28/04/2026

PPE2 – Active Directory

Dossier technique

Mise en place d'une infrastructure

Active Directory haute disponibilité

Domaine MindLab.lan

SAAD Brandon

BTS SIO – Option SISR

Candidat libre – Session 2026

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

SESSION 2026

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

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE

Nom, prénom	**SAAD Brandon**
Statut du candidat	Candidat libre
Date de réalisation	28/04/2026
Organisation support	MindLab — Société fictive (cadre pédagogique)
Lieu	Sites de Senlis (siège) et Paris (centre R&D)
Modalité	Réalisation individuelle
Intitulé de la réalisation	Mise en place d'un environnement Active Directory redondant
Période de réalisation	Avril 2026

Compétences travaillées (option SISR) :

- 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 — Cahier des charges :

Sur l'environnement de virtualisation, mettre en œuvre une infrastructure répartie sur deux sites (Senlis et Paris) comprenant :

- Deux serveurs Active Directory (contrôleur principal + redondance)
- Un serveur de fichiers avec partages communs et personnels
- Des unités d'organisation, groupes et utilisateurs représentatifs
- Un routage inter-sites et une segmentation par VLAN
- Des services DHCP avec basculement (failover) et DNS secondaire
- Des stratégies de groupe (GPO) appliquées aux postes de travail

Ressources matérielles et logicielles :

- VMware Workstation / Hyper-V
- Windows Server 2022 (3 instances : DC-01, DC-02, FS-01)
- Windows 10 Pro (postes clients)

- Outils d'administration : Gestionnaire de serveur, GPMC, DNS Manager, DHCP Manager

Table des matières

I. Présentation de la mission

1.1. Introduction

La présente mission consiste à mettre en place et à documenter une infrastructure Active Directory répartie sur les deux sites de l'entreprise MindLab. L'objectif est de fournir aux utilisateurs un environnement de travail centralisé, sécurisé et hautement disponible, en s'appuyant sur les rôles standards d'un Windows Server 2022.

Pour réaliser cela, je vais déployer un premier contrôleur de domaine (DC-01) sur le site de Senlis et créer une nouvelle forêt MindLab.lan. J'ajouterai ensuite un second contrôleur de domaine (DC-02) sur le site de Paris afin d'assurer la redondance du service d'annuaire et la continuité d'activité en cas de défaillance du serveur principal.

À cette base s'ajouteront les services essentiels au bon fonctionnement de l'infrastructure : un service DNS répliqué, un service DHCP haute disponibilité avec basculement (failover), une organisation logique en unités d'organisation (OU), ainsi qu'un ensemble de stratégies de groupe (GPO) déployées sur les postes clients.

1.2. Objectifs de la mission

Les objectifs poursuivis dans cette mission sont les suivants :

- Garantir la centralisation de l'authentification et de la gestion des utilisateurs sur l'ensemble des sites de MindLab
- Assurer la haute disponibilité des services d'annuaire et d'attribution d'adresses IP via la redondance des contrôleurs de domaine et le basculement DHCP
- Mettre en place une résolution de noms fiable, en interne comme en externe, à l'aide d'un service DNS intégré à Active Directory
- Faciliter l'administration des postes clients par l'application de stratégies de groupe communes
- Documenter chaque étape de la réalisation pour permettre la reproduction de l'infrastructure et son évolution future

II. Contexte

2.1. Présentation de l'entreprise MindLab

MindLab est une société fictive du secteur des sciences cognitives appliquées et de l'intelligence artificielle. Créée en 2018, elle compte aujourd'hui environ 80 collaborateurs répartis sur deux sites principaux : un siège social situé à Senlis (Oise) qui regroupe la direction, le service Ressources Humaines et l'équipe Communication, et un centre de Recherche & Développement basé à Paris qui héberge les équipes techniques et les laboratoires.

L'entreprise développe et commercialise des solutions logicielles destinées aux laboratoires de recherche et aux universités. Ses besoins informatiques sont structurants : centralisation des comptes utilisateurs, sécurisation des partages de fichiers entre les deux sites, continuité de service, traçabilité des accès et homogénéité de la configuration des postes de travail.

2.2. Scénario

Suite à une croissance soutenue et à l'ouverture du site parisien, la direction de MindLab a constaté plusieurs limites dans son organisation informatique actuelle :

- L'authentification des utilisateurs est gérée localement sur chaque poste, ce qui complique la gestion des comptes lors des arrivées et départs
- Aucun mécanisme de redondance n'existe pour les services critiques, exposant l'entreprise à un risque d'arrêt prolongé en cas de panne
- Les paramètres réseau des postes clients sont configurés manuellement, source d'erreurs et de surcharge pour le support technique
- Les partages de fichiers sont éparpillés sur plusieurs postes, sans gestion centralisée des droits

Pour répondre à ces problématiques, MindLab souhaite déployer une infrastructure Active Directory complète, répartie sur ses deux sites, accompagnée des services réseau associés (DNS, DHCP, partages de fichiers, GPO).

Le site de Senlis hébergera le contrôleur de domaine principal DC-01 ainsi qu'un serveur de fichiers FS-01. Le site de Paris hébergera un second contrôleur de domaine DC-02 assurant la redondance du domaine. Les deux sites seront reliés par une liaison inter-sites permettant la réplication Active Directory et le routage entre les sous-réseaux locaux.

2.3. Cahier des charges

Les attendus formalisés par la direction technique de MindLab sont les suivants :

- Mise en place d'un contrôleur de domaine principal DC-01 et création de la forêt MindLab.lan
- Mise en place d'un second contrôleur de domaine DC-02 sur le site de Paris pour assurer la redondance

- Configuration du service DNS avec une zone directe et une zone inversée pour chaque sous-réseau, répliquées entre les deux contrôleurs de domaine
- Mise en œuvre du service DHCP avec basculement (failover) entre DC-01 et DC-02 pour les six étendues de l'entreprise
- Création des unités d'organisation, groupes et utilisateurs représentatifs des services de MindLab
- Mise en place d'une stratégie de groupe (GPO) appliquée au domaine pour la distribution d'un partage commun
- Vérification du bon fonctionnement de l'ensemble (résolution DNS, attribution DHCP, ouverture de session)

2.4. Architecture réseau

L'architecture cible repose sur deux sites interconnectés, chacun segmenté en plusieurs VLAN selon le service métier. Cette segmentation permet d'isoler les flux et de simplifier l'application des politiques de sécurité.

Plan d'adressage des serveurs :

Serveur	Adresse IP / Masque
DC-01 (Senlis – contrôleur principal)	192.168.80.60 /28
DC-02 (Paris – contrôleur secondaire)	192.168.81.60 /28
FS-01 (Senlis – serveur de fichiers)	192.168.80.61 /28

Étendues DHCP du domaine MindLab.lan :

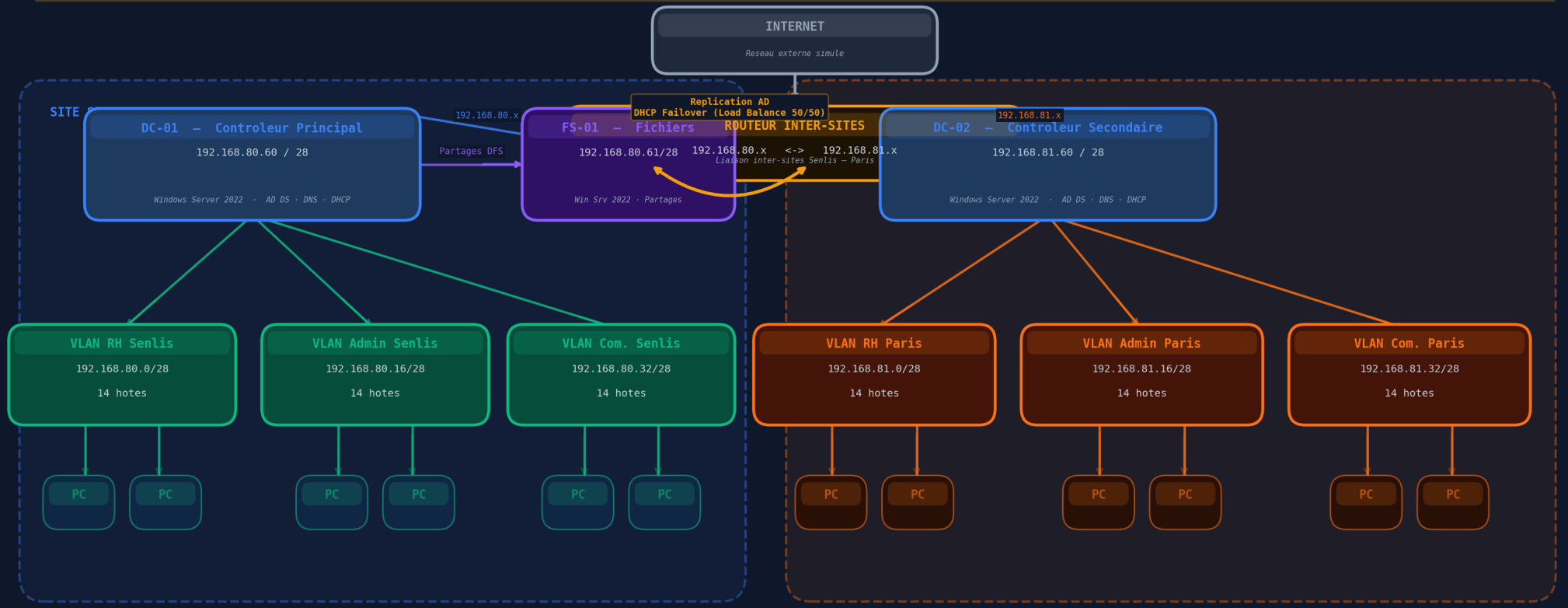
Étendue	Sous-réseau	Service / Site
DHCP-Senlis-RH1	192.168.80.0/28	Senlis – Ressources Humaines
DHCP2-Senlis-Admin	192.168.80.16/28	Senlis – Administratif
DHCP3-Senlis-Com	192.168.80.32/28	Senlis – Communication
DHCP4-Paris-RH	192.168.81.0/28	Paris – Ressources Humaines
DHCP5-Paris-Admin	192.168.81.16/28	Paris – Administratif
DHCP6-Paris-Com	192.168.81.32/28	Paris – Communication

Chaque sous-réseau est dimensionné en /28 (14 adresses utilisables), ce qui correspond au nombre de postes attendus par service. Cette granularité permet à la fois d'optimiser le plan d'adressage et de faciliter l'identification des flux par lecture de l'adresse IP.

