



# Compte-rendu LDAP et Active Directory

12/03/25 23h50

Nous avons essayé de faire un serveur LDAP basé sur Active Directory sur un pc afin de gérer l'authentification et l'accès aux ressources réseau. L'objectif était de comprendre le fonctionnement de LDAP, d'assurer une bonne intégration avec le poste client (Gabriel et Kaatché) et d'établir une liaison efficace entre le/les utilisateur/s et les services du réseau.

## Définition de LDAP et lien avec Active Directory :

LDAP (Lightweight Directory Access Protocol) est un protocole standard utilisé pour interroger et modifier des services d'annuaire. Il permet de gérer des informations sur les utilisateurs, les groupes et les ressources au sein d'un réseau. LDAP fonctionne comme un annuaire hiérarchique où les données sont stockées sous forme d'objets organisés en une structure arborescente.

Active Directory (AD) est une implémentation de service d'annuaire développée par Microsoft, qui repose sur LDAP pour l'authentification et la gestion des utilisateurs. AD permet de centraliser la gestion des identités et des accès aux ressources dans un environnement Windows, tout en offrant des fonctionnalités supplémentaires telles que la gestion des stratégies de groupe (GPO) et l'intégration avec d'autres services réseau.

## Matériel Utilisé :

Système d'exploitation : Windows 10 et Windows Server 2019 ( sur vm)

Outils de virtualisation : VirtualBox

Postes clients (Gabriel et Kaatché) : Windows 10 ( vm)

Infrastructure matérielle : 2 ordinateurs, dont un dédié en tant que serveur de fichiers et contrôleur de domaine Active Directory

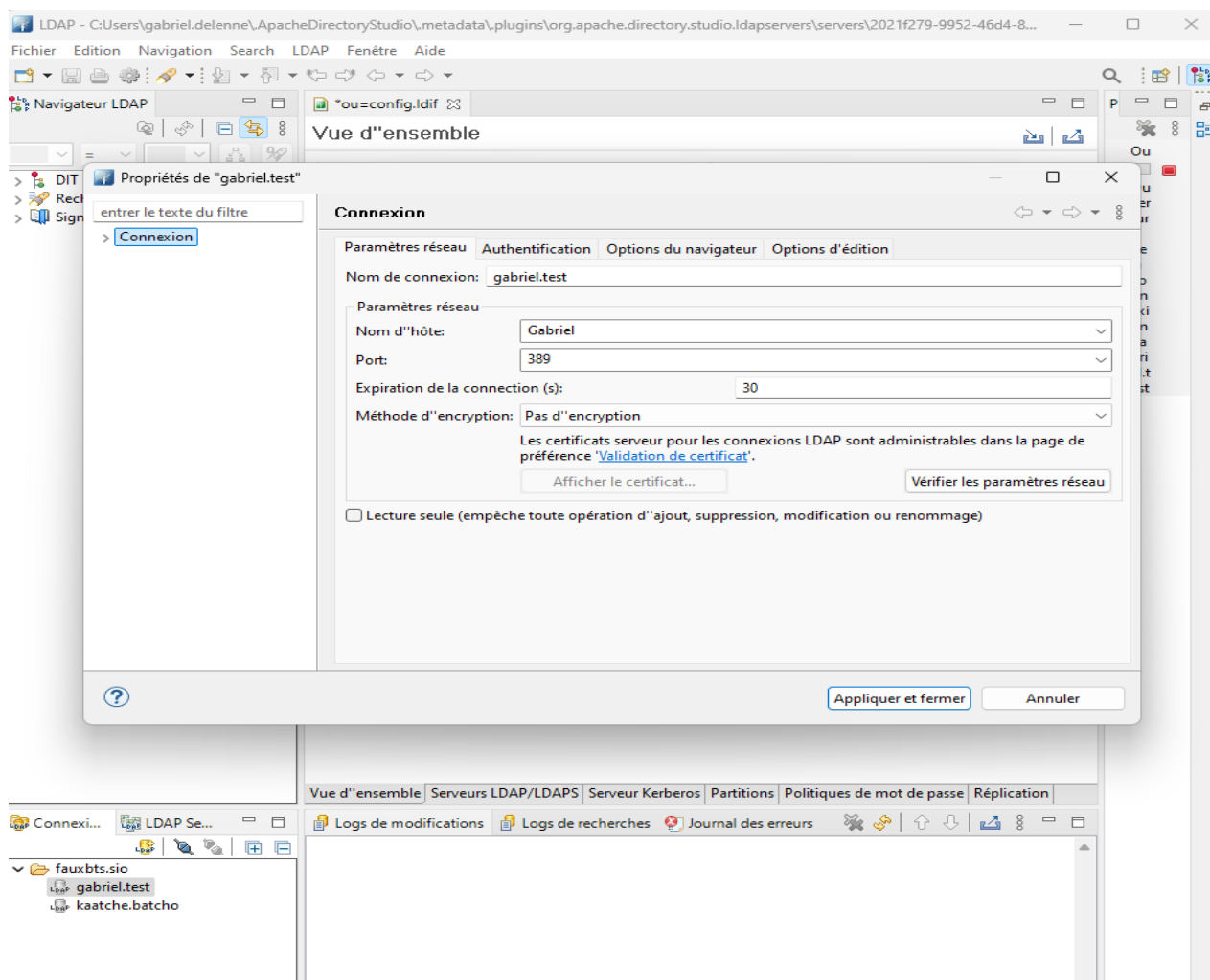


Parameter	LDAP	AD
Abbreviation for	Lightweight Directory Access Protocol	Active Directory
Phylosophy	A protocol for applications that queries and modifies items in directory systems like Active Directory that supports LDAP	A database used for authentciation, directory, policy, and other services in a Windows working environment. Its directory structure is hierarchical and it contanis infromation of all users in the network.
Funcionality	It is one of the protocols used for communication with Active Directory	AD is a directory database
Standard	LDAP is a standard	It is a Microsoft's product
Supported Platforms	Made mainly for Linux/Unix digital environment	AD is a Microsoft's directory made for Windows users, applications, and devices

### Déroulé :

1) Installation du poste client sur VM avec windows 10 et de la machine pour héberger le contrôleur de domaine AD :

Explications tentative à l'oral avec ApacheLDAP studio :





The screenshot shows the Apache Directory Studio interface for configuring an LDAP server. The window title is "LDAP - C:\Users\gabriel.delenne\ApacheDirectoryStudio\metadata\plugins\org.apache.directory.studio.ldap.servers\servers\2021f279-9952-46d4-8...". The menu bar includes "Fichier", "Edition", "Navigation", "Search", "LDAP", "Fenêtre", and "Aide".

The main area is titled "Vue d'ensemble" (Overview) and contains several sections:

- Serveurs LDAP/LDAPS:** Two instances are listed, both with "Activer le serveur LDAP" checked. The first has port 10389 (default 10389), and the second has port 10636 (default 10636). A link "Configuration avancée LDAP/LDAPS..." is provided.
- Partitions:** A section stating "Il y a 2 partitions définies :". A list shows "example (dc=example,dc=com) [JDBM]" and "system (ou=system) [JDBM]". A link "Configuration avancée des partitions..." is provided.
- Serveur Kerberos:** "Activer le serveur Kerberos" is checked. The port is 60088 (default 60088). "Activer le serveur Kerberos Change Password" is also checked, with port 60464 (default 60464). A link "Configuration avancée Kerberos..." is provided.
- Options:** "Autoriser l'accès anonyme" is checked. "Activer le contrôle d'accès" and "Masquer les mots de passe" are unchecked.

The bottom of the window features a tabbed interface with "Vue d'ensemble", "Serveurs LDAP/LDAPS", "Serveur Kerberos", "Partitions", "Politiques de mot de passe", and "Réplication". Below the tabs are "Logs de modifications", "Logs de recherches", and "Journal des erreurs".

On the left, the "Navigateur LDAP" (LDAP Navigator) shows a tree structure with "DIT", "Recherches", and "Signets". At the bottom left, a "Connexi..." (Connections) window shows a tree for "fauxbts.sio" with users "gabriel.test" and "kaatche.batcho".

On the right, a vertical sidebar contains a list of error messages, including "Ou Un e erre ur est sur ven ue lors de l'o uve rtur e de la con nex ion - ERR \_04 121 \_C AN NO T\_R ES OL VE\_ HO ST NA ME Ca nn ot con nec t to the ser ver, Ho stn am e 'Ga brie l' cou ld not".



The screenshot shows the Apache Directory Studio interface for configuring LDAP servers. The main window is titled "LDAP - C:\Users\gabriel.delenne\ApacheDirectoryStudio\metadata\plugins\org.apache.directory.studio.ldapservers\servers\2021f279-9952-46d4-8...". The menu bar includes "Fichier", "Edition", "Navigation", "Search", "LDAP", "Fenêtre", and "Aide".

