

EK
NETSEC
LABS

PROJET AD REDONDANCE

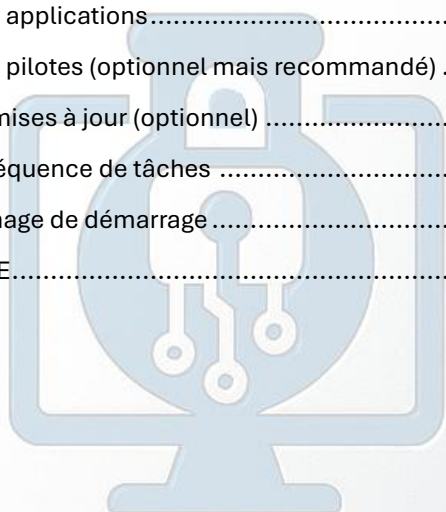
ELIAS KARISS © EK NETSEC LABS - TOUS DROITS RESERVES

Table des matières

Introduction du projet – Annuaire Active Directory avec redondance	4
Contexte	4
Objectifs pédagogiques	4
Périmètre technique (résumé)	4
Schéma d'architecture (SVG)	5
Plan d'adressage	5
Réseau Management (bridged) – <i>administration uniquement</i>	5
Réseau Labo isolé (Host-Only) – AD/DHCP/PXE/GPO	6
Plages DHCP par service (via Politiques DHCP)	6
Arborescence AD & Groupes (référence)	6
Unités d'Organisation (OU)	6
Groupes de sécurité (exemples, scope Global)	7
Conventions de nommage	7
GPO (principes à appliquer)	7
Notes de mise en œuvre (à suivre dans les chapitres)	7
Installation du premier serveur Windows – WIN-SRV-HOST-001	8
Vérifier le réseau VMware	8
Créer un nouveau réseau Host-Only :	8
Créer la machine virtuelle	9
Installation initiale de Windows Server	9
Renommer le serveur	10
Récupérer les informations réseau de l'hôte	11
Configurer les adresses IP statiques	11
Ethernet0 – Bridged (Management)	12
Ethernet1 – Host-Only (Labo AD)	13
Vérifier la connectivité	14
Installation et configuration des rôles sur WIN-SRV-HOST-001	15
Installation des rôles (préparation)	15
Promotion du serveur en contrôleur de domaine	15
Vérification du domaine	15
Configuration du DNS sur WIN-SRV-HOST-001	16
Vérifier la zone directe	16
Créer une zone de recherche inversée	16

Tester la résolution DNS	18
Configuration du DHCP sur WIN-SRV-HOST-001	19
Ouvrir la notification	19
Assistant de post-déploiement.....	19
Vérifier l'autorisation DHCP	20
Création d'une étendue DHCP (Scope)	21
Ouvrir la console DHCP.....	21
Assistant de nouvelle étendue	21
Définir les exclusions	22
Durée du bail	22
Configurer les options DHCP	22
Activer l'étendue	23
Créer les stratégies par service	23
Structuration d'Active Directory – OU, Groupes et Utilisateurs	24
Créer l'arborescence des unités d'organisation	24
Créer les groupes de sécurité	27
Déléguer les droits aux chefs de service.....	28
Préparer le fichier CSV des utilisateurs	31
Importer les utilisateurs	32
Partie GPO (Fond d'écran).....	34
Installer une VM cliente pour les tests	34
Créer un dossier partagé pour les GPO	35
Partie GPO (Déploiement logiciels & Agents)	40
Préparer les fichiers MSI.....	40
Mise en place de WSUS	43
Installation du rôle WSUS.....	43
Configuration post-installation	43
Création des groupes WSUS.....	46
Mise en place de la redondance AD/DNS/DHCP	50
Préparer la VM WIN-SRV-HOST-2	50
Joindre la machine au domaine	50
Promouvoir en contrôleur de domaine secondaire.....	51
Vérifier la réplication AD & DNS	52
Mise en place du DHCP en redondance (Failover).....	55
Étapes de vérification	57
Mise en place de DNSSEC	57

