BTS SIO option SISR

EPREUVE E5

Administration des Systèmes et réseaux

Promotion 2023-2025

Mise en place d'un Active directory

Lionel Hervé

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024/2025**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : Hervé Lionel	**N° candidat : 02443844601**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 2024/2025

Organisation support de la réalisation professionnelle

Entreprise fictive **Dualya** prestataire **TRIUM IT**.

Intitulé de la réalisation professionnelle

Active directory

Période de réalisation : 2023 / 2025 Lieu : CFA Fab'Academy Bouguenais (UIMM) .....

Modalité : ☐ **Seul(e)** ☒ **En équipe**

Compétences travaillées

☒ Concevoir une solution d'infrastructure réseau

☒ Installer, tester et déployer une solution d'infrastructure réseau

☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

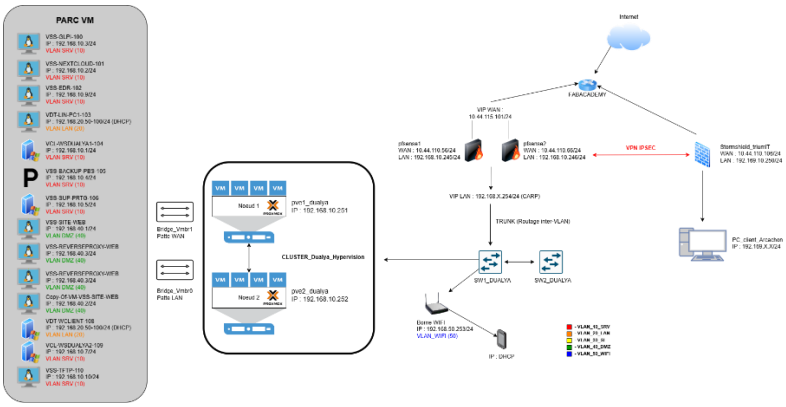
Conditions de réalisation[1] (ressources fournies, résultats attendus)

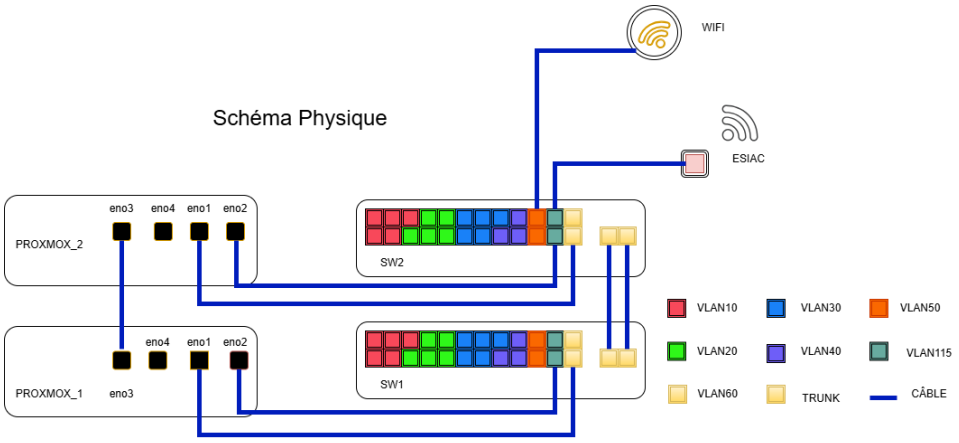
Mise en place d'un Windows serveur 2O22 ainsi qu'un AD-DS et de ses rôle DHCP, DNS, création d'uo, d'utilisateurs, de GPO et une réplication de L'AD.

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Le schéma logique :





Voir annexe plan logique et physique et adressage IP.

Modalités d'accès aux productions[3] et à leur documentation[4]

Nom	Hyperviseur	IP	Système d'exploitation	Performances allouées	Rôles
VSS-GLPI-100	DUALYA-1/2	192.168.10.3/24	Debian 12	1CPU 2 cores, 8 GO RAM, 32GO	GLPI ticketing
VSS-NEXTCLOUD-101	DUALYA-1/2	192.168.10.2/24	Debian 12	1 CPU 2cores, 8GO RAM, 64 GO	NEXCLOUD Stockage
VDT-LIN-PC1-103	DUALYA-1/2	192.168.20.X/24	Debian 12	1CPU 2 cores, 8 GO RAM, 32GO	Linux client
VCL-WSDUALYA1-104	DUALYA-1/2	192.168.10.1/24	Windows server 2022	1CPU 2 cores, 8 GO RAM, 32GO, 50GO	Windows server DNS DHCP COMPTE
VSS-BACKUP-PBS-105	DUALYA-1/2	192.168.10.4/24	Proxmox backup server	1CPU 2cores, 4GO RAM, 100GO, 30GO	Proxmox backup server backup des VM
VSS-SUP-PRTG-106	DUALYA-1/2	192.168.10.5/24	Windows server 2022	1 CPU 2cores, 8GO RAM, 64 GO	Windows server 2022 Supervision
VSS-PFSENSE-107	DUALYA-1/2	192.168.10.245/24	Pfsense	1 CPU 2cores, 8GO RAM, 20 GO	Pfsense firewall
VCL-WSDUALYA2-109	DUALYA-1/2	192.168.10.7/24	Windows server 2022	1 CPU 2cores, 8GO RAM, 80 GO	Windows server redondance DNS DHCP COMPTE
VSS-EDR-102	DUALYA-1/2	192.168.10.9/24	Debian 12	1CPU 2 cores, 8 GO RAM, 32GO	WAZUH EDR
VSS-SRV-TFTP-110	DUALYA-1/2	192.168.10.10/24	Debian 12	1CPU 1 cores, 2 GO RAM, 32GO	TFTP
VSS-1111-WEB	DUALYA-1/2	192.168.40.1/24	Debian 12	1CPU 1 cores, 2 GO RAM, 32GO	Debian WEB
VSS-PFSENSE2-113	DUALYA-1/2	192.168.10.246/24	Pfsense		
VDT-WCLIENT-108	DUALYA-1/2	192.168.20.X/24	Windows 10		
Copy-of-VSS-SITE-WEB	DUALYA-1/2	192.168.40.2/24	Debian 12		
VSS-REVERSEPROXY-WEB	DUALYA-1/2	192.168.40.3/24	Debian 12		

MDP Machine Virtuel : R3u$BTS25

MDP Machine Client : MDPclient44

MDP EDR (WAZUH) : o7uGQdj1.n?ktn7gNUvxmPWvSq8JDktC

MDP STORMSHIELD ARCACHON : Succ$BTS23

Tous nos mots de passe sont dans un coffre-fort : Keep Pass.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2023\2025**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Table des matières

Introduction

TRIUM IT est une entreprise spécialisée dans la fourniture de solutions informatiques avancées et sur mesure pour les entreprises de toutes tailles. Notre mission est d'aider nos clients à optimiser leurs infrastructures informatiques, à améliorer leur sécurité et à augmenter leur productivité grâce à des technologies de pointe et des services de haute qualité.

L'entreprise Dualya nous a sollicité pour mettre en œuvre ses solutions pour centraliser les utilisateurs et la sécurité des deux sites de Paris et Arcachon.

Dans ce guide, nous allons couvrir les étapes essentielles pour mettre en place un environnement Windows Server 2022, en commençant par l'installation de Windows Server, l'ajout du rôle Active Directory Domain Services (AD-DS), la création de domaines, et l'ajout de rôles tels que DHCP et DNS. Nous aborderons également la gestion des unités d'organisation, la création et la connexion d'utilisateurs, la mise en place de profils itinérants et la création de GPO (Group Policy Objects) pour le mappage de lecteurs. Enfin, nous verrons comment faire une réplication de l'Active Directory pour garantir la redondance et la disponibilité de vos services.

Contexte :

Présentation du groupe Dualya :

L'entreprise Dualya est une société de décoration d'intérieur, implantée en région parisienne depuis 2018. Elle a vu son activité s'accroitre au sein de son siège depuis sa création, ce qui a engendré la création de nouvelles agences cette année. Le bilan sur l'année écoulée est très positif puisque la société dégage un chiffre d'affaires d'un million cinq cent mille euros et Dualya ne compte pas en rester là. Son expansion passe par le recrutement de nouveaux collaborateurs au sein de l'agence parisienne et de l'ouverture d'une seconde agence dans un secteur en plein développement, le bassin d'Arcachon. En effet, cette zone à fort potentiel connait un succès retentissant depuis la sortie du film « Les petits mouchoirs ». Les résidents des zones urbaines, en mal de nature et qui ont la possibilité de s'offrir des villas sur le littoral sautent donc le pas, ainsi, la majorité des maisons est à rénover, Dualya a du pain sur la planche.

Fonctionnement du groupe Dualya :

Fonctionnement du groupe Dualya La société Dualya obtient ses clients via le bouche à oreille ou la visite sur le site Web de l'entreprise, à partir du moment où un client identifie la société ou que Dualya identifie un client, ces derniers entrent en contact soit par mail, soit par téléphone. Dans ce cas, c'est le service Design qui prend en charge le client et qui interprète sa demande, cette demande donne lieu à un devis. Après validation du client, un bon de commande est adressé au service Administratif qui prend le relais contractuellement, toujours sous l'œil attentif du service Design qui prend le relais contractuellement, toujours sous l'œil attentif du service Design qui
réalise la prestation (Au côté d'entreprise prestataire), jusqu'à l'aboutissement du projet et de la facturation. Les échanges entre service se font par voix orales, téléphone ou mails. Chaque collaborateur dispose d'un PC portable 15 pouces, en parfait état de fonctionnement et sous Windows 10. Ils disposent également de deux moniteurs, d'un clavier et d'une souris filaire. De manière à faciliter les échanges, les collaborateurs sont dotés de téléphones portables professionnels et ont un compte mail. La gestion des mails est assurée par Office, ce qui permet aux Utilisateurs de bénéficier de la suite Office 365 (Suite bureautique). Chaque Utilisateur à sa propre adresse mail, la convention de nommage est la suivante : prenom.nom@dualya.fr. De plus, chaque service bénéficie d'une adresse mail, la convention de nommage est la suivante : service@dualya.fr (Exemple : administratif@dualya.fr). Enfin, il existe un mail commun au groupe : groupe.interne@dualya.fr.

Composition du groupe Dualya :

L'agence parisienne, en comptant les nouveaux arrivants, se composent des collaborateurs suivants :

- **Direction :**
    - Philippe Pastel
- **Ressources Humaines :**
    - Pierre Parry
- **Administratif :**
    - Ulysse Alain
    - Baptiste Ludwig
- **Marketing :**
    - Jade Caillaux
    - Sophie Ratier
- **Design :**
    - Rémy Loiseau
    - Pierre Sabord
    - Sacha Lens
    - Jeanne Reil

L'agence arcachonnaise compte les collaborateurs suivants :

- **Administratif :**
    - Serge Lay
- **Marketing :**
    - Sybille Gautier
    - Hélène Varon
- **Design :**
    - Pauline Provost
    - Cécilia Claire
    - Yann Bertrand

Votre rôle

Vous intervenez en tant que prestataire informatique (Groupe d'entreprise pédagogique). Votre objectif est d'accompagner Dualya dans son évolution numérique. Le projet concerne donc les outils que le groupe Dualya aimerait pouvoir utiliser afin de coordonner ses collaborateurs et leur proposer un service informatique optimal.

1. Présentation de TRIUM IT

TRUM IT : L'Innovation au Service de Votre Infrastructure **TRIUM IT** est une startup dynamique lancée en septembre 2023, spécialisée dans le secteur de l'informatique. Composée de trois collaborateurs passionnés et experts, notre entreprise est dédiée à fournir des solutions innovantes pour optimiser et sécuriser les infrastructures IT. Grâce à notre approche sur-mesure et à notre expertise en gestion de réseau, cybersécurité, et systèmes, nous accompagnons nos clients dans la transformation numérique de leur entreprise. Nous plaçons l'innovation et la qualité au cœur de notre démarche pour répondre aux besoins croissants des entreprises modernes.

Notre Mission :

Offrir des solutions IT performantes et fiables, permettant à nos clients d'atteindre leurs objectifs avec efficacité et sérénité.

Notre Vision :

Devenir un acteur incontournable des infrastructures IT en anticipant les évolutions technologiques et en proposant des services sur mesure, adaptés aux défis de demain.

Nos Valeurs :

Nous plaçons **l'excellence, la transparence, l'innovation et la collaboration** au cœur de notre engagement. Nous bâtissons des relations de confiance solides avec nos clients et partenaires, en favorisant la responsabilité et une quête constante de progrès.

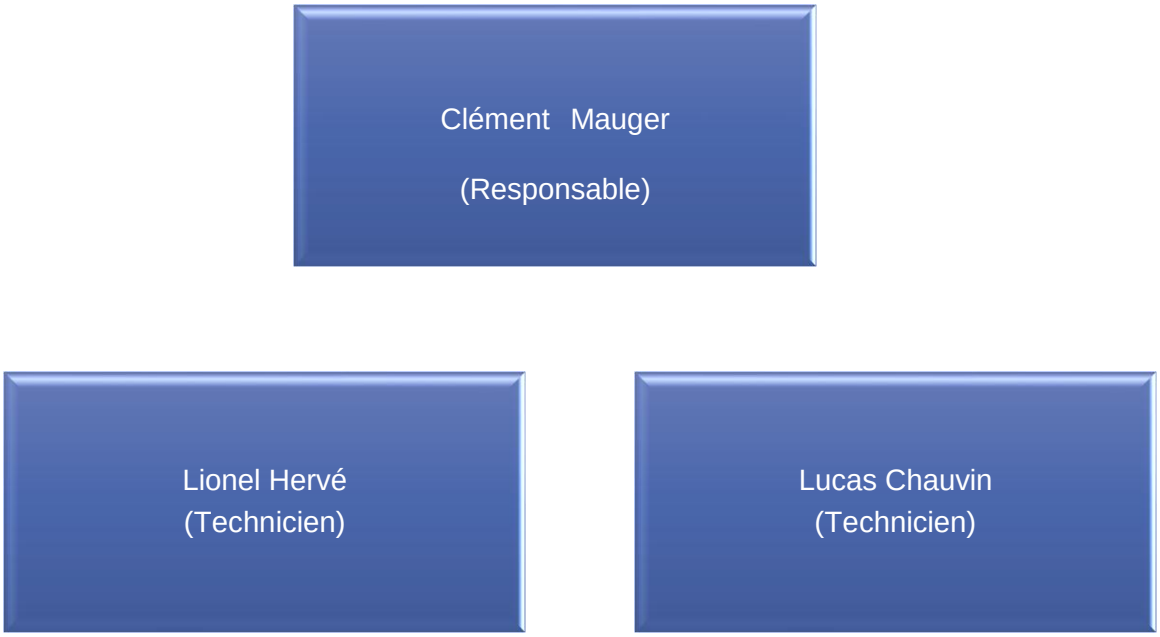
Nos Services :

Des solutions complètes et innovantes pour optimiser votre infrastructure réseau et votre virtualisation.

- **Conception et Déploiement d'Infrastructures Réseaux :** Nous concevons et mettons en place des infrastructures réseau robustes et évolutives. Que ce soit pour des réseaux locaux (LAN) ou étendus (WAN), nous garantissons une connectivité optimale et sécurisée.
- **Points forts :** Analyse des besoins, équipements de pointe, conformité aux normes actuelles.
- **Support et Maintenance de Virtualisation :** Nous assurons le support des environnements virtualisés pour garantir leur performance et disponibilité. De VMware à Proxmox, nous couvrons un large éventail de technologies pour maximiser vos investissements.
- **Points forts :** Diagnostic rapide, gestion efficace des ressources virtuelles, optimisation continue.
- **Solutions de Sécurité Réseau :** Protégez vos données et systèmes avec nos solutions de sécurité sur mesure : firewalls et segmentation réseau.

- **Points forts :** Analyse proactive des menaces, configurations adaptées, audit de sécurité approfondi.

1.1 Organigramme de l'entreprise :



2. Comparaisons des solutions et choix :

Nôtres choix c'est porté sur deux solutions : **Windows Serveur** et **Samba** dans cette partie nous allons parler de ses deux solutions lister les avantages et inconvénient de chacun.

Pour la première solution nous allons vous présenter la solution Windows Serveur 2022.

Qu'est-ce que **Windows serveur 2022** ?

Windows Server 2022 est la dernière version du système d'exploitation serveur de Microsoft, conçu pour les environnements professionnels nécessitant des capacités de gestion, de virtualisation et de sécurité avancées. Voici quelques-unes de ses principales fonctionnalités :

- **Sécurité multicouche avancée** : Windows Server 2022 inclut des fonctionnalités de sécurité avancées telles que **Secured-Core**, qui protège les équipements matériels, les microprogrammes et les fonctionnalités de système d'exploitation contre les menaces avancées.
- **Connectivité sécurisée** : Introduit des connexions HTTPS chiffrées plus rapides et sécurisées, ainsi que le chiffrement SMB AES 256 standard.
- **Hybride avec Azure** : Améliore la gestion des serveurs hybrides grâce à une gestion des machines virtuelles considérablement améliorée et une intégration facilitée avec Azure.
- **Optimisation des conteneurs** : Offre des tailles d'image réduites pour un téléchargement accéléré, une implémentation simplifiée de la stratégie réseau et des outils de conteneurisation pour les applications .NET.

Ces fonctionnalités font de Windows Server 2022 une plateforme flexible et sécurisée pour gérer des applications, des bases de données et des services réseau au sein d'infrastructures locales ou hybrides.

Windows Server
2022

Pour la deuxième solution nous allons vous présenter le software **Samba**.

Qu’est-ce que **Samba** ?

Samba est une suite logicielle libre qui permet d'interopérer avec le protocole de partage de fichiers SMB/CIFS des systèmes Microsoft Windows. Elle est principalement utilisée pour partager des fichiers et des imprimantes entre des ordinateurs sous Unix/Linux et des ordinateurs Windows. Voici quelques caractéristiques clés de Samba :

- **Partage de fichiers** : Permet aux utilisateurs de partager des fichiers entre des systèmes Windows et Unix/Linux.
- **Partage d'imprimantes** : Les imprimantes connectées à un système Unix/Linux peuvent être partagées avec des ordinateurs Windows.
- **Authentification et autorisation** : Samba peut intégrer des mécanismes d'authentification et d'autorisation, comme Active Directory, pour contrôler l'accès aux ressources partagées.
- **Interopérabilité** : Fonctionne bien avec divers systèmes d'exploitation, facilitant la collaboration dans des environnements hétérogènes.
  Grâce à Samba, il est possible de créer un serveur de fichiers et d'imprimantes qui peut être facilement utilisé par des ordinateurs fonctionnant sous divers systèmes d'exploitation, ce qui en fait un outil précieux pour les réseaux d'entreprise et domestiques.

Samba est un logiciel open source.

Voici un tableau de comparaison des deux solutions :

Caractéristiques	Windows serveur 2022	Samba
Origine	Microsoft	Open Source (The Samba Team)
Licence	Propriétaire	GNU Général Public Licence (GPL)
Système d'exploitation	Windows Server	Multiplateforme (Linux, Windows, MacOS, ...)
Coût	Abonnement ou achat unique	Gratuit
Fonctionnalités AD	Active Directory Intégré	Samba peut agir comme un contrôleur de domaine (PDC, BDC)
Compatibilité SMB	SMB 3.11	SMB 3.0
Sécurité	Avancées en matière de sécurité (Secured-core server, Credential Guard, ...)	Securité basée sur les Configuration et les politiques
Support	Support professionnel de Microsoft	Communauté et documentation en ligne
Scalabilité	Haute, adaptée, aux entreprises	Modérée, adaptée aux petites et moyennes entreprises
Intégration avec Azure	Intégration native avec Azure	Intégration via des solutions tierces
Administration	Gestionnaire de Serveur, PowerShell	Commande en ligne de commande (CLI)

Conclusion :

Nous avons choisi d'opter pour Windows Server 2022 en raison de sa stabilité éprouvée et de son adoption large dans de nombreuses infrastructures. Cette solution offre une performance optimale et des fonctionnalités de sécurité avancées, répondant ainsi aux besoins de notre organisation.

3. Gestion de projet

L’installation et la gestion d’un serveur Windows sont des étapes essentielles pour la mise en place d’une infrastructure réseau fiable et sécurisée dans une organisation. **Windows Server 2022**,

la dernière version du système d'exploitation serveur de Microsoft, offre des outils puissants pour gérer l’ensemble des services réseau et des ressources partagées.

Ce guide détaillé présente les étapes nécessaires à l'installation, la configuration et la gestion de divers rôles et services essentiels sur un serveur Windows, tels que **Active Directory Domain Services (AD-DS)**, **DHCP**, **DNS** et la gestion des utilisateurs. L'objectif principal est de permettre aux administrateurs de configurer un environnement sécurisé et efficace en mettant en œuvre des pratiques de gestion des utilisateurs, de la sécurité, ainsi que des stratégies de groupe.

Voici les étapes du projet à suivre :

Installation de Windows Serveur 2022

Cette étape consiste à installer le système d'exploitation Windows Server 2022 sur une machine dédiée. Il faut s'assurer que la configuration matérielle et les exigences minimales du serveur sont respectées.

Ajout du rôle AD-DS (Active Directory Domain Services)

L'ajout du rôle AD-DS permet de configurer le serveur pour fonctionner comme un contrôleur de domaine, ce qui est essentiel pour gérer l'authentification, les utilisateurs et les ordinateurs du réseau.

Création d’un domaine

Une fois AD-DS installé, il est nécessaire de créer un domaine. Ce domaine sera la base de la gestion des utilisateurs et des ressources dans l'environnement Active Directory. Le processus inclut la définition du nom du domaine et la configuration des paramètres de sécurité et de réseau.

Ajout d’un PC Windows client au domaine

Après avoir créé le domaine, il est nécessaire d'ajouter un ordinateur client (Windows) au domaine pour que ce dernier puisse bénéficier de la gestion centralisée des utilisateurs et des ressources.

Ajout d’un rôle DHCP (Dynamic Host Configuration Protocol)

Le rôle DHCP permet d'attribuer dynamiquement des adresses IP aux ordinateurs et appareils du réseau. Il faut installer et configurer le serveur DHCP pour gérer efficacement l'attribution des adresses IP aux périphériques.

Ajout du rôle DNS (Domain Name System)

Le rôle DNS permet de résoudre les noms de domaine en adresses IP. L'ajout de ce rôle est essentiel pour que le serveur puisse résoudre les requêtes réseau des clients et des serveurs du domaine.

Création d’unités d’organisation (OU)

Les unités d'organisation sont utilisées pour organiser les objets Active Directory (tels que les utilisateurs, les groupes et les ordinateurs) en catégories logiques. Cela permet une gestion simplifiée et une application plus précise des stratégies de groupe (GPO).

Création des utilisateurs

Dans cette section, vous apprendrez à créer des comptes d'utilisateurs dans Active Directory. Ces utilisateurs auront des identifiants uniques pour se connecter au domaine et accéder aux ressources partagées.

Création de profils itinérants

Les profils itinérants permettent aux utilisateurs de se connecter à différents ordinateurs tout en conservant leurs paramètres et fichiers personnels. Cela facilite la mobilité des utilisateurs dans l'environnement Active Directory.

Connexion d’un utilisateur au domaine

Une fois les comptes d'utilisateurs créés, il est nécessaire de configurer les ordinateurs clients pour permettre aux utilisateurs de se connecter au domaine et d'accéder aux ressources.

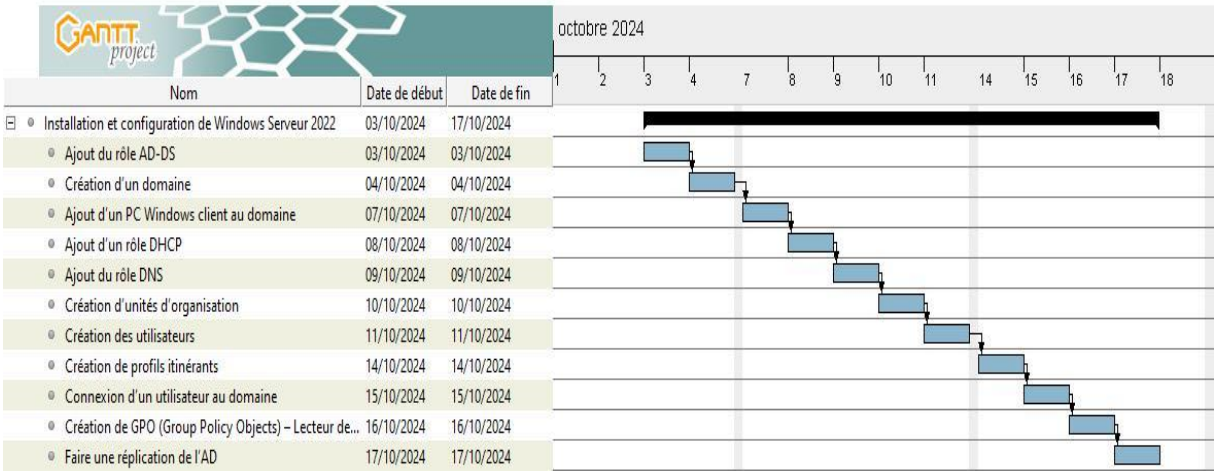
Création de GPO (Group Policy Objects) – Lecteur de mappage

Les stratégies de groupe (GPO) permettent de définir et d'appliquer des paramètres de sécurité, des configurations et des restrictions sur les utilisateurs et ordinateurs du domaine. Cette section porte sur la création d'une GPO pour la gestion des lecteurs mappés, permettant aux utilisateurs d'accéder à des lecteurs partagés sur le réseau.

