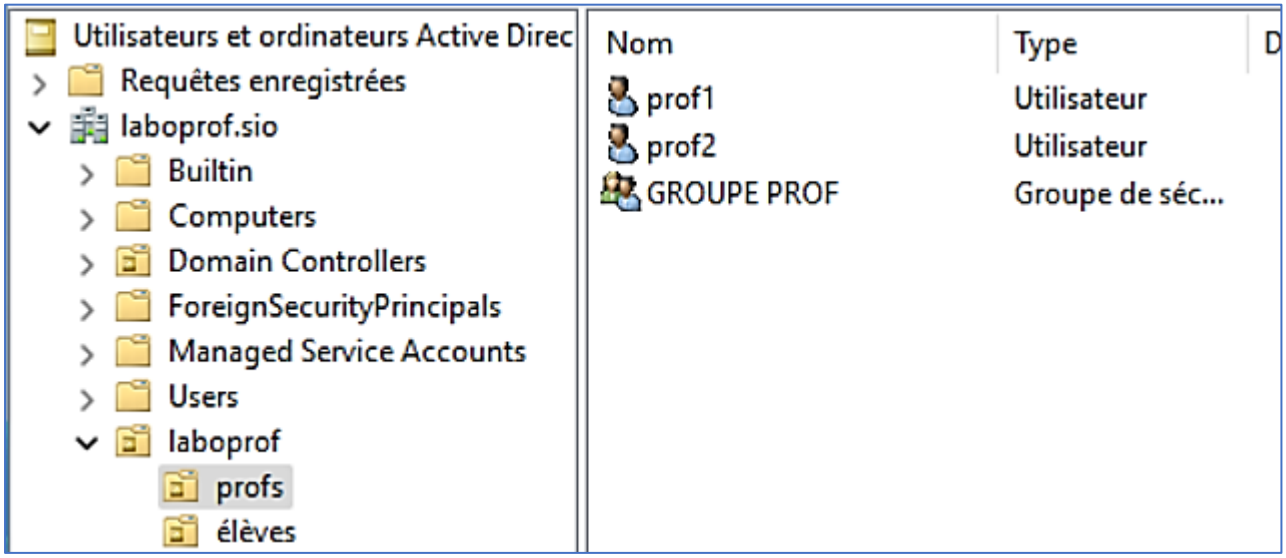


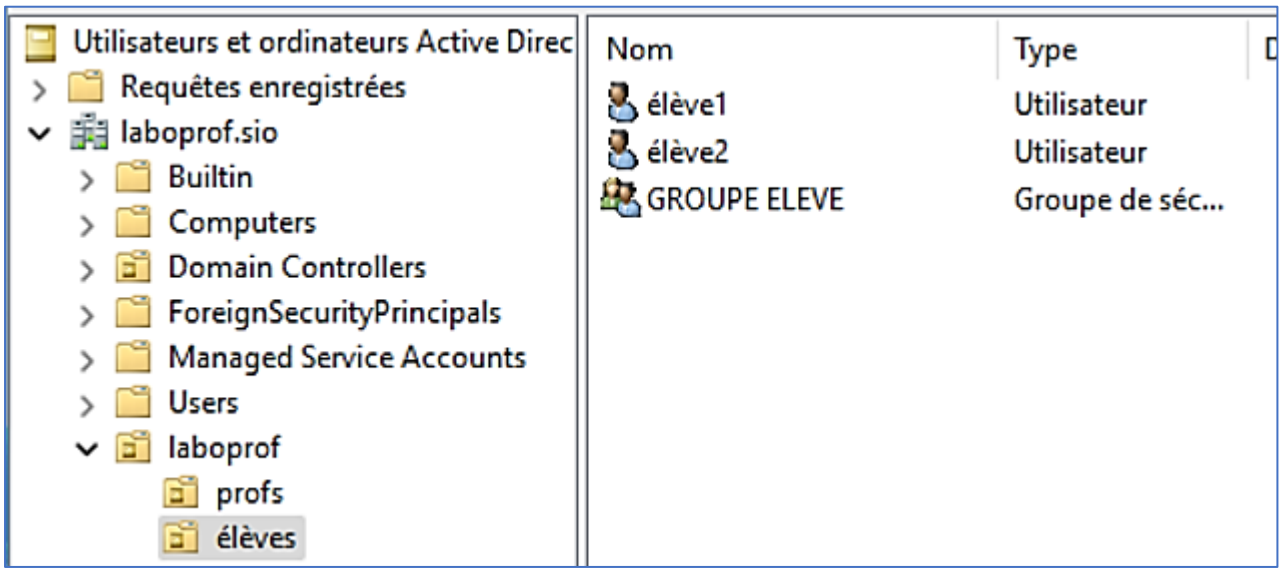
- Cliquez le bouton « **OK** », vous obtenez ceci :



- Cliquez à nouveau le bouton « **OK** » pour valider l'ajout de ces utilisateurs au groupe « profs ». Répétez ces opérations afin de créer un groupe que vous nommerez « **GROUPE ELEVE** » et dans lequel vous ajouterez les utilisateurs concernés (« élève1 » et « élève2 »).

Vous devez obtenir l'arborescence suivante :





Notre Active Directory est maintenant prêt.

Remarque :

Il est important de bien structurer votre Active Directory en fonction de l'organisation de votre entreprise. Le découpage en unités d'organisation (« OU ») et groupes d'utilisateurs facilitera la gestion future de votre Active Directory notamment lorsque vous devrez mettre en place diverses stratégies (voir tutoriels suivants).

Dans un prochain tutoriel, nous verrons comment partager des ressources comme des lecteurs réseau en utilisant les groupes d'utilisateurs, les unités d'organisation et les droits associés.