2.5. Besoins logiciels

Infrastructure Active Directory — Haute Disponibilite — MindLab.lan

PPE 1 | BTS SIO SISR | SAAD Brandon | Session 2026



PLAN D'ADRESSAGE :

DC-01	192.168.80.60/28	Controleur principal — Senlis	DC-02	192.168.81.60/28	Controleur secondaire — Paris	FS-01	192.168.80.61/28	Serveur de fichiers — Senlis
VLAN RH Senlis	192.168.80.0/28	14 hotes — Ressources Humaines Senlis	VLAN Admin Senlis	192.168.80.16/28	14 hotes — Administratif Senlis	VLAN Com. Senlis	192.168.80.32/28	14 hotes — Communication Senlis
VLAN RH Paris	192.168.81.0/28	14 hotes — Ressources Humaines Paris	VLAN Admin Paris	192.168.81.16/28	14 hotes — Administratif Paris	VLAN Com. Paris	192.168.81.32/28	14 hotes — Communication Paris

Pour la mise en œuvre de cette infrastructure, les ressources suivantes ont été utilisées :

- 3 instances Windows Server 2022 (DC-01, DC-02, FS-01)
- Plusieurs postes Windows 10 Pro pour les tests clients
- Une plateforme de virtualisation (VMware Workstation)
- Les rôles natifs de Windows Server 2022 : AD DS, DNS, DHCP, Gestion des stratégies de groupe

2.6. Présentation des solutions utilisées

2.6.1. Active Directory

Active Directory (AD) est le service d'annuaire développé par Microsoft pour les réseaux Windows. Il centralise dans une base de données unique l'ensemble des informations relatives aux utilisateurs, groupes, ordinateurs et ressources d'un domaine. Il permet à un administrateur de gérer de façon homogène les comptes, les droits d'accès, les politiques de sécurité et l'application de configurations sur les postes.

Active Directory s'appuie sur plusieurs composants : la forêt (qui regroupe un ou plusieurs domaines partageant un même schéma), le domaine (unité administrative principale), les unités d'organisation (OU) qui permettent une hiérarchisation interne, et les contrôleurs de domaine qui hébergent une copie de la base d'annuaire et répondent aux demandes d'authentification.

2.6.2. DNS et DHCP

Le service DNS (Domain Name System) assure la résolution des noms en adresses IP et inversement. Dans un environnement Active Directory, le DNS est indispensable car les contrôleurs de domaine s'enregistrent dans la zone DNS pour annoncer les services qu'ils proposent (LDAP, Kerberos, etc.).

Le service DHCP (Dynamic Host Configuration Protocol) attribue dynamiquement aux postes clients leur adresse IP, leur masque, leur passerelle et leurs serveurs DNS. Couplé à la fonctionnalité de basculement (failover), il garantit que les postes obtiennent toujours une configuration réseau valide, même en cas d'arrêt d'un des serveurs DHCP.

2.6.3. Stratégies de groupe (GPO)

Les stratégies de groupe (Group Policy Objects) permettent à l'administrateur de centraliser la configuration des postes et des sessions utilisateurs. Une GPO peut imposer des paramètres aussi variés qu'un fond d'écran, le mappage automatique d'un lecteur réseau, des règles de mot de passe, des restrictions logicielles, ou la redirection de dossiers.

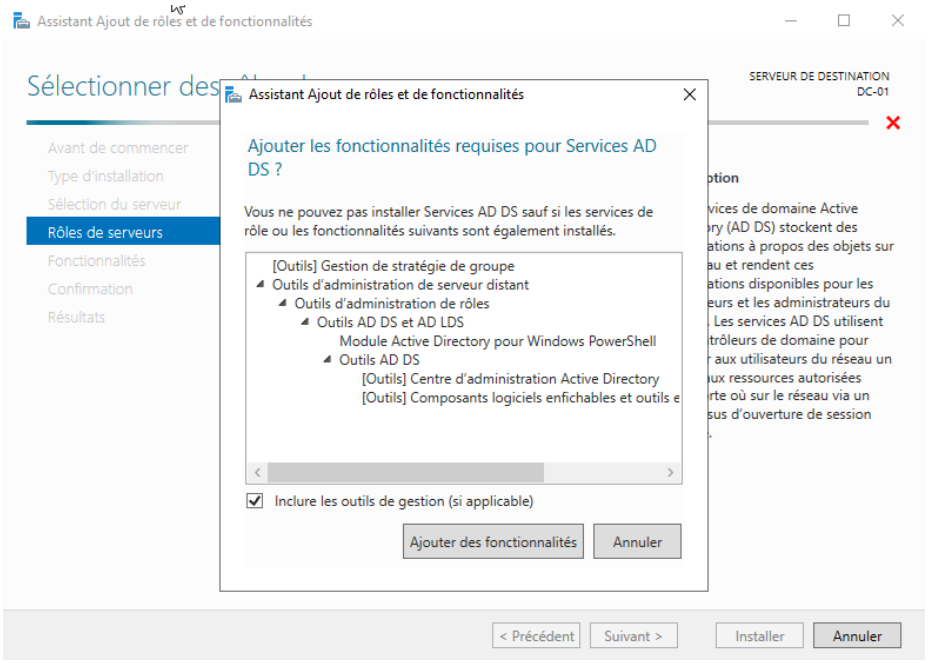
III. Contrôleur de domaine et redondance

3.1. Mise en place du contrôleur de domaine principal DC-01

Le contrôleur de domaine est l'élément central de l'infrastructure Active Directory. Il héberge la base d'annuaire, applique les politiques de sécurité, traite les demandes d'authentification (Kerberos, NTLM) et participe à la réplication des données entre tous les contrôleurs du domaine.

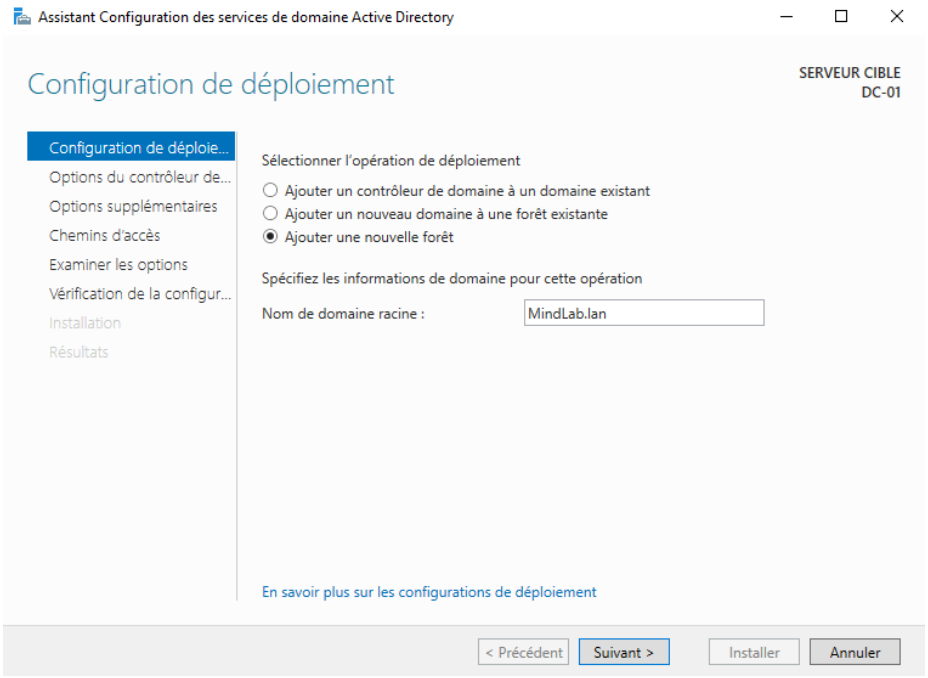
La première étape consiste donc à installer le rôle AD DS (Active Directory Domain Services) sur le serveur DC-01. Pour cela, j'ouvre le Gestionnaire de serveur, je clique sur « Ajouter des rôles et fonctionnalités » et je sélectionne « Services AD DS » dans la liste des rôles disponibles.

L'assistant me propose d'installer automatiquement les fonctionnalités requises, notamment la console de Gestion des stratégies de groupe (GPMC), les outils d'administration AD DS et le module PowerShell associé.



Une fois le rôle AD DS installé, il faut promouvoir le serveur DC-01 en contrôleur de domaine. C'est lors de cette étape que je vais créer la nouvelle forêt MindLab.lan, puisque l'entreprise n'a pas encore de domaine existant.

Je sélectionne donc l'option « Ajouter une nouvelle forêt » puis je saisis le nom de domaine racine : MindLab.lan.



L'assistant continue ensuite avec les options du contrôleur de domaine (niveau fonctionnel de la forêt et du domaine, mot de passe DSRM pour le mode restauration, options DNS, etc.). Je conserve les paramètres par défaut, qui correspondent aux bonnes pratiques pour un déploiement Windows Server 2022.

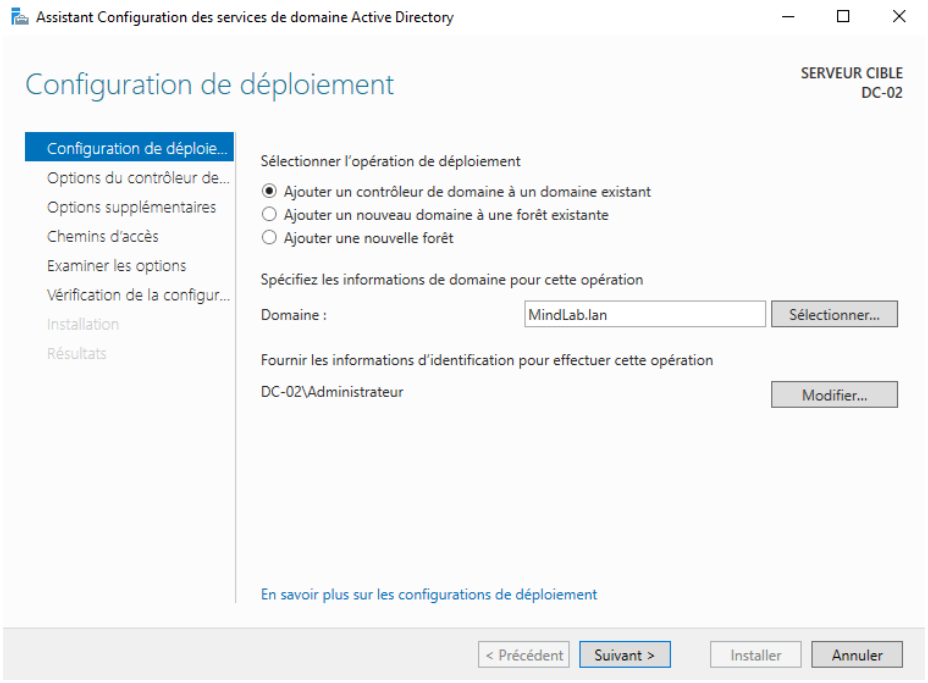
Une fois les vérifications préalables passées avec succès, l'installation du contrôleur de domaine se lance et le serveur redémarre automatiquement à la fin du processus. Le serveur DC-01 est désormais contrôleur de domaine de la forêt MindLab.lan. Il assure à la fois la fonction d'annuaire AD et celle de serveur DNS, puisqu'une zone DNS principale intégrée à Active Directory a été automatiquement créée pour MindLab.lan.