Faire une réplication de l’AD

La réplication de l'Active Directory assure que les informations et les modifications apportées dans une partie du domaine (par exemple, un contrôleur de domaine) sont propagées et synchronisées avec d'autres contrôleurs de domaine. Cela garantit la disponibilité et la cohérence des données dans tout le réseau.

Gantt prévisionnel :

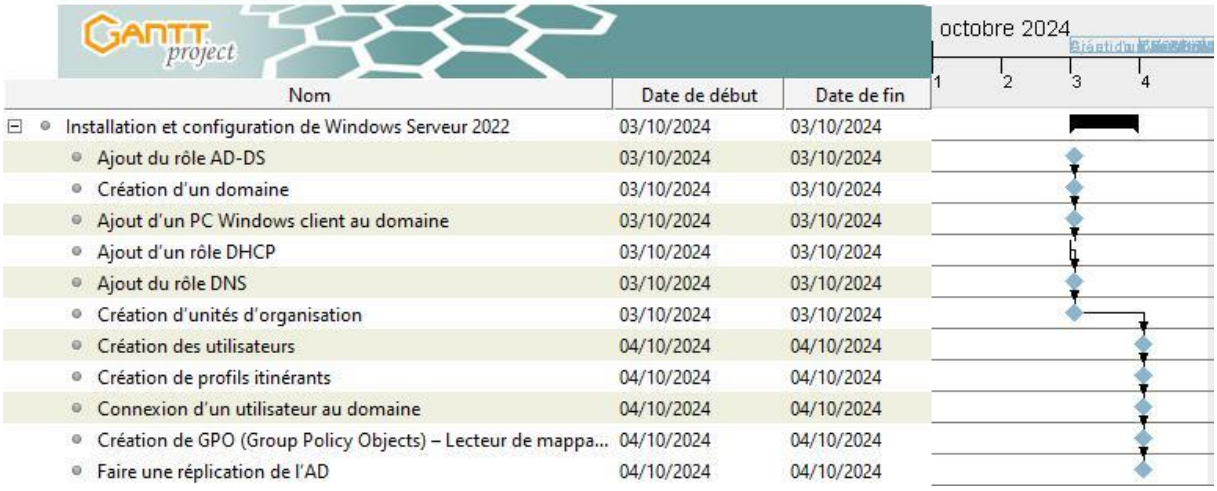


Nom	Date de début	Date de fin
Installation et configuration de Windows Serveur 2022	03/10/2024	17/10/2024
Ajout du rôle AD-DS	03/10/2024	03/10/2024
Création d'un domaine	04/10/2024	04/10/2024
Ajout d'un PC Windows client au domaine	07/10/2024	07/10/2024
Ajout d'un rôle DHCP	08/10/2024	08/10/2024
Ajout du rôle DNS	09/10/2024	09/10/2024
Création d'unités d'organisation	10/10/2024	10/10/2024
Création des utilisateurs	11/10/2024	11/10/2024
Création de profils itinérants	14/10/2024	14/10/2024
Connexion d'un utilisateur au domaine	15/10/2024	15/10/2024
Création de GPO (Group Policy Objects) – Lecteur de...	16/10/2024	16/10/2024
Faire une réplication de l'AD	17/10/2024	17/10/2024

Voici quelques éléments qui peuvent retarder la planification :

Le retard de livraison des serveurs, le manque de ressources humaines, des imprévue de la vie, des intervention plus urgentes et prioritaire...

Gantt réelle :



Nom	Date de début	Date de fin
Installation et configuration de Windows Serveur 2022	03/10/2024	03/10/2024
Ajout du rôle AD-DS	03/10/2024	03/10/2024
Création d'un domaine	03/10/2024	03/10/2024
Ajout d'un PC Windows client au domaine	03/10/2024	03/10/2024
Ajout d'un rôle DHCP	03/10/2024	03/10/2024
Ajout du rôle DNS	03/10/2024	03/10/2024
Création d'unités d'organisation	03/10/2024	03/10/2024
Création des utilisateurs	04/10/2024	04/10/2024
Création de profils itinérants	04/10/2024	04/10/2024
Connexion d'un utilisateur au domaine	04/10/2024	04/10/2024
Création de GPO (Group Policy Objects) – Lecteur de mappa...	04/10/2024	04/10/2024
Faire une réplication de l'AD	04/10/2024	04/10/2024

4 Procédure d’installation et de configuration

Pour mener à bien l'installation et la configuration de Windows Server 2022, ainsi que l'ajout de ses différents rôles, nous suivrons une série d'étapes précises et méthodiques. En utilisant Proxmox, une plateforme de virtualisation puissante et flexible, vous pourrez déployer et gérer efficacement des serveurs virtuels.

Dans cette section, nous vous guiderons à travers chaque étape, depuis l'installation de Windows Server 2022 jusqu'à la configuration des rôles essentiels tels qu’AD DS (Active Directory Domain Services), DHCP, DNS, et d'autres. Vous découvrirez comment créer un domaine, ajouter des utilisateurs et des unités d'organisation, configurer des profils itinérants et des stratégies de groupe (GPO), et mettre en place la réplication de l'Active Directory.

Pré-requis pour Windows Server 2022:

- Une machine virtuelle sur Proxmox
- 8 GO de Ram Minimum
- 80 GO de stockage ou plus
- 1 Processeur 2 coeurs
- Un ISO de Windows Server 2022

Pré-requis Pour Windows 10 ou 11 au choix :

- Une machine virtuelle sur Proxmox
- 4 GO de Ram minimum
- 64 GO de stockage ou plus
- 1 processeur 2 cœurs
- Un ISO de Windows 10 ou 11

Machine Virtuelle ProxMox Windows Server 2022.

4.1 Ajout du rôle AD-DS

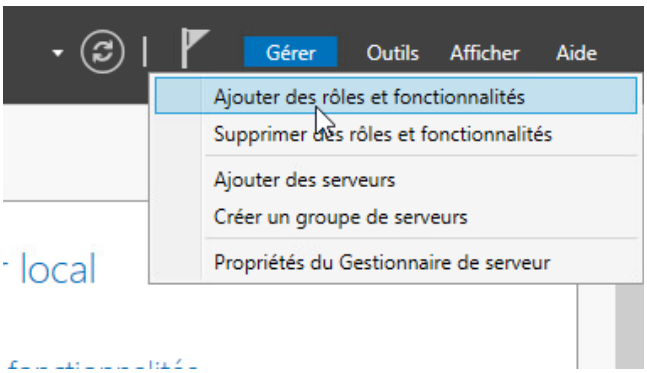
Qu'est-ce qu'un rôle AD-DS :

AD DS, ou Active Directory Domain Services, est une technologie de Microsoft qui joue un rôle crucial dans la gestion des réseaux d'entreprise. En résumé, voici les points principaux :

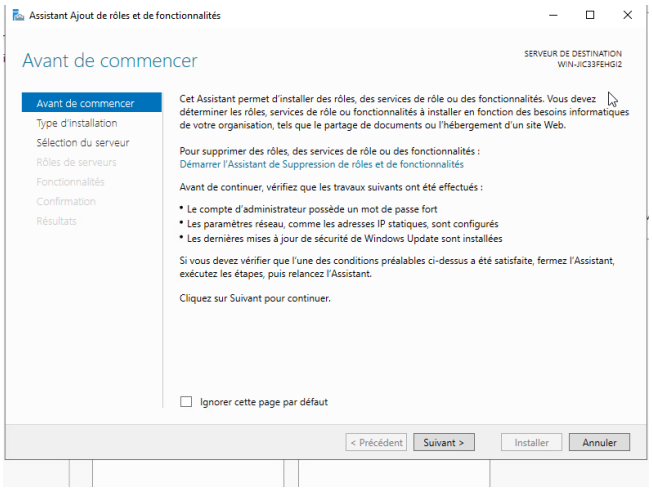
- **Authentification et Autorisation :** Vérifie l'identité des utilisateurs et des ordinateurs, et gère les permissions d'accès aux ressources réseau.
- **Gestion des Utilisateurs et des Groupes :** Permet de créer, modifier et gérer des comptes d'utilisateurs et des groupes.
- **Politiques de Groupe :** Déploie des politiques de sécurité et de configuration à travers tout le réseau.
- **Répertoire Hiérarchique :** Maintient une base de données contenant des informations sur les ressources réseau, facilitant les recherches et la gestion.
- **Répartition des Rôles :** Attribue différents rôles à divers serveurs pour assurer la redondance et répartir la charge.

AD DS est un outil essentiel pour la gestion centralisée et sécurisée des réseaux informatiques.

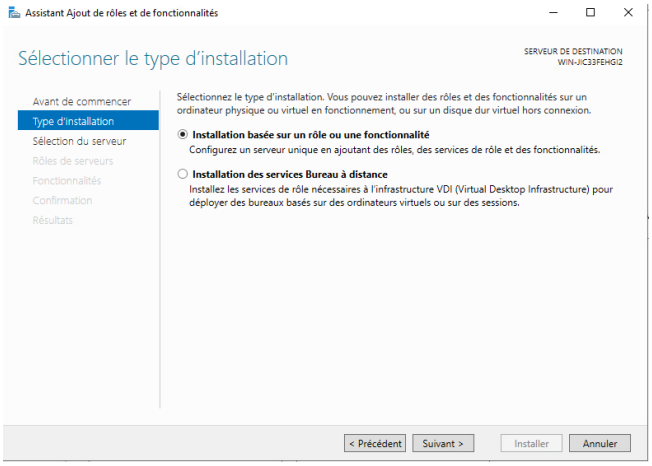
- **Installation d'un rôle AD-DS Pas à Pas.**



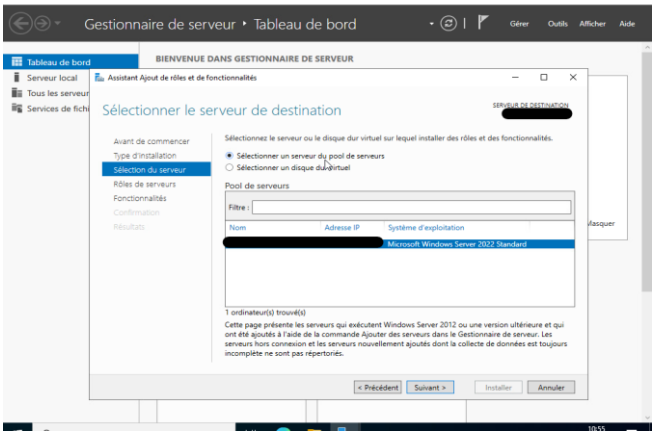
Pour installer le rôle AD-DS cliquer sur **gérer** et **ajouter des rôles et fonctionnalités**.



Passez l'étape "**Avant de commencer**".

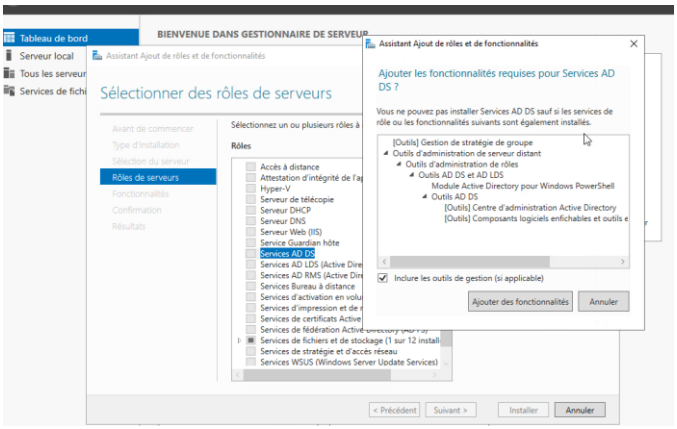


Poursuivez ensuite en laissant le type d'installation sur le choix "**Installation basée sur un rôle ou une fonctionnalité**".

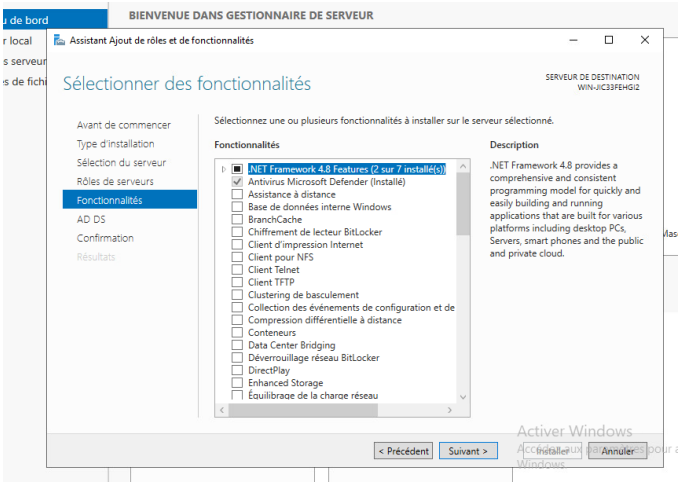


Sélectionnez votre serveur local. En principe, c'est le choix par défaut.

Pour notre exemple il sera en **192.168.10.1/24**.

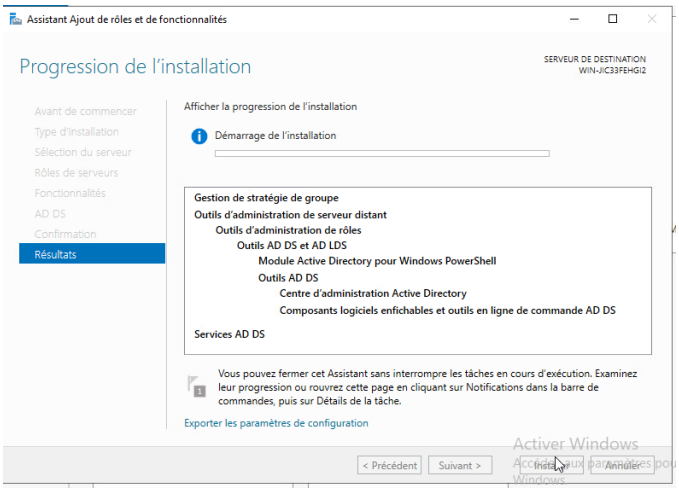


Nous n'installons pas de fonctionnalités en plus, donc poursuivez sans rien sélectionner.

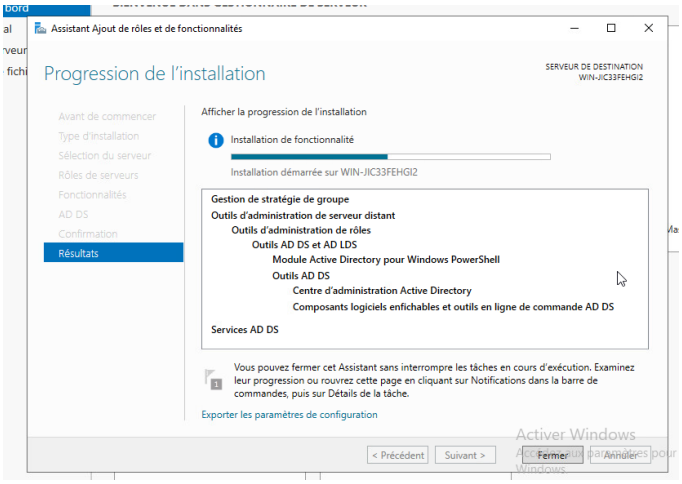


Faire suivant.

Cliquez sur "**Installer**" pour démarrer l'installation, qui peut prendre quelques minutes.



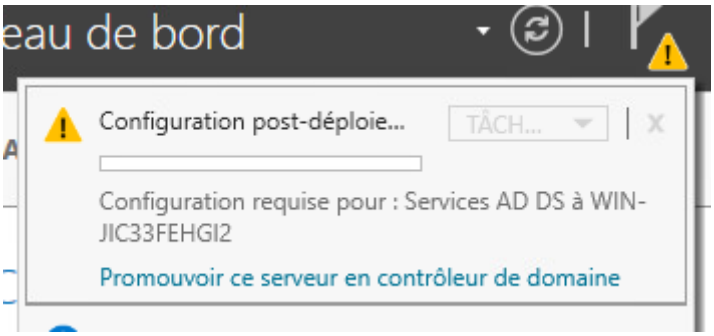
L'installation du rôle AD-DS va commencer.



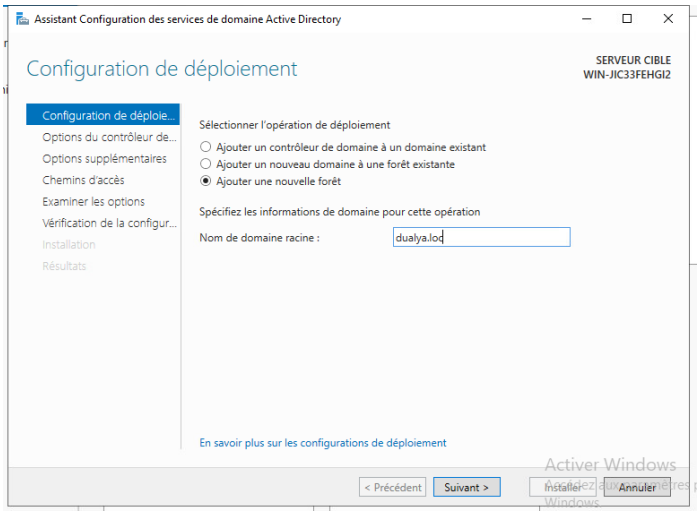
Laisser l'installation se faire.

Cliquez sur "**Fermer**" quand ce sera terminé une fois l'installation du rôle nous allons pouvoir promouvoir un domaine.

4.1.1 Promouvoir un domaine active directory

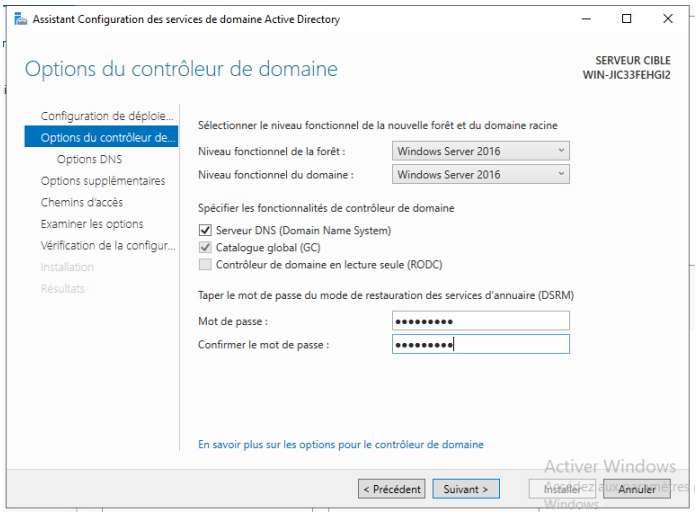


Cliquer sur promouvoir ce serveur en contrôleur de domaine.

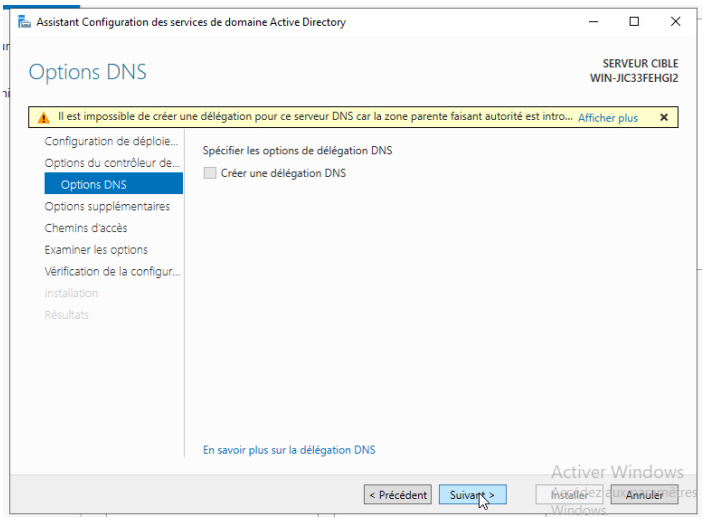


Faire ajouter une nouvelle forêt.

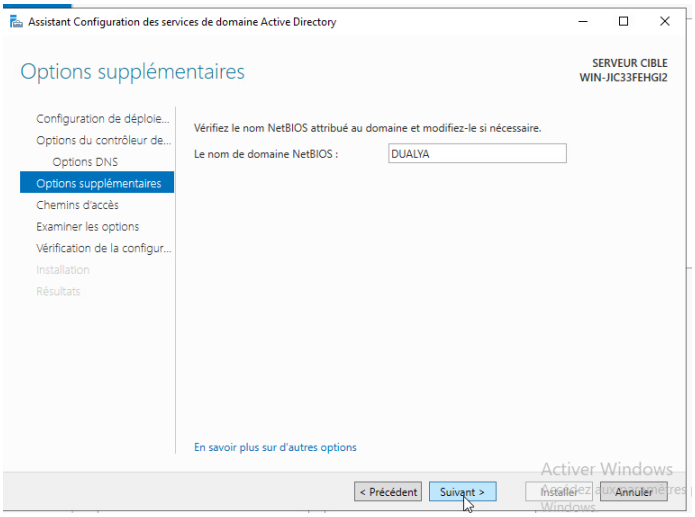
Non du domaine racine : **dualya.loc**



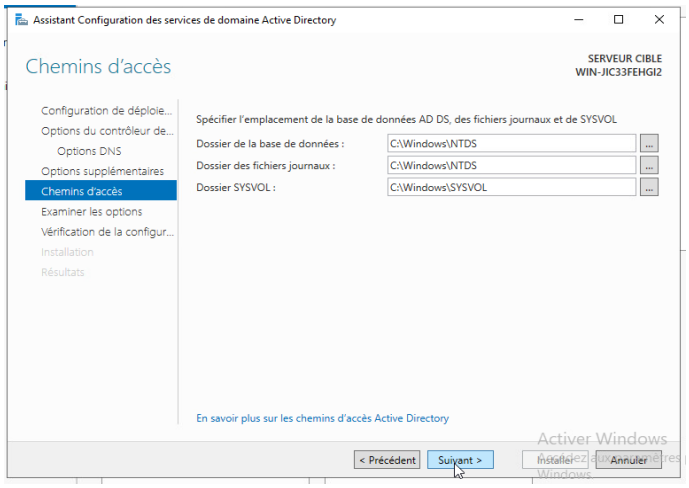
Entrer un mot de complexe et copier dans votre Keep Pass.



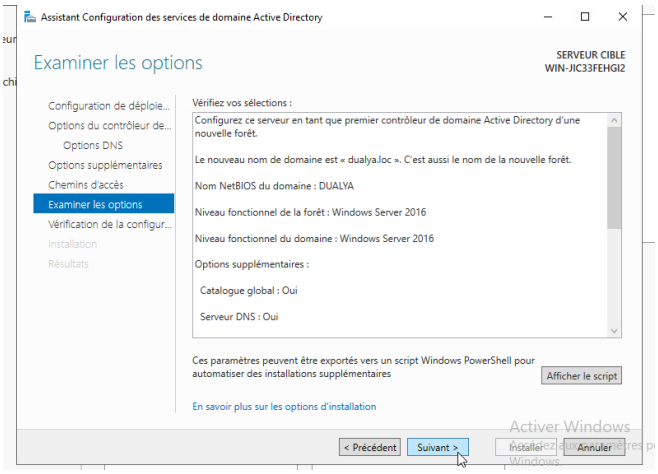
Faire suivant.