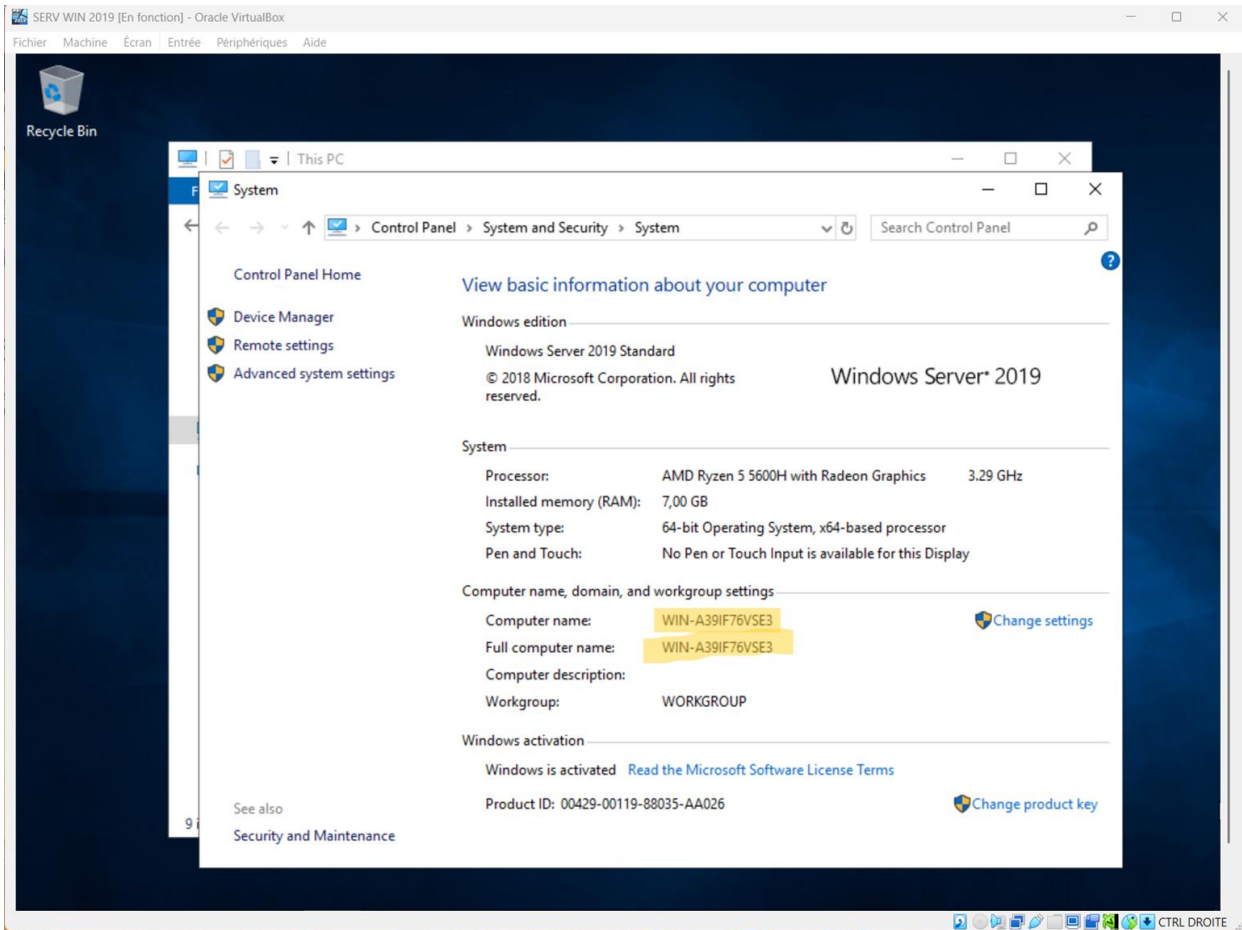
The "Navigateur LDAP" (LDAP Navigator) on the left shows a tree structure with "DIT", "Recherches", and "Signets". The main area is titled "Vue d'ensemble" (Overview) and contains several configuration sections:

- Serveurs LDAP/LDAPS:** Two LDAP servers are configured. The first is active with port 10389 (default 10389). The second is active with port 10636 (default 10636). A link for "Configuration avancée LDAP/LDAPS..." is provided.
- Partitions:** It states "Il y a 2 partitions définies :". Two partitions are listed: "example (dc=example,dc=com) [JDBM]" and "system (ou=system) [JDBM]". A link for "Configuration avancée des partitions..." is provided.
- Options:** Includes "Autoriser l'accès anonyme" (checked), "Activer le contrôle d'accès" (unchecked), and "Masquer les mots de passe" (unchecked).
- Serveur Kerberos:** The Kerberos server is active with port 60088 (default 60088). "Activer le serveur Kerberos Change Password" is checked with port 60464 (default 60464). A link for "Configuration avancée Kerberos..." is provided.

At the bottom, there are tabs for "Vue d'ensemble", "Serveurs LDAP/LDAPS", "Serveur Kerberos", "Partitions", "Politiques de mot de passe", and "Réplication". Below these are "Logs de modifications", "Logs de recherches", and "Journal des erreurs".

A small table at the bottom left shows the status of the LDAP server:

Serveur	Etat
LDAP	Arrêté





Un contrôleur de domaine est un serveur qui gère l'authentification et les autorisations des utilisateurs et des machines au sein d'un réseau Active Directory. Il joue un rôle central dans la gestion de la sécurité et des ressources d'une entreprise en assurant une administration centralisée.

Il sert pour :

L'authentification des utilisateurs : Lorsqu'un utilisateur tente de se connecter à un poste du réseau, le contrôleur de domaine vérifie son identité à l'aide de son nom d'utilisateur et de son mot de passe.

La gestion des autorisations : Il contrôle l'accès aux fichiers, imprimantes et autres ressources du réseau en fonction des droits définis par l'administrateur.

Le stockage des informations Active Directory : Il contient une base de données centralisée où sont enregistrés les comptes utilisateurs, les groupes, les ordinateurs et les stratégies de sécurité.

Pourquoi renommer la machine avant l'installation d'Active Directory ?

Lorsque l'on installe un contrôleur de domaine, son nom d'ordinateur est enregistré dans plusieurs services critiques, notamment DNS et Active Directory. Renommer la machine après installation peut entraîner des dysfonctionnements, comme des erreurs de résolution de nom ou des problèmes d'authentification des postes clients.



The screenshot shows a Windows Server 2019 desktop environment. In the foreground, the 'System Properties' dialog box is open, specifically the 'Computer Name/Domain Changes' tab. The 'Computer name' field contains 'AD-TPSISR' and is highlighted. The 'Full computer name' is 'AD-TPSISR'. Under 'Member of', the 'Workgroup' radio button is selected, and the text 'WORKGROUP' is entered in the field below. The 'OK' button is highlighted. In the background, the 'System Information' window is visible, displaying details about the computer. The title is 'Information about your computer'. It shows 'Windows Server 2019 Standard' and 'Windows Server 2019 Corporation. All rights'. Hardware specifications include 'AMD Ryzen 5 5600H with Radeon Graphics' at '3.29 GHz' and '7,00 GB' of RAM. It also notes '64-bit Operating System, x64-based processor' and 'No Pen or Touch Input is available for this Display'. Under 'Name, and workgroup settings', the 'Name' is 'WIN-A39IF76VSE3' and the 'Workgroup' is 'WORKGROUP'. Under 'Windows activation', it states 'Windows is activated' and provides the 'Product ID: 00429-00119-88035-AA026'. The desktop background is dark blue with a 'Recycle Bin' icon in the top left. The taskbar at the bottom shows various application icons and the system tray with the text 'CTRL DROITE'.



```
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

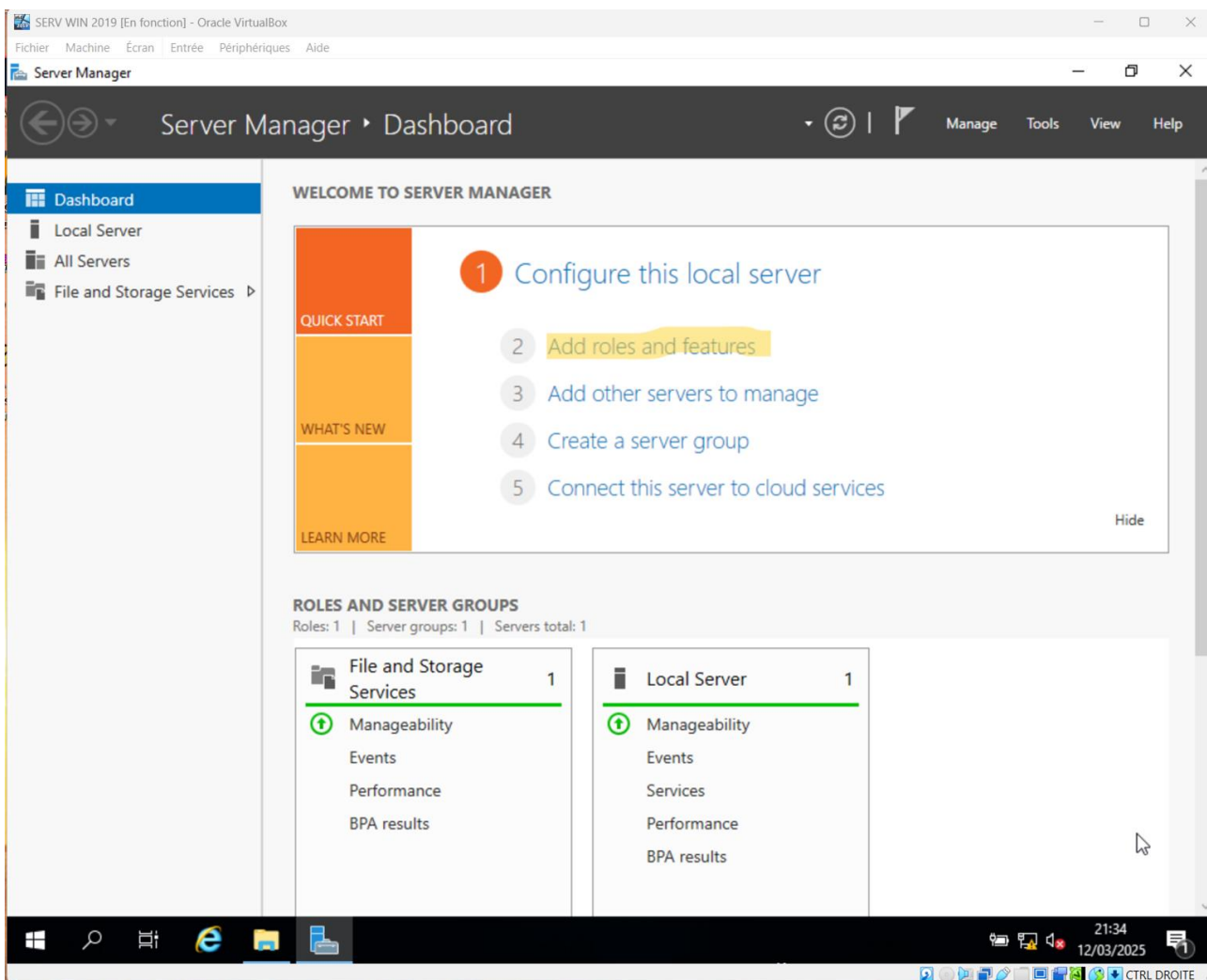
Windows IP Configuration

Ethernet adapter Ethernet:

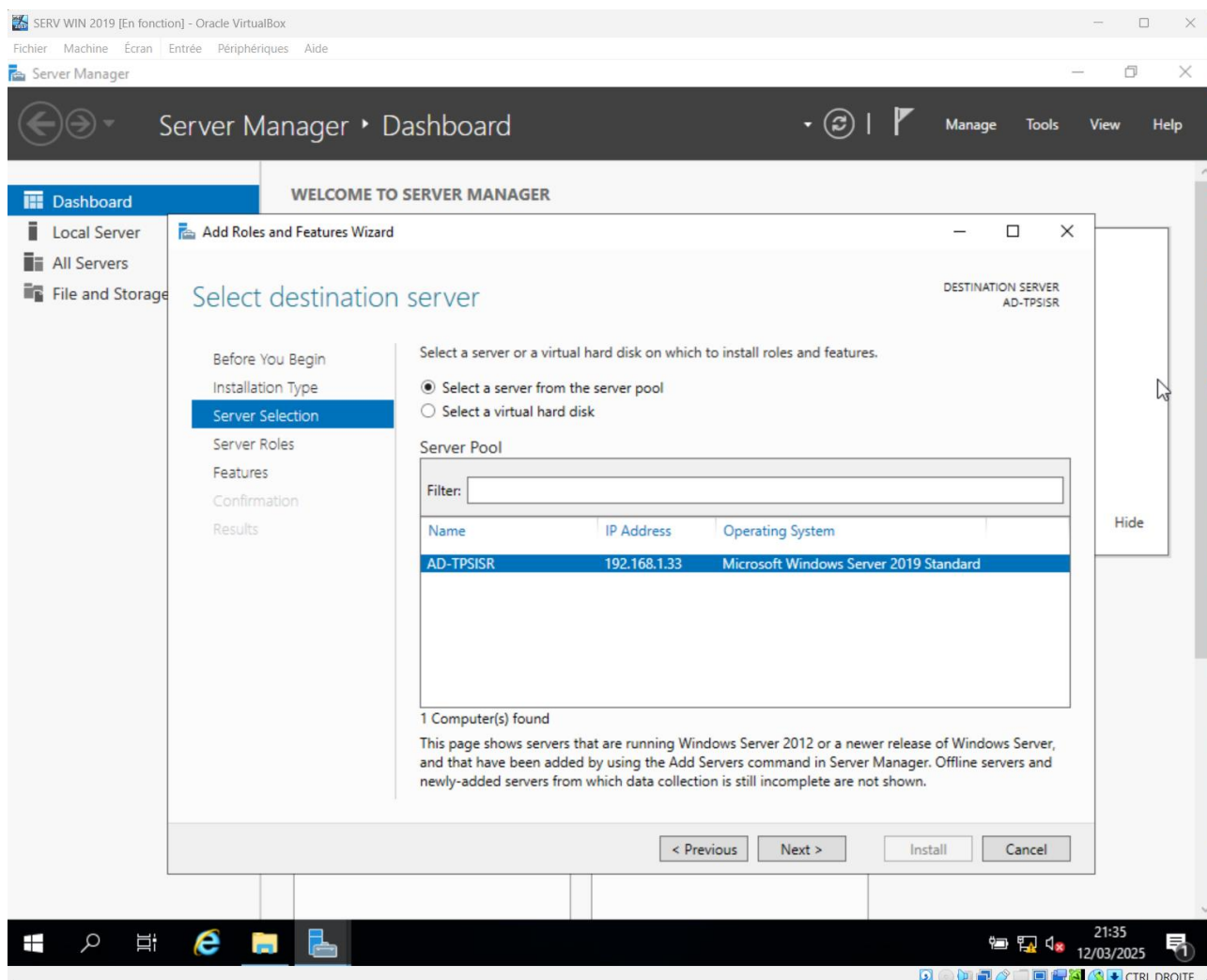
    Connection-specific DNS Suffix  . : home
    IPv6 Address. . . . . : 2a01:cb1c:832a:f900:4046:c001:58b:27b8
    Link-local IPv6 Address . . . . . : fe80::bb5a:55a9:f990:6ca0%5
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::aacf:7bff:fef1:1150%5
                               192.168.1.1

C:\Users\Administrator>
```