3.2. Mise en place du contrôleur de domaine secondaire DC-02

Pour garantir la haute disponibilité du service d'annuaire, je vais maintenant ajouter un second contrôleur de domaine, DC-02, sur le site de Paris. En cas d'arrêt de DC-01, ce contrôleur prendra automatiquement le relais pour les demandes d'authentification et la résolution DNS, assurant ainsi la continuité de service pour les utilisateurs.

La procédure est similaire à celle de DC-01 : j'installe le rôle AD DS sur le serveur DC-02 via le Gestionnaire de serveur. À nouveau, l'assistant ajoute les fonctionnalités requises pour la gestion de l'annuaire.

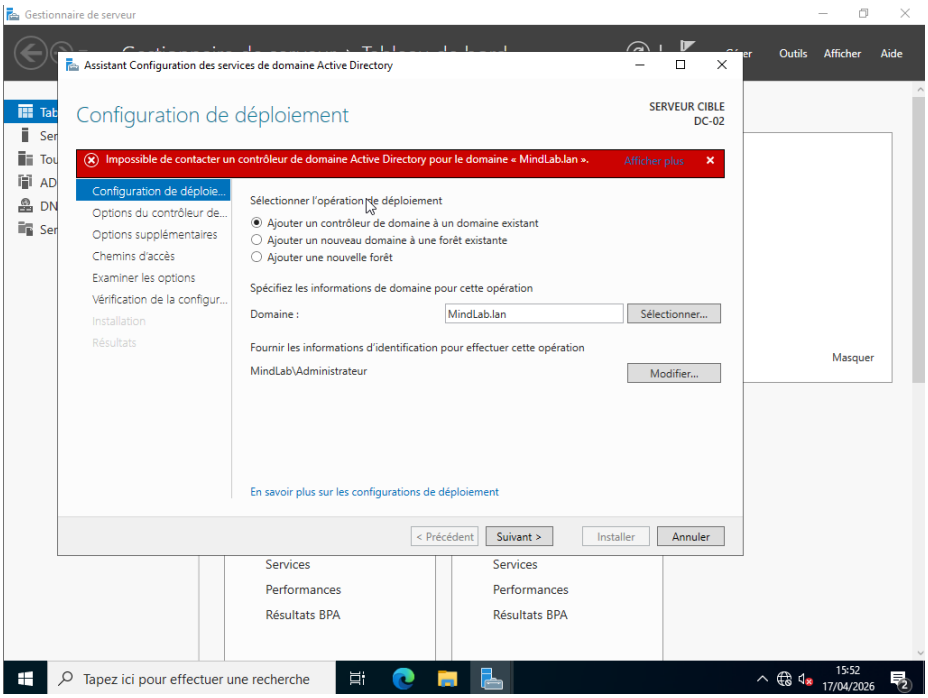
Une fois le rôle installé, je promeus DC-02 en contrôleur de domaine. Cette fois, je ne vais pas créer une nouvelle forêt, puisque MindLab.lan existe déjà. Je choisis donc l'option « Ajouter un contrôleur de domaine à un domaine existant » et je renseigne le nom du domaine cible : MindLab.lan.



L'assistant me demande de fournir des identifiants disposant des droits d'administration sur le domaine. J'utilise donc le compte MindLab\Administrateur.

Difficulté rencontrée — Résolution DNS lors de la promotion :

Lors de la première tentative de promotion de DC-02, l'assistant a affiché le message d'erreur suivant : « Impossible de contacter un contrôleur de domaine Active Directory pour le domaine MindLab.lan ».

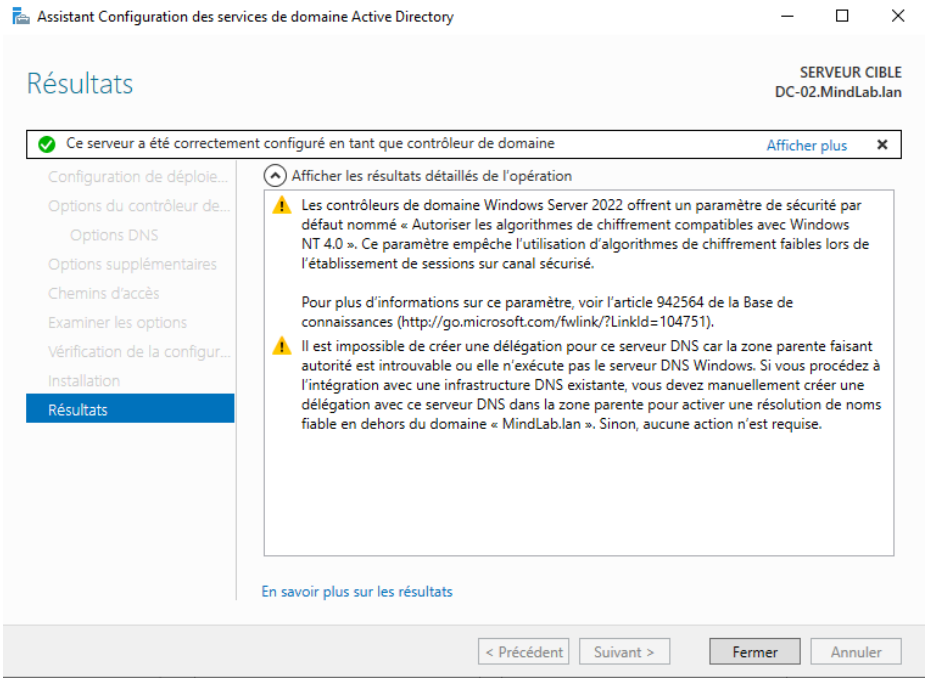


Cette erreur signifie que DC-02 n'arrive pas à localiser DC-01 par résolution DNS. La cause est classique : la carte réseau de DC-02 n'avait pas DC-01 (192.168.80.60) configuré en serveur DNS primaire. Sans

cette configuration, le futur contrôleur ne peut pas résoudre les enregistrements SRV qui annoncent les services Active Directory du domaine.

Pour corriger l'erreur, je modifie les paramètres de la carte réseau de DC-02 et je définis 192.168.80.60 comme serveur DNS préféré. Une fois cette modification effectuée, je relance l'assistant de promotion : la résolution du domaine s'effectue cette fois sans difficulté et l'installation peut se poursuivre.

À l'issue de l'installation, le serveur redémarre. Le résultat de la promotion confirme que DC-02 a bien été configuré en tant que contrôleur de domaine du domaine MindLab.lan. Les avertissements affichés (paramètre de chiffrement NT 4.0 et délégation DNS introuvable) sont informatifs et n'empêchent pas le bon fonctionnement de l'annuaire dans notre contexte.



La redondance du domaine MindLab.lan est désormais opérationnelle : les deux contrôleurs de domaine partagent la même base d'annuaire et peuvent traiter indépendamment les demandes des utilisateurs et des postes.

IV. Service DNS

4.1. Présentation

Le service DNS (Domain Name System) constitue la pierre angulaire de toute infrastructure Active Directory. Il assure la traduction des noms de domaine pleinement qualifiés (FQDN) en adresses IP et, inversement, des adresses IP en noms via la résolution inverse. Dans un environnement AD, le DNS héberge également les enregistrements SRV qui permettent aux postes clients de localiser les contrôleurs de domaine, les serveurs Kerberos et les autres services d'annuaire.

Sur l'infrastructure MindLab.lan, le DNS est intégré à Active Directory : la zone est stockée directement dans la base AD et bénéficie ainsi de la réplication multimaître entre DC-01 et DC-02. Cela signifie qu'un enregistrement créé sur l'un des contrôleurs est automatiquement répliqué sur l'autre, sans intervention manuelle.

4.2. Zone de recherche directe

La zone de recherche directe MindLab.lan a été créée automatiquement lors de la promotion de DC-01 en contrôleur de domaine. Elle contient les enregistrements de type A (correspondance nom → adresse IP) pour chacune des machines du domaine, ainsi que les enregistrements de type SOA (Start of Authority) et NS (Name Server) qui définissent les serveurs faisant autorité sur la zone.

Lorsqu'un poste rejoint le domaine, son enregistrement A est créé automatiquement dans la zone, à condition que les mises à jour dynamiques soient autorisées (ce qui est le cas par défaut pour les zones intégrées à AD).

4.3. Zones de recherche inversée

La résolution inverse permet de retrouver le nom DNS d'une machine à partir de son adresse IP. Ce mécanisme est utile pour le diagnostic réseau et pour certains services de sécurité ou de journalisation. Pour le mettre en place, il faut créer une zone de recherche inversée par sous-réseau concerné.

Dans le cas de MindLab, deux zones inverses sont nécessaires, correspondant aux deux préfixes /24 utilisés sur l'infrastructure :

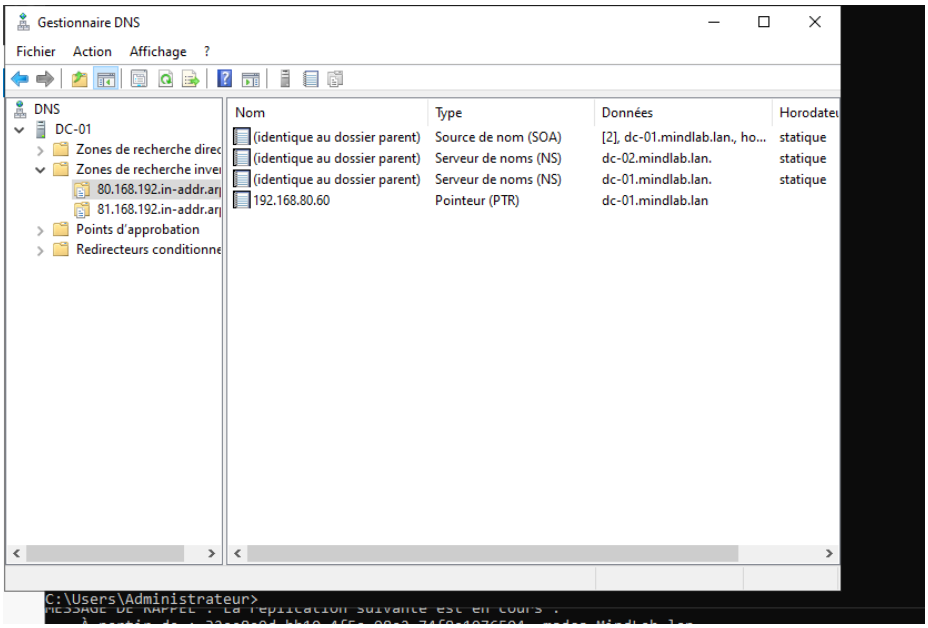
- 80.168.192.in-addr.arpa pour le sous-réseau 192.168.80.0/24 (Senlis)
- 81.168.192.in-addr.arpa pour le sous-réseau 192.168.81.0/24 (Paris)

Pour créer ces zones, j'ouvre le Gestionnaire DNS depuis le menu Outils du Gestionnaire de serveur, puis je fais un clic droit sur « Zones de recherche inversée » et je sélectionne « Nouvelle zone ».