Préparer l'environnement DNSSEC	57
Signer la zone DNS	57
Réplication sur le second DC	59
Configurer une GPO pour appliquer DNSSEC sur les postes clients	59
Sécurisation du service DHCP	61
Afficher les baux d'adresses actifs	61
Autoriser un hôte spécifique	62
Déploiement PXE (WDS + MDT)	64
Installer le rôle WDS	64
Configurer WDS.....	64
Installer et configurer MDT (Microsoft Deployment Toolkit)	67
Importer le système d'exploitation	67
Importer les applications.....	68
Importer les pilotes (optionnel mais recommandé)	69
Ajouter les mises à jour (optionnel)	69
Créer une séquence de tâches	69
Générer l'image de démarrage.....	71
Démarrage PXE.....	72



EK
NETSEC
LABS

INTRODUCTION DU PROJET – ANNUAIRE ACTIVE DIRECTORY AVEC REDONDANCE

CONTEXTE

- Créer un environnement de test proche d'une production afin de :
- Tester des scripts et des automatisations.
- S'entraîner à la redondance AD/DNS et à la continuité de service.
- Mettre en place un déploiement PXE et des GPO orientées métier.
- Construire un socle de supervision (état des postes, services, journaux) et un plan de sauvegarde.

OBJECTIFS PEDAGOGIQUES

- Concevoir une architecture AD redondée et sécurisée.
- Installer, configurer et valider AD DS, DNS, DHCP, WSUS, WDS/PXE, DNSSEC.
- Structurer l'arborescence AD (OU, groupes, délégations, GPO par service).
- Automatiser l'approvisionnement utilisateurs/Groupes (PowerShell, CSV) et le déploiement applicatif (GPO).
- Déployer une mini-application Python (GUI) pour déléguer l'ajout/suppression d'utilisateurs aux chefs de service.
- Mettre en place la supervision (agent Zabbix) et la sauvegarde (serveur Linux).
- Valider la tolérance aux pannes et le plan de tests (bascule DC, PXE, GPO, scripts).

PERIMETRE TECHNIQUE (RESUME)