Le contrôleur de domaine doit toujours avoir une adresse IP fixe pour garantir la stabilité du réseau. En effet, si son adresse change régulièrement (comme c'est le cas avec le DHCP), les clients et les services qui s'appuient sur lui pourraient ne plus le trouver, entraînant des erreurs d'authentification et des problèmes de résolution de noms DNS.



Le Gestionnaire de serveur est un outil graphique intégré à Windows Server qui permet aux administrateurs de gérer facilement les rôles, fonctionnalités, et la configuration de leur serveur. Il centralise la gestion du système et évite d'avoir à utiliser plusieurs outils en ligne de commande.



Je choisis mon serveur



The screenshot shows the Windows Server Manager interface. The main window is titled "Server Manager Dashboard" and displays the "Add Roles and Features Wizard". The wizard is currently at the "Server Roles" step. The "Destination Server" is identified as "AD-TPSISR".

**WELCOME TO SERVER MANAGER**

**Dashboard**

- Local Server
- All Servers
- File and Storage

**Add Roles and Features Wizard**

**Select server roles**

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
AD DS  
Confirmation  
Results

Select one or more roles to install on the selected server.

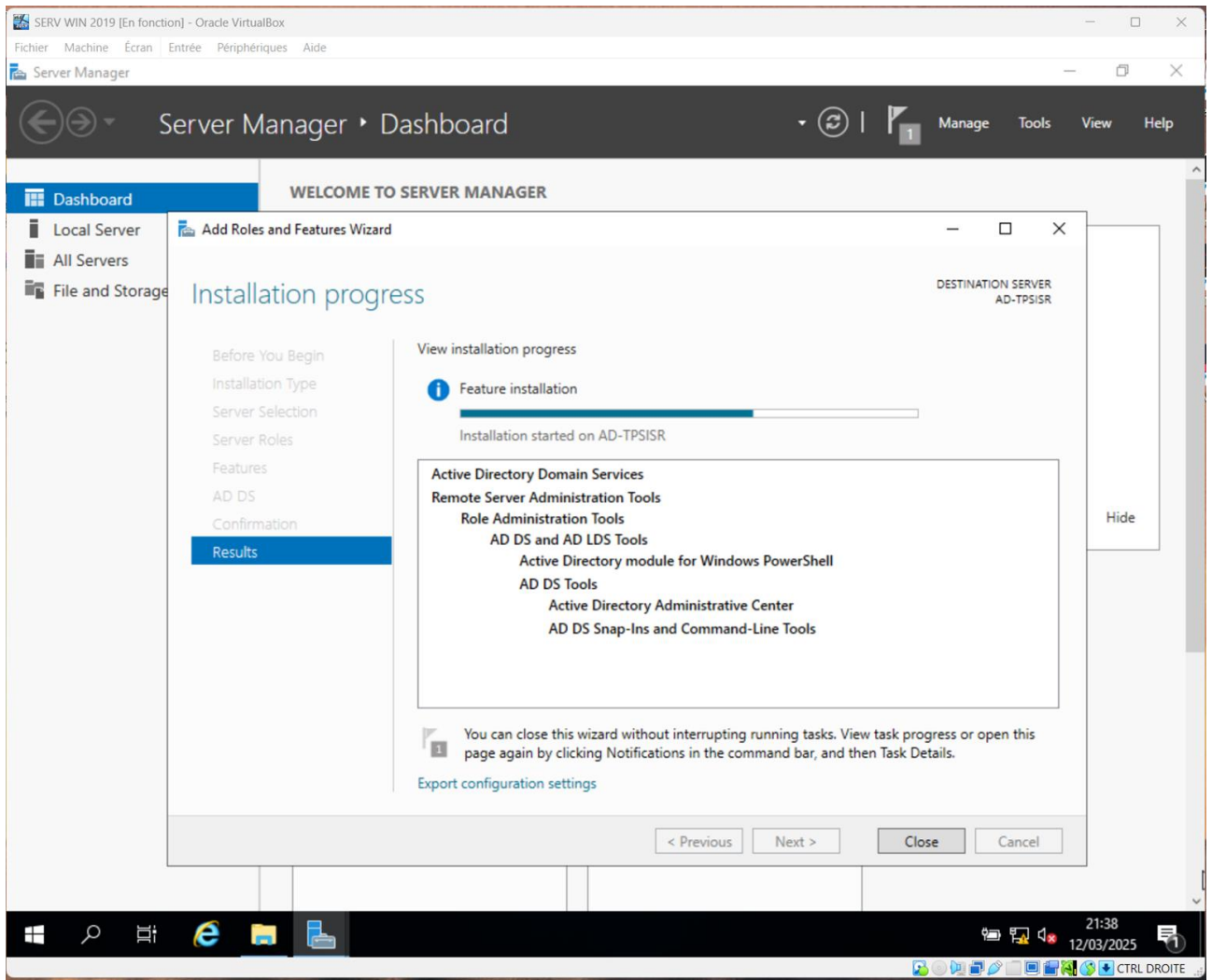
Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
<input checked="" type="checkbox"/> Active Directory Domain Services	
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Device Health Attestation	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Host Guardian Service	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	
<input type="checkbox"/> Volume Activation Services	
<input type="checkbox"/> Web Server (IIS)	
<input type="checkbox"/> Windows Deployment Services	
<input type="checkbox"/> Windows Server Update Services	