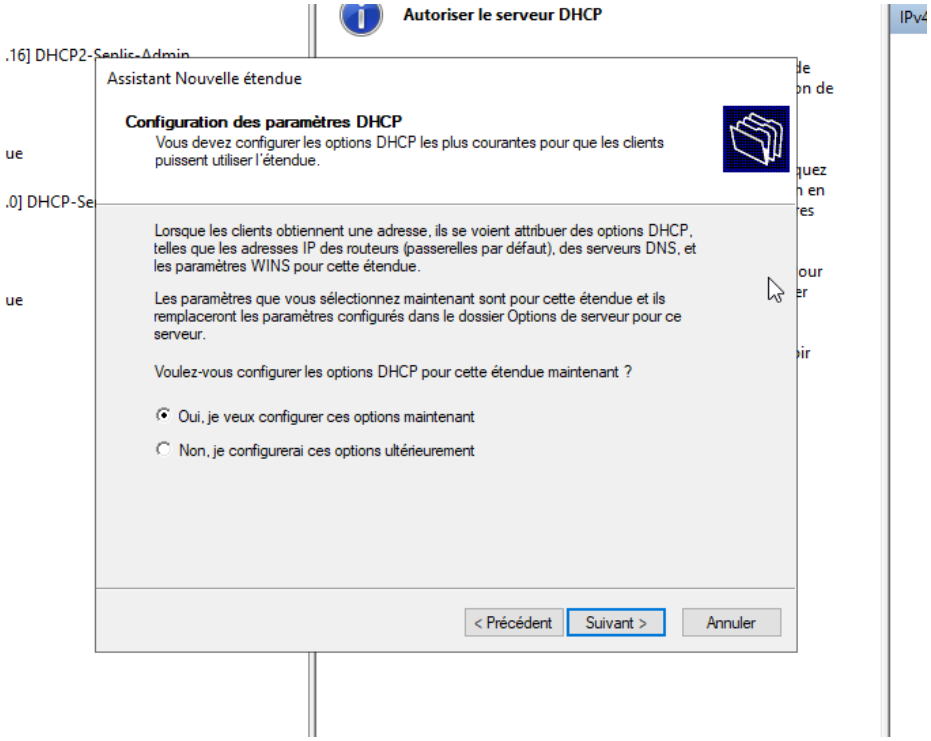
Dans l'assistant, je choisis le type « Zone principale » et je coche l'option « Enregistrer la zone dans Active Directory », ce qui permet la réplication automatique entre DC-01 et DC-02. Je sélectionne ensuite l'étendue de réplication « Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : MindLab.lan ».

Je saisis l'identifiant réseau, par exemple 192.168.80, et l'assistant génère automatiquement le nom de la zone : 80.168.192.in-addr.arpa. Je termine en autorisant uniquement les mises à jour dynamiques sécurisées, ce qui constitue la bonne pratique pour les zones intégrées à AD.

Une fois les deux zones créées, je peux constater dans le gestionnaire DNS que les enregistrements PTR (pointeurs) se créent automatiquement pour les serveurs et les postes du domaine. Les contrôleurs DC-01 et DC-02 apparaissent comme serveurs de noms (NS) sur la zone, confirmant la réplication.



L'enregistrement PTR (pointeur) permet de fournir le nom de domaine associé à une adresse IP. Quand un poste client rejoint le domaine, le serveur DNS crée automatiquement un enregistrement A et un enregistrement PTR si les zones ont été correctement configurées.

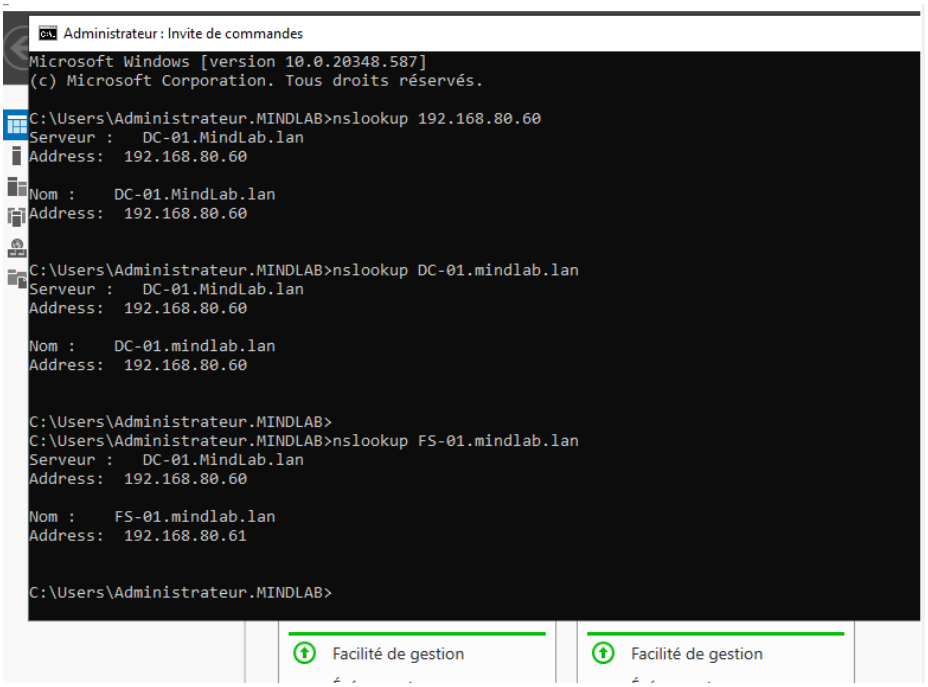


4.4. Vérification de la résolution

Pour valider le bon fonctionnement du DNS, j'utilise la commande nslookup depuis l'invite de commandes d'un poste joint au domaine. Cette commande interroge directement le serveur DNS et permet de vérifier à la fois la résolution directe (nom → IP) et la résolution inverse (IP → nom).

Les tests effectués sont les suivants :

- nslookup 192.168.80.60 → renvoie DC-01.MindLab.lan (résolution inverse)
- nslookup DC-01.mindlab.lan → renvoie 192.168.80.60 (résolution directe)
- nslookup FS-01.mindlab.lan → renvoie 192.168.80.61 (résolution du serveur de fichiers)



Les résolutions répondent correctement, ce qui confirme que le service DNS est opérationnel sur l'infrastructure MindLab.lan.

V. Service DHCP

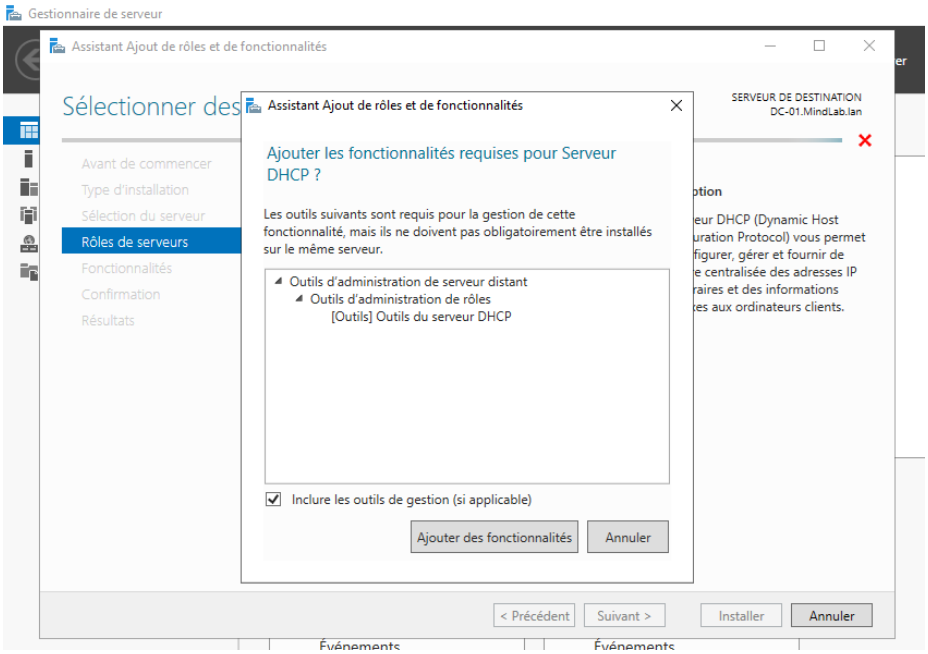
5.1. Présentation

Le protocole DHCP (Dynamic Host Configuration Protocol) automatise l'attribution des paramètres réseau (adresse IP, masque, passerelle, serveurs DNS) aux postes clients. Il évite la configuration manuelle de chaque machine et limite considérablement les risques de conflit d'adresses.

Dans le contexte de MindLab, le service DHCP doit couvrir six sous-réseaux différents, correspondant aux services Ressources Humaines, Administratif et Communication de chacun des deux sites. Pour garantir la haute disponibilité, le service sera déployé en mode failover entre DC-01 et DC-02.

5.2. Installation du rôle DHCP

L'installation du rôle DHCP suit la procédure habituelle d'ajout de rôle via le Gestionnaire de serveur. Sur DC-01, je sélectionne le rôle « Serveur DHCP » dans la liste, et l'assistant me propose d'installer les outils d'administration associés.



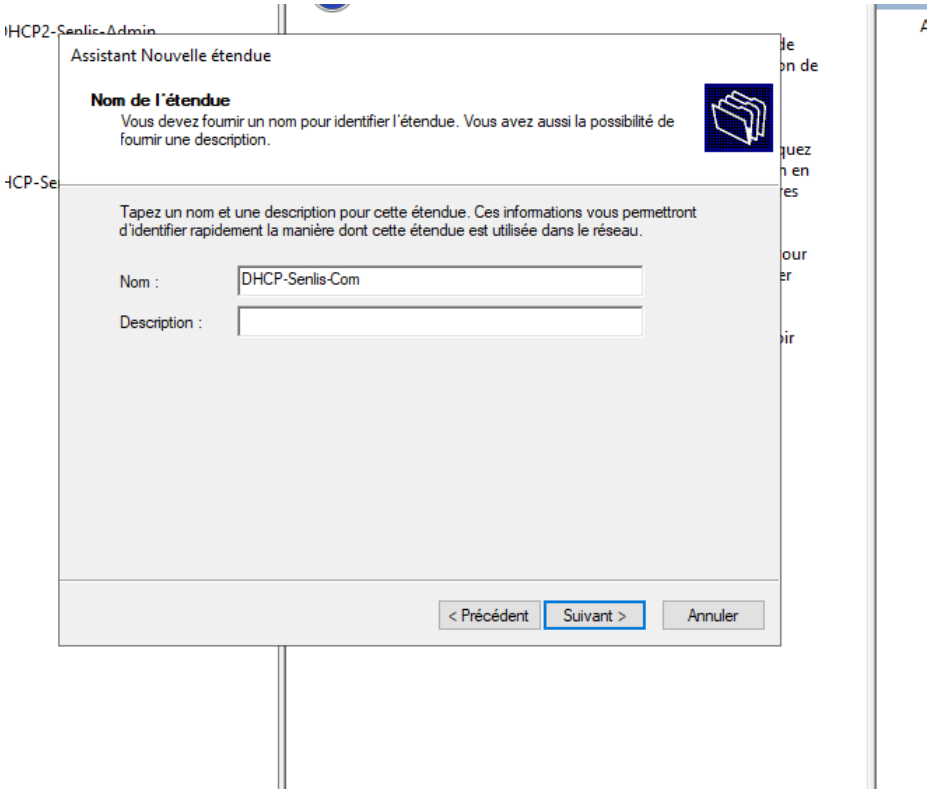
Une fois l'installation terminée, le Gestionnaire de serveur affiche un avertissement indiquant qu'une configuration post-déploiement est requise. Je clique sur « Terminer la configuration DHCP ».