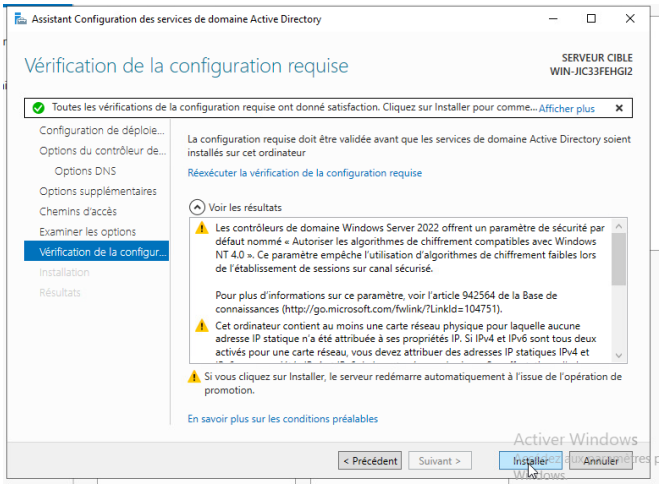
Le nom NETBIOS de votre domaine est ensuite déterminé, vous pouvez éventuellement le changer.



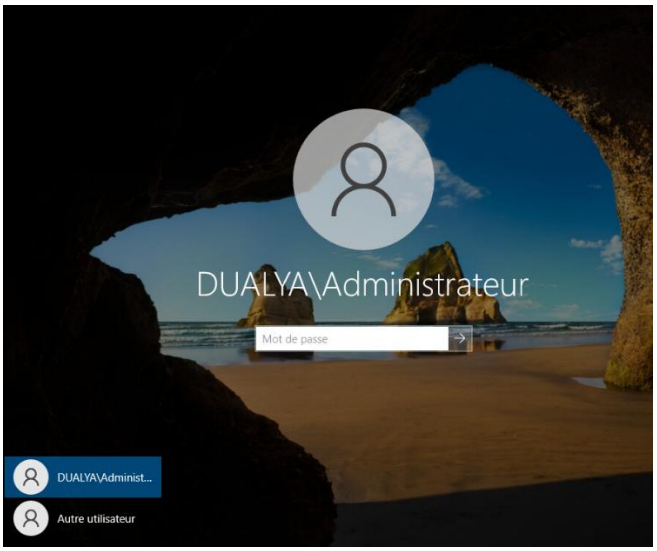
Vous devez ensuite préciser les chemins de stockage de l'AD.



Un dernier écran résume votre paramétrage.



Cliquer sur installer le serveur va redémarrer pour valider la création du domaine.



Le domaine **dualya.loc** a été créé vous pouvez vous y connecter avec le MDP que vous avez créé.

4.1.2 Ajout d'un rôle DHCP

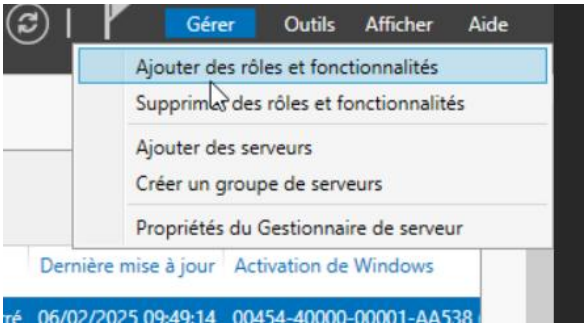
Qu'est-ce que le rôle DHCP :

Le rôle DHCP (Dynamic Host Configuration Protocol) est essentiel pour la gestion des adresses IP dans les réseaux informatiques. Voici un résumé :

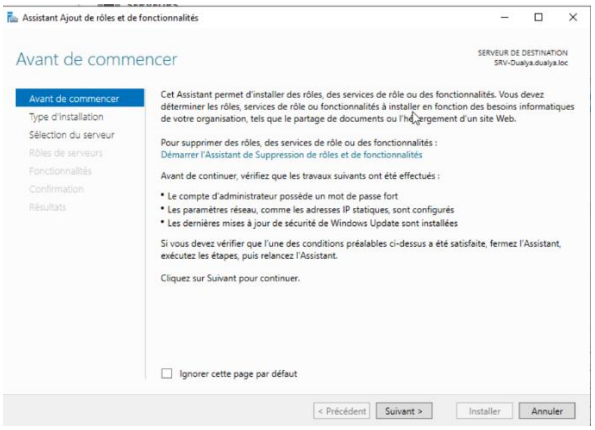
- **Attribution Dynamique des Adresses IP :** Le serveur DHCP attribue automatiquement des adresses IP aux appareils connectés au réseau.
- **Configuration Réseau :** Il fournit également des informations de configuration réseau comme les serveurs DNS et la passerelle par défaut.

- **Gestion des Adresses IP :** Il gère un pool d'adresses IP et évite les conflits en s'assurant qu'aucune adresse n'est attribuée deux fois.
- **Facilité de Gestion :** Simplifie la gestion des réseaux, surtout dans les grandes entreprises.
- **Intégration avec AD DS :** Il peut être configuré pour mettre à jour les enregistrements DNS et être autorisé dans Active Directory pour une sécurité supplémentaire.

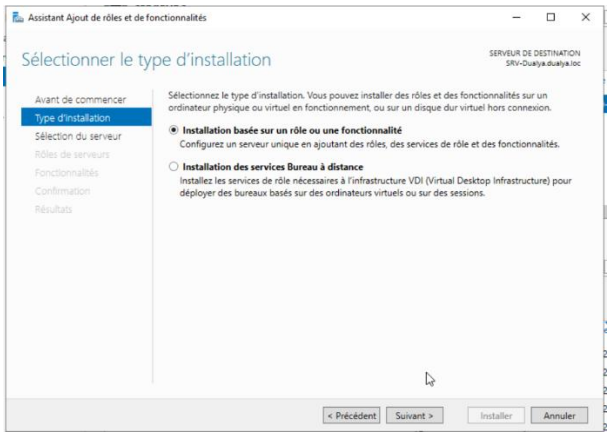
En résumé, DHCP facilite et automatise la gestion des adresses IP, rendant les réseaux plus efficaces et faciles à administrer.



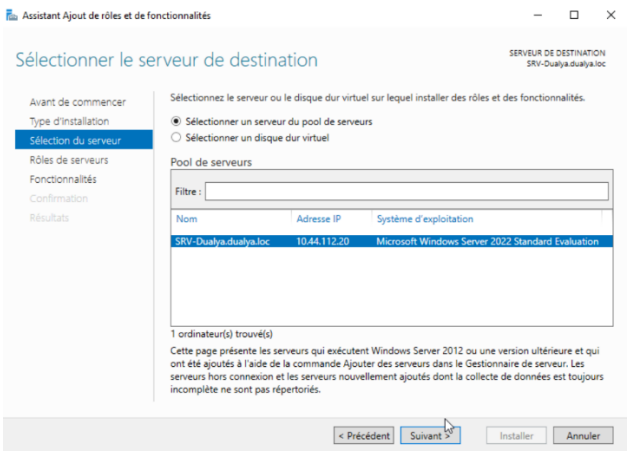
Cliquer sur **Gérer** et **Ajouter des rôles et fonctionnalités**.



Cliquer sur **suivant**.

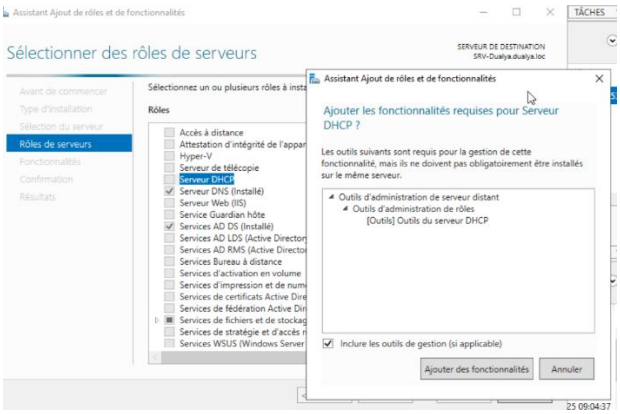


Type d'installation : **Installation basée sur un rôle ou une fonctionnalité**.

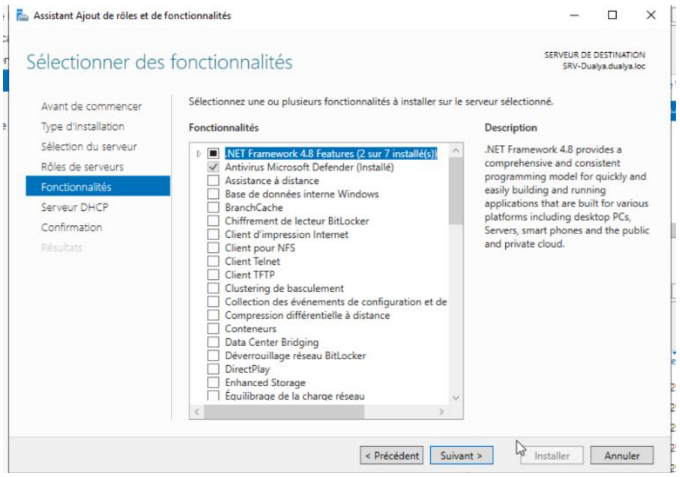


Adresse IP **192.168.10.1**

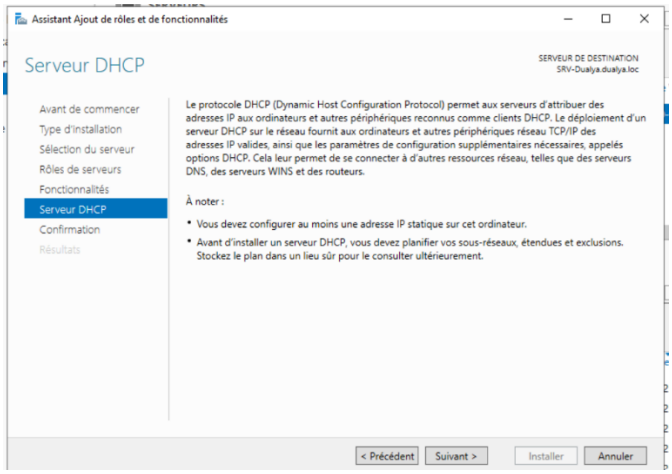
Cliquer sur **suivant.**



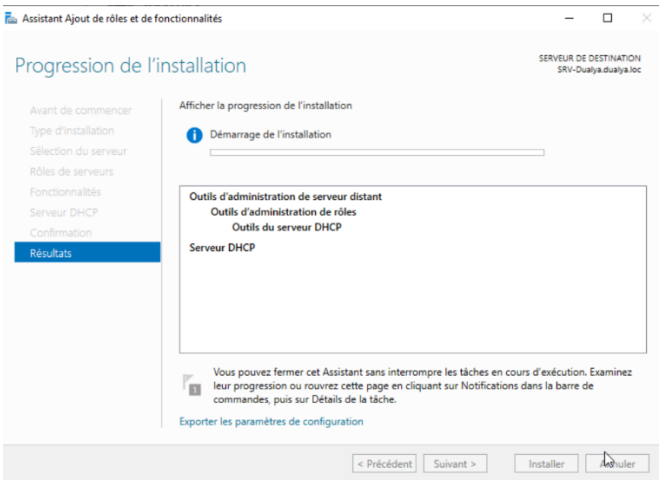
Sélectionner le rôle **DHCP.**



Cliquer sur **suivant.**

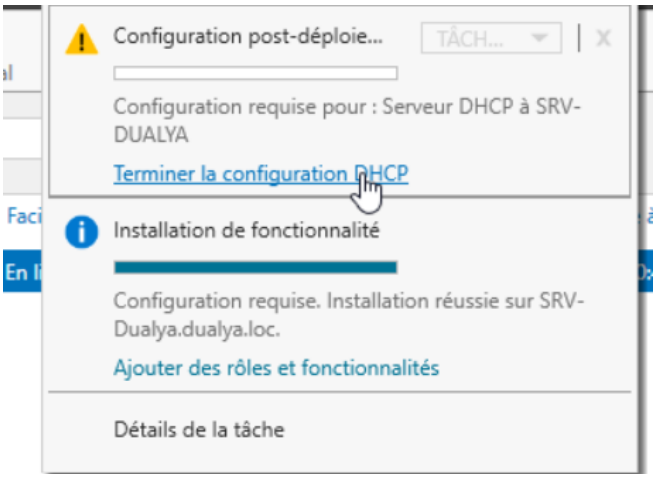


Cliquer sur **suivant.**

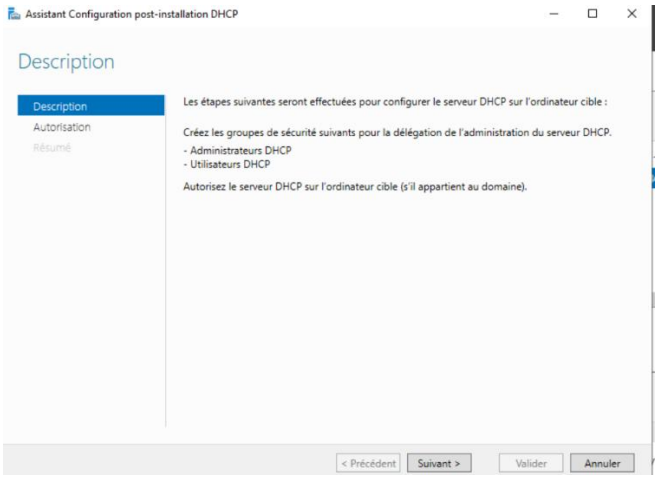


L'installation va commencer.

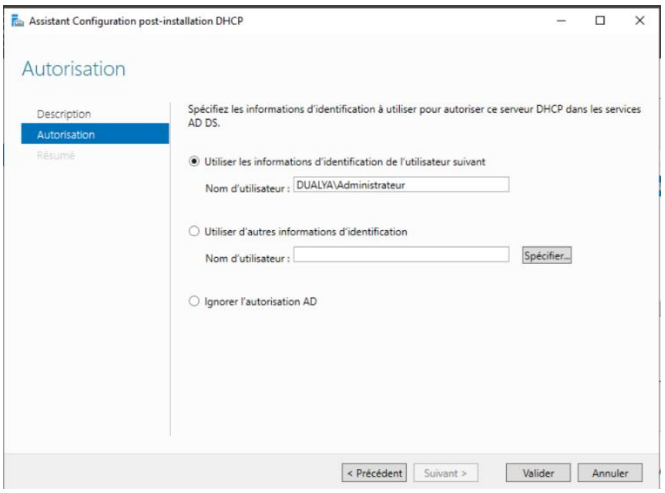
Configurer le DHCP :



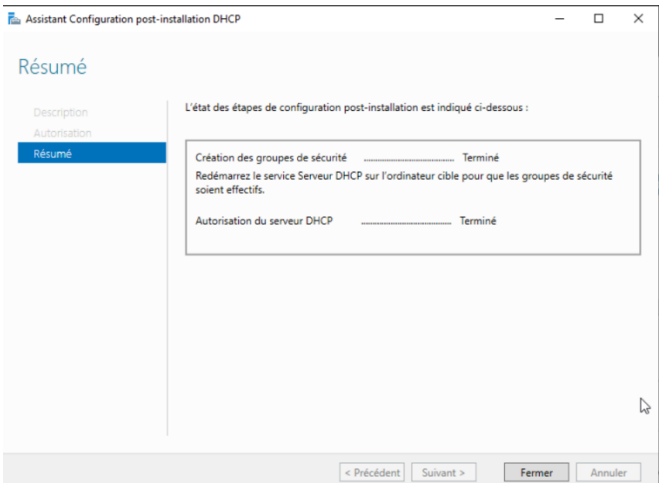
Cliquer sur **Terminer la configuration DHCP**.



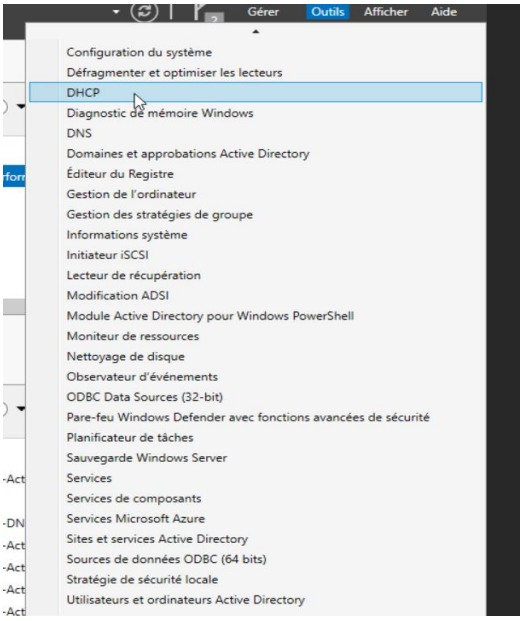
Cliquer sur **suivant**.



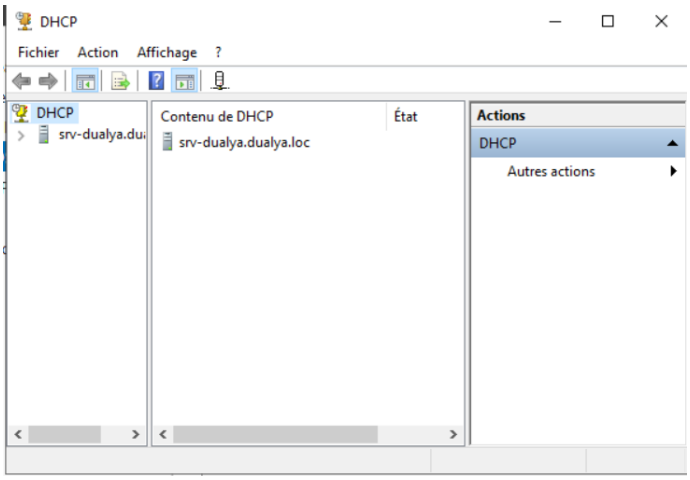
Choisir **utiliser les informations d'identification de l'utilisateur suivant** et cliquer sur **valider**.



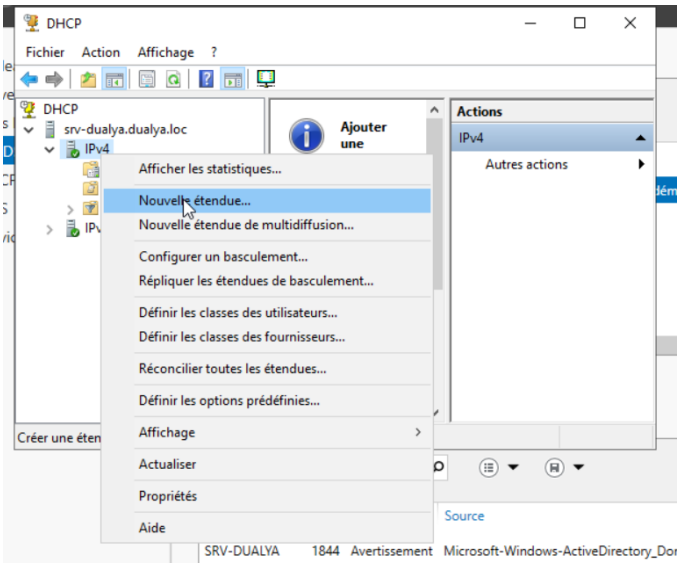
Cliquer sur **fermer**.



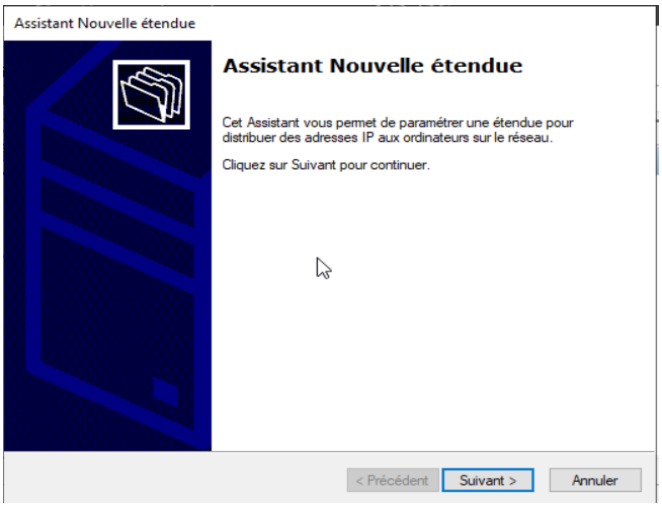
Cliquer sur **outil** puis **DHCP**.



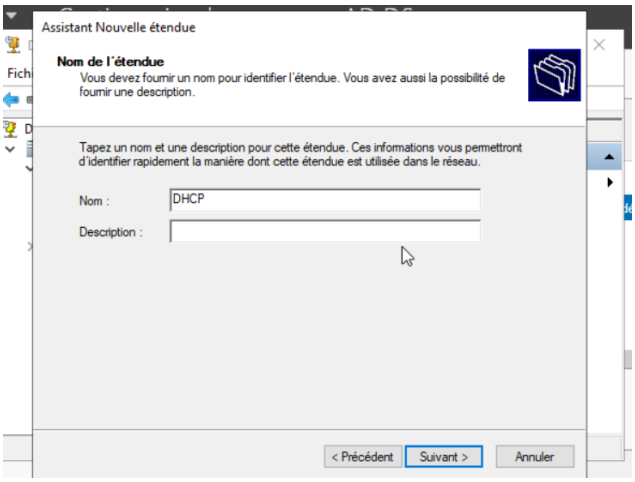
La fenêtre du rôle **DHCP** s'ouvre.



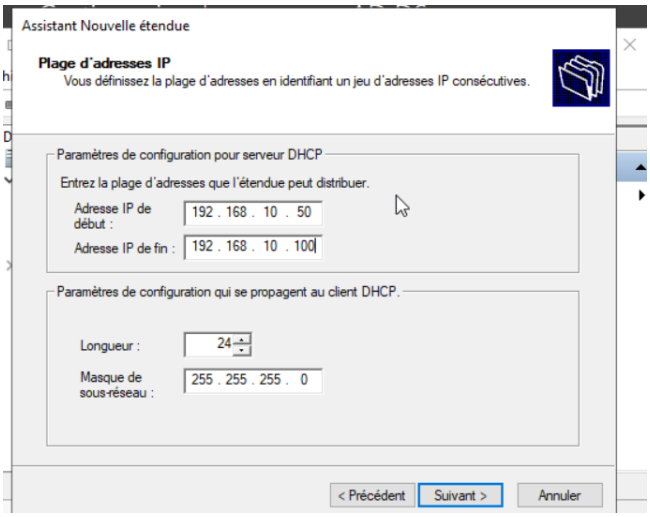
Faire clic droit sur **IPV4** puis sur **nouvelle étendue**.



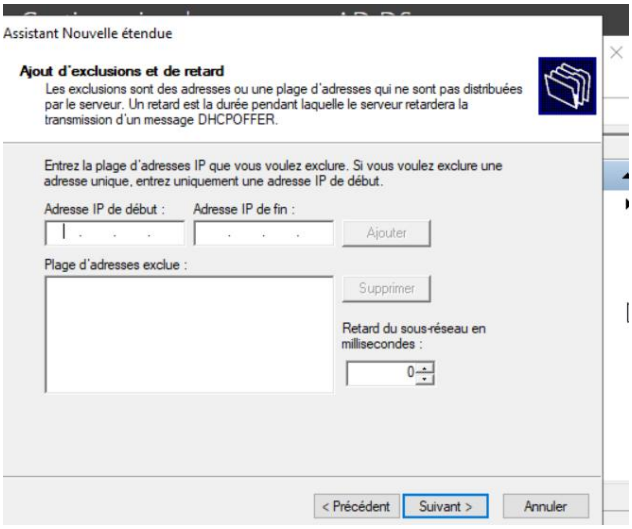
L'assistant de la nouvelle étendue s'affiche.



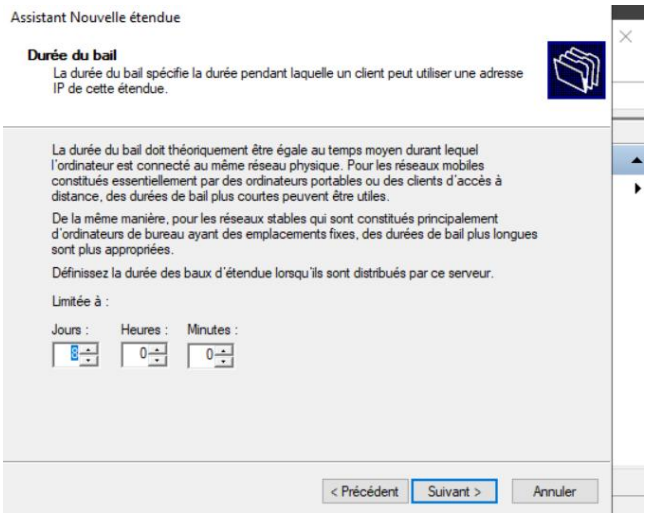
Nommer le non de la nouvelle étendue.