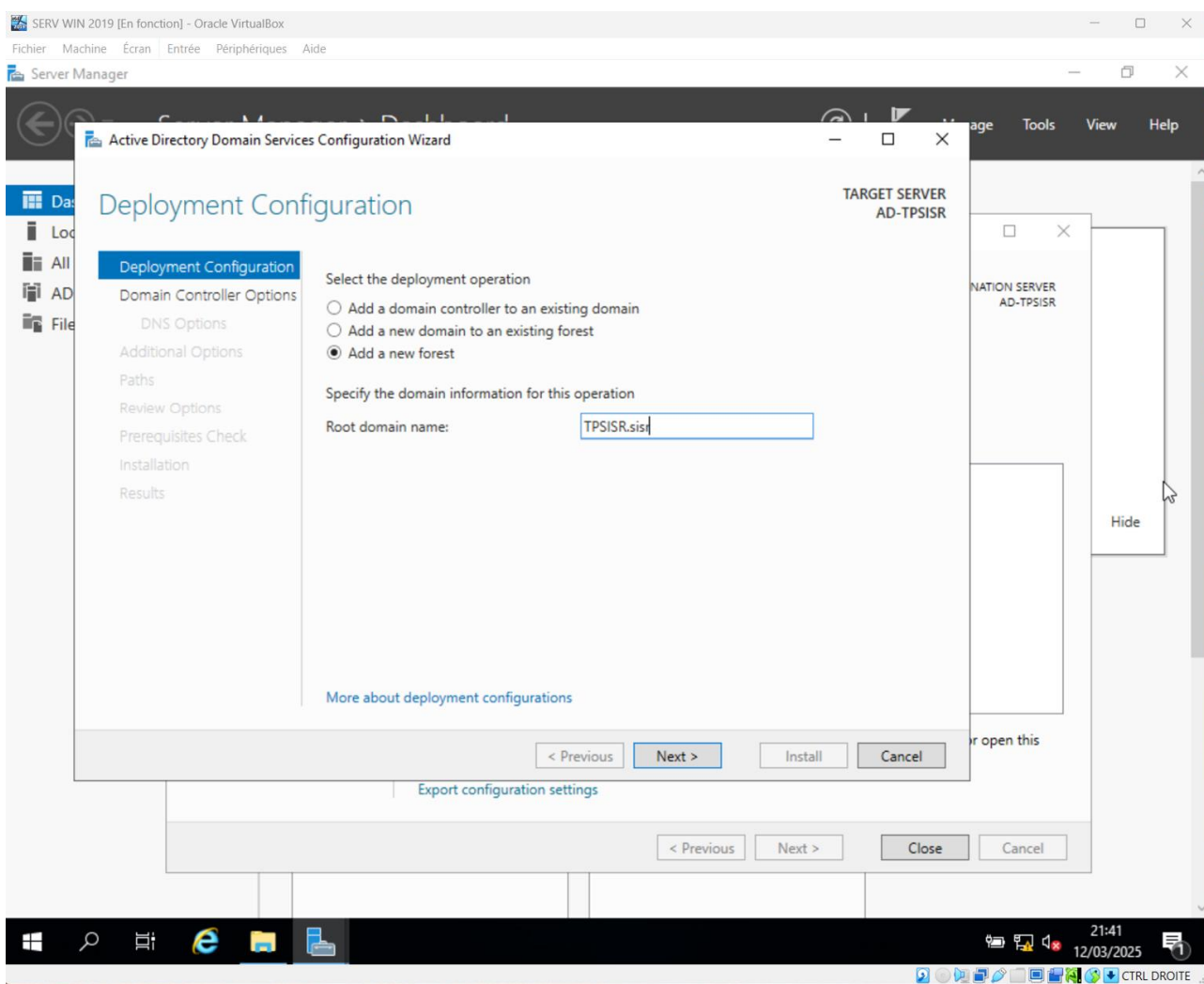
< Previous   Next >   Install   Cancel

21:36  
12/03/2025  
CTRL DROITE

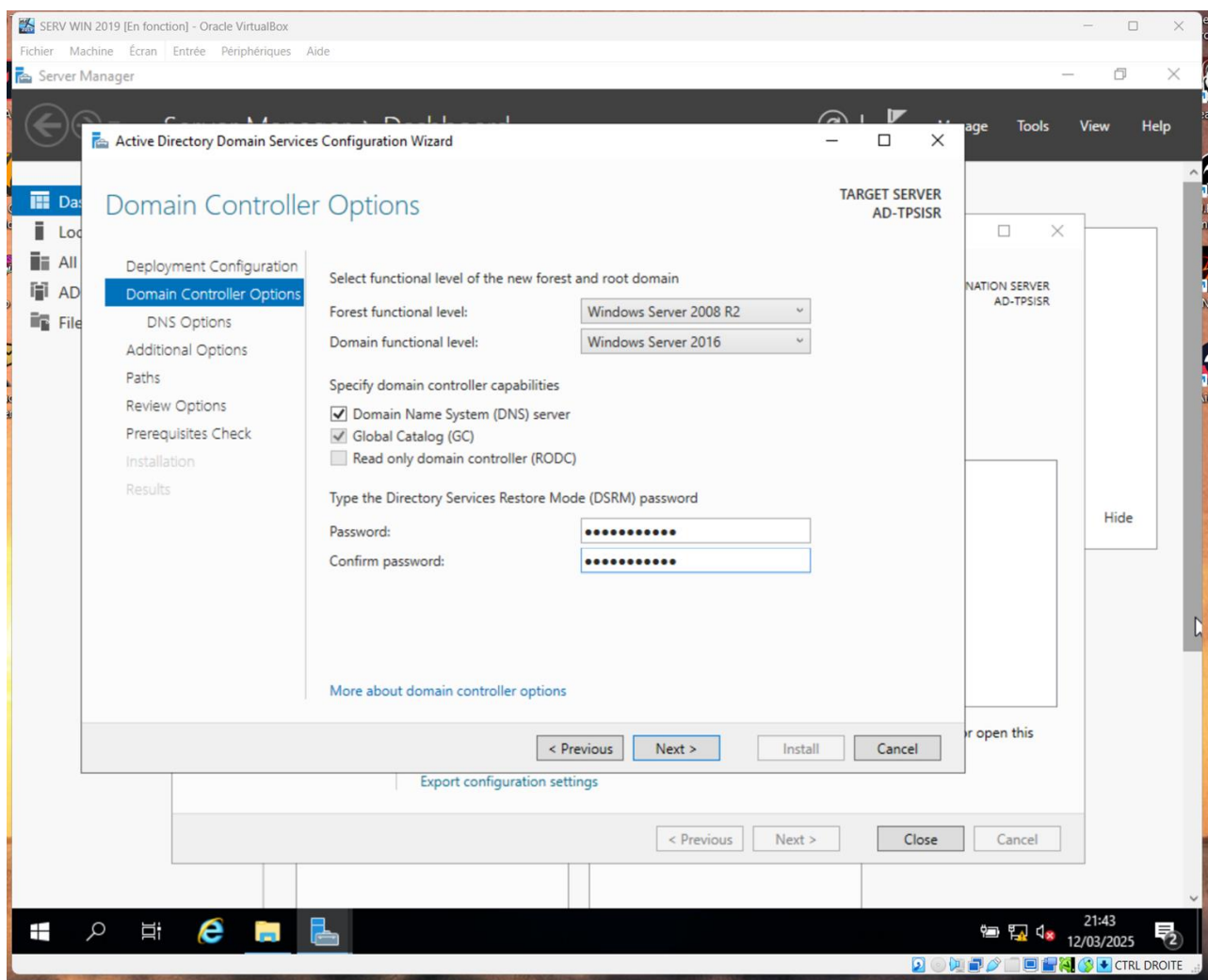


Le rôle choisi ici est l'ad ds , il est le composant principal d'Active Directory sur Windows Server. Il permet de créer et gérer un domaine, qui centralise l'administration des utilisateurs, des ordinateurs et des ressources réseau.