Cette étape réalise deux actions au sein de l'Active Directory : la création des deux groupes de sécurité « Administrateurs DHCP » et « Utilisateurs DHCP », qui permettent de déléguer la gestion du service, et l'autorisation du serveur DHCP dans l'annuaire. Cette autorisation est obligatoire dans un environnement AD : un serveur DHCP non autorisé refusera de démarrer pour éviter les conflits avec un éventuel DHCP non maîtrisé.

5.3. Création des étendues DHCP

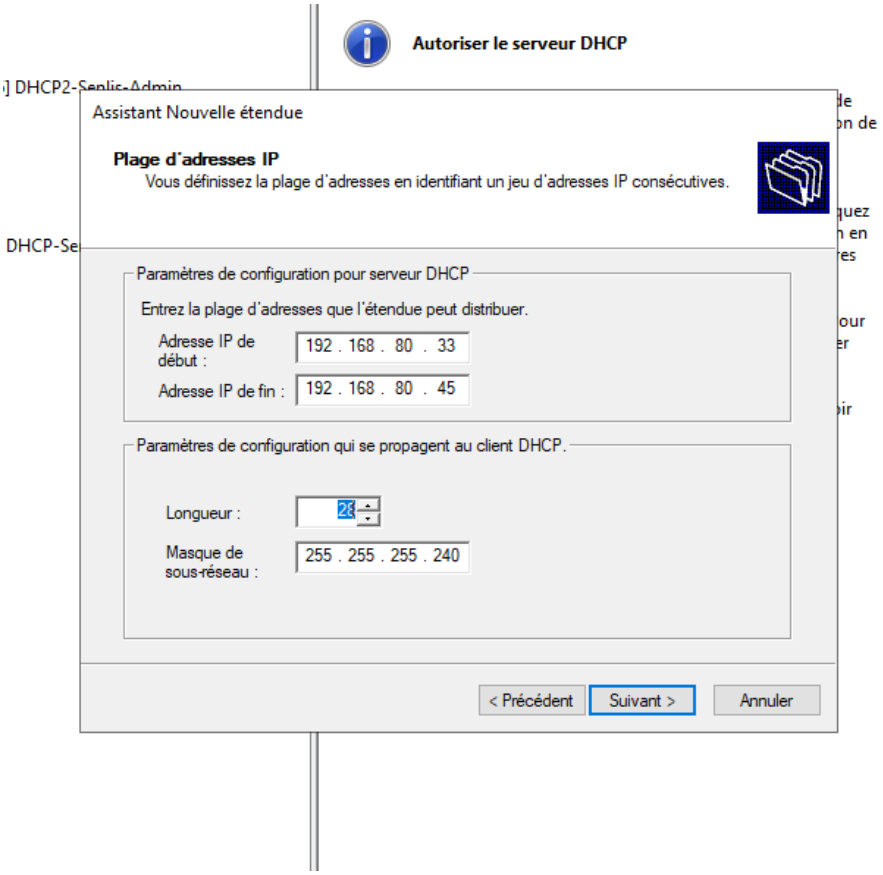
Une étendue DHCP correspond à une plage d'adresses IP que le serveur peut distribuer pour un sous-réseau donné. Pour chaque service de MindLab, je crée une étendue dédiée. Les étapes ci-dessous décrivent la création de la première étendue (Senlis – Communication), la procédure étant identique pour les cinq autres.

Dans la console DHCP, je fais un clic droit sur IPv4 et je sélectionne « Nouvelle étendue ». L'assistant me demande tout d'abord un nom et une description :

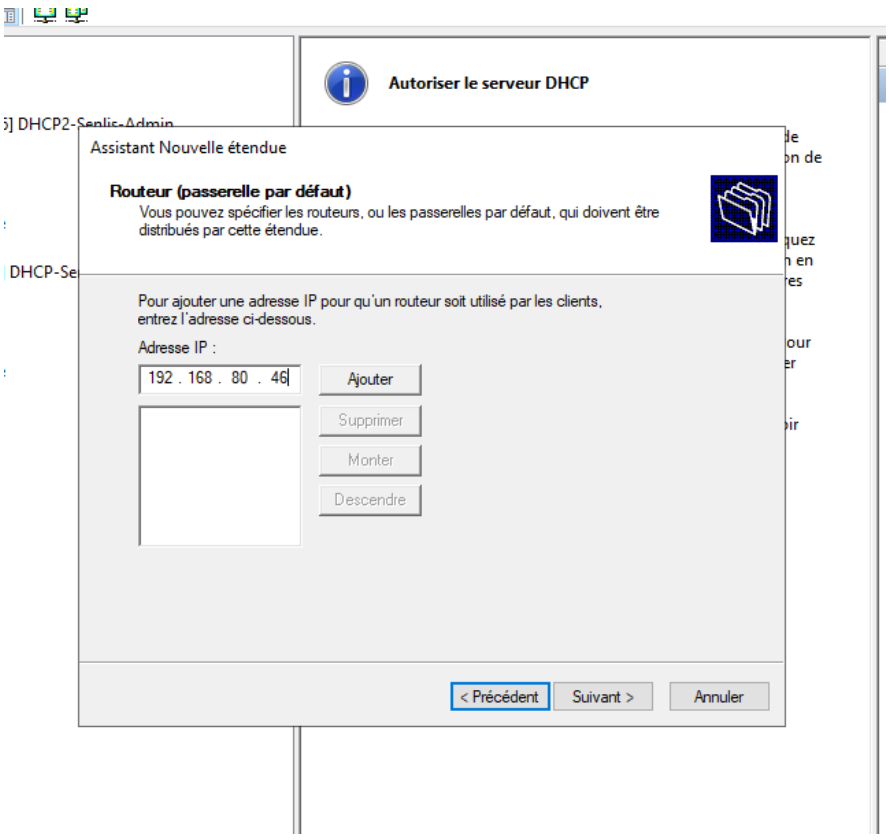


Je nomme l'étendue DHCP-Senlis-Com pour identifier rapidement le service et le site concernés.

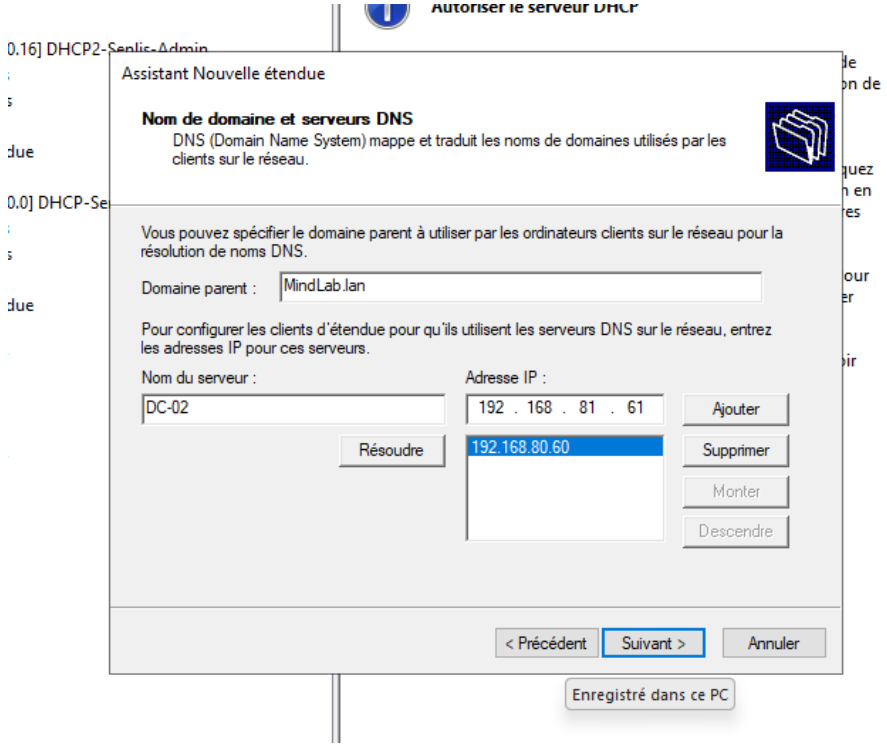
Je définis ensuite la plage d'adresses distribuables. Pour le réseau 192.168.80.32/28, je saisis l'adresse de début 192.168.80.33 et l'adresse de fin 192.168.80.45 (en réservant la dernière utilisable pour la passerelle). Le masque /28 correspond à 255.255.255.240.



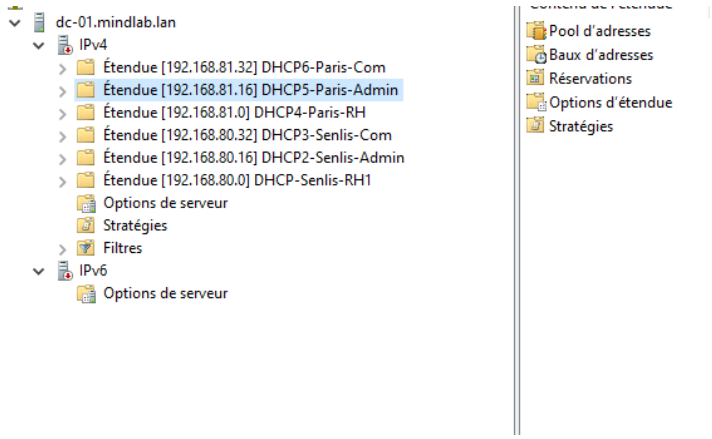
L'assistant continue avec la configuration de la passerelle par défaut. Je renseigne ici l'adresse IP de l'interface du routeur correspondant au sous-réseau (192.168.80.46 pour le VLAN concerné) :



L'étape suivante est cruciale : la configuration des serveurs DNS qui seront communiqués aux clients. Je saisis le nom de domaine parent MindLab.lan, puis j'ajoute les adresses des deux contrôleurs de domaine afin que les postes puissent toujours résoudre les noms même en cas de panne de l'un des deux DC :



Une fois l'étendue créée et activée, je répète la procédure pour les cinq autres étendues. À l'issue, la console DHCP de DC-01 présente bien les six étendues attendues, couvrant l'ensemble des services et des sites de l'entreprise.