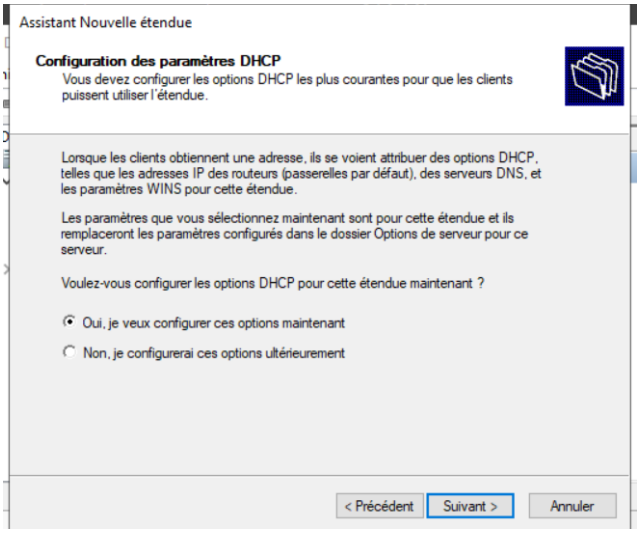
Créer la plage d'adresse IP du **DHCP** pour nous sa seras **192.168.10.50** à **192.168.10.100.**



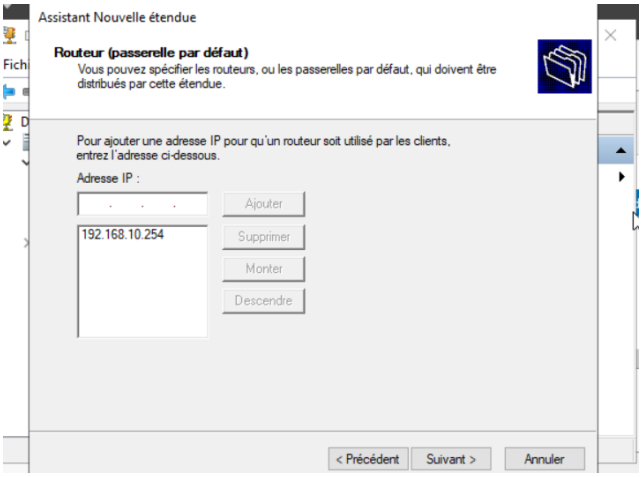
Cliquer sur **suivant.**



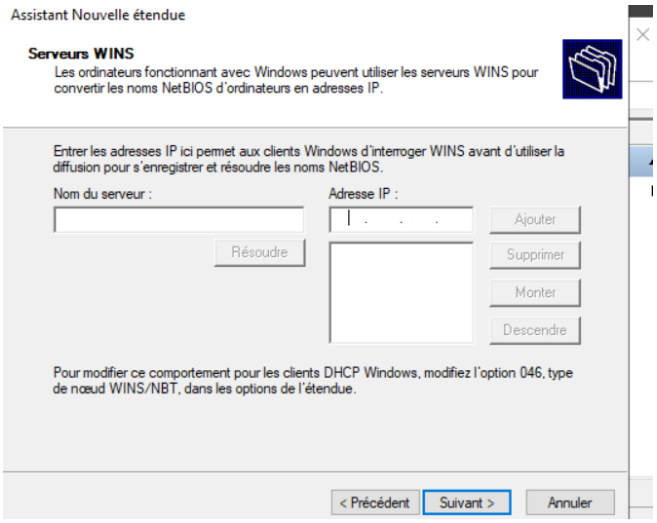
Vous pouvez laisser la durée du bail sur 8 jours et faire **suivant**.



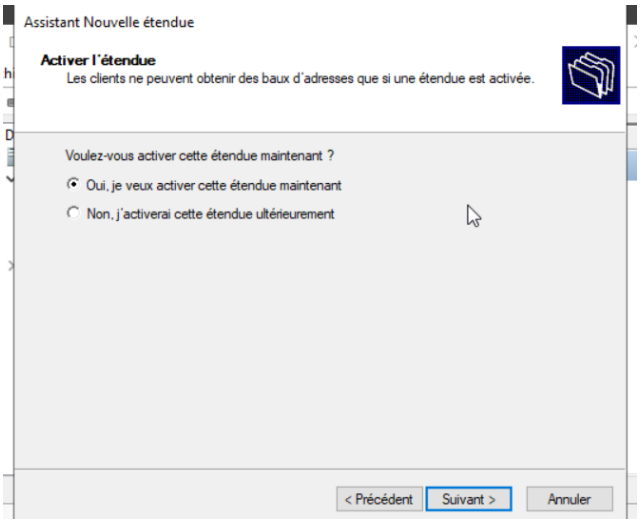
Laisser sur **Oui, je veux configurer ces options maintenant** et faire **suivant**.



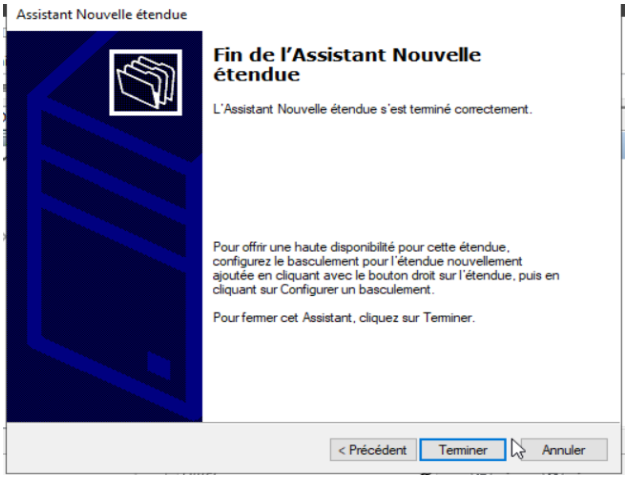
Ajouter la **Gateway** qui seras **192.168.10.254**.



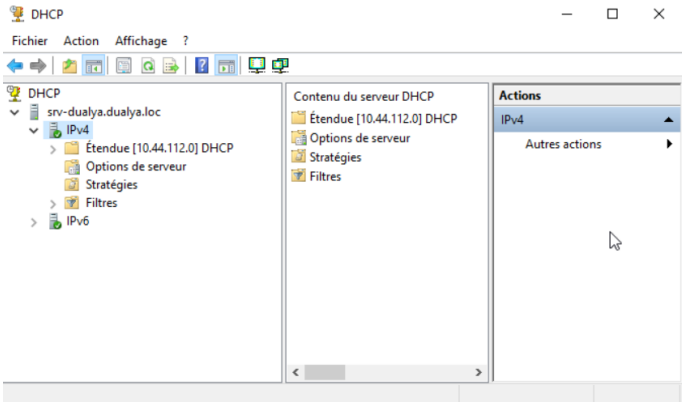
Cliquer sur **suivant**.



Laisser sur **Oui, je veux activer cette étendue maintenant** et faire **suivant**.



Cliquer sur **Terminer**.



Votre rôle **DHCP** ainsi que la configuration de **la nouvelle étendue** ont été créé.

4.1.3 Ajout d'un rôle DNS

Qu'est-ce qu'un rôle DNS ?

Dans le contexte d'Active Directory (AD), le DNS joue un rôle fondamental en assurant la connectivité et la fonctionnalité des services AD. Voici quelques points clés sur son rôle :

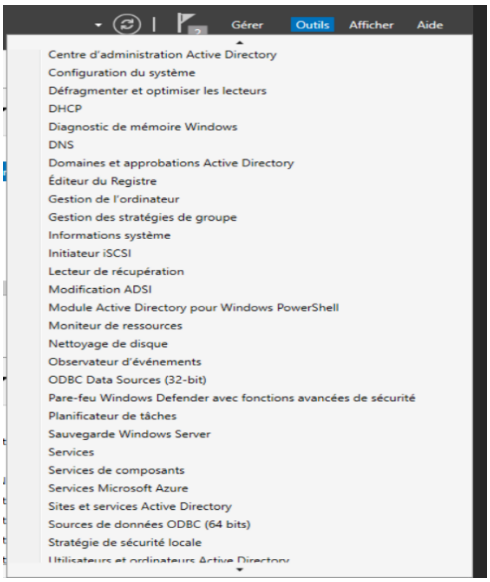
1. **Localisation des contrôleurs de domaine** : Le DNS permet aux clients et aux serveurs de localiser les contrôleurs de domaine dans un environnement AD. Lorsqu'un utilisateur se connecte ou qu'un service a besoin d'accéder à AD, le DNS est utilisé pour trouver les contrôleurs de domaine appropriés.
2. **Répartition du service** : Grâce au DNS, les différentes ressources de l'Active Directory, telles que les serveurs LDAP ou les serveurs Kerberos, sont facilement accessibles. Cela inclut la répartition des enregistrements SRV (Service Locator), qui permettent aux clients de localiser les services réseau au sein du domaine AD.
3. **Fonctionnalité de réplication** : Le DNS est essentiel pour la réplication des données entre les contrôleurs de domaine. Il permet de garantir que les données de l'Active Directory restent cohérentes sur tous les contrôleurs de domaine.
4. **Nom unique pour chaque objet** : Chaque objet dans AD a un nom unique, et le DNS aide à résoudre ces noms et adresses IP, facilitant ainsi la communication et l'accès aux ressources réseau.

En somme, sans le DNS, de nombreux services et fonctionnalités d'Active Directory ne pourraient pas fonctionner correctement. Il agit en quelque sorte comme un système nerveux, reliant toutes les parties de l'infrastructure AD.

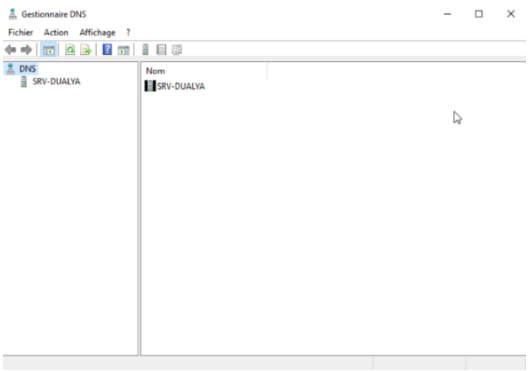
Tout d'abord nous allons créer deux zones la première est **une zone de recherche directe** qui permet de résoudre **un nom de domaine en une adresse IP**.

La deuxième est **une zone de recherche inversé** qui permet de résoudre **une adresse IP en un nom de domaine**.

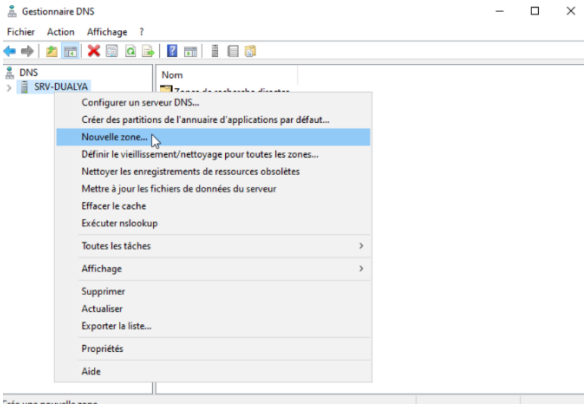
Zone de recherche directe :



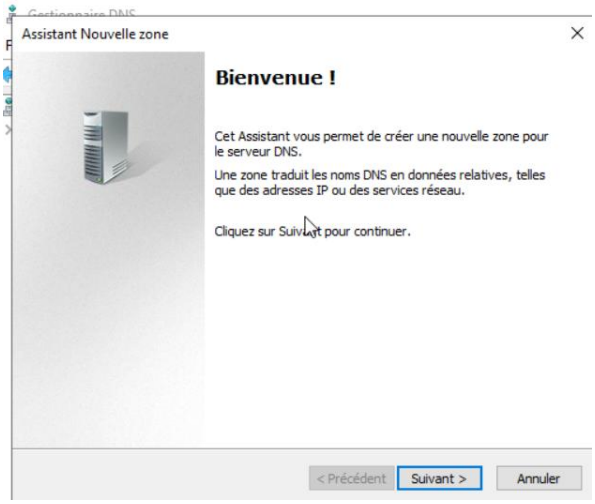
Une fois le rôle installé cliquer sur **Outils** et **DNS**.



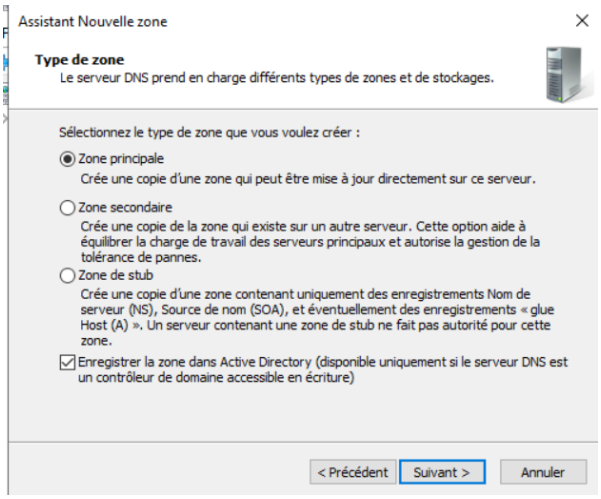
Le gestionnaire **DNS** s'ouvre.



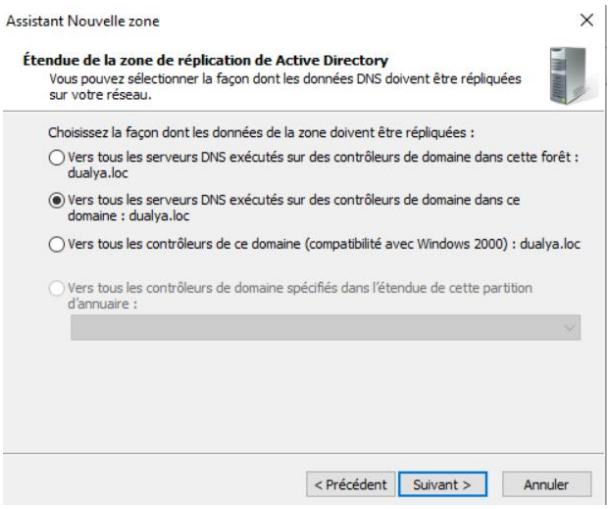
Faite clic droit et **nouvelle zone**.



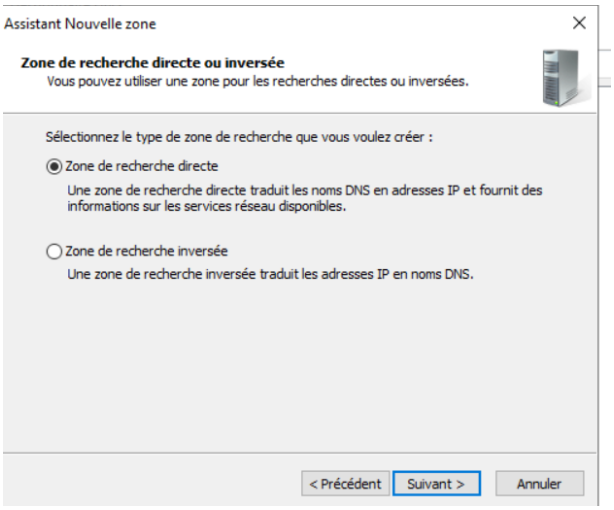
Le wizzard d'assistance va s'ouvrir.



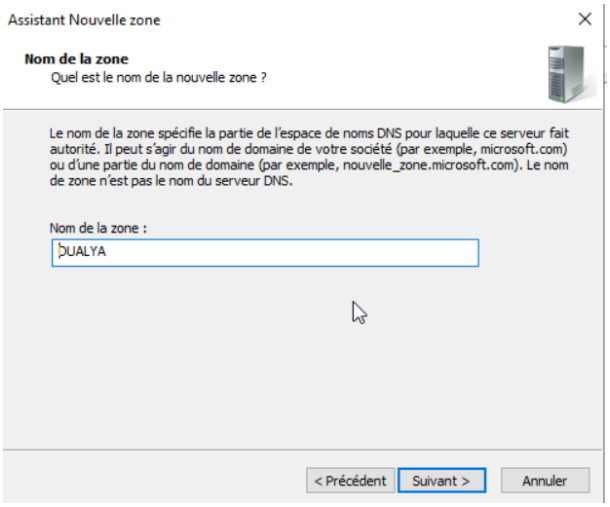
Sélectionner **zone principale** et faire **suivant**.



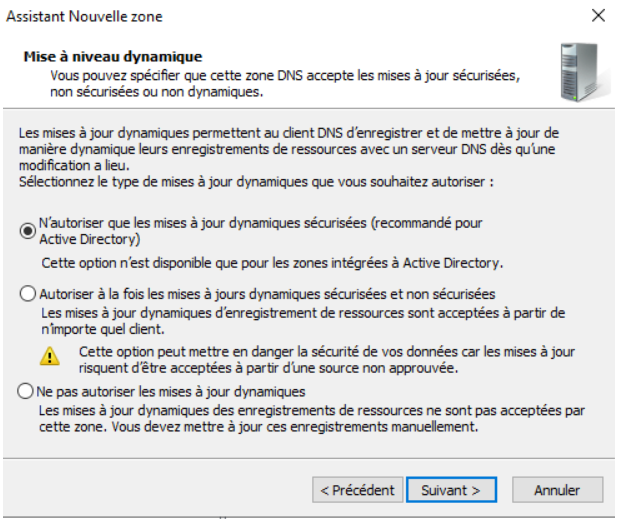
Sélectionner **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : dualya.loc** et faire **suivant.**



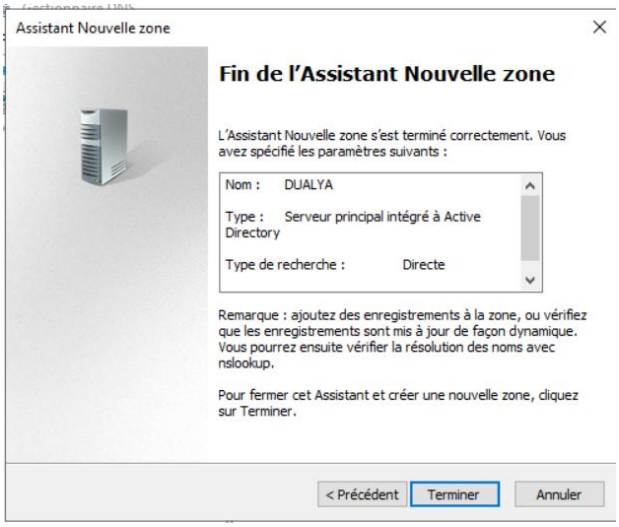
Laisser sur **Zone de recherche directe** et faire **suivant**.



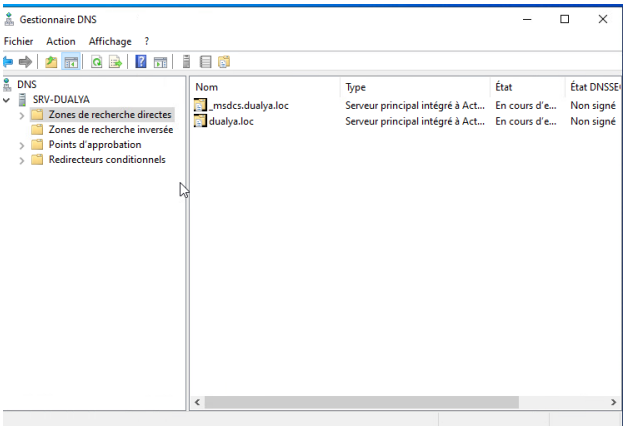
Nommer la zone.



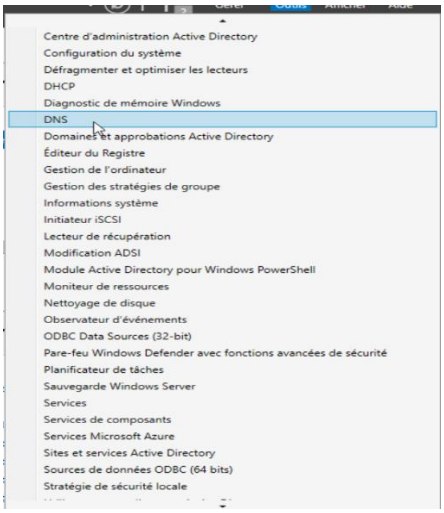
Faire **suivant**.



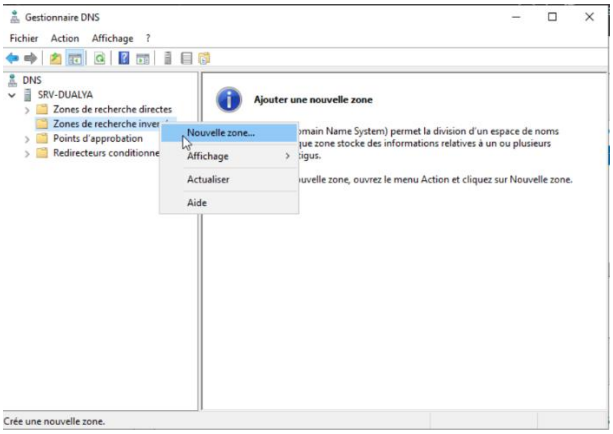
Cliquer sur **Terminer** la zone de recherche directe sera créé.