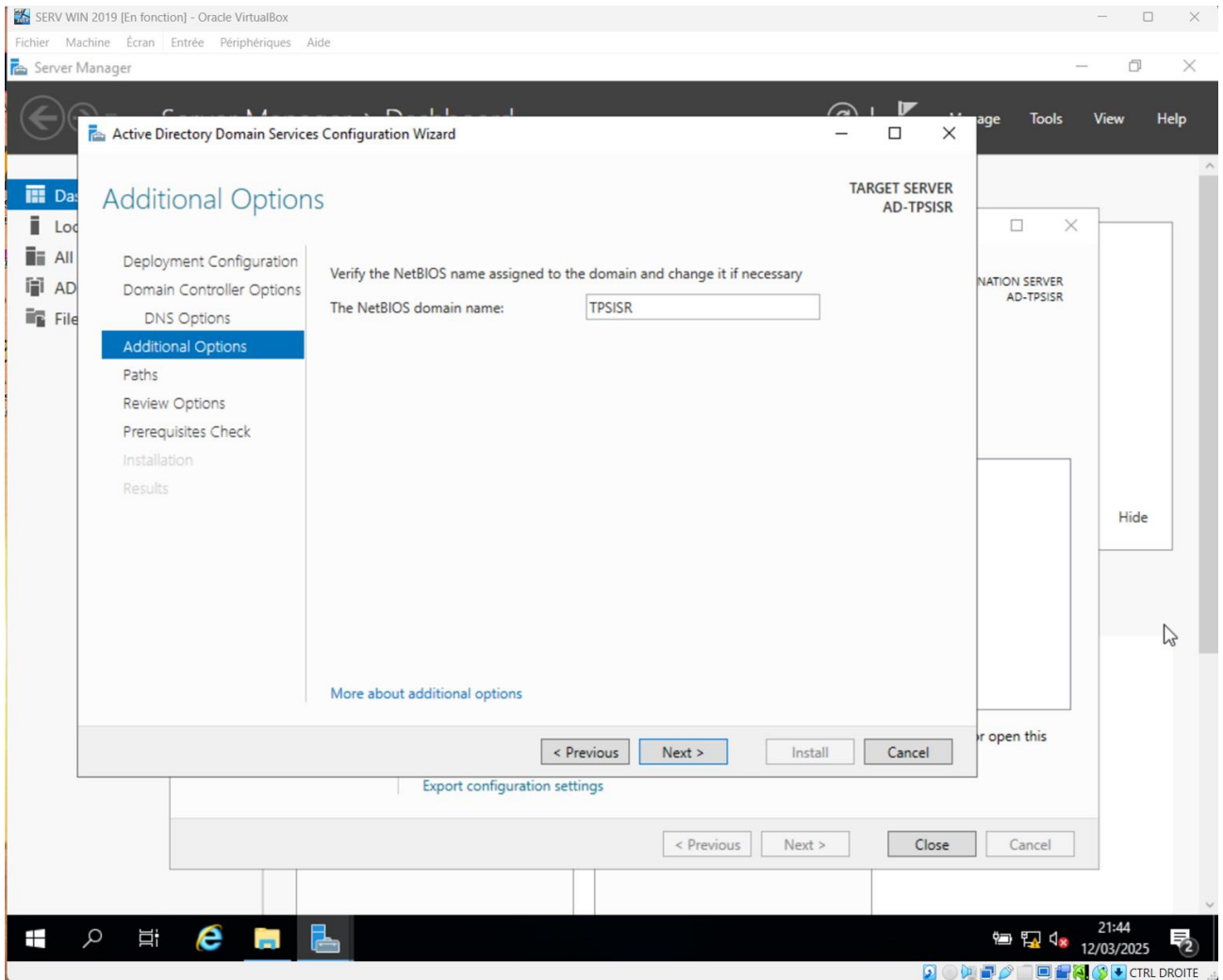




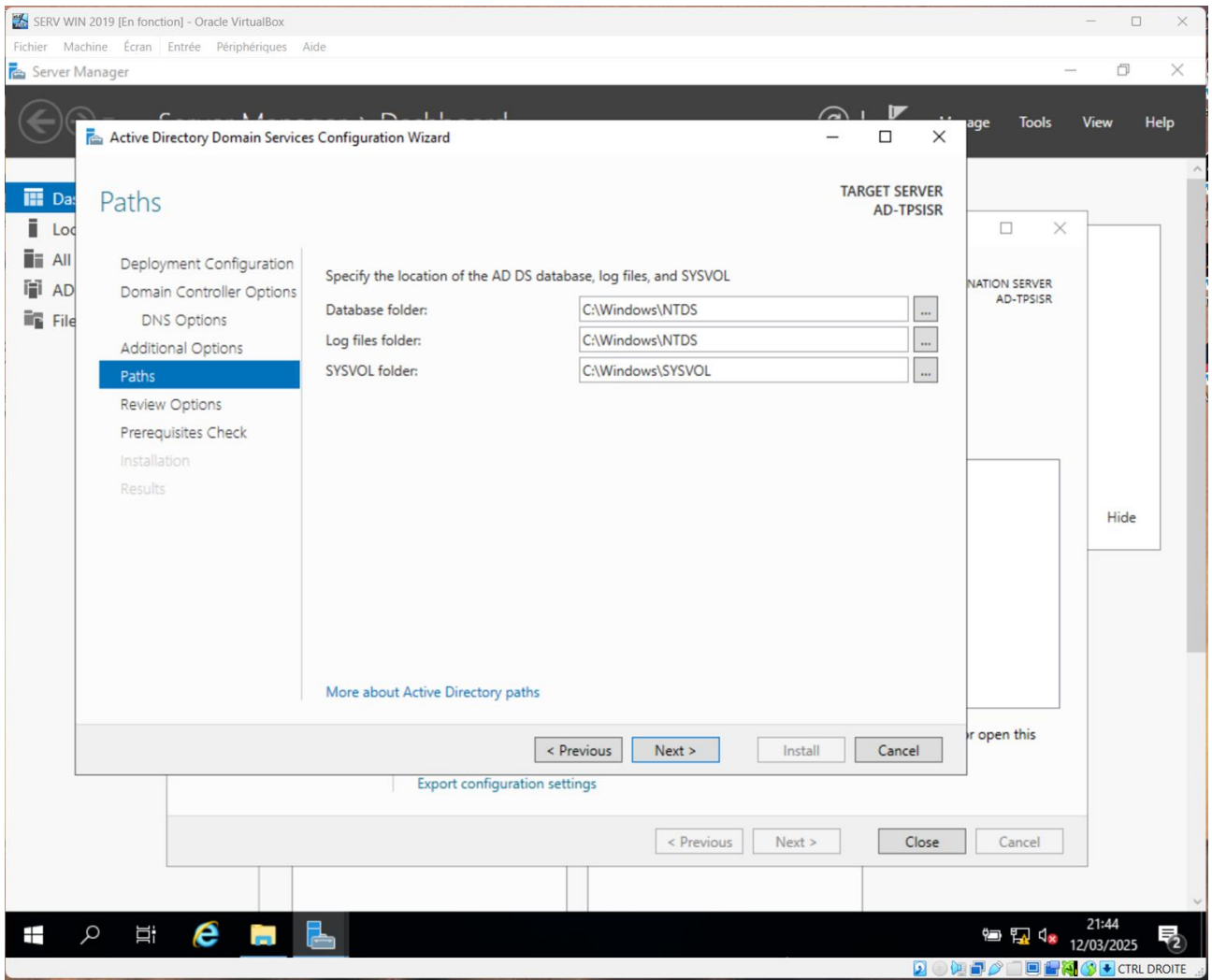
Le déploiement d'Active Directory avec des arbres permet une gestion flexible et évolutive d'une infrastructure réseau, particulièrement dans des organisations de grande taille. Les arbres sont utilisés pour organiser les domaines sous une hiérarchie unique, tandis que les forêts regroupent plusieurs arbres ayant une base de données partagée, permettant de gérer plusieurs espaces de noms et d'établir des relations de confiance entre eux.



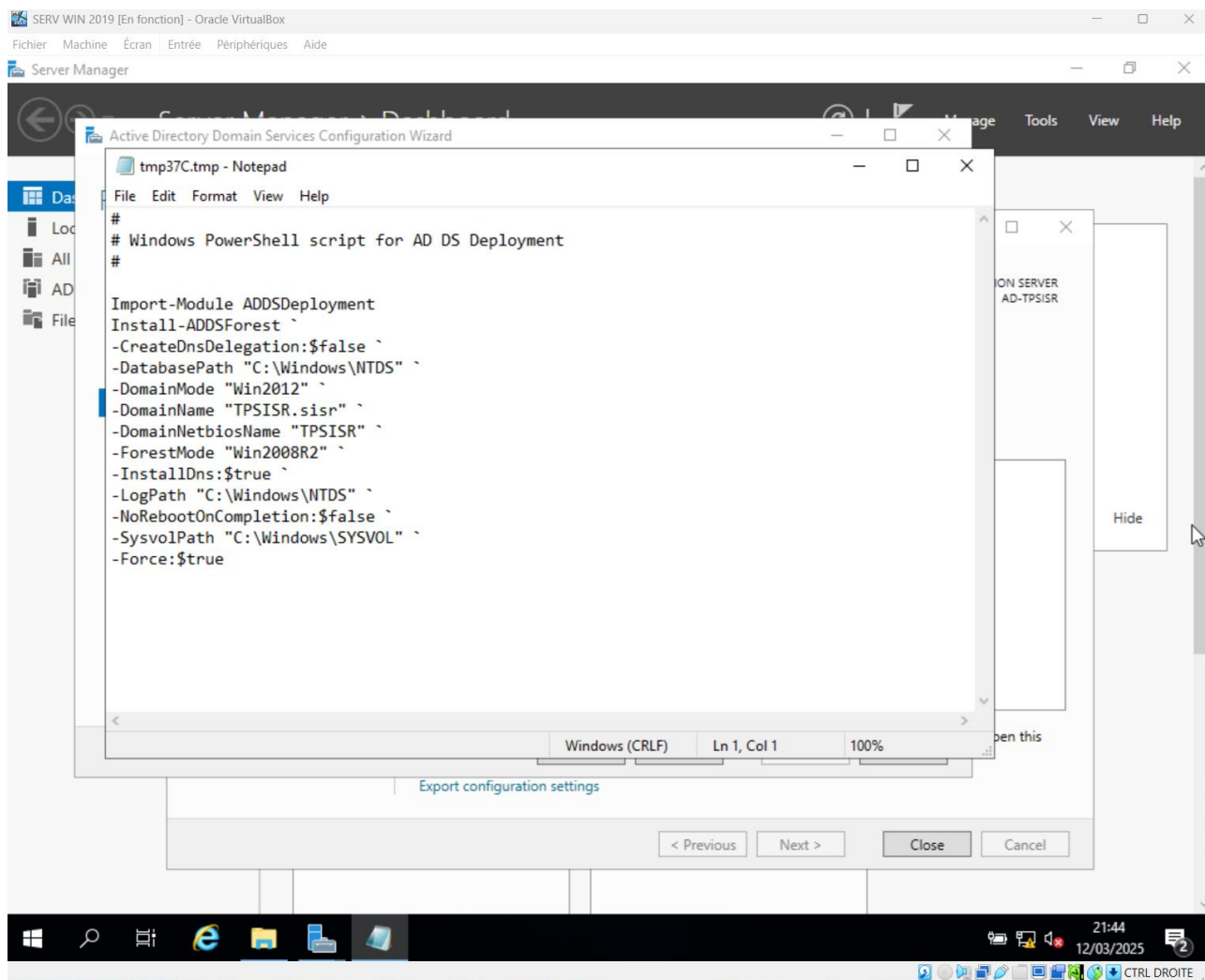
Les niveaux fonctionnels de la forêt et du domaine dans Active Directory déterminent les fonctionnalités disponibles et la compatibilité avec les versions de Windows Server.



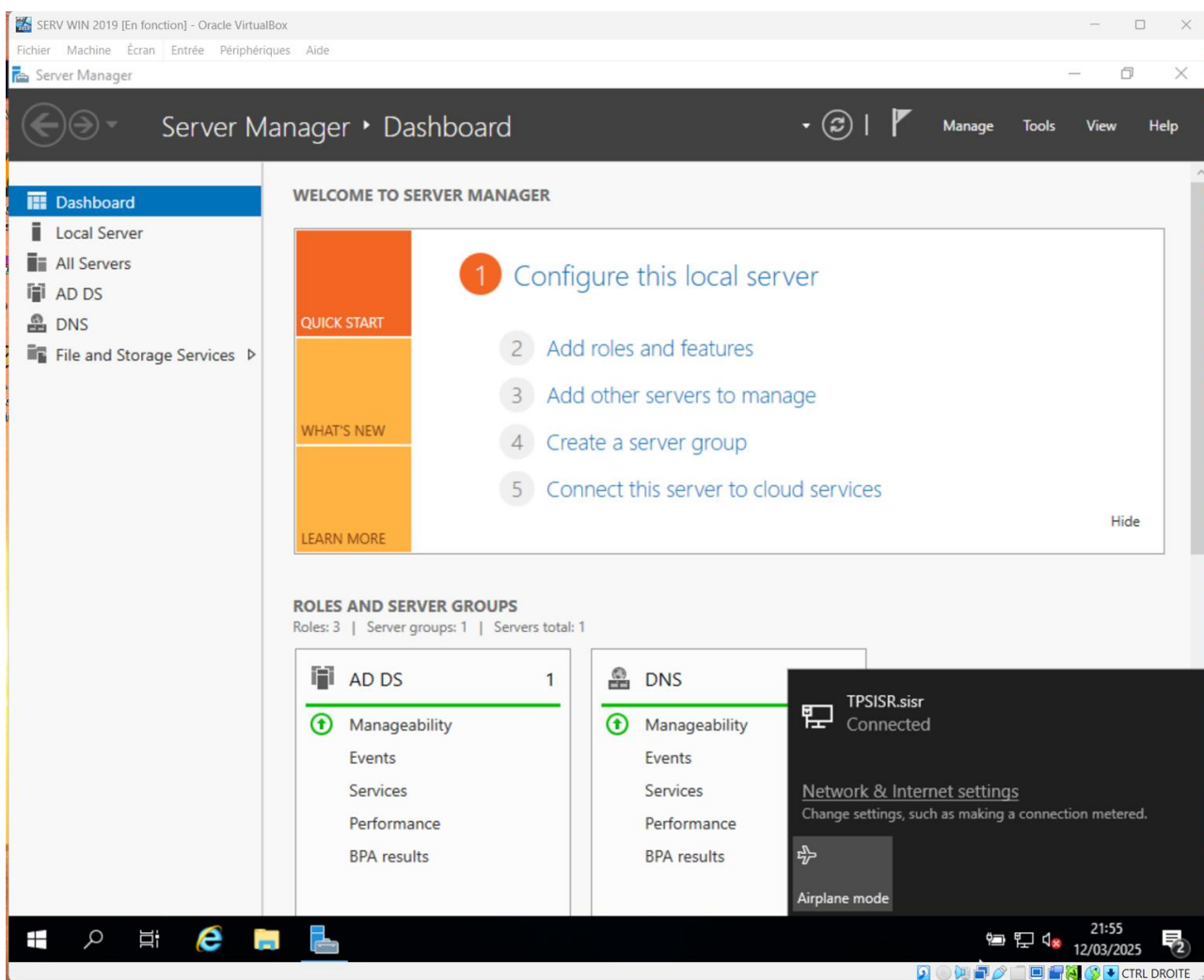
Récupération automatique du NETBIOS.