Récapitulatif des étendues DHCP configurées :

Nom	Plage	Service / Site
DHCP-Senlis-RH1	192.168.80.0/28	Senlis – RH
DHCP2-Senlis-Admin	192.168.80.16/28	Senlis – Administratif

DHCP3-Senlis-Com	192.168.80.32/28	Senlis – Communication
DHCP4-Paris-RH	192.168.81.0/28	Paris – RH
DHCP5-Paris-Admin	192.168.81.16/28	Paris – Administratif
DHCP6-Paris-Com	192.168.81.32/28	Paris – Communication

VI. Mise en place du basculement DHCP (Failover)

6.1. Principe du DHCP Failover

Le basculement DHCP, ou DHCP Failover, est une fonctionnalité native de Windows Server 2012 et supérieur qui permet à deux serveurs DHCP de partager la responsabilité d'attribution des adresses pour un même ensemble d'étendues. Ce mécanisme assure la continuité du service même en cas de panne d'un des serveurs.

Deux modes de fonctionnement sont possibles :

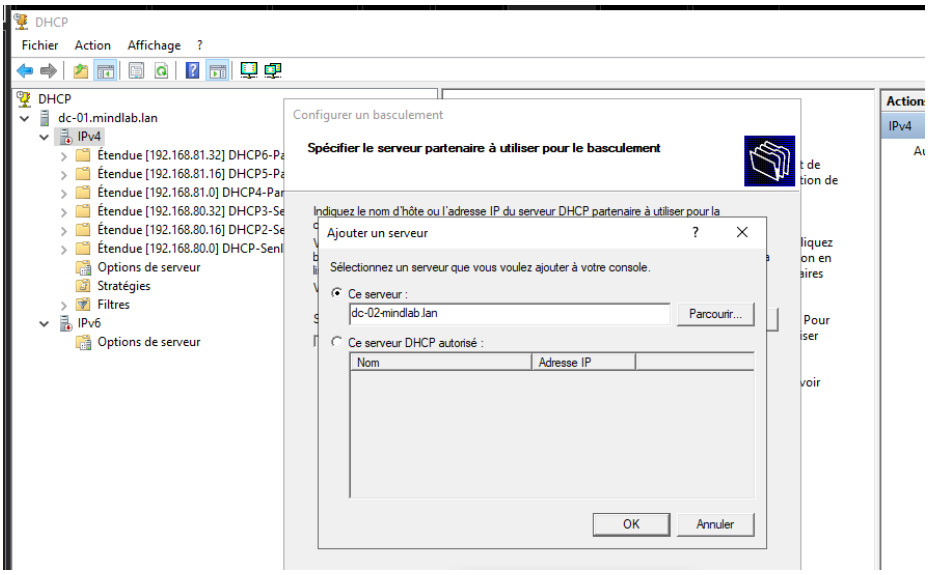
- Le mode Hot Standby (veille active) : un serveur principal traite l'ensemble des requêtes, le second n'intervient qu'en cas de défaillance du premier
- Le mode Load Balance (équilibrage de charge) : les deux serveurs traitent simultanément les requêtes selon une répartition configurable

Pour MindLab, je retiens le mode Load Balance avec une répartition 50/50, qui présente l'avantage de répartir la charge entre les deux contrôleurs en fonctionnement nominal et d'éprouver continuellement la disponibilité du second serveur.

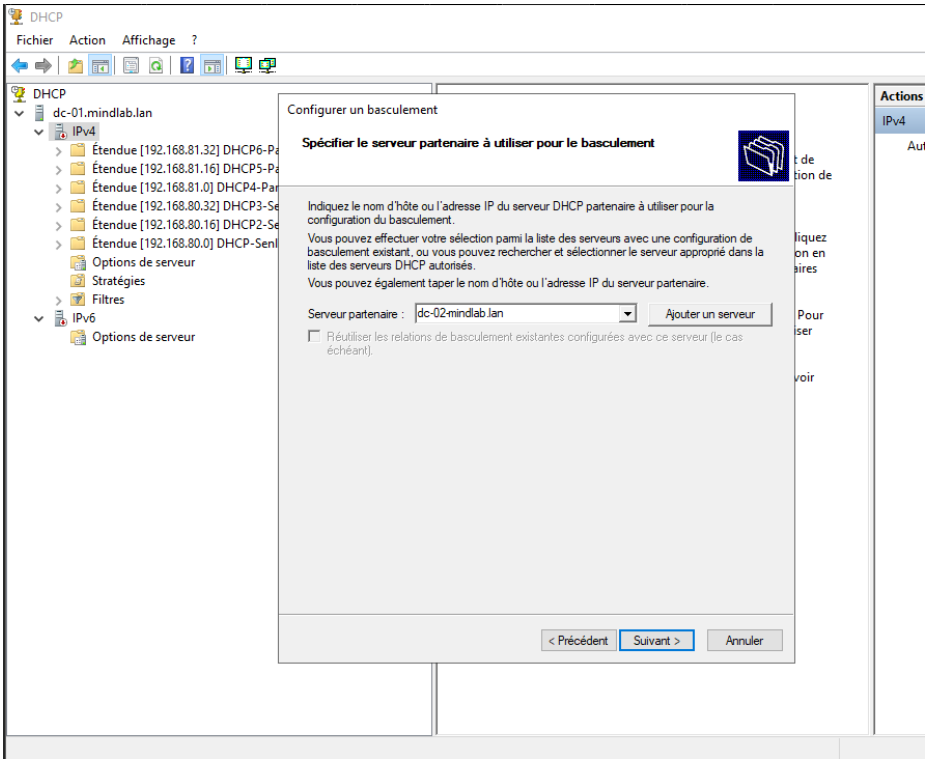
6.2. Configuration du basculement

La configuration du failover se fait depuis la console DHCP de DC-01. Je fais un clic droit sur IPv4 et je sélectionne « Configurer un basculement ».

L'assistant me demande de spécifier le serveur partenaire qui sera le second membre du cluster DHCP. Je clique sur « Ajouter un serveur » et je sélectionne dc-02-mindlab.lan dans la liste des serveurs DHCP autorisés :

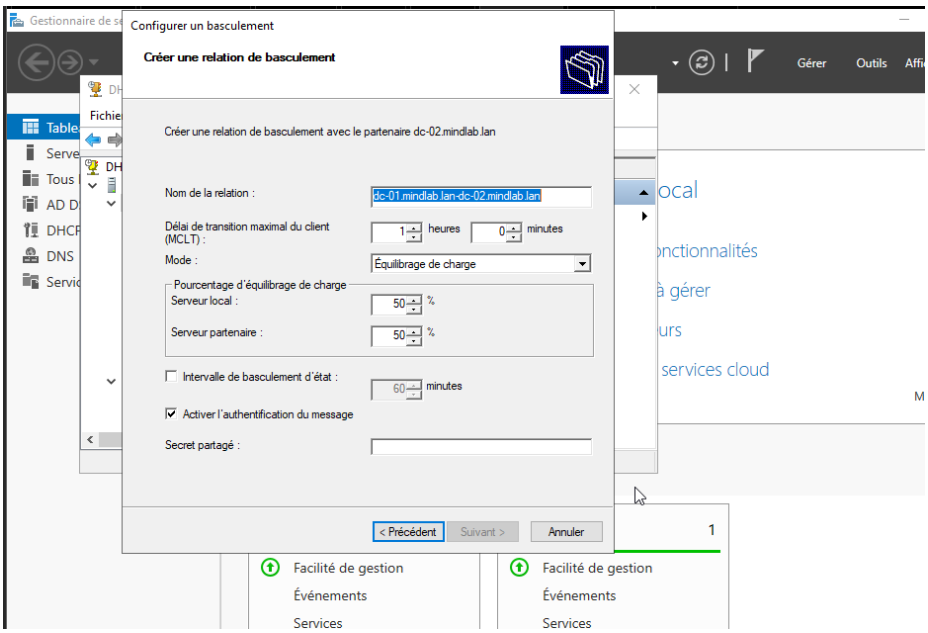


Une fois le serveur partenaire ajouté, l'assistant affiche le récapitulatif des étendues qui seront dupliquées sur DC-02 :

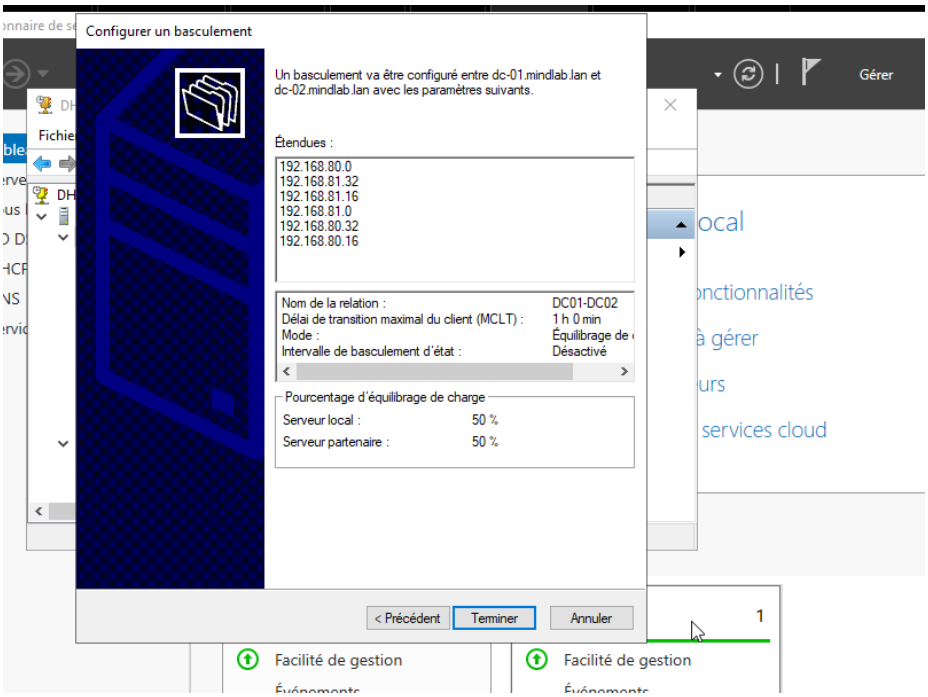


L'étape suivante consiste à définir les paramètres de la relation de basculement :