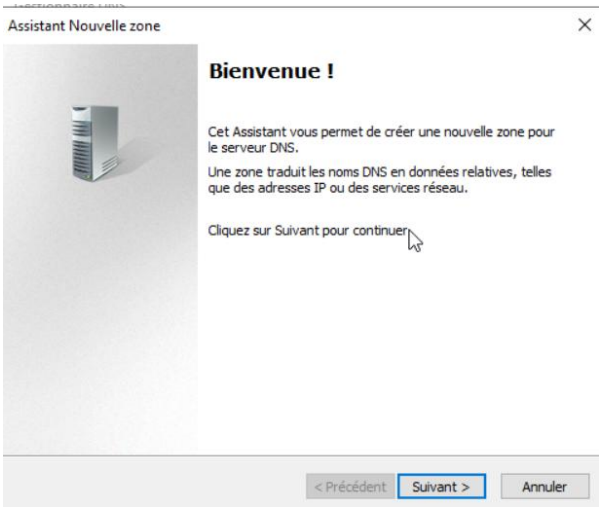
Zone de recherche inversé :



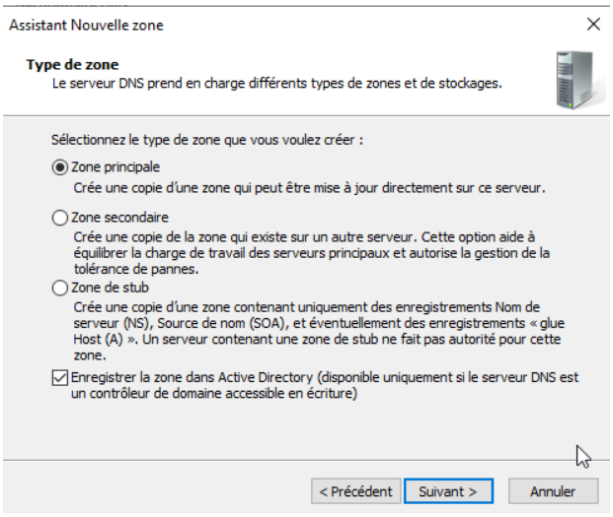
Cliquer sur **Outils** et **DNS.**



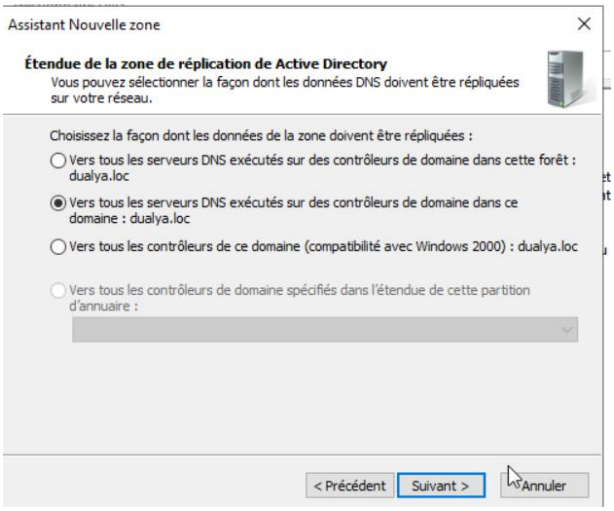
Le gestionnaire **DNS** s'ouvre faite clic droit sur **Zone de recherche inverse** et **Nouvelle zone.**



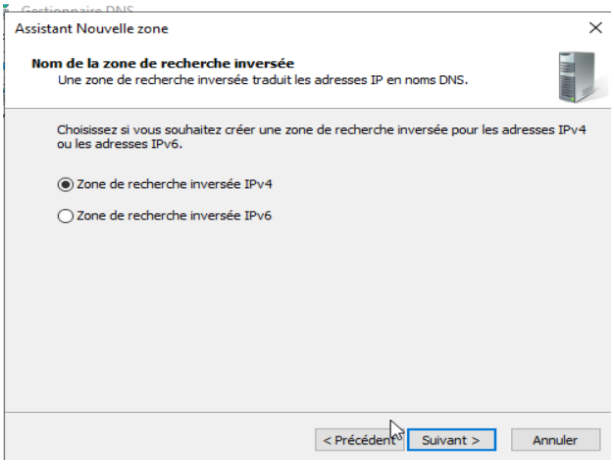
L'assistant nouvelle zone s'ouvre faire **suivant.**



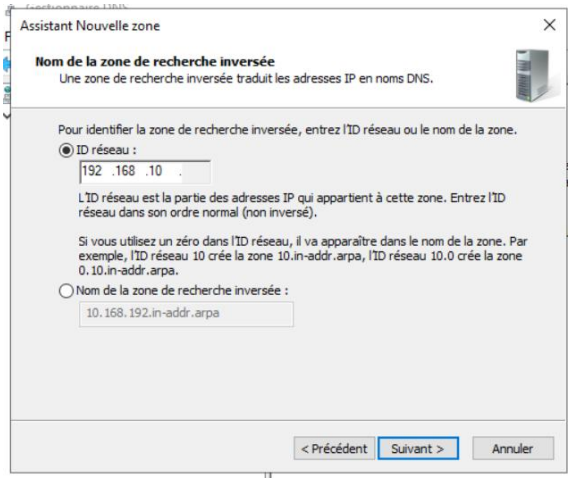
Laisser sur **Zone principale** et faire **suivant.**



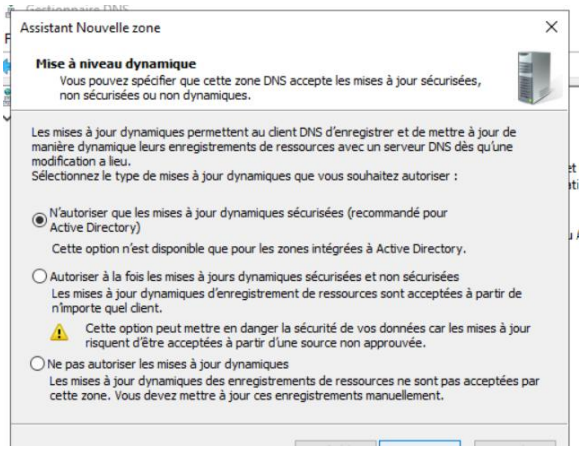
Sélectionner **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : dualya.loc** et faire **suivant.**



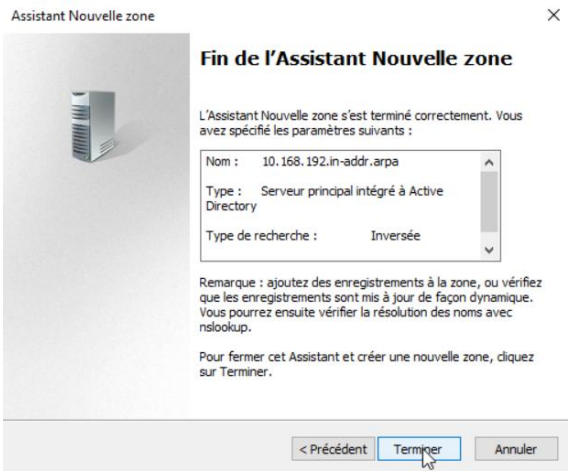
Sélectionner **Zone de recherche inversée IPv 4** et faire **suivant.**



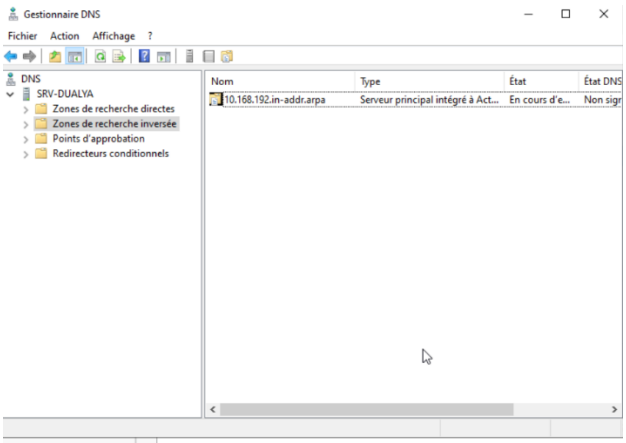
Entrer l'ID réseau **192.168.10** (selon votre configuration de votre réseau).



Faire **suivant.**



Fin de l'assistance la **Zone de recherche inversé** a été créé**.**



La zone de recherche inversée a été créé dans **le gestionnaire DNS**.

4.1.4 Ajouter un PC Windows client au domaine

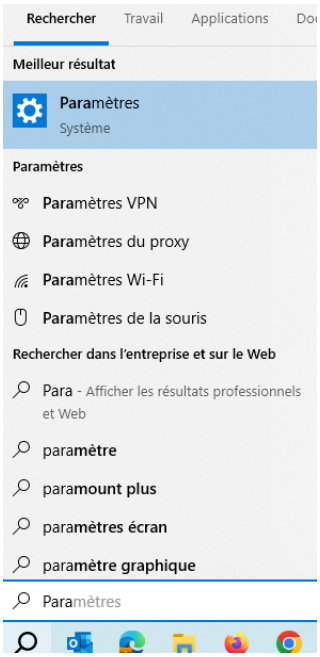
Pourquoi ajouter un poste client au domaine :

Ajouter un poste client à un domaine offre plusieurs avantages, particulièrement dans un environnement de travail professionnel ou d'entreprise. Voici quelques raisons principales :

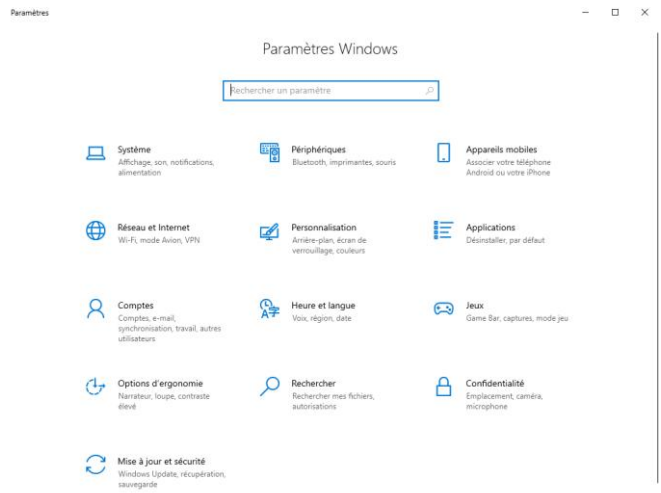
1. **Gestion centralisée** : Vous pouvez gérer les utilisateurs, les groupes et les périphériques à partir d'une seule console d'administration. Cela simplifie les tâches administratives comme la création de nouveaux comptes d'utilisateurs, la réinitialisation des mots de passe et l'application de politiques de sécurité.
2. **Sécurité accrue** : Les politiques de sécurité peuvent être appliquées uniformément à tous les ordinateurs du domaine. Vous pouvez contrôler quels utilisateurs ont accès à quelles ressources, surveiller et enregistrer les activités des utilisateurs, et déployer des mises à jour de sécurité plus efficacement.
3. **Accès simplifié aux ressources partagées** : Les utilisateurs peuvent accéder facilement aux imprimantes, aux dossiers partagés et à d'autres ressources réseau sans avoir à se connecter séparément à chaque ressource. Les autorisations et l'accès peuvent être gérés de manière centralisée.
4. **Sauvegarde et restauration centralisées** : Les données critiques peuvent être sauvegardées sur des serveurs centralisés, ce qui facilite la restauration en cas de perte de données sur les postes clients.
5. **Déploiement de logiciels** : Vous pouvez installer ou mettre à jour des logiciels sur tous les ordinateurs du domaine à partir d'une console centrale, ce qui réduit le temps et les efforts nécessaires pour maintenir les systèmes à jour.

Ces avantages rendent les environnements de domaine particulièrement utiles dans les grandes organisations où la gestion et la sécurité des ressources informatiques sont primordiales.

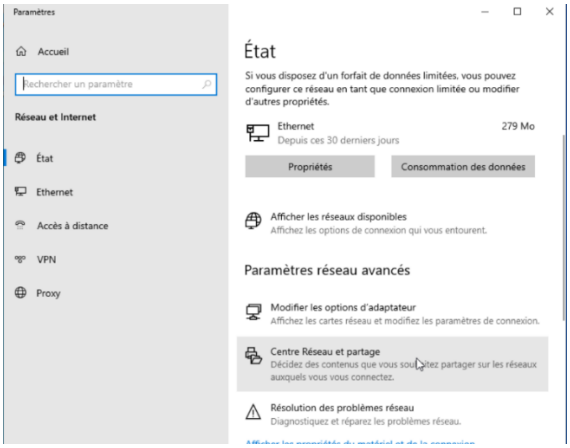
Nous allons voir comment faire étape par étape pour ajouter un PC client dans un domaine.



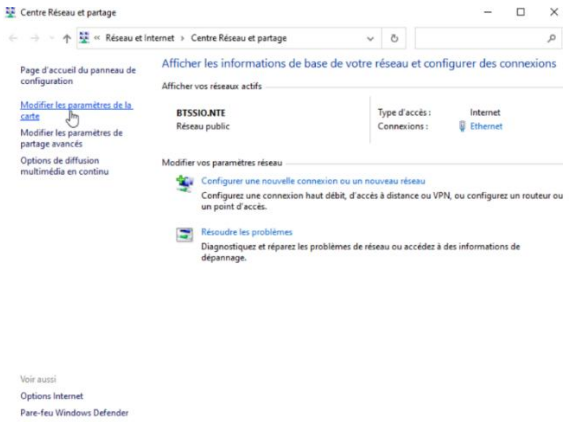
Dans la barre de recherche en bas a gauche du pc client taper **Paramètres** et cliquer sur l'icône **Paramètres système.**



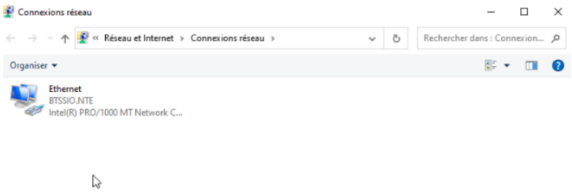
Cliquer sur **Réseau** et **Internet**.



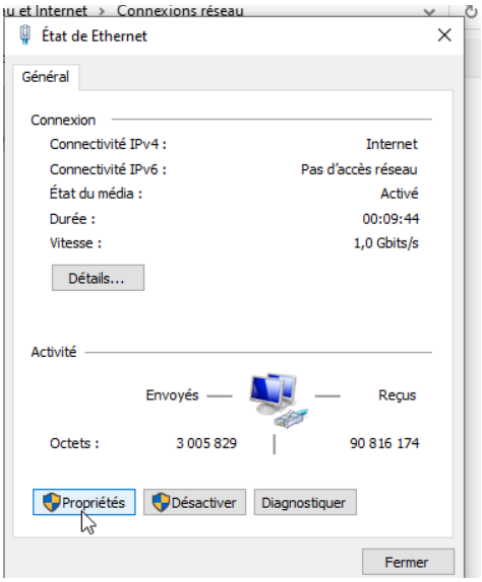
Cliquer sur **Centre Réseau et Partage**.



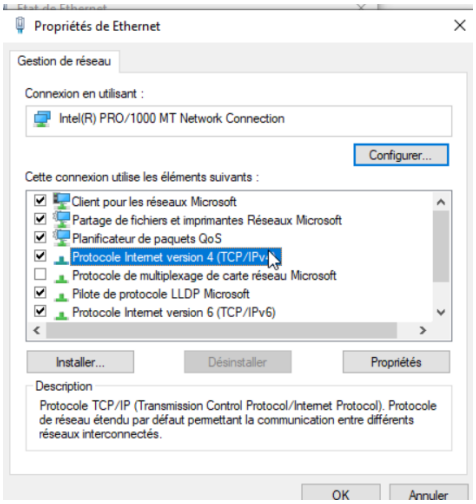
Cliquer en haut à gauche sur **Modifier les paramètres de la carte**.



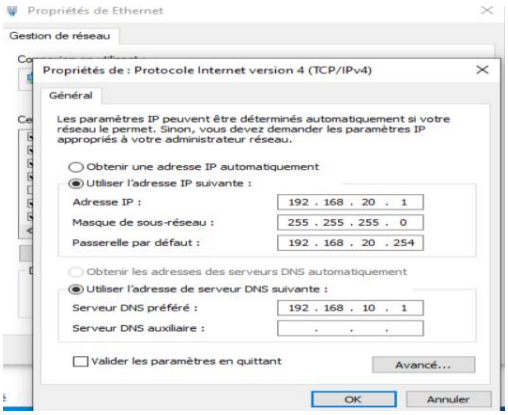
Faite clic droit sur la carte réseau.



Cliquer sur **Propriétés**.

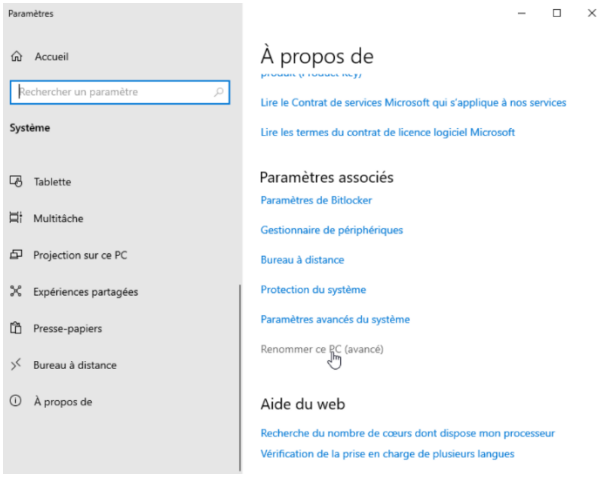


Cliquer sur **Protocole internet version 4**.

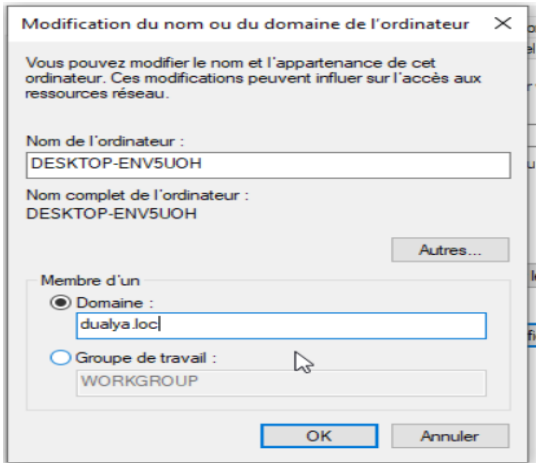


Vous pouvez laisser sur **Obtenir un adresse IP automatiquement** ou bien rentrer une **IP fixe**.

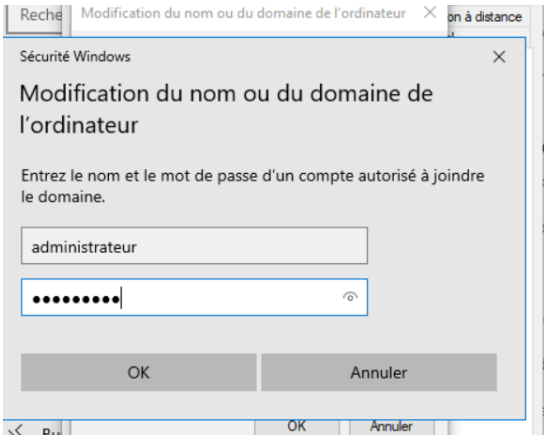
Il faut bien remplir le **DNS** qui est l'adresse **IP du serveur** ou il y a l'AD.



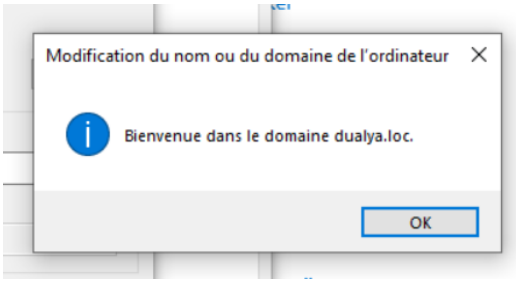
Retourner dans **Paramètres Systèmes** et **Paramètres associés** et **Renommer ce PC (avancé)**.



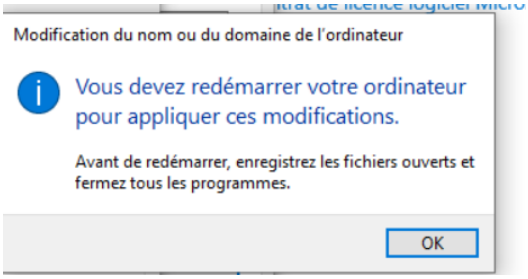
Dans Membre d'un domaine écrire **le non de vôtre domaine** pour nous sa sera **dualya.loc**.



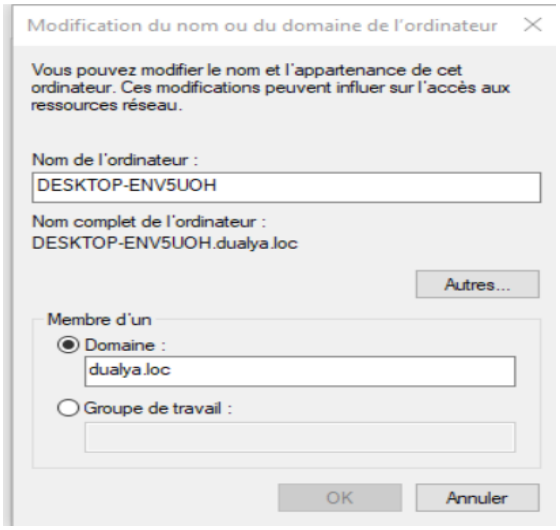
Entrer **Administrateur** et votre **MDP**.



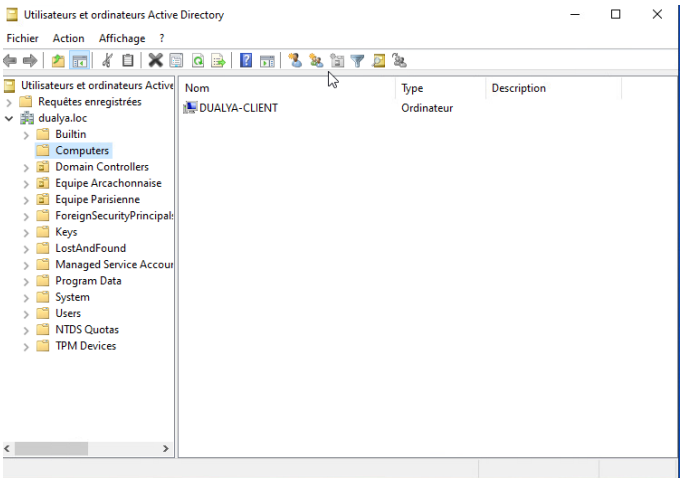
Votre PC Client est entré dans le domaine.



Votre PC client doit redémarrer pour appliquer les modifications.



Votre PC Client est bien rentré dans le domaine dualya.loc.



Retourner sur votre serveur cliquer sur **Outils** et **Utilisateurs et ordinateurs Active Directory**.

Ensuite sur **Computer** et vous verrez que vote **pc client** est bien dans **l'Active Directory**.

4.2 Création d’unités d’organisation

Qu’est-ce qu’une unité d’organisation (OU) dans l’Active Directory ?

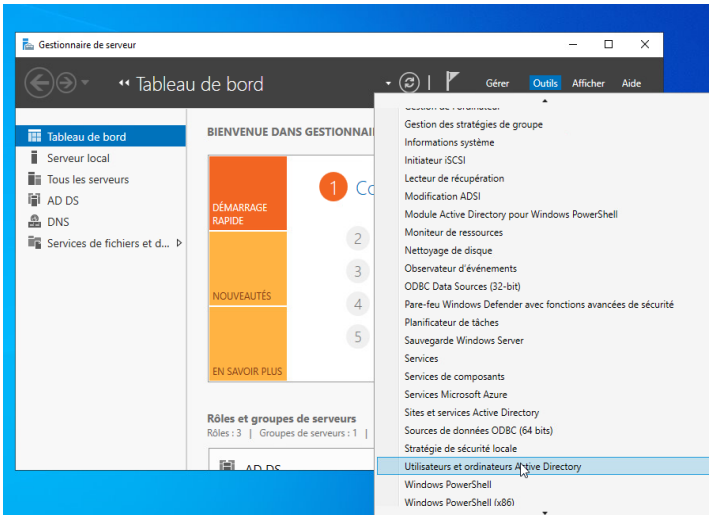
Une unité d'organisation (OU) dans Active Directory est un conteneur utilisé pour organiser et gérer les objets tels que les utilisateurs, les groupes et les ordinateurs au sein d'un domaine. Elle permet une gestion hiérarchique et structurée des ressources de l'entreprise.

Les principales caractéristiques des unités d'organisation incluent :

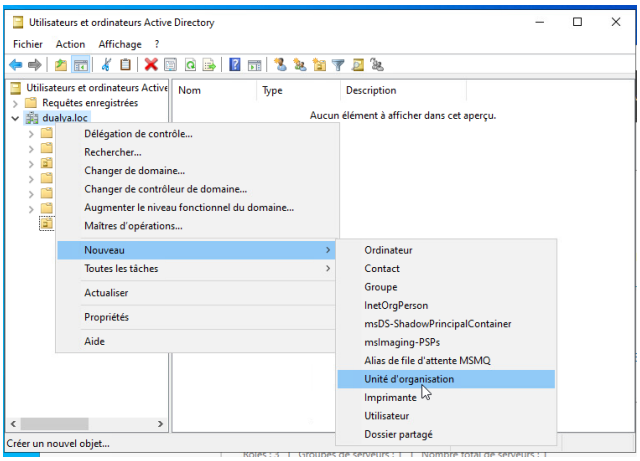
1. **Structure hiérarchique** : Les OUs peuvent contenir d'autres OUs, créant ainsi une structure arborescente qui reflète l'organisation de l'entreprise.
2. **Application des GPOs** : Vous pouvez appliquer des Group Policy Objects (GPOs) pour définir des paramètres et des politiques sur les objets dans l'OU.
3. **Délégation de l'administration** : Vous pouvez accorder des permissions spécifiques à des administrateurs pour gérer les objets dans une OU sans affecter l'ensemble du domaine.
4. **Simplification de la gestion** : Les OUs permettent de regrouper et de gérer des objets similaires, facilitant ainsi l'administration.

Les unités d'organisation sont essentielles pour une gestion efficace et sécurisée des ressources informatiques dans un environnement Active Directory.

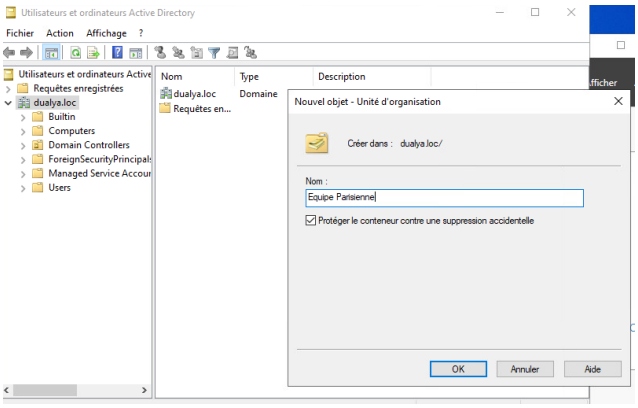
Nous allons voir comment créer des unités d’organisation :



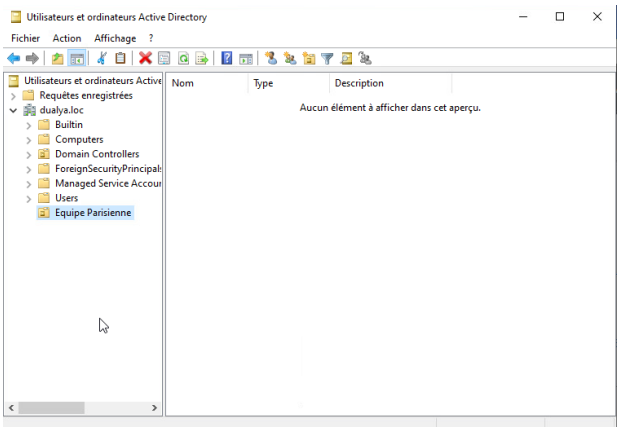
Cliquer sur **Outils** et **Utilisateurs et ordinateurs Active Directory**.