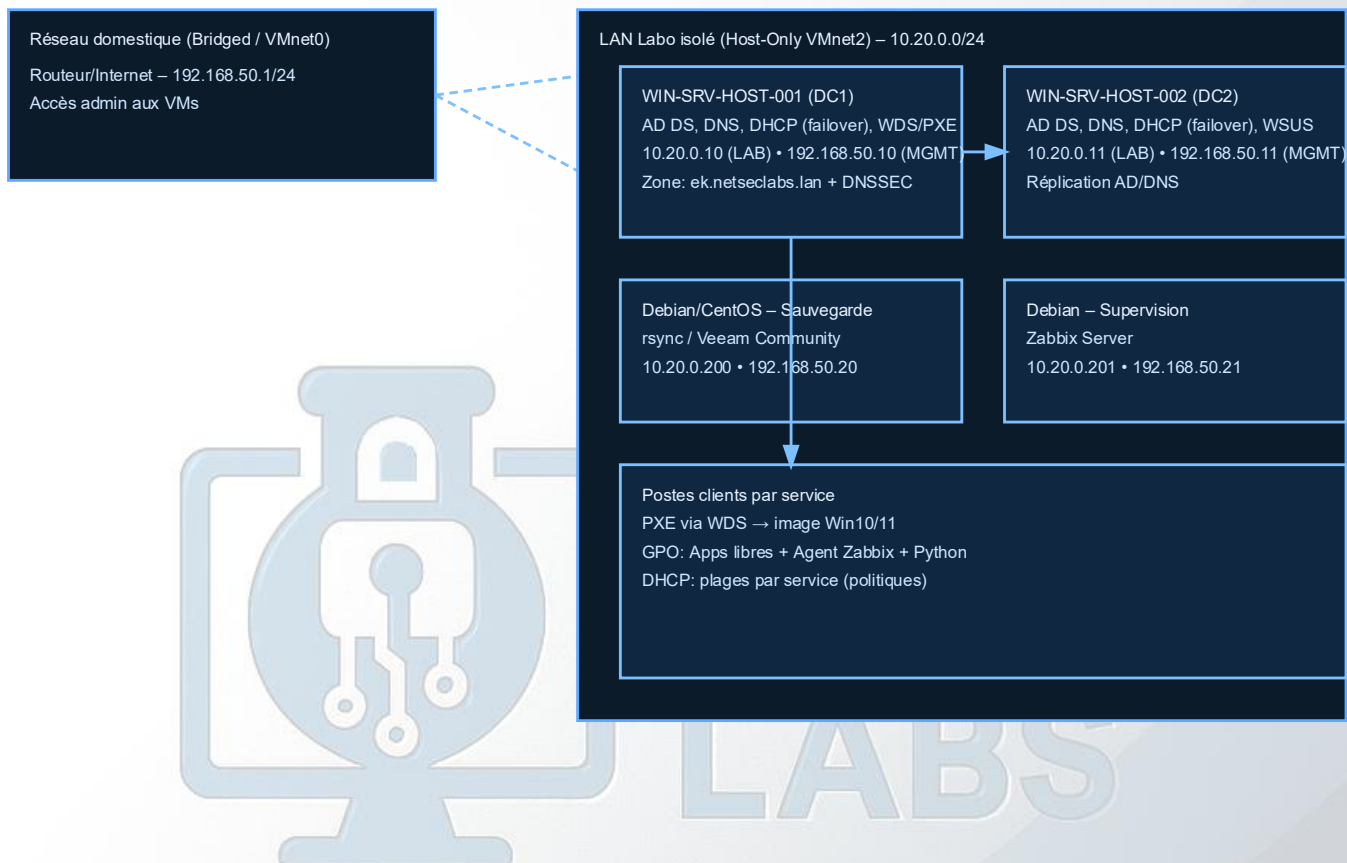
- Hyperviseur : VMware (interfaces bridgées VMnet0 pour la gestion ; + réseau labo isolé recommandé pour DHCP/PXE).
- Domaine : ek.netseclabs.lan.
- DC1 : WIN-SRV-HOST-001 – AD DS, DNS, DHCP (failover), WDS/PXE.
- DC2 : WIN-SRV-HOST-002 – AD DS, DNS, DHCP (failover), WSUS.
- Linux : Backup (rsync/veeam community) + Zabbix Server (ou équivalent).

⚠ Bonnes pratiques en labo :

Conserver une NIC bridgée pour l'administration.

Ajouter une NIC "Host-Only" (réseau isolé) pour DHCP/PXE, afin d'éviter tout conflit avec le DHCP du réseau domestique.

SCHEMA D'ARCHITECTURE (SVG)



PLAN D'ADRESSAGE

Réseau Management (bridged) – *administration uniquement*

Sous-réseau : 192.168.1.0/24

Passerelle : 192.168.1.254

DNS pour MGMT : 192.168.1.254 et 1.1.1.1

Hôte	Nom	IP (MGMT)	Remarques
DC1	WIN-SRV-HOST-001	192.168.1.10	Accès RDP/gestion
DC2	WIN-SRV-HOST-002	192.168.1.11	Accès RDP/gestion
Backup	(Debian/CentOS)	192.168.1.20	Sauvegardes
Zabbix	(Debian)	192.168.1.21	Supervision

Astuce : conserver ce réseau sans DHCP côté Windows pour éviter tout conflit avec le routeur domestique.