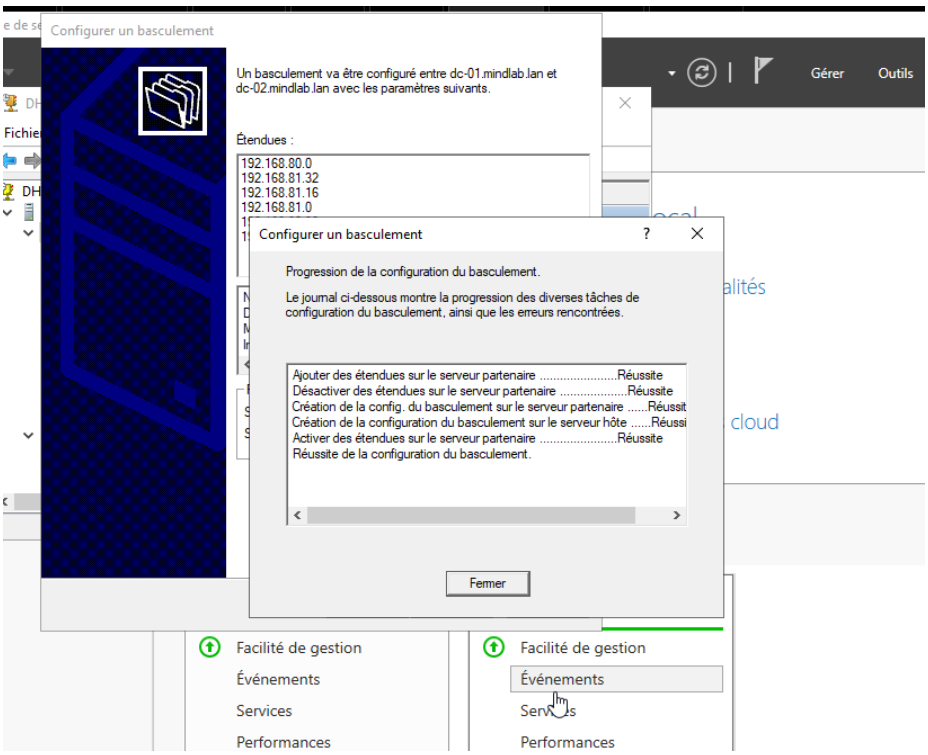
- Nom de la relation : dc-01.mindlab.lan-dc-02.mindlab.lan
- MCLT (Maximum Client Lead Time) : 1 heure — ce paramètre définit la durée pendant laquelle un serveur peut accorder un bail si l'autre est injoignable
- Mode : Équilibrage de charge
- Pourcentage : 50% sur chaque serveur
- Activation de l'authentification du message avec un secret partagé pour sécuriser les échanges entre les deux serveurs



Je confirme la configuration. L'assistant affiche un récapitulatif avant validation :

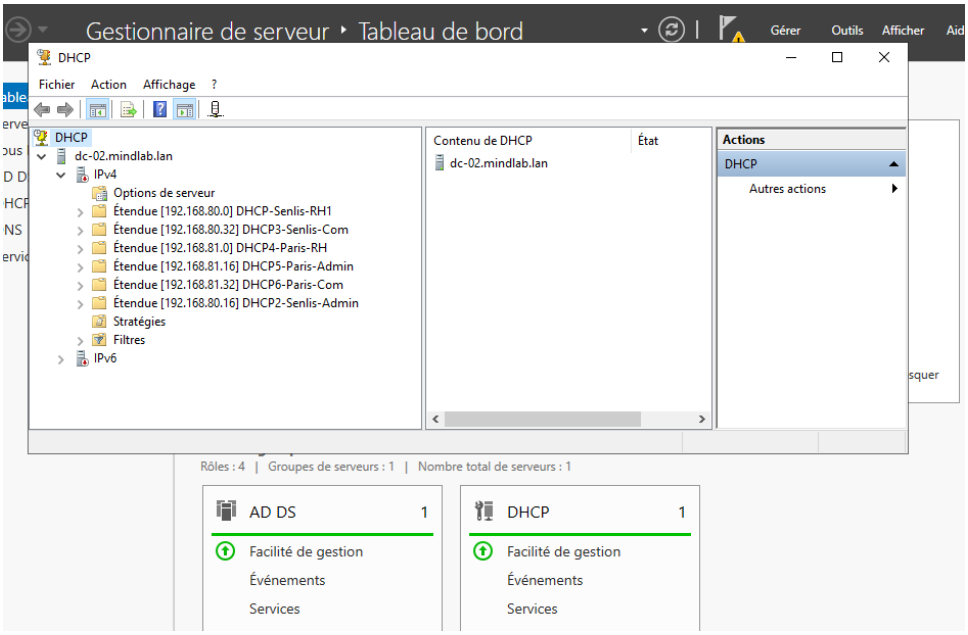


L'assistant exécute alors plusieurs actions automatiquement : création des étendues sur le serveur partenaire DC-02, désactivation temporaire du côté partenaire pendant la copie, mise en place de la configuration de basculement des deux côtés, puis activation finale. Le journal de progression confirme que chaque étape s'est déroulée avec succès :



6.3. Vérification du basculement

Pour valider le bon fonctionnement, j'ouvre la console DHCP du serveur DC-02. Toutes les étendues précédemment créées sur DC-01 y apparaissent avec les mêmes plages d'adresses, les mêmes options et le même statut actif :



La haute disponibilité du service DHCP est désormais opérationnelle. En cas d'arrêt de DC-01, DC-02 continuera à attribuer des adresses dans les six étendues, garantissant ainsi la continuité de service pour l'ensemble des postes de MindLab.

Pour aller plus loin :

Pour que les requêtes DHCP des sous-réseaux distants atteignent les serveurs DHCP, il est nécessaire de configurer le relai DHCP sur les routeurs (commande ip helper-address sur Cisco). Sur l'infrastructure MindLab, chaque interface VLAN des routeurs reçoit deux ip helper-address, pointant respectivement vers DC-01 (192.168.80.60) et DC-02 (192.168.81.60), afin que la redondance reste effective côté réseau.

VII. Stratégies de groupe

7.1. Présentation

Une stratégie de groupe, ou GPO (Group Policy Object), est un objet Active Directory qui regroupe un ensemble de paramètres applicables à des ordinateurs ou à des utilisateurs. Les GPO permettent à l'administrateur de centraliser et d'industrialiser la configuration des postes de travail, sans avoir à intervenir manuellement sur chaque machine.

Une GPO peut être liée à un site, à un domaine ou à une unité d'organisation. Lors de l'ouverture de session ou du démarrage du poste, le client interroge le contrôleur de domaine, récupère les GPO qui le concernent et applique les paramètres définis.

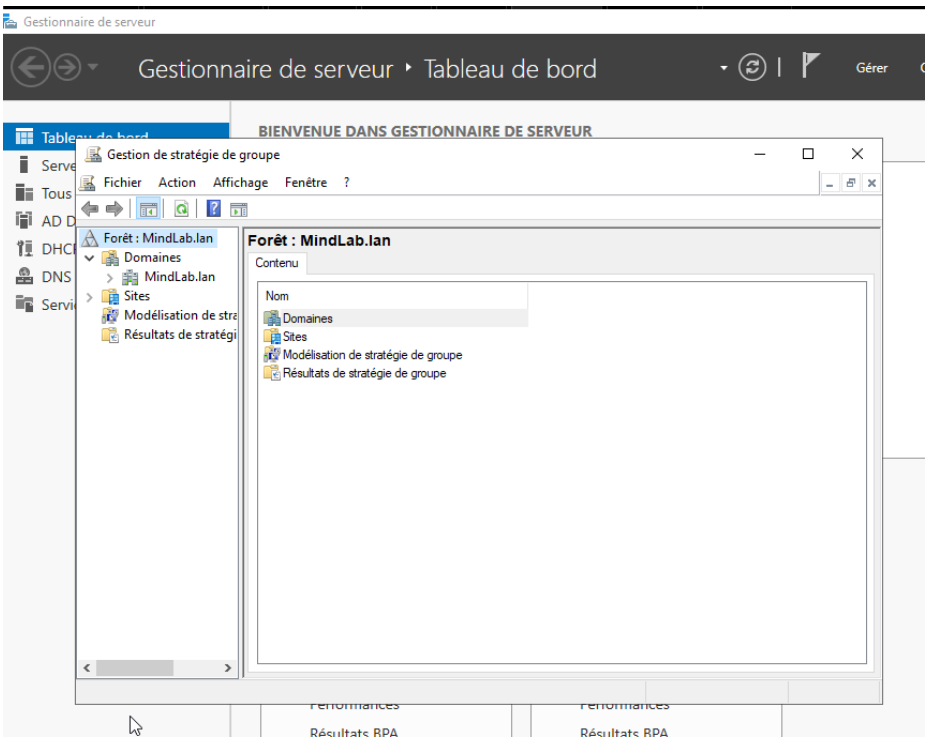
Les GPO se divisent en deux grandes catégories :

- La configuration ordinateur, qui s'applique à la machine quel que soit l'utilisateur connecté (paramètres système, sécurité, services)
- La configuration utilisateur, qui s'applique à l'utilisateur quel que soit le poste utilisé (préférences, redirections, mappages réseau, restrictions logicielles)

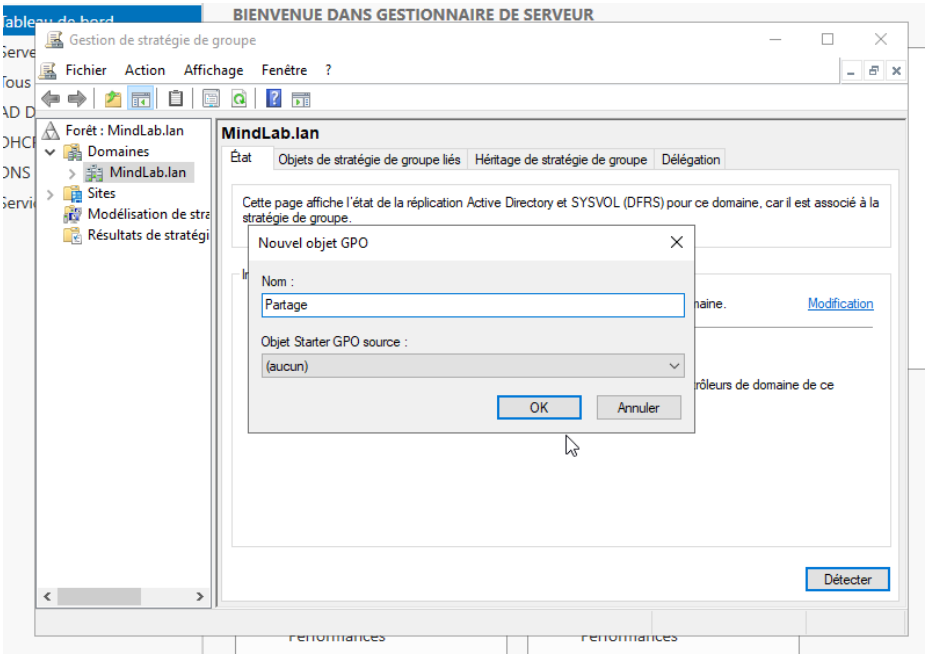
7.2. Création de la GPO « Partage »

Pour MindLab, je vais créer une première GPO destinée à automatiser le mappage du futur partage commun sur tous les postes du domaine. Cette GPO simplifiera l'accès aux ressources partagées et évitera aux utilisateurs de devoir saisir manuellement le chemin UNC.

Pour créer la GPO, j'ouvre la console « Gestion des stratégies de groupe » depuis le menu Outils du Gestionnaire de serveur. Je développe la forêt MindLab.lan, puis le domaine MindLab.lan.



Je fais un clic droit sur le domaine MindLab.lan et je sélectionne « Créer un objet GPO dans ce domaine, et le lier ici… ». Je nomme la nouvelle GPO « Partage » :



Une fois la GPO créée, je fais un clic droit dessus et je sélectionne « Modifier » pour ouvrir l'Éditeur de gestion des stratégies de groupe. Je navigue jusqu'au nœud Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs.