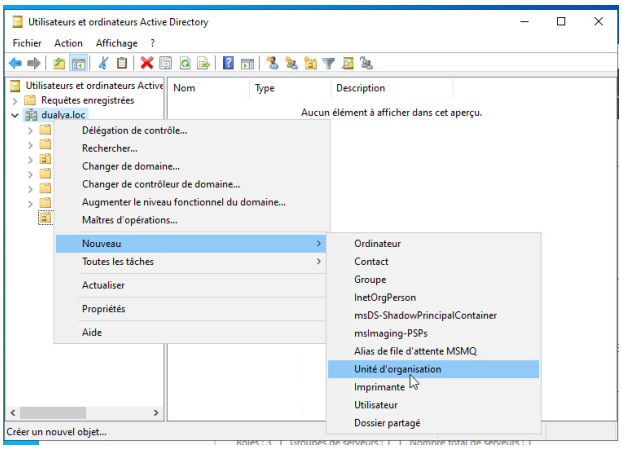
Faire clic droit sur **dualya.loc nouveau** et **Unité d'organisation**.



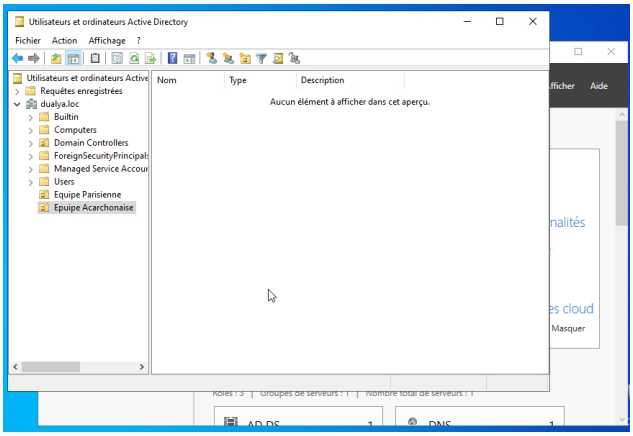
Nommer la première **unité d'organisation Equipe Parisienne** ou **(selon l'organisation de votre entreprise)**.



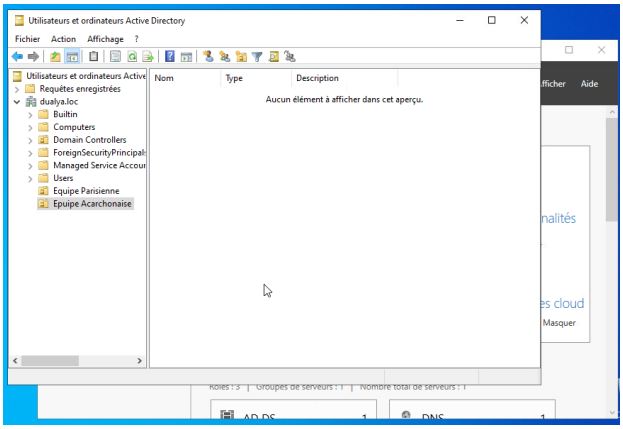
L'unité d'organisation **Equipe Parisienne** a été créer.



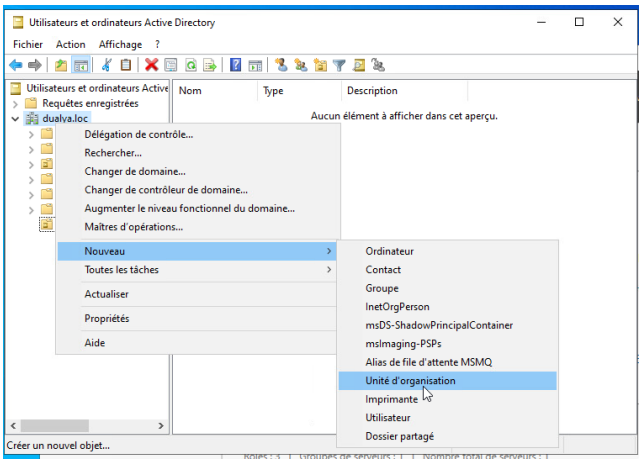
Faite de même pour L'équipe Arcachonnaise.



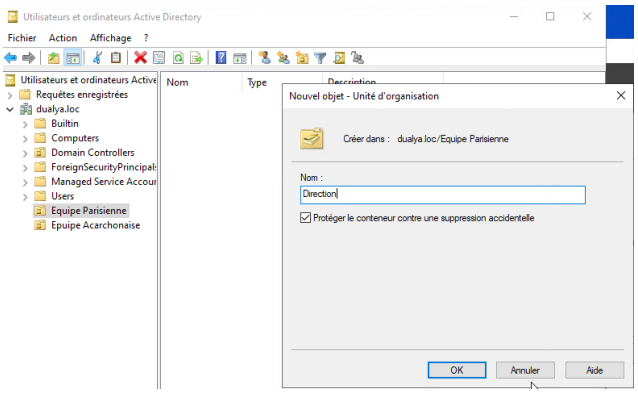
L'équipe Arcachonnaise a été créée.



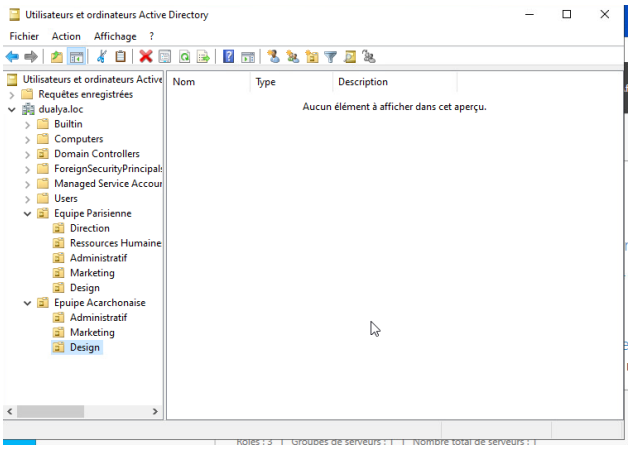
Les deux équipes ont été créés.



Faite clic droit sur **Equipe Parisienne nouveaux** et **unité d'organisation**.



Créer les différentes **unités d'organisation** de chaque **équipe**.



Toutes les **unités d'organisations** ont été créent.

Nous allons procéder à la créations de des utilisateurs.

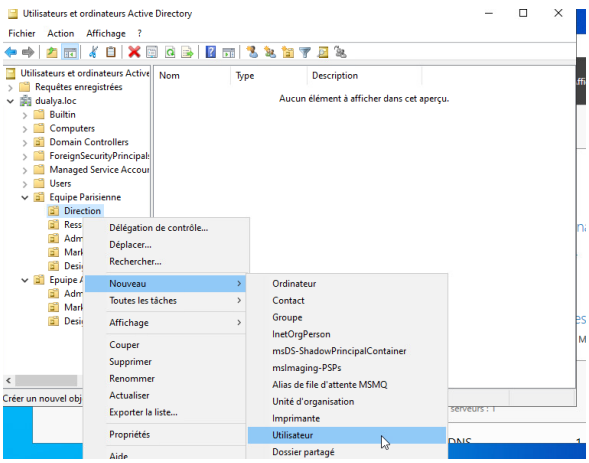
4.2.1 Créations des utilisateurs

Qu’est-ce que la création des utilisateurs dans l’AD ?

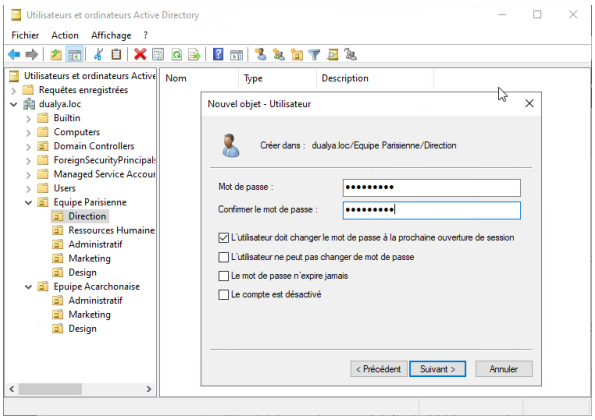
La création des utilisateurs dans Active Directory (AD) fait référence au processus de l'ajout de nouveaux comptes utilisateurs à un environnement réseau administré par Active Directory. Active Directory est un service d'annuaire développé par Microsoft pour la gestion des ressources réseau telles que les utilisateurs, les ordinateurs et les groupes.

Voici comment fonctionne la création des utilisateurs dans AD :

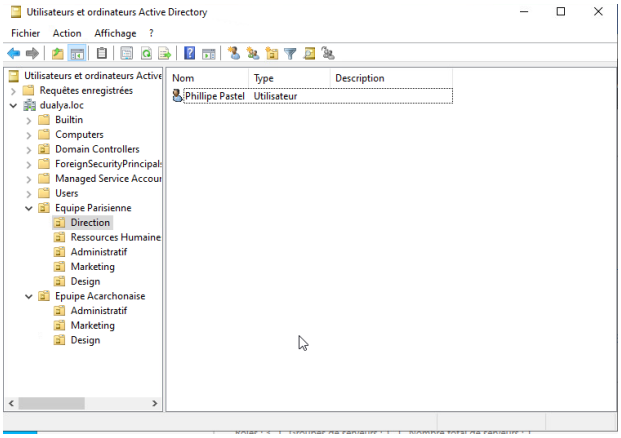
1. **Définir les informations de l’utilisateur :** Vous devez fournir des informations de base sur l'utilisateur, comme le nom d'utilisateur, le prénom, le nom de famille, l'adresse e-mail, et d'autres détails pertinents.
2. **Attribuer des autorisations et des groupes** : Vous pouvez assigner l'utilisateur à des groupes spécifiques qui détermineront ses permissions et accès au sein du réseau. Par exemple, un utilisateur peut être ajouté au groupe "Utilisateurs du domaine", "Administrateurs", etc.
3. **Configurer les paramètres de sécurité** : Définir les politiques de mot de passe, les droits d'accès, et autres paramètres de sécurité pour garantir que l'utilisateur puisse se connecter en toute sécurité.
4. **Finaliser la création de l’utilisateur :** Une fois toutes les informations et les paramètres configurés, l'utilisateur est ajouté à l'annuaire Active Directory, et peut alors se connecter au réseau et accéder aux ressources selon les autorisations qui lui ont été accordées.



Faire clic droit sur ou **Direction**, **Nouveau** et **Utilisateur**.



Choisir un premier mot de passe qui seras à changer lors de la première connexion du nouveau profil et faire **suivant**.



L'utilisateur a été créer faite de même pour la composition de votre équipe.

Nous pouvons également créer les utilisateurs dans Active Directory en automatisant le processus à l'aide d'un script PowerShell. Ce qui permet d'automatiser la gestion des comptes utilisateurs, de gagner du temps et de minimiser les erreurs manuelles. Cela assure également une cohérence et une efficacité accrues, particulièrement utile dans des environnements nécessitant la création ou la modification de nombreux comptes.

Voici le script PowerShell :

```
# Définir le mot de passe
# On utilise ConvertTo-SecureString pour convertir une chaîne de texte en un SecureString.
# Ici, "MDPuser44" est le mot de passe en clair que l'on souhaite affecter à chaque utilisateur.
$password = ConvertTo-SecureString "MDPuser44" -AsPlainText -Force


# Liste des utilisateurs à créer
# Un tableau est utilisé pour stocker les informations de chaque utilisateur à créer.
# Chaque élément du tableau est un hashtable contenant les clés "Username", "FullName" et "Department".
$users = @(
    # Agence parisienne
    @{ Username = "philippe.pastel"; FullName = "Philippe Pastel"; Department = "Direction" }
    @{ Username = "pierre.parry"; FullName = "Pierre Parry"; Department = "Ressources Humaines" }
    @{ Username = "ulysse.alain"; FullName = "Ulysse Alain"; Department = "Administratif" }
    @{ Username = "baptiste.ludwig"; FullName = "Baptiste Ludwig"; Department = "Administratif" }
    @{ Username = "jade.caillaux"; FullName = "Jade Caillaux"; Department = "Marketing" }
    @{ Username = "sophie.ratier"; FullName = "Sophie Ratier"; Department = "Marketing" }
    @{ Username = "remy.loiseau"; FullName = "Rémy Loiseau"; Department = "Design" }
    @{ Username = "pierre.sabord"; FullName = "Pierre Sabord"; Department = "Design" }
    @{ Username = "sacha.lens"; FullName = "Sacha Lens"; Department = "Design" }
    @{ Username = "jeanne.reil"; FullName = "Jeanne Reil"; Department = "Design" }

    # Agence arcachonnaise
    @{ Username = "serge.lay"; FullName = "Serge Lay"; Department = "Administratif" }
    @{ Username = "sybille.gautier"; FullName = "Sybille Gautier"; Department = "Marketing" }
    @{ Username = "helene.varon"; FullName = "Hélène Varon"; Department = "Marketing" }
    @{ Username = "pauline.provost"; FullName = "Pauline Provost"; Department = "Design" }
    @{ Username = "cecilia.claire"; FullName = "Cécilia Claire"; Department = "Design" }
    @{ Username = "yann.bertrand"; FullName = "Yann Bertrand"; Department = "Design" }
)
```

```
# Création des utilisateurs
# La boucle foreach parcourt chaque utilisateur dans le tableau $users.
foreach ($user in $users) {
    # Extraction des informations de l'utilisateur depuis le hashtable courant
    $username = $user.Username
    $fullname = $user.FullName
    $department = $user.Department

    # Définir l'OU (Organizational Unit) en fonction du département de l'utilisateur
    # Cette chaîne sera utilisée pour définir l'emplacement de l'utilisateur dans Active Directory.
    $ouPath = "OU=$department,DC=dualya,DC=fr"

    # Créer l'utilisateur dans Active Directory
    New-ADUser -Name $fullname `                          # Nom complet de l'utilisateur
               -GivenName $fullname.Split(" ")[0] `       # Prénom
               -Surname $fullname.Split(" ")[1] `         # Nom de famille
               -SamAccountName $username `                # Nom d'utilisateur pour se connecter
               -UserPrincipalName "$username@dualya.fr" ` # Nom principal de l'utilisateur
               -Path $ouPath `                            # Chemin de l'OU où l'utilisateur sera créé
               -AccountPassword $password `               # Mot de passe de l'utilisateur
               -ChangePasswordAtLogon $true               # L'utilisateur doit changer son MDP lors de la première connexion
               -Enabled $true                             # Activer le compte immédiatement

    # Afficher un message de confirmation après la création de l'utilisateur
    Write-Host "Utilisateur $username créé avec succès dans $ouPath."
}

# Commande pour installer les outils nécessaires à la gestion d'Active Directory
# Si ce n'est pas déjà fait, RSAT-AD-PowerShell doit être installé pour pouvoir utiliser les cmdlets AD.
Install-WindowsFeature RSAT-AD-PowerShell

# Importer le module Active Directory pour accéder aux cmdlets comme New-ADUser
Import-Module ActiveDirectory
```


4.2.2 Connection d’un utilisateur au domaine

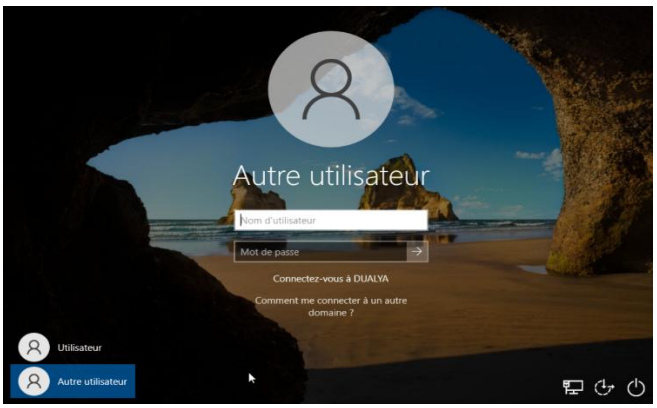
Qu’est-ce que la connexion d’un utilisateur au domaine ?

La connexion d’un utilisateur à un domaine dans un environnement Active Directory (AD) signifie que l’utilisateur se connecte à un réseau administré où les ressources et les accès sont contrôlés de manière centralisée. Voici comment cela fonctionne :

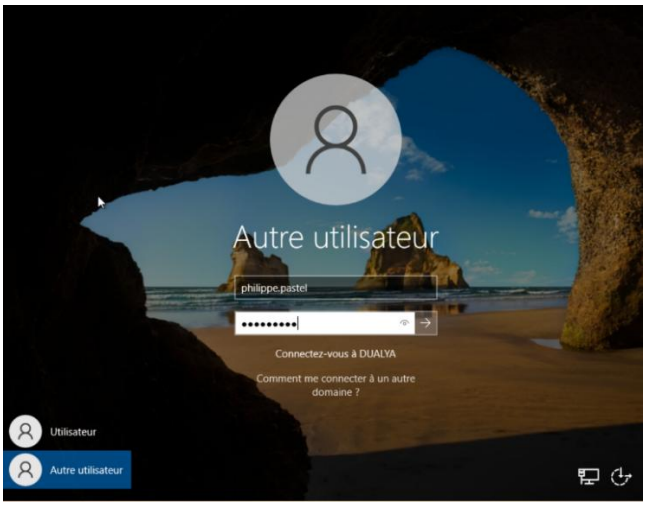
1. **Authentification de l’utilisateur :** L'utilisateur entre son nom d'utilisateur et son mot de passe sur son ordinateur ou autre dispositif de connexion.
2. **Vérification des informations** : L'ordinateur de l'utilisateur envoie ces informations au contrôleur de domaine Active Directory pour vérification. Le contrôleur de domaine compare les informations d'identification avec celles stockées dans la base de données Active Directory.
3. **Création de la session** : Si les informations d'identification sont correctes, le contrôleur de domaine accorde l'accès, et l'utilisateur est authentifié. Cela permet de créer une session utilisateur sur le réseau.
4. **Attribution des ressources** : Une fois connecté, l'utilisateur a accès aux ressources du domaine selon les permissions qui lui ont été attribuées, comme les fichiers partagés, les imprimantes réseau, et les applications d'entreprise.
5. **Application des politiques de groupe** : Les politiques de groupe configurées dans Active Directory sont appliquées à l'utilisateur. Cela peut inclure des restrictions d'accès, des configurations logicielles, et d'autres paramètres de sécurité.

C'est un processus sécurisé et centralisé qui permet aux administrateurs de gérer les utilisateurs et les ressources efficacement au sein d'un réseau d'entreprise.

Voici les étapes pour connecter les utilisateurs au domaine tout se passe depuis le pc Windows client intégrer au domaine :

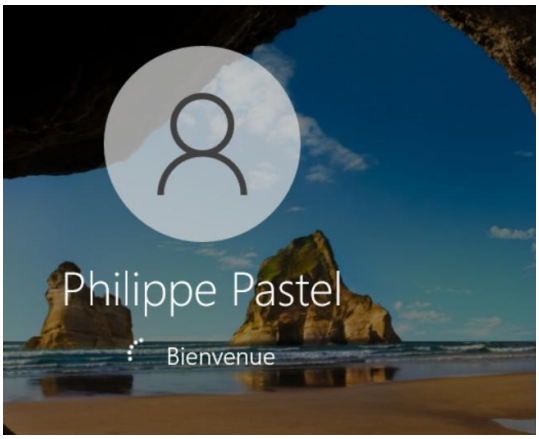


Faire autre utilisateur.



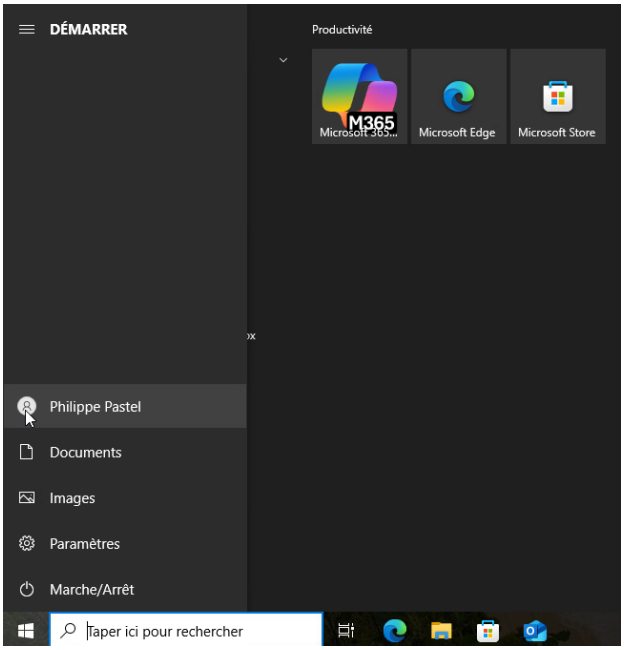
Utiliser un profil que vous avez créé auparavant avec la composition de votre entreprise. Dans notre cas nous allons utiliser l'utilisateur Philippe Pasteur qui est le directeur de l'entreprise Dualya.

Il va vous demander le password crée avec l'utilisateur et redéfinir un nouveau mot de passe pour vous connecter à la nouvelle session.



Le nouvel utilisateur c’est connecter au domaine avec le pc Windows client.

Faite de même avec tous les utilisateurs de votre entreprise.



L’utilisateur Philippe Pastel c’est connecter.

4.2.3 Création de profil itinérant

Qu’est-ce qu’un profil itinérant ?

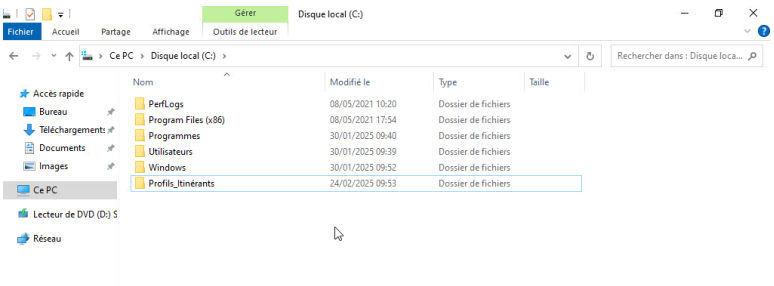
Un **profil itinérant** dans Active Directory (AD) est un profil utilisateur qui est stocké sur un serveur central plutôt que sur l'ordinateur local de l'utilisateur. Cela permet aux utilisateurs de se connecter à différents ordinateurs au sein du même réseau tout en conservant leurs paramètres, documents, et autres données personnelles.

Voici comment cela fonctionne :

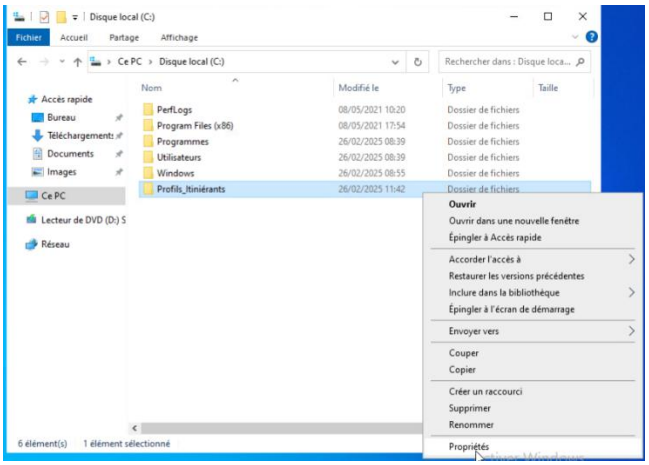
1. **Stockage centralisé** : Les profils itinérants sont stockés sur un serveur de fichiers centralisé. Cela signifie que les données de l'utilisateur sont accessibles depuis n'importe quel ordinateur du réseau.
2. **Mobilité accrue** : Les utilisateurs peuvent changer d'ordinateur sans perdre leurs données personnelles. Par exemple, si un utilisateur se connecte à un autre poste de travail, son environnement (bureau, paramètres, documents) sera le même.
3. **Sécurité des données** : Les données sont centralisées et régulièrement sauvegardées sur le serveur, réduisant ainsi le risque de perte de données en cas de panne de l'ordinateur.
4. **Gestion simplifiée** : Les administrateurs peuvent gérer et mettre à jour les profils plus facilement depuis un emplacement centralisé.