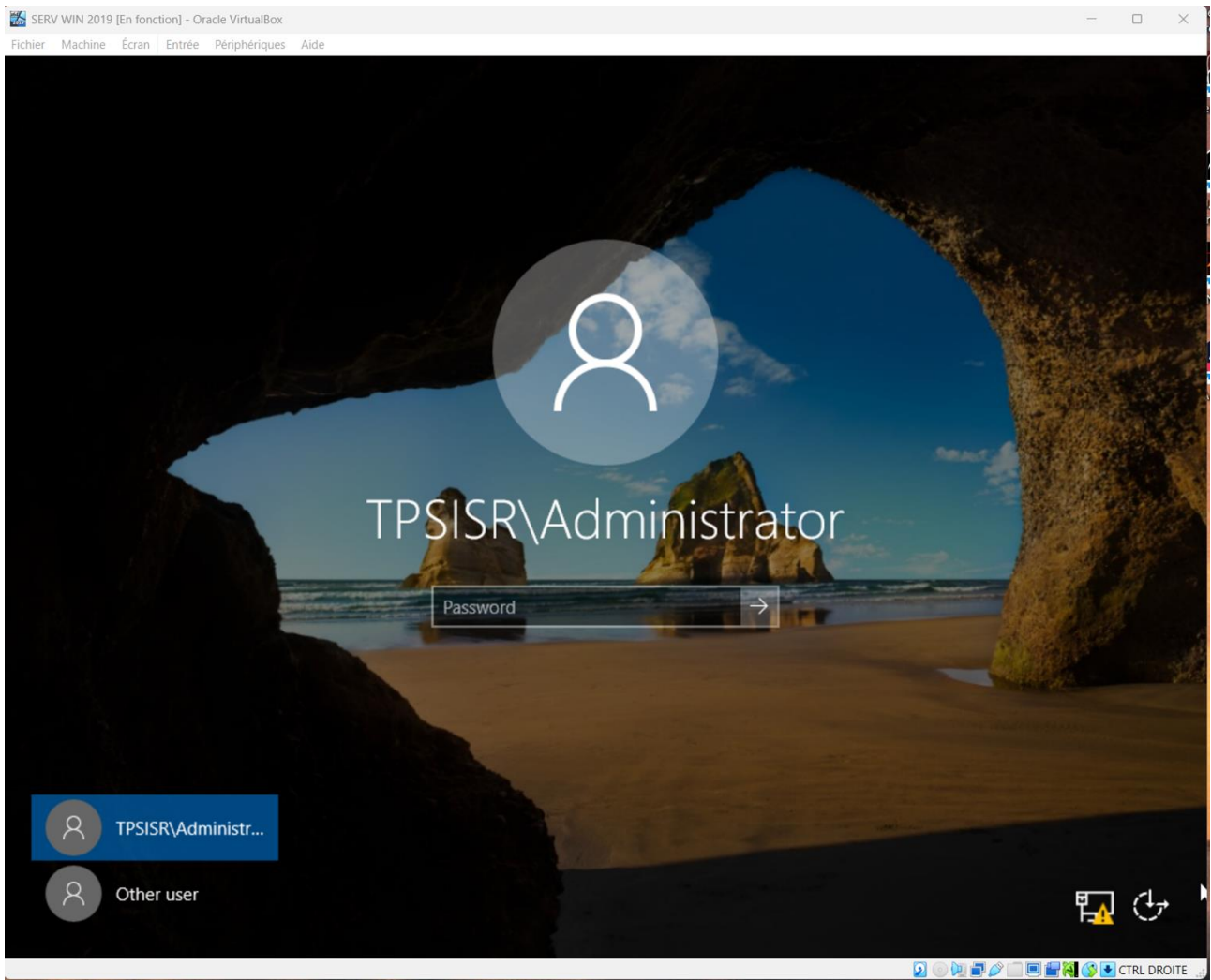
Emplacement d'installation.