Réseau Labo isolé (Host-Only) – AD/DHCP/PXE/GPO

- Sous-réseau : 10.20.0.0/24
- Passerelle : 10.20.0.1
- DNS (clients) : 10.20.0.10, 10.20.0.11
- Réservations/Infra statiques :
 - DC1 : 10.20.0.10
 - DC2 : 10.20.0.11
 - WSUS (sur DC2) : 10.20.0.20
 - Backup : 10.20.0.200
 - Zabbix : 10.20.0.201

PLAGES DHCP PAR SERVICE (VIA POLICIES DHCP)

Créer un scope unique 10.20.0.0/24 et des plages/politiques par service (conditions possibles : préfixes MAC de tes VMs, classes utilisateur, Option 60/82 en labo).

Service	Plage	Taille approx.
Informatique (Admins/Techs)	10.20.0.32 – 10.20.0.63	/27 (~30 hôtes)
Commercial	10.20.0.64 – 10.20.0.95	/27
Marketing	10.20.0.96 – 10.20.0.127	/27
Production	10.20.0.128 – 10.20.0.159	/27
RH	10.20.0.160 – 10.20.0.191	/27
Direction	10.20.0.192 – 10.20.0.223	/27

- Exclusions réservées : 10.20.0.1–.31 (infra/routeur), .224–.254 (appliances/tests).
- Options DHCP :
 - 003 Router : 10.20.0.1
 - 006 DNS : 10.20.0.10, 10.20.0.11
 - 015 Suffixe DNS : ek.netseclabs.lan
 - 066/067 PXE : nom/IP du WDS (DC1) / boot\lx64\wdnsnbp.com

ARBORESCENCE AD & GROUPES (REFERENCE)

Unités d'Organisation (OU)

- OU=0-Infrastructure (Serveurs, Comptes de service, GPO de sécurité)
- OU=1-Postes (par service : IT, Commercial, Marketing, Production, RH, Direction)
- OU=2-Utilisateurs
 - OU=IT
 - OU=Commercial
 - OU=Marketing
 - OU=Production
 - OU=RH
 - OU=Direction
- OU=3-Groupes (sécurité & distribution)
- OU=4-Policies (liens GPO, staging)

Groupes de sécurité (exemples, scope Global)

- GG-IT-Admins, GG-IT-Techs (*droits d'admin sur postes/OU IT*)
- GG-COM-Users, GG-MKT-Users, GG-PRD-Users, GG-RH-Users, GG-DIR-Users
- GG-IT-Chefs, GG-COM-Chefs, ... (*droit délégué d'ajout/suppression d'utilisateurs dans leur OU via l'app Python*)

Déléguer les droits à l'OU [Service] : Créer/Supprimer comptes utilisateurs, Réinitialiser mot de passe, Ajouter au groupe [Service].

Conventions de nommage

Postes : `EK-[SRV|PC]-[SERVICE]-####` (ex. `EK-PC-IT-0001`)

Utilisateurs : `prenom.nom` (login), UPN `prenom.nom@ek.netseclabs.lan`

Groupes : `GG-[SERVICE]-[Role]`

Partages : `\\\\fs\\PROFIL\\%username%`, `\\\\fs\\DONNEES\\[Service]`

GPO (PRINCIPES A APPLIQUER)

- Base sécurité : verrouiller SMBv1, pare-feu, NTP DC, mots de passe, RDP, journaux.
- Fond d'écran par service (branding labo).
- Applications libres (exemples) :
 - IT : 7-Zip, Git, Notepad++, RSAT
 - Commercial : LibreOffice, SumatraPDF
 - Marketing : GIMP, Inkscape, VLC
 - Production : VLC, 7-Zip
 - RH/Direction : LibreOffice, SumatraPDF
- Agent supervision : Zabbix Agent (service, clé auto, serveur 10.20.0.201).
- Python + App GUI : installer Python (x64), déposer l'app (Tkinter/PySimpleGUI), publier un raccourci GPO aux chefs de service.