Les profils itinérants sont particulièrement utiles dans les environnements où les utilisateurs changent fréquemment d'ordinateurs, comme dans les bureaux ou les écoles.

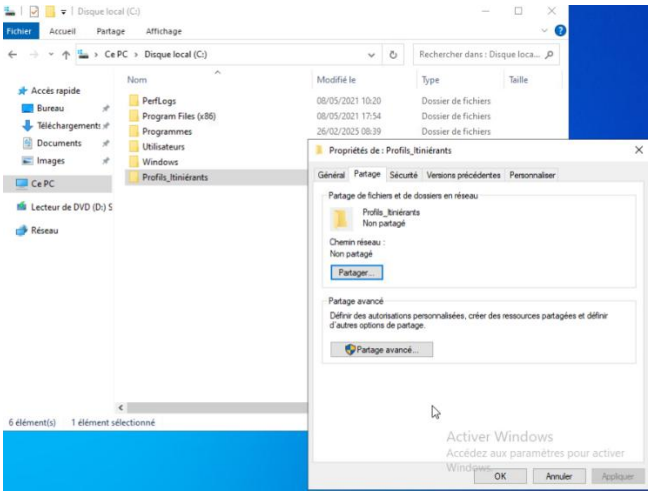
Voici la procédure à suivre :



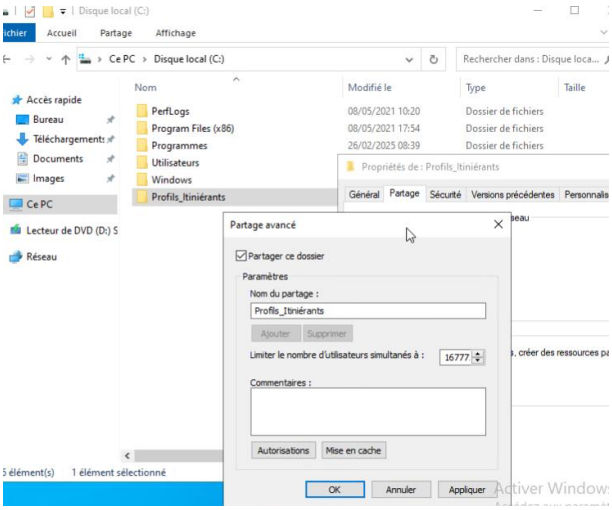
Créer un répertoire à la racine **c :** sur le SRV on l’appellera Profils_Itiniérants.



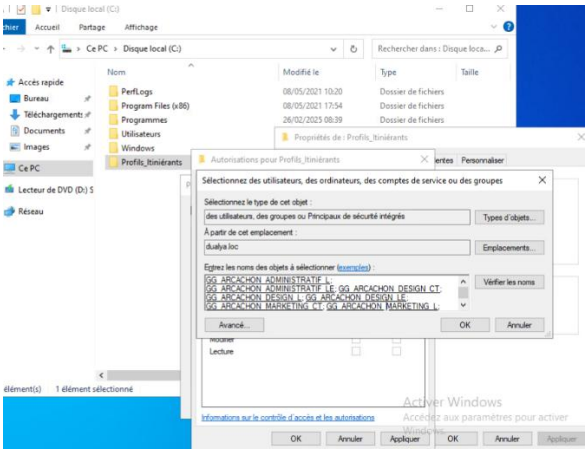
Faite clic droit sur **Propriété**.



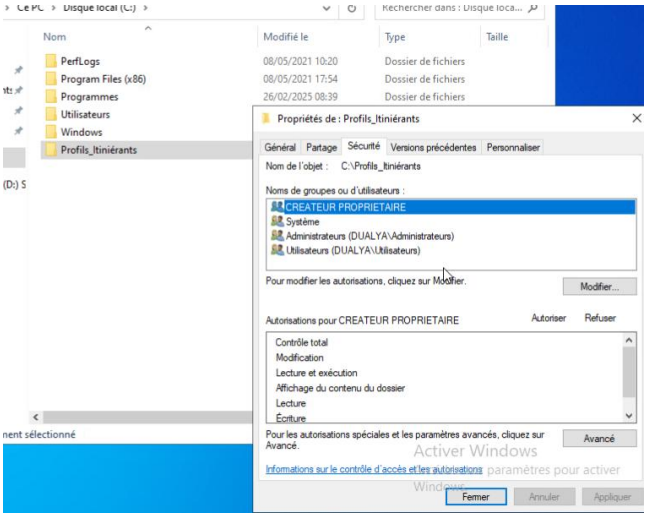
Faite **Partage avancé.**



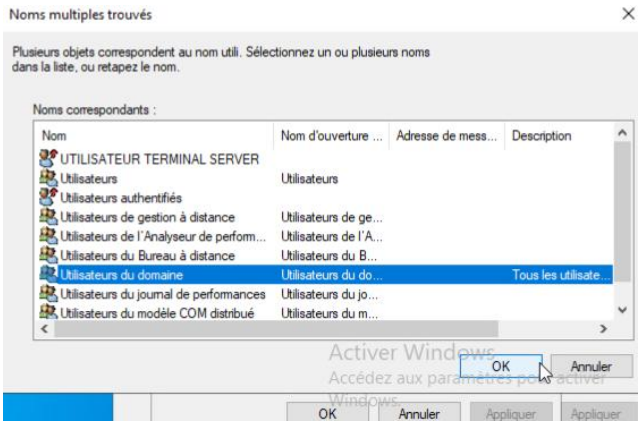
Cliquer sur **Partager ce dossier**.



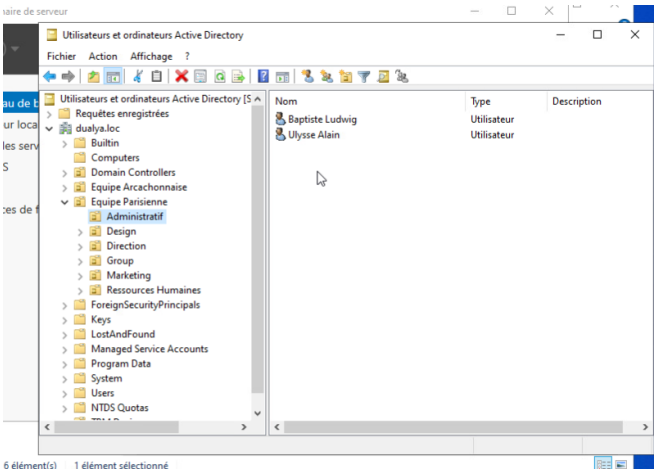
Sélectionner les utilisateurs ou les groupes.



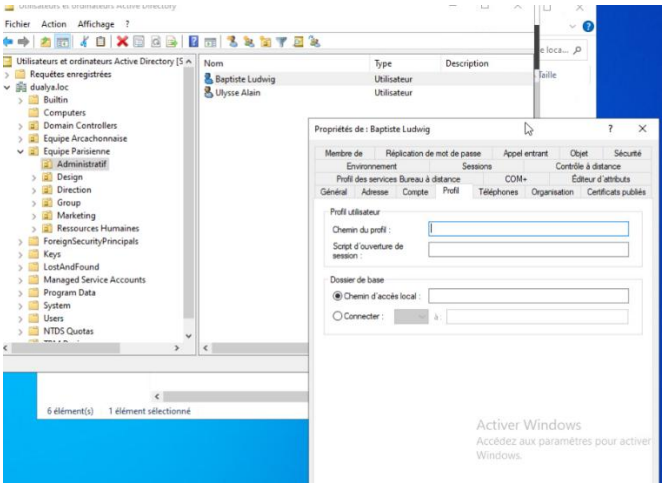
Aller sur l'onglet **Sécurité**.



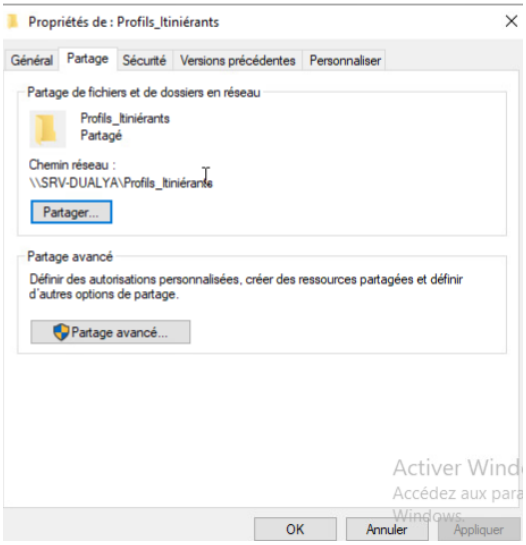
Sélectionner les **Utilisateurs du domaine**.



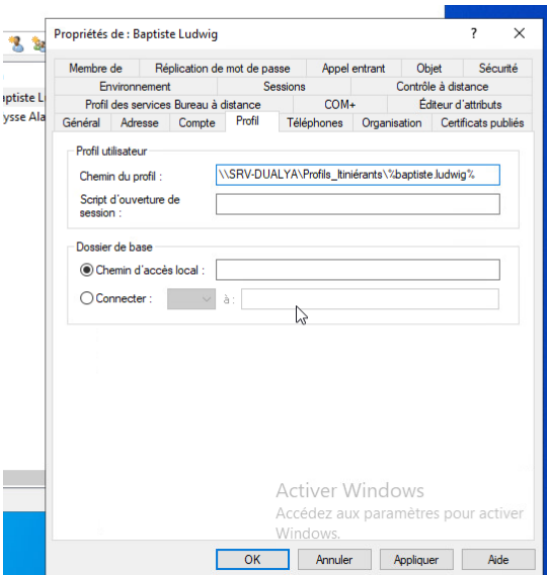
Sélectionner un Utilisateur du domaine.



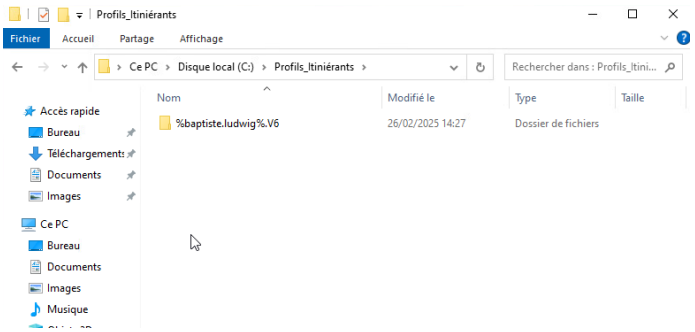
Faite clic droit sur **Baptistes Ludwig** ou selon votre organisation et cliquer sur l'onglet **Profil**.



Récupérer le chemin d'accès qui est **\\SRV-DUALYA\Profils_Itinérants**.



Copier le chemin du profil **\\SRV-DUALYA\Profils_Itinérants\%baptiste.ludwig%**



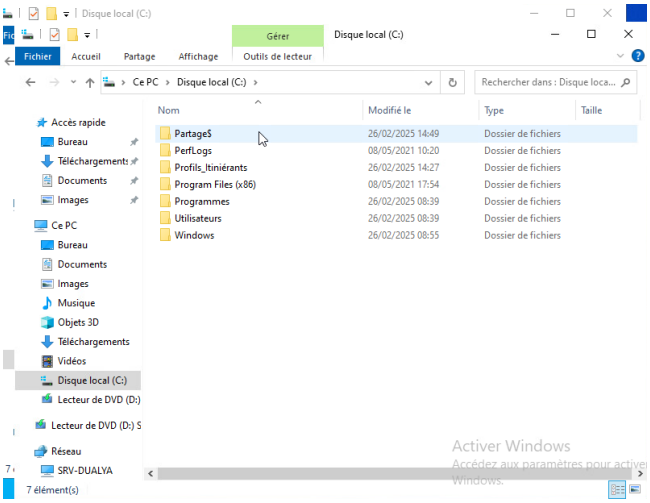
Le profil itinérant de Baptiste Ludwig il va pouvoir ce connecté à un pc Win client avec son compte et récupéré tous ses documents.
Il va pouvoir aussi se connecter à un autre pc qui seras également dans le même domaine et récupérer sa session.

4.3 Création de GPO lecteur de mappage

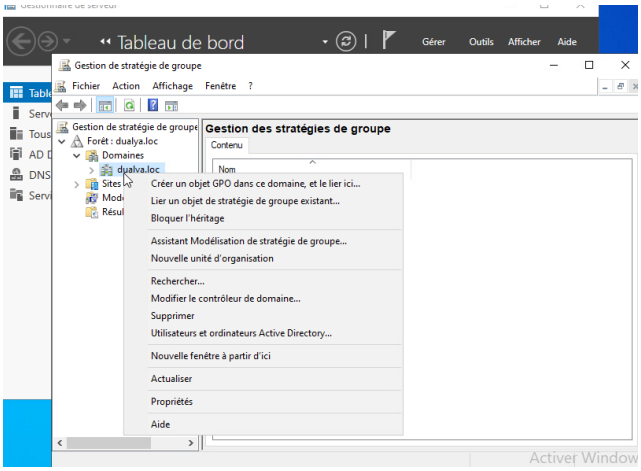
Qu'est-ce que la création d'une GPO lecteur de mappage ?

La création d'une GPO (Group Policy Object) pour le mappage de lecteurs réseau permet aux administrateurs de configurer et de gérer les connexions aux lecteurs réseau de manière centralisée.

Voici les étapes pour réaliser la GPO de mappage de lecteur réseau.

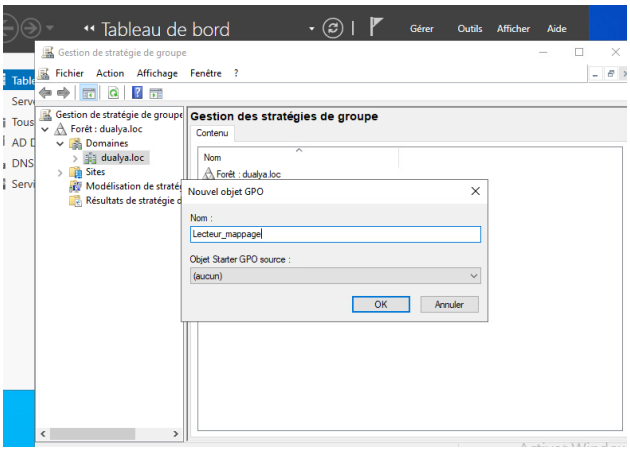


Sur la machine SRV-Dualya créer un dossier **Partage$** a la racine **C :** et faite le partage.

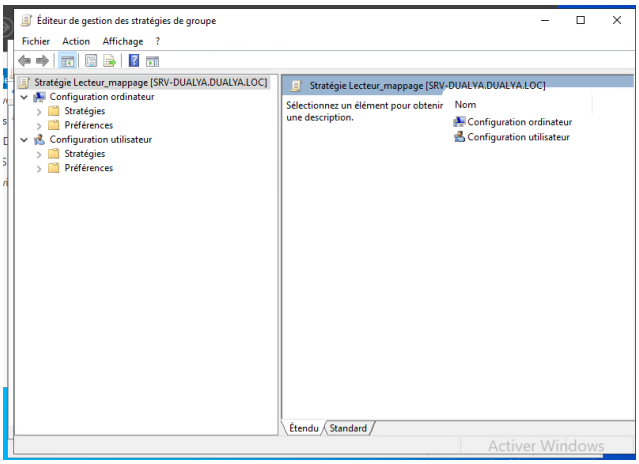


Aller dans **Outils** puis **Gestion de stratégie de groupe.**

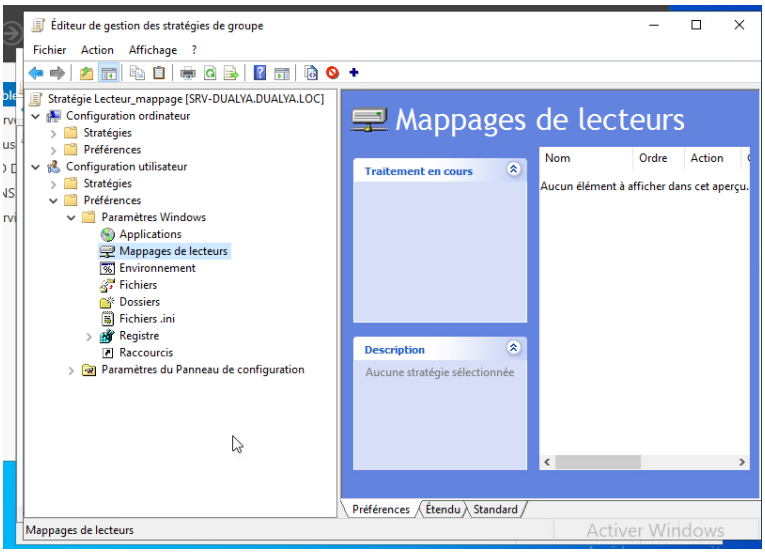
Faite clic droit sur **Créer un objet GPO dans ce domaine.**



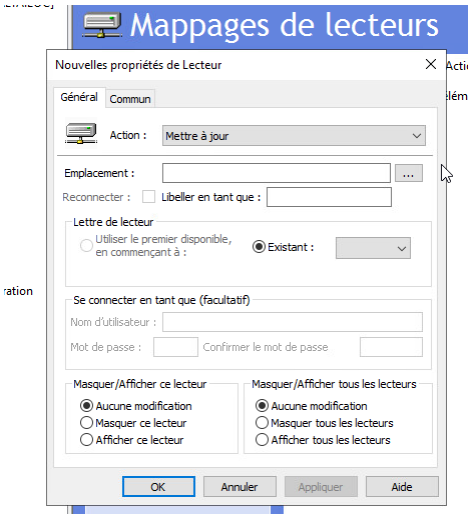
Nommer la GPO **Lecteur_mappage** et faite **OK.**



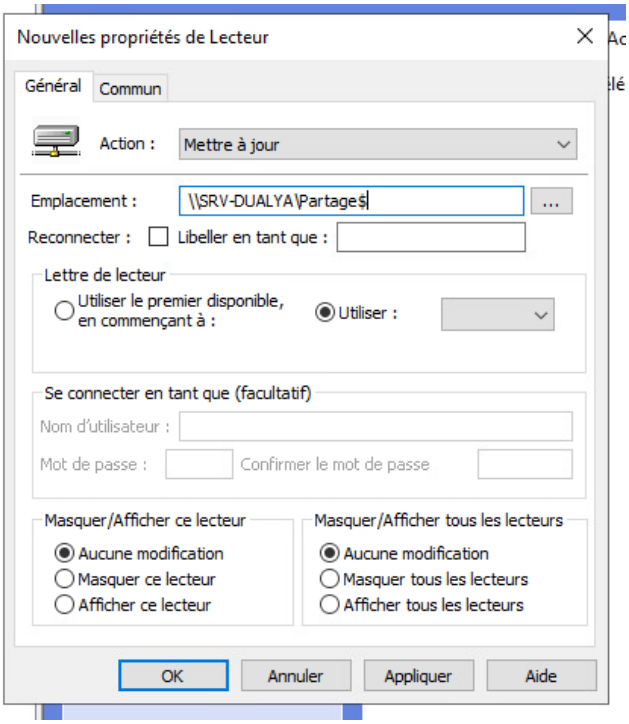
Aller sur **Configuration utilisateur** et **Préférences, Paramètres Windows et Mappages de lecteurs.**



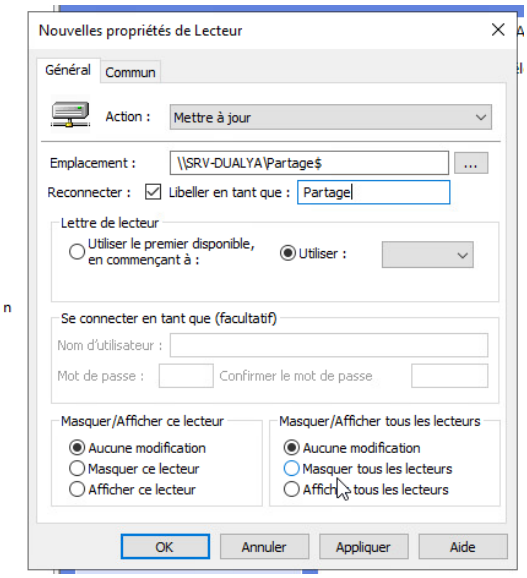
Faire clic droit sur **Mappages de lecteurs.**



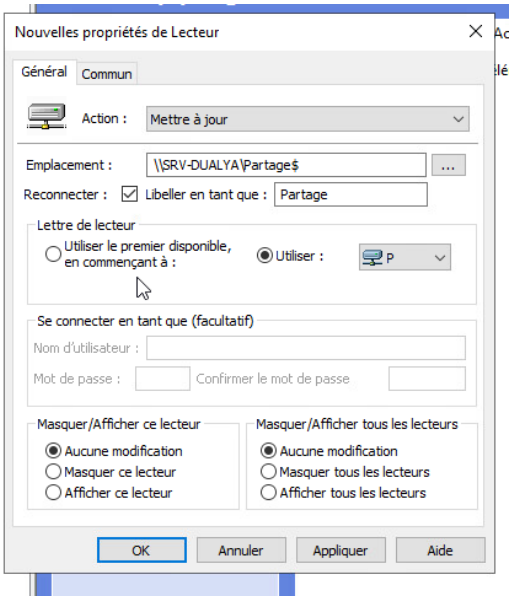
Action laisser **sur mettre à jour**.



Renseigner le chemin d'accès au partage **\\SRV-DUALYA\Partage$**.



Reconnecter le lecteur de mappage et le nommer **Partage**.

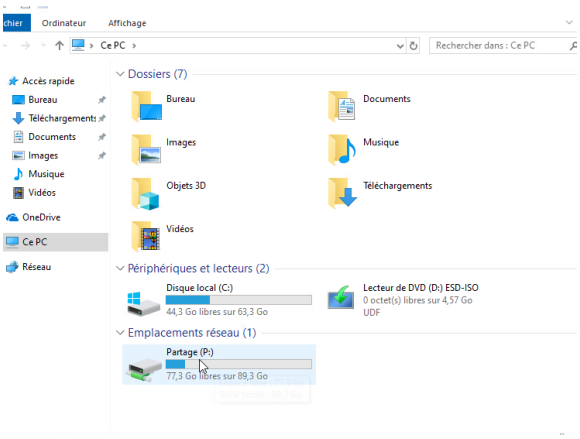


Choisir une **lettre de lecteur** nous utiliserons **le lecteur P** pour partage.

Teste nous allons nous connecter avec un utilisateur du domaine pour si le lecteur de mappage est bien remonté.

Pour ce faire nous utiliserons l'utilisateur Baptiste Ludwig ou un autre.

Nous allons nous connecter à la session de Baptiste Ludwig qui fait partie du domaine **dualya.loc.**



La GPO de lecteur de Mappage à bien remonté sur la session de Baptiste Ludwig.

4.4 Faire une réplication de l’AD

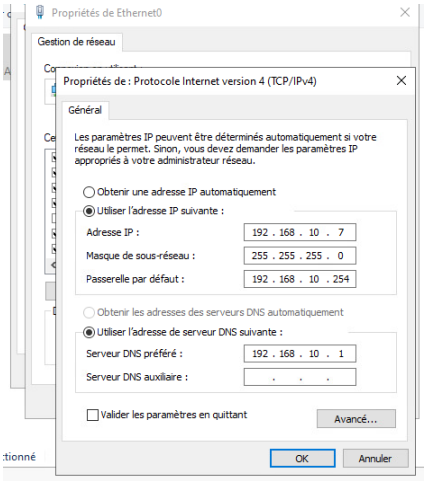
Qu’est-ce que la réplication de l’AD ?