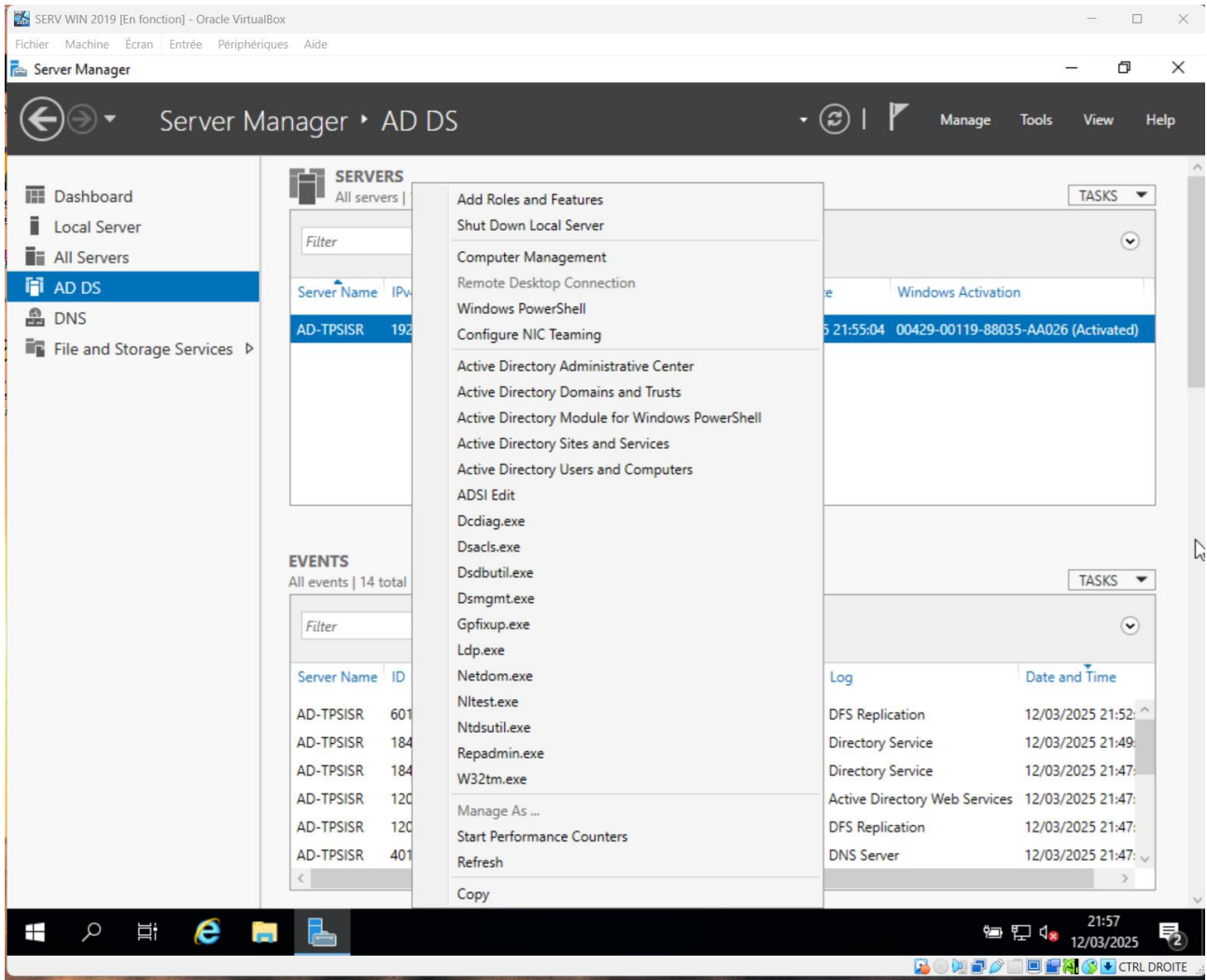


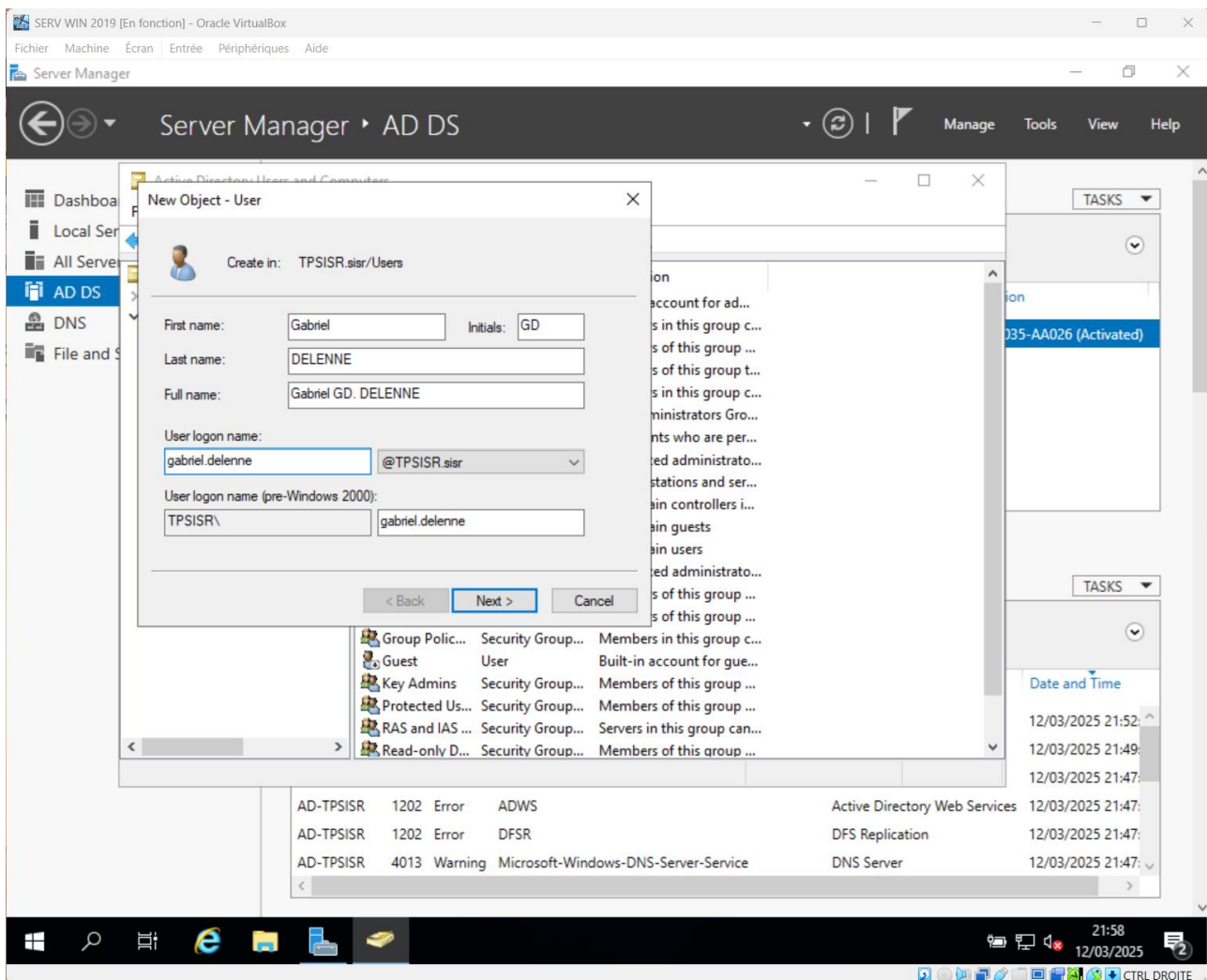
Script des manipulations précédentes en PowerShell