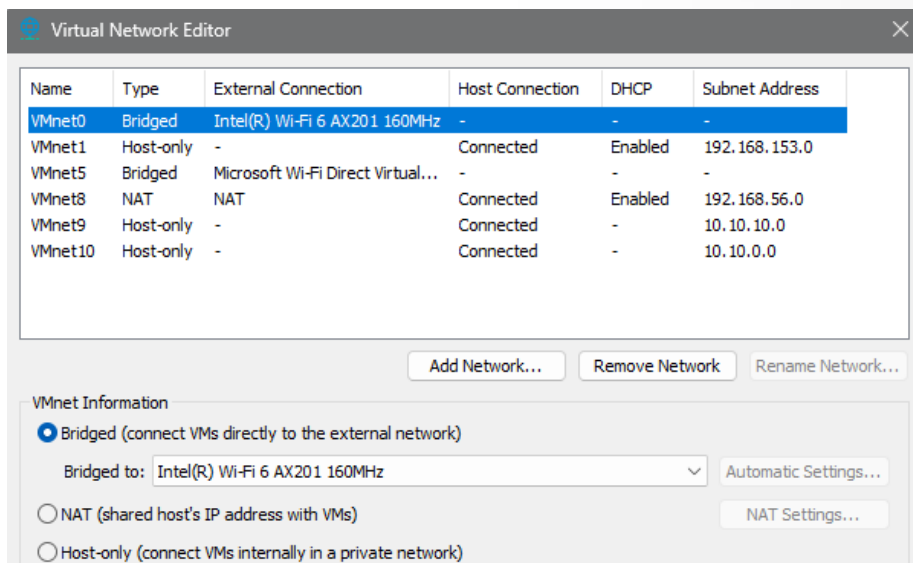
NOTES DE MISE EN ŒUVRE (A SUIVRE DANS LES CHAPITRES)

- Installer les VMs et attribuer les IP statiques.
- Promouvoir DC1 (création du domaine), puis DC2 (réplication).
- Configurer DHCP failover (load-balance 50/50 ou hot-standby 80/20).
- Activer DNSSEC (signature de zone ek.netseclabs.lan).
- Installer WDS/PXE (intégration AD, boot images Win10/11).
- Déployer WSUS (approbations par groupes de postes).
- Mettre en service Zabbix & Backup.
- Rédiger et tester les scripts PowerShell (groupes, utilisateurs, CSV).

INSTALLATION DU PREMIER SERVEUR WINDOWS – WIN-SRV-HOST-001

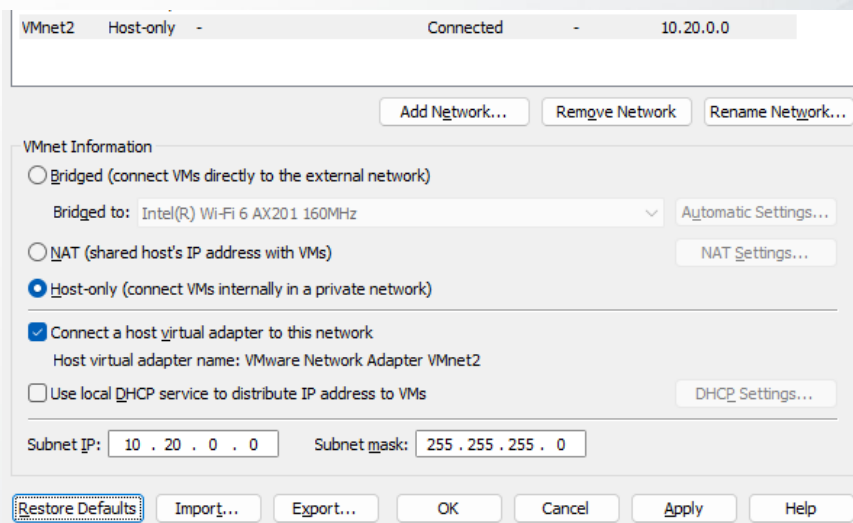
VERIFIER LE RESEAU VMWARE

- Ouvrir **Virtual Network Editor**.
- Vérifier que **VMnet0** est configuré en mode **Bridged** et relié à la carte réseau physique de l'hôte (Intel AX201).
- S'assurer que VMnet0 n'a pas de DHCP activé.