La réplication de l'Active Directory Domain Services (AD DS) est un processus essentiel pour maintenir la cohérence et la mise à jour des informations à travers les différents contrôleurs de domaine dans un environnement Active Directory. Voici un aperçu de ce processus :

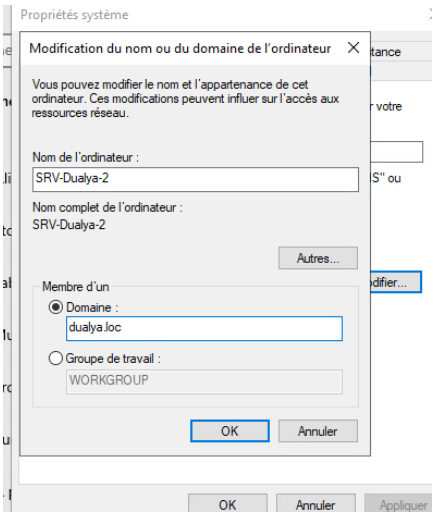
1. **Objet de connexion** : Un objet de connexion est créé pour représenter une connexion de réplication entre un contrôleur de domaine source et un contrôleur de domaine de destination. Ces objets de connexion sont stockés sous l'objet Paramètres NTDS sur le serveur de destination.
2. **Vérificateur de cohérence des données (KCC)** : Le KCC est un processus intégré qui s'exécute sur tous les contrôleurs de domaine et génère la topologie de réplication pour la forêt Active Directory. Il crée des topologies de réplication distinctes selon que la réplication se produit au sein d'un site (intrasite) ou entre des sites (intersites).
3. **Types de réplication** :
    - **Réplication intrasite** : Se produit au sein d'un même site Active Directory et est généralement rapide en raison de la proximité des contrôleurs de domaine.
    - **Réplication intersites** : Se produit entre différents sites Active Directory et peut nécessiter une configuration supplémentaire pour gérer la planification et les coûts de bande passante.
4. **Informations répliquées** : La réplication Active Directory assure que les données telles que les utilisateurs, les ordinateurs, les stratégies de groupe et les enregistrements DNS sont synchronisées entre les contrôleurs de domaine.

Ce processus garantit que chaque contrôleur de domaine dispose des mêmes données à jour, assurant ainsi la cohérence et la fiabilité de l'annuaire Active Directory.

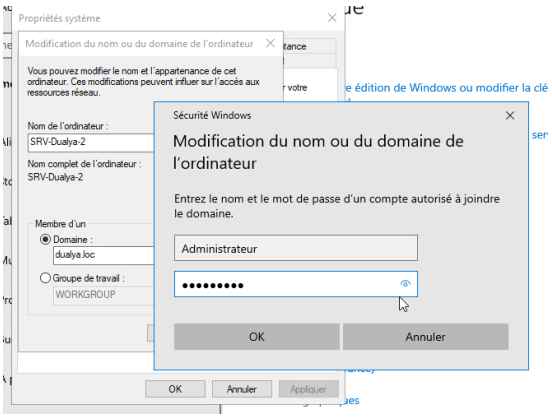
Voici la procédure de réalisation.



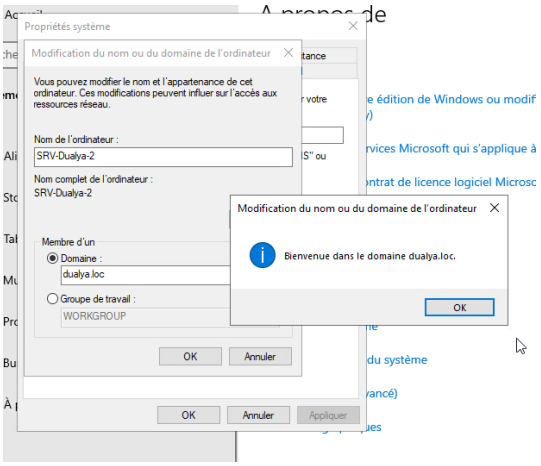
Tout d'abord il faut paramétrer l'IP du second SRV en IP Fixe en **192.168.10.7** et le mettre le **DNS** du premier **SRV** qui **192.168.10.1**. (Selon votre réseau d'entreprise).



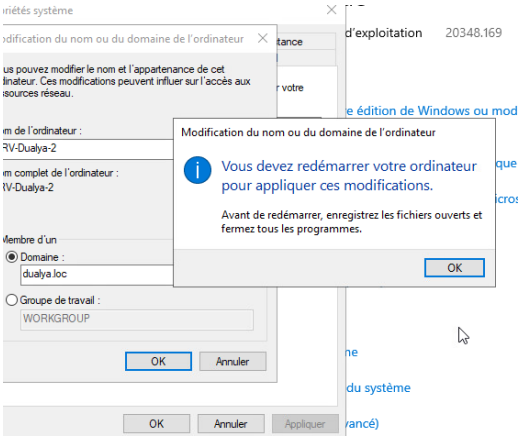
Renommer le SRV en **SRV-Dualya-2**, le rajouter au domaine existant **dualya.loc.**



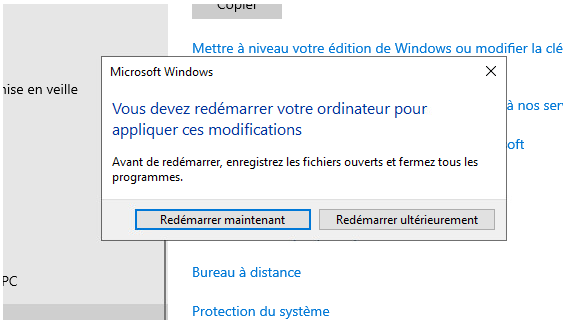
Entrer le MDP de l'administrateur.



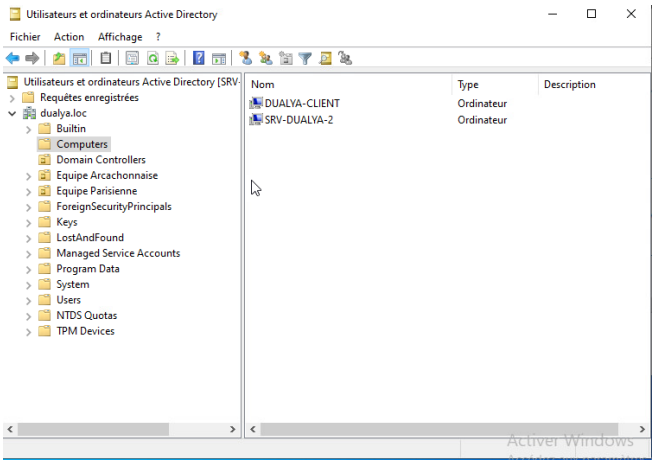
Le SRV 2 a été rajouter au domaine.



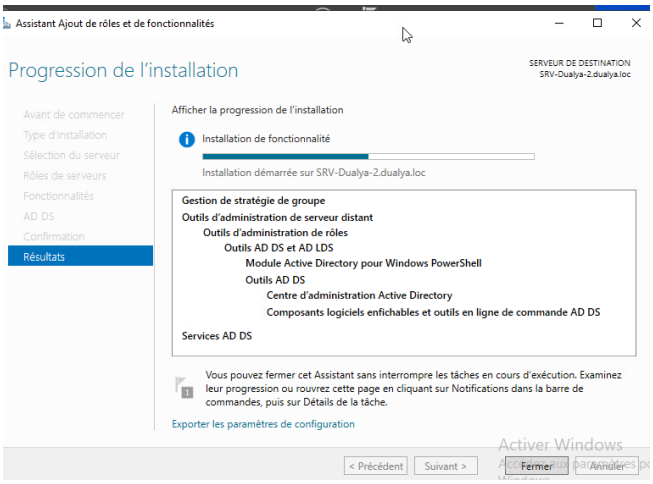
Le SRV 2 va redémarrer.



Faire **redémarrer maintenant**.

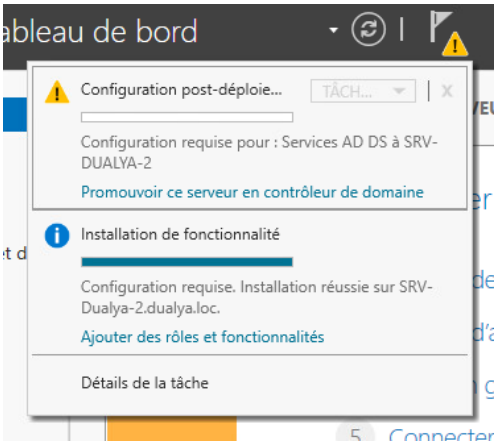


Le SRV 2 a bien été rajouter au domaine.

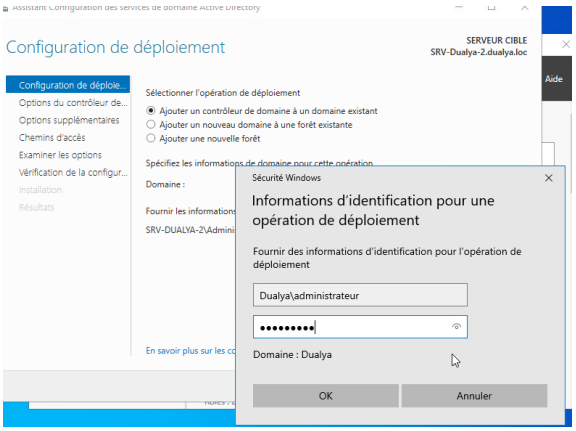


La prochaine étape consiste à installer le rôle **AD-DS**.

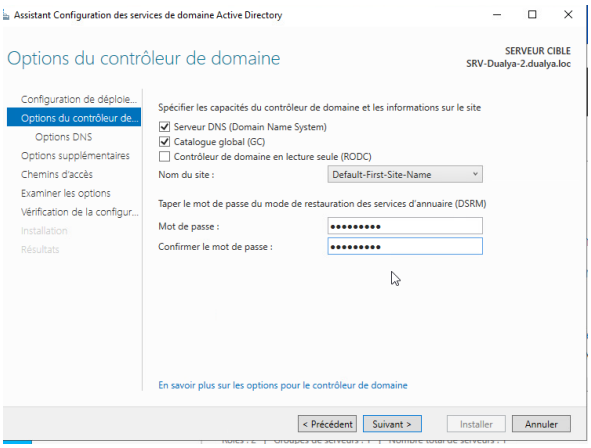
C'est le même principe d'installation que le **SRV 1.**



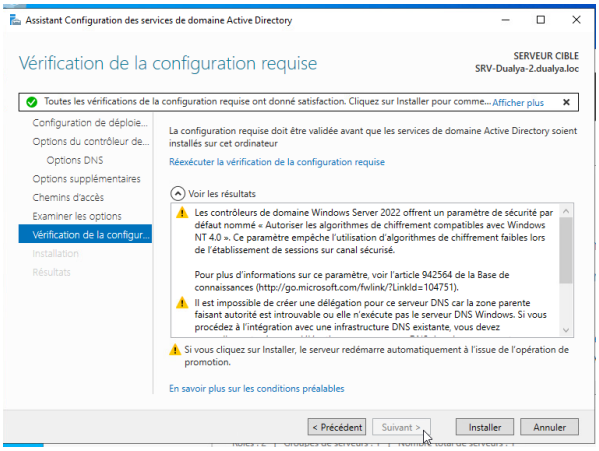
Cliquer sur **Promouvoir ce serveur en contrôleur de domaine.**



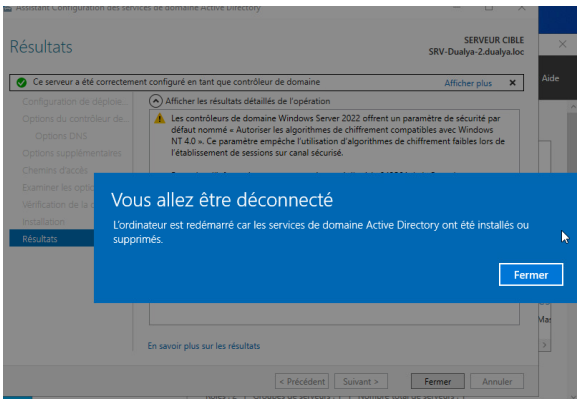
Faite **Ajouter un contrôleur de domaine à un domaine existant**.



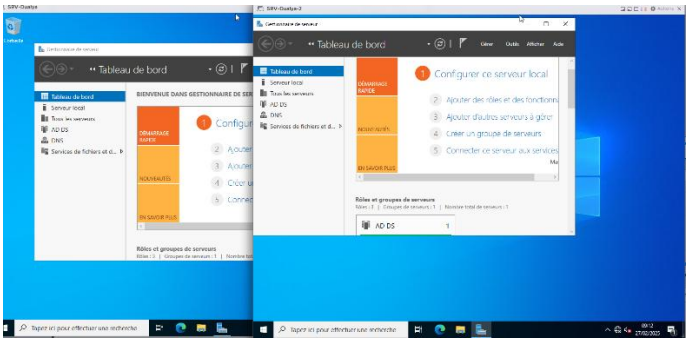
Entrer un MDP ou le même et faire suivant.



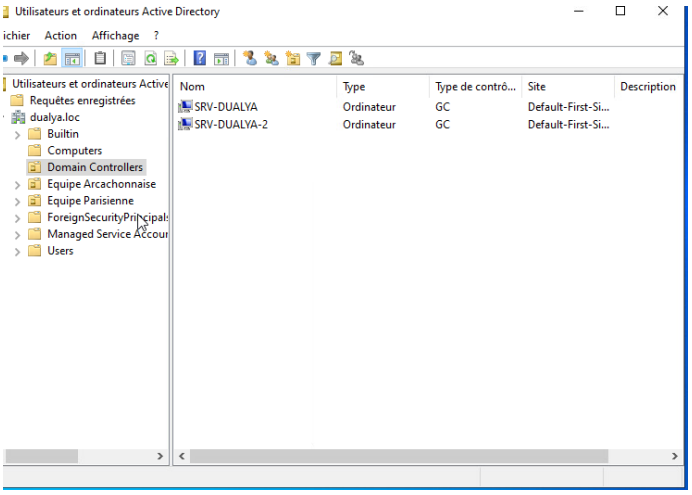
Cliquer sur **Installer**.



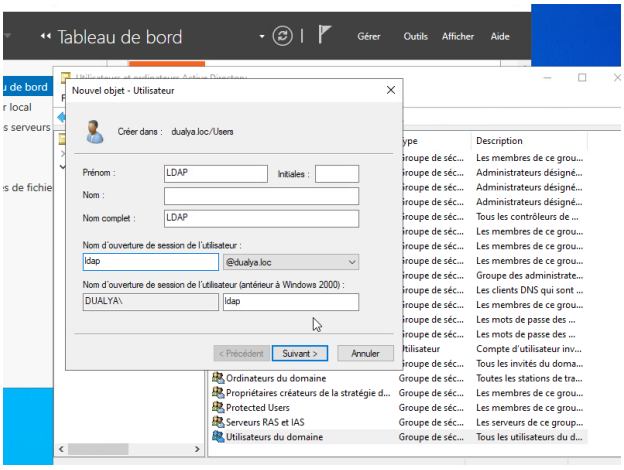
Vous allez être déconnecté.



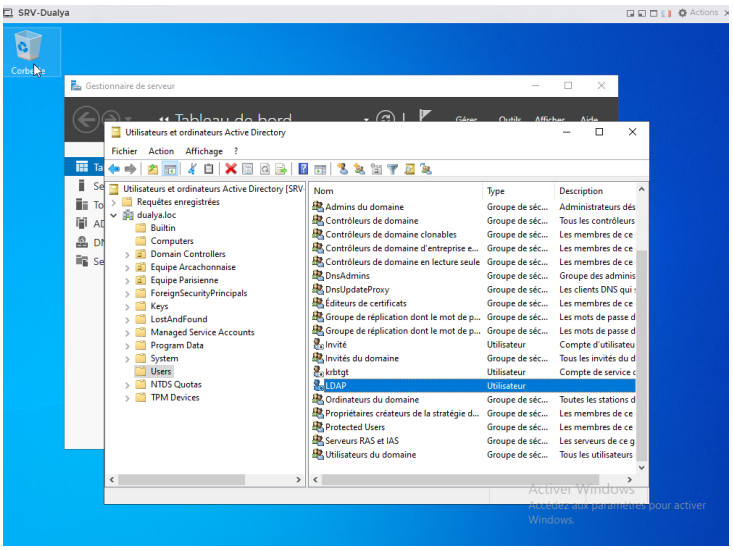
On peut constater que la réplication à bien été pris en compte.



On peut constater que les deux contrôleurs de domaine ont bien été créé.



Nous avons fait un teste en créent un utilisateur LDAP a partie du second serveur et voir s'il a été répliquer le sur premier serveur.



Nous pouvons voir que sur le premier serveur l'utilisateur LDAP a bien été répliquer.

La réplication de L'AD est fonctionnelle.

Conclusion

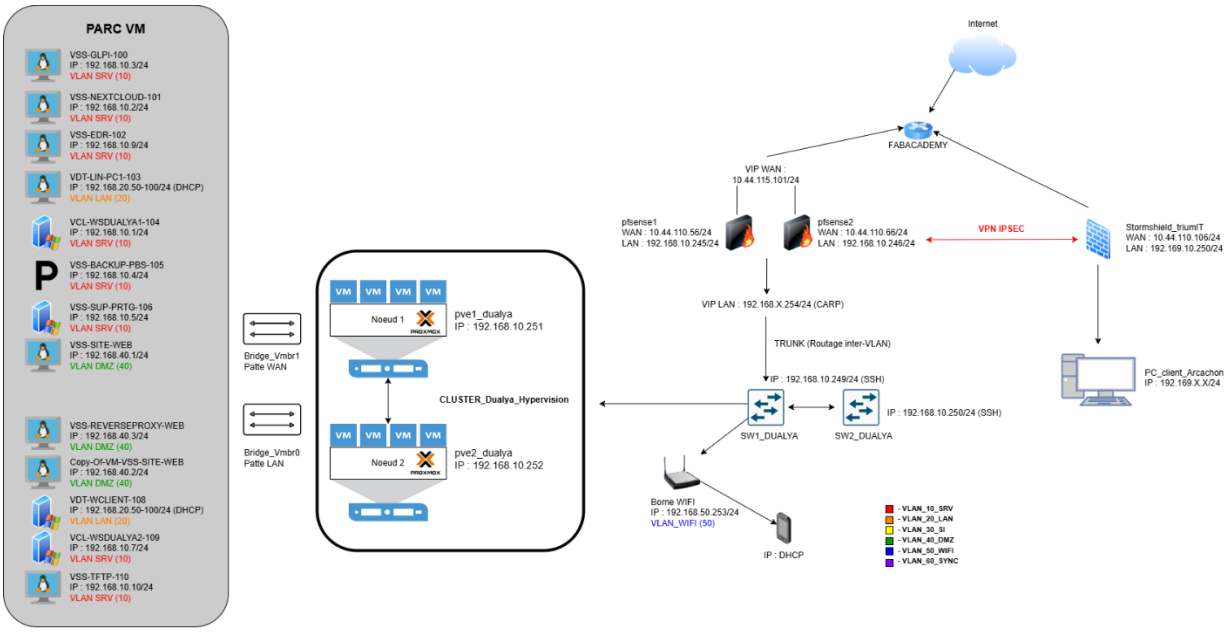
En suivant ce guide détaillé, vous avez désormais les connaissances nécessaires pour installer et configurer Windows Server 2022 et ses fonctionnalités avancées. Grâce à l'ajout des rôles AD-DS, DHCP et DNS, la gestion des unités d'organisation, la création de profils itinérants et la mise en place de GPO pour le mappage de lecteurs, vous êtes bien équipé pour assurer une gestion efficace et sécurisée de votre infrastructure réseau.

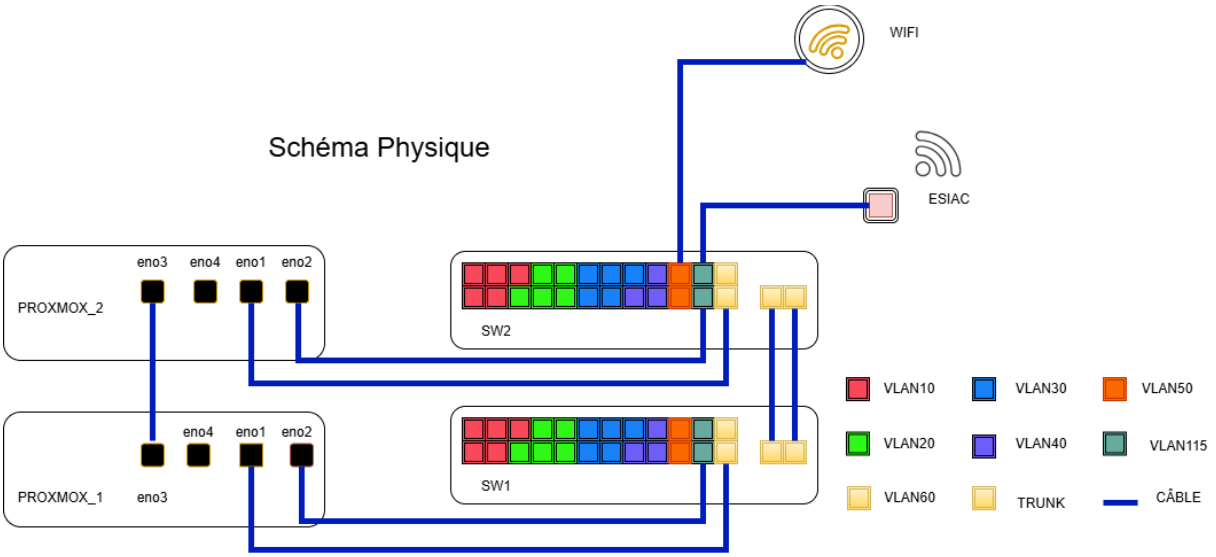
La réplication de l'Active Directory garantit également la redondance et la disponibilité continue de vos services essentiels. L'équipe de **TRIUM IT** reste à votre disposition pour tout accompagnement supplémentaire et pour vous aider à maximiser l'utilisation de ces technologies au sein de votre organisation. Ensemble, nous pouvons transformer vos défis informatiques en opportunités de croissance et de succès.

La difficulté rencontrée pour la configuration était pour moi la création de profil itinérant qui fut la plus compliquer à résoudre.

Mais je me suis aidé de différents tuto et vidéos pour réussir cette partie.

Annexe plan logique, physique, adressage IP.





Serveur Dualya :

Nom	Serveur Physique	Version	Stockage	IP Gestion :
DUALYA-1	Dell PowerEdge R630	Pve-manager 8.4,1	100 GO (iso) ,700GO (VM)	192.168.10.251
DUALYA-2	Dell PowerEdge R630	Pve-manager 8.4,1		192.168.10,252
PBS	X	PBS	240GO	

Lien IP du cluster 172.168.0.251/24 172.168.0.252/24

Adressage IP :

Nom	Hyperviseur	IP	Système d'exploitation	Performances allouées	Rôles
VSS-GLPI-100	DUALYA-1/2	192.168.10.3/24	Debian 12	1CPU 2 cores, 8 GO RAM, 32GO	GLPI ticketing
VSS-NEXTCLOUD-101	DUALYA-1/2	192.168.10.2/24	Debian 12	1 CPU 2cores, 8GO RAM, 64 GO	NEXCLOUD Stockage
VDT-LIN-PC1-103	DUALYA-1/2	192.168.20.X/24	Debian 12	1CPU 2 cores, 8 GO RAM, 32GO	Linux client
VCL-WSDUALYA1-104	DUALYA-1/2	192.168.10.1/24	Windows server 2022	1CPU 2 cores, 8 GO RAM, 32GO, 50GO	Windows server DNS DHCP COMPTE
VSS-BACKUP-PBS-105	DUALYA-1/2	192.168.10.4/24	Proxmox backup server	1CPU 2cores, 4GO RAM, 100GO, 30GO	Proxmox backup server backup des VM
VSS-SUP-PRTG-106	DUALYA-1/2	192.168.10.5/24	Windows server 2022	1 CPU 2cores, 8GO RAM, 64 GO	Windows server 2022 Supervision
VSS-PFSENSE-107	DUALYA-1/2	192.168.10.245/24	Pfsense	1 CPU 2cores, 8GO RAM, 20 GO	Pfsense firewall
VCL-WSDUALYA2-109	DUALYA-1/2	192.168.10.7/24	Windows server 2022	1 CPU 2cores, 8GO RAM, 80 GO	Windows server redondance DNS DHCP COMPTE
VSS-EDR-102	DUALYA-1/2	192.168.10.9/24	Debian 12	1CPU 2 cores, 8 GO RAM, 32GO	WAZUH EDR
VSS-SRV-TFTP-110	DUALYA-1/2	192.168.10.10/24	Debian 12	1CPU 1 cores, 2 GO RAM, 32GO	TFTP
VSS-1111-WEB	DUALYA-1/2	192.168.40.1/24	Debian 12	1CPU 1 cores, 2 GO RAM, 32GO	Debian WEB
VSS-PFSENSE2-113	DUALYA-1/2	192.168.10.246/24	Pfsense		
VDT-WCLIENT-108	DUALYA-1/2	192.168.20.X/24	Windows 10		
Copy-of-VSS-SITE-WEB	DUALYA-1/2	192.168.40.2/24	Debian 12		
VSS-REVERSEPROXY-WEB	DUALYA-1/2	192.168.40.3/24	Debian 12		