Redémarrage puis vérification application rôle AD DS

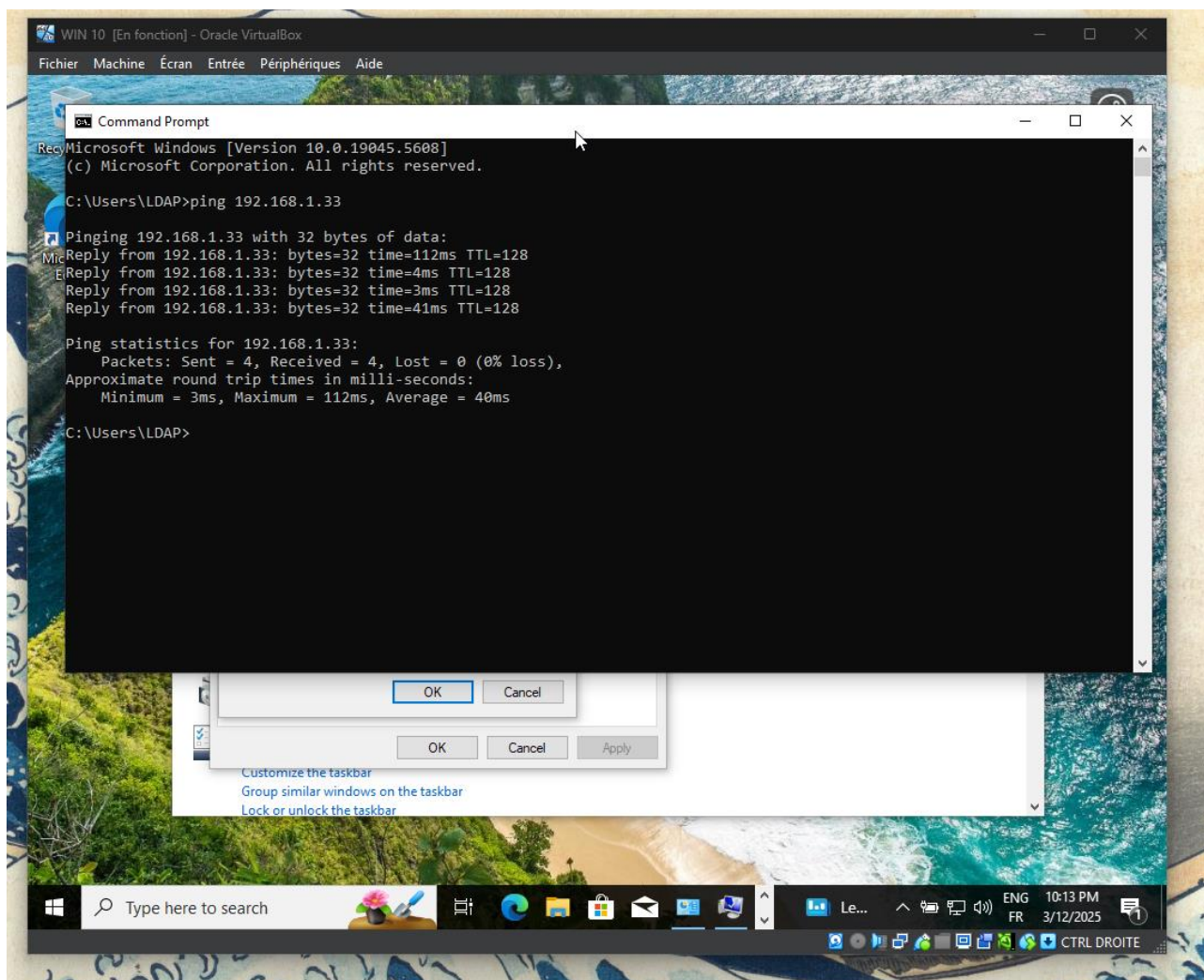




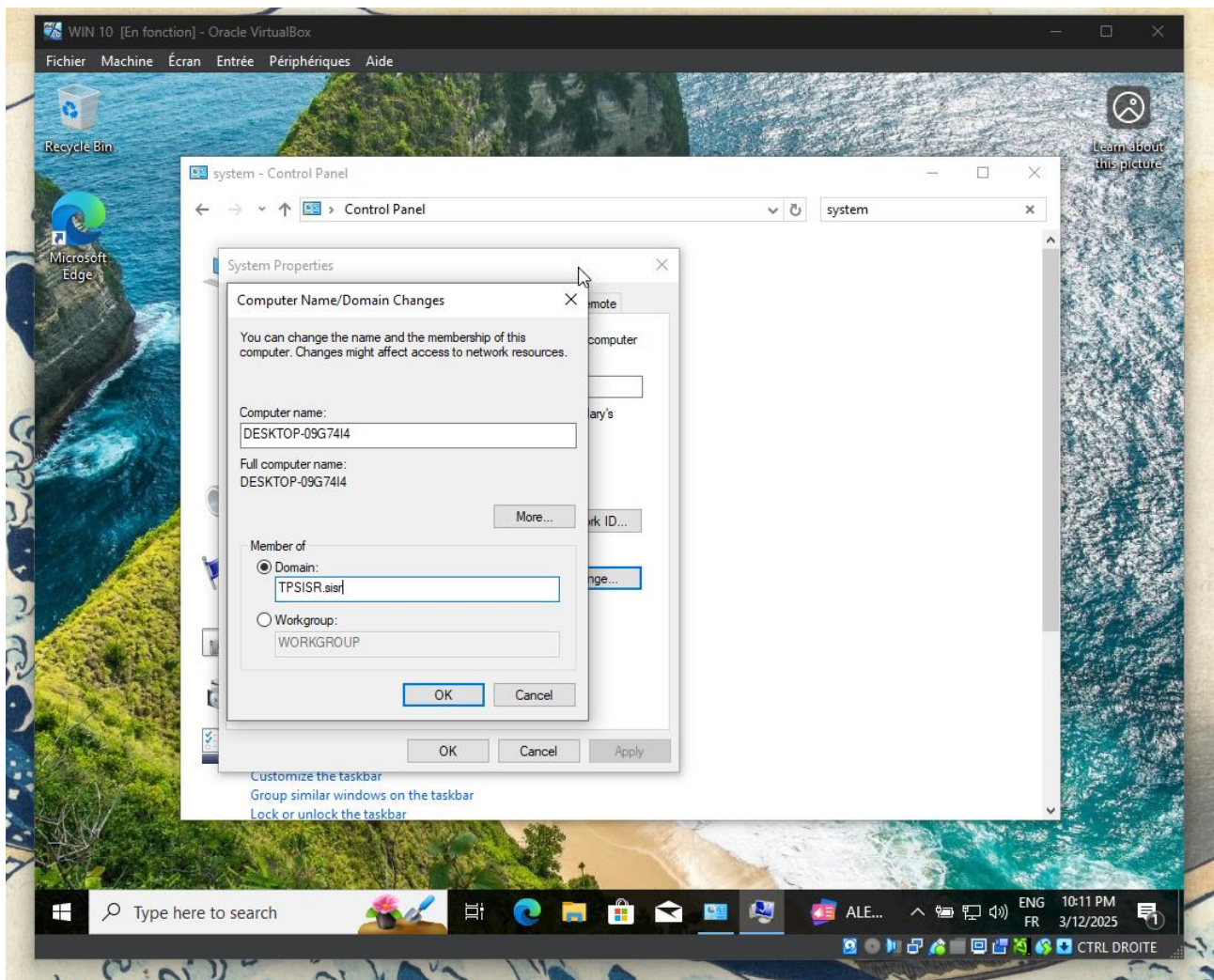


Création des entrées pour les utilisateurs de notre domaine

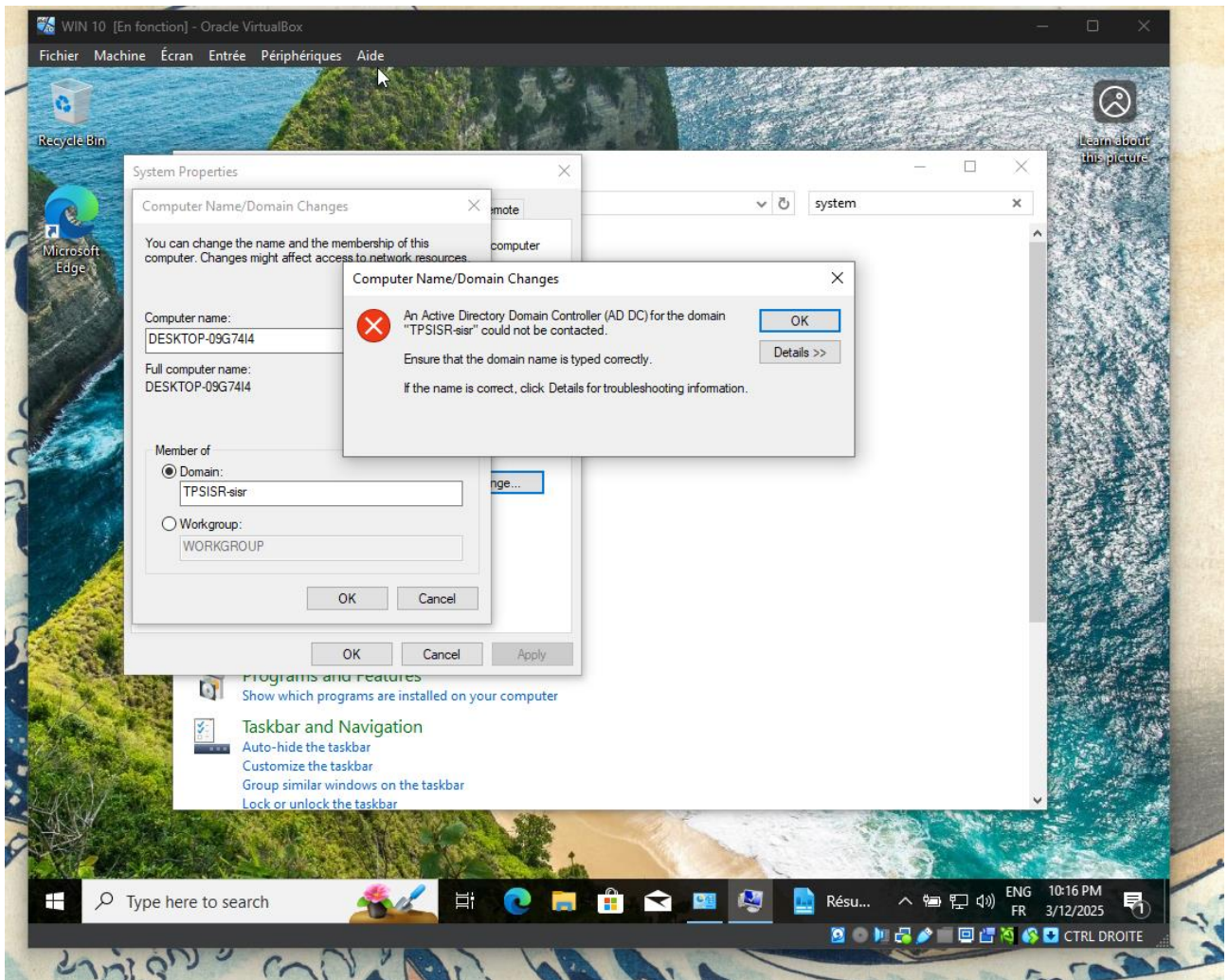
# Passage sur machine client :



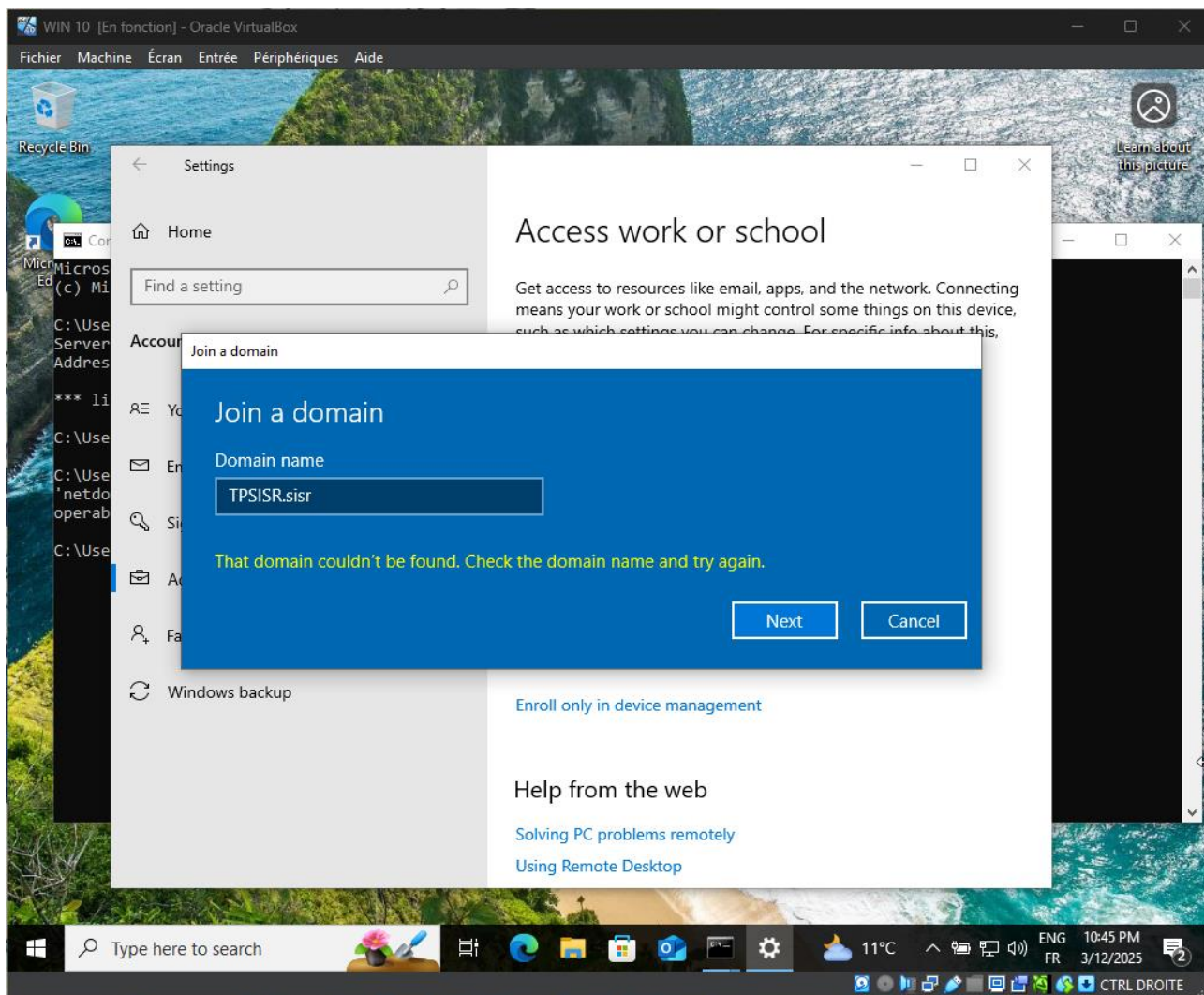
Test de connectivité entre l'ad et le client : good



Tentative de joindre le pc à l'AD



Erreur 1 ( 10h16)





Erreur 2 ( 10h46)

**Bref.**

Problèmes rencontrés tout au long de ce projet :

Tout au long de ce projet, plusieurs problèmes techniques ont été rencontrés, ce qui a retardé et complexifié l'avancement des différentes étapes de la mise en place du réseau et du déploiement de l'Active Directory.

PS 12/03/25 23h46 On a changé de manière de faire car on eu des problèmes avant.

*Problèmes avec Apache LDAP : La mise en place du serveur Apache Directory pour gérer le LDAP a présenté des difficultés liées à la configuration des schémas et à l'intégration avec le domaine Active Directory. Des erreurs de communication entre le serveur Apache et les contrôleurs de domaine ont été rencontrées, nécessitant une révision des paramètres de connexion et une meilleure gestion des permissions d'accès.*

*Pare-feu : Le pare-feu a été une source de problèmes de connectivité. Plusieurs fois, les communications entre les différents serveurs et postes clients ont été bloquées, empêchant la propagation des informations dans le réseau ou l'activation de certains services essentiels à la mise en place du domaine. Des ajustements spécifiques des règles du pare-feu ont été nécessaires pour permettre le bon fonctionnement des services réseau.*



*Problèmes DNS : Le DNS (Domain Name System) a également posé des défis, notamment en ce qui concerne la résolution de noms entre les différents serveurs et le contrôleur de domaine. Des erreurs de configuration DNS ont empêché la bonne identification des machines sur le réseau, ce qui a rendu impossible l'intégration des PC dans le domaine. L'ajustement des zones DNS et la synchronisation des enregistrements ont été nécessaires pour corriger ces erreurs.*

*Mises à jour des PC sur WIN10 (physique): Les mises à jour des PC ont également créé des retards, notamment en raison de l'incompatibilité des systèmes d'exploitation ou de certaines configurations matérielles obsolètes. Plusieurs postes ont dû être mis à jour ou réinstallés pour garantir qu'ils respectaient les prérequis nécessaires à l'intégration dans le domaine Active Directory.*

En conclusion, tout au long de ce projet, nous avons rencontré de nombreux défis techniques, principalement liés au matériel et à sa configuration. Ces problèmes que ce soit des soucis de compatibilité matérielle, des échecs de démarrage des services ou des difficultés liées aux paramètres réseau, chaque obstacle a nécessité une investigation et des ajustements.

Cependant, malgré ces défis, nous avons pu résoudre la plupart des problèmes en ajustant la configuration du matériel, en mettant à jour certains composants et en appliquant des solutions spécifiques pour garantir la stabilité du système.