Je fais ensuite un clic droit sur la zone vide et je crée un nouveau lecteur mappé en spécifiant l'emplacement (\\MindLab.lan\Commun) et la lettre de lecteur (par exemple E:). À l'ouverture de session suivante, ou après un gpupdate /force, le lecteur réseau apparaît automatiquement dans l'explorateur Windows des postes du domaine.

7.3. Bonnes pratiques d'administration des GPO

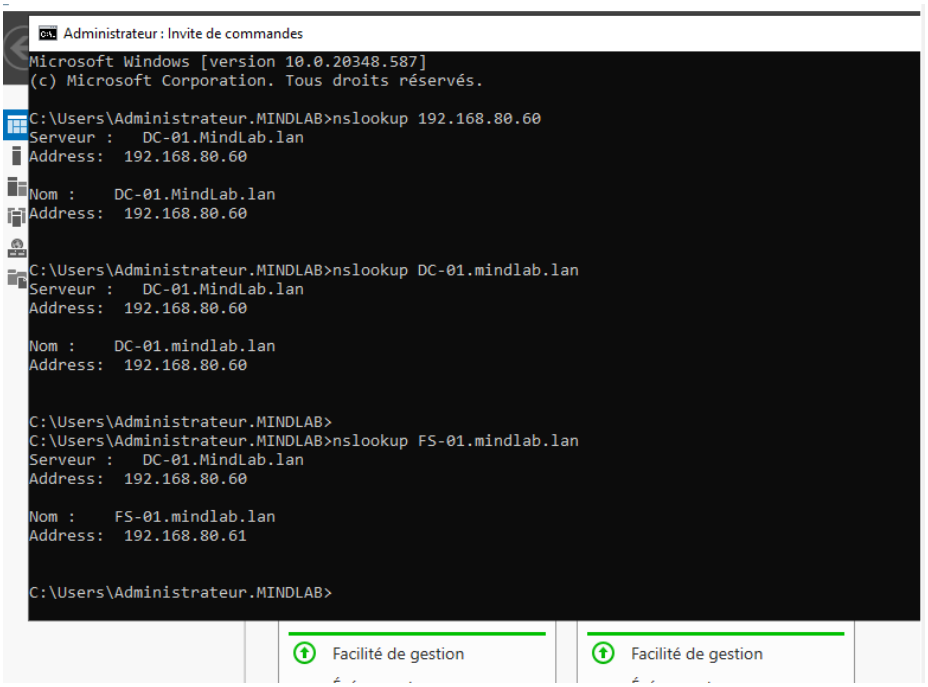
Lors de la création et de la maintenance des GPO, plusieurs bonnes pratiques permettent de garder une infrastructure saine :

- Nommer les GPO de façon explicite, en indiquant leur portée ou leur fonction (ex. : « Partage », « Verrouillage des comptes »)
- Ne pas modifier la GPO « Default Domain Policy », qui doit rester réservée aux paramètres globaux de sécurité (mots de passe, verrouillage)
- Lier les GPO au niveau le plus précis possible (OU plutôt que domaine) pour limiter leur portée
- Documenter chaque GPO et son objectif, afin de faciliter la reprise par un autre administrateur
- Tester les GPO sur un poste pilote avant leur déploiement à l'ensemble du parc

VIII. Vérifications et tests d'ensemble

8.1. Tests de résolution DNS

Pour valider la cohérence du déploiement, je réalise plusieurs tests de bout en bout depuis un poste joint au domaine. La commande nslookup permet d'interroger le service DNS et de vérifier que les noms des serveurs sont correctement résolus, dans les deux sens.



Le test confirme que le serveur DNS interrogé est bien DC-01.MindLab.lan (192.168.80.60) et que les requêtes directes et inversées retournent les bonnes correspondances. Le serveur de fichiers FS-01 est également résolu correctement à l'adresse 192.168.80.61.

8.2. Tests d'attribution DHCP

Sur un poste client, je libère puis renouvelle le bail DHCP avec les commandes ipconfig /release puis ipconfig /renew. Le poste obtient une adresse cohérente avec son VLAN, ainsi que la passerelle et les serveurs DNS attendus. La commande ipconfig /all confirme que le serveur DHCP ayant délivré le bail est bien DC-01 ou DC-02 selon la répartition.

Pour tester le basculement, j'éteins le contrôleur DC-01 et je relance un renouvellement de bail sur le poste : la requête est cette fois servie par DC-02, sans rupture pour l'utilisateur. La haute disponibilité fonctionne donc comme attendu.

8.3. Tests d'authentification

Je crée un compte utilisateur de test dans Active Directory, puis je tente une ouverture de session depuis un poste client. La connexion s'effectue avec succès, ce qui valide à la fois la configuration de l'annuaire, la résolution DNS du contrôleur et l'application des paramètres réseau via DHCP.

Pour tester la redondance, j'arrête DC-01 et je redémarre le poste client : l'ouverture de session continue à fonctionner, traitée cette fois par DC-02. C'est l'illustration concrète du bénéfice apporté par la mise en place d'un second contrôleur de domaine.

8.4. Bilan des tests

Synthèse des tests effectués :

Test	Attendu	Résultat
Résolution directe	Nom → IP correcte	OK
Résolution inverse	IP → Nom correct	OK
Attribution DHCP	Adresse, masque, passerelle, DNS	OK
Basculement DHCP	DC-02 prend le relais	OK
Ouverture de session	Authentification AD réussie	OK
Redondance AD	DC-02 traite l'authentification	OK
Application GPO	Lecteur réseau monté	OK

IX. Compétences BTS SIO travaillées

La réalisation de cette PPE m'a permis de mobiliser et de développer plusieurs compétences inscrites au référentiel du BTS SIO option SISR. Ces compétences sont regroupées ci-dessous selon les blocs de compétences de l'épreuve E5 « Administration des systèmes et des réseaux ».

9.1. Bloc 1 — Support et mise à disposition de services informatiques

Gérer le patrimoine informatique :

- Recensement des équipements et logiciels nécessaires à la mise en œuvre de l'infrastructure
- Documentation de la configuration matérielle et logicielle des serveurs DC-01, DC-02 et FS-01
- Tenue à jour de l'inventaire des comptes, groupes et unités d'organisation au sein d'Active Directory

Répondre aux incidents et aux demandes d'assistance :

- Diagnostic et résolution de l'erreur DNS rencontrée lors de la promotion de DC-02
- Mise en place d'outils de vérification (nslookup, ipconfig, gpupdate) pour le support quotidien

9.2. Bloc 2 — Administration des systèmes et des réseaux (SISR)

Concevoir une solution d'infrastructure réseau :

- Définition du plan d'adressage IP segmenté en /28 par service et par site
- Conception de l'architecture redondante avec deux contrôleurs de domaine et basculement DHCP
- Choix d'une zone DNS intégrée à AD pour bénéficier de la réplication multimaître

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

- Installation et configuration des rôles AD DS, DNS Server et DHCP Server sur Windows Server 2022
- Promotion des contrôleurs de domaine et création de la forêt MindLab.lan
- Mise en œuvre du basculement DHCP en mode équilibrage de charge 50/50
- Création et déploiement d'une stratégie de groupe (GPO) liée au domaine

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

- Vérification de la réplication AD et DNS entre DC-01 et DC-02
- Tests fonctionnels de bout en bout : DNS, DHCP, ouverture de session, application GPO
- Procédures de simulation de panne (arrêt d'un DC) pour valider la haute disponibilité

9.3. Compétences transversales

- Capacité à rédiger une documentation technique structurée et illustrée

- Maîtrise du vocabulaire spécifique aux infrastructures Microsoft (forêt, domaine, OU, GPO, etc.)
- Méthodologie de résolution d'incidents : observation → hypothèse → action corrective → vérification
- Lecture et interprétation des journaux d'événements et des messages d'erreur

X. Conclusion et bilan

10.1. Synthèse de la mission

À l'issue de cette PPE, j'ai pu mettre en place sur l'infrastructure fictive de la société MindLab une solution Active Directory complète et hautement disponible. L'ensemble des objectifs définis dans le cahier des charges a été atteint :

- Le contrôleur de domaine principal DC-01 a été déployé et la forêt MindLab.lan a été créée
- Le contrôleur de domaine secondaire DC-02 assure la redondance et la continuité de service
- Le service DNS dispose de zones directes et inversées intégrées à AD et répliquées entre les deux DC
- Le service DHCP couvre les six étendues correspondant aux services et aux sites de l'entreprise
- Le basculement DHCP est opérationnel en mode équilibrage de charge 50/50
- Une première GPO de mappage de lecteur a été créée et liée au domaine

10.2. Bilan personnel

Cette mission a constitué une opportunité particulièrement enrichissante de mettre en pratique les concepts vus en formation. La conception d'une infrastructure complète, depuis le plan d'adressage jusqu'au déploiement des stratégies de groupe, m'a permis de comprendre concrètement les interactions entre les différents services Microsoft : AD DS s'appuie sur DNS, DHCP communique des paramètres DNS, les GPO sont stockées dans AD et répliquées via le DNS, etc.

L'incident de résolution DNS rencontré lors de la promotion de DC-02 a été particulièrement formateur. Il m'a rappelé l'importance fondamentale du DNS dans une infrastructure AD et m'a confronté à la nécessité d'adopter une démarche méthodique de diagnostic : lire le message d'erreur attentivement, formuler une hypothèse, vérifier la configuration concernée, puis tester à nouveau.

La rédaction de cette documentation technique est également un exercice à part entière. Elle m'a obligé à prendre du recul sur les manipulations effectuées, à les structurer de façon logique et à les expliquer dans des termes accessibles. Une bonne documentation est un livrable au moins aussi important que la solution technique elle-même : c'est elle qui garantit la pérennité, la reprise en cas de départ d'un administrateur et l'évolution future de l'infrastructure.

10.3. Perspectives d'évolution

L'infrastructure mise en place constitue un socle solide qui pourra être enrichi par plusieurs évolutions :

- Mise en place du serveur de fichiers FS-01 avec partages communs et personnels (DFS Namespaces, droits NTFS et droits de partage)
- Déploiement de stratégies de groupe complémentaires : verrouillage des comptes, complexité des mots de passe, redirection de dossiers, restrictions logicielles

- Mise en place d'un service de sauvegarde planifiée pour la base AD et les partages de fichiers
- Intégration d'une solution de supervision (PRTG, Zabbix) pour surveiller l'état des contrôleurs et des services
- Renforcement de la sécurité par la mise en œuvre d'un PKI (Public Key Infrastructure) pour les certificats internes
- Étude d'une solution de fédération d'identité ou d'intégration avec un annuaire cloud (Microsoft Entra ID)

En définitive, cette PPE m'a permis non seulement de manipuler les principaux services d'une infrastructure Microsoft moderne, mais aussi de structurer ma démarche de technicien : conception, mise en œuvre, vérification et documentation. Ce sont ces quatre étapes que je m'efforcerai de respecter sur l'ensemble des projets à venir, qu'ils s'inscrivent dans le cadre de mon BTS ou dans un environnement professionnel.