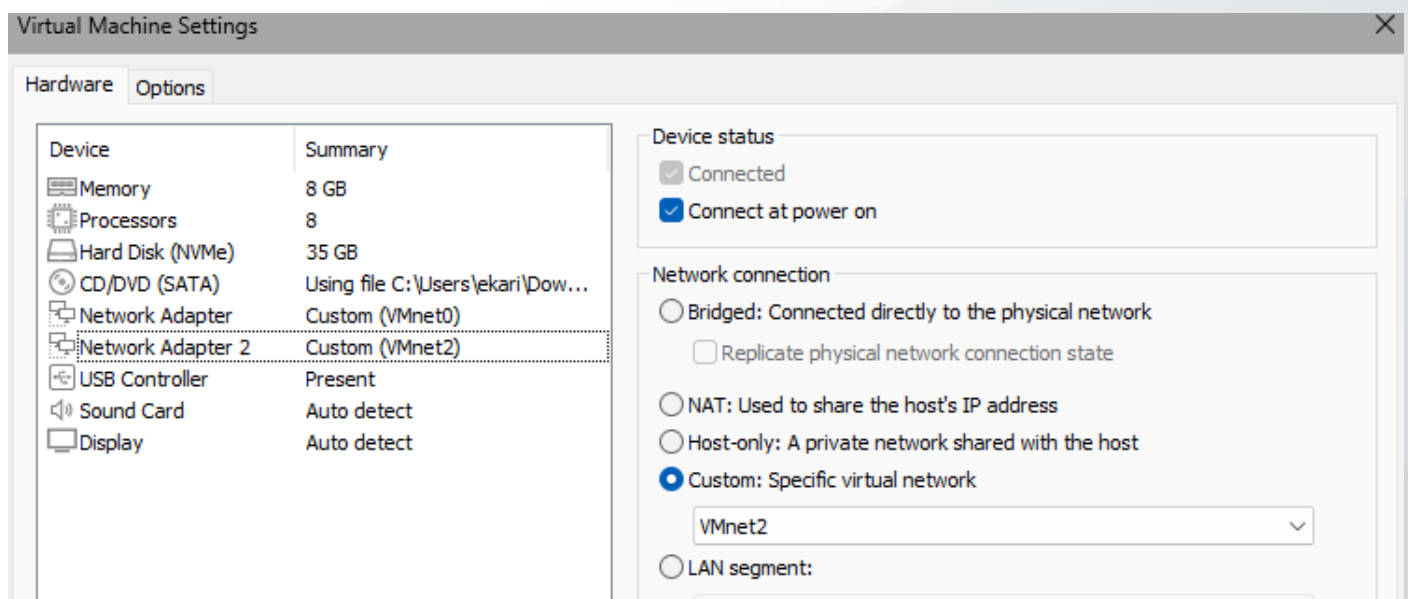
Créer un nouveau réseau Host-Only :

- Cliquer sur **Add Network** → choisir **VMnet2**.
- Sélectionner **Host-Only (connect VMs internally in a private network)**.
- Désactiver le **DHCP VMware** pour VMnet2 (c'est le serveur Windows qui jouera ce rôle).
- Définir le **Subnet IP** : 10.20.0.0 / 255.255.255.0.



CREER LA MACHINE VIRTUELLE

- Ouvrir **VMware Workstation**.
- Créer une nouvelle VM.
- Sélectionner l'ISO **Windows Server 2022 Standard**.
- Allouer les ressources :
 - **Mémoire** : 8 Go.
 - **Processeurs** : 8 cœurs.
 - **Disque** : 35 Go.
- Ajouter deux cartes réseau à la VM :
 - Carte 1 → **Custom : VMnet0 (Bridged)**.
 - Carte 2 → **Custom : VMnet2 (Host-Only)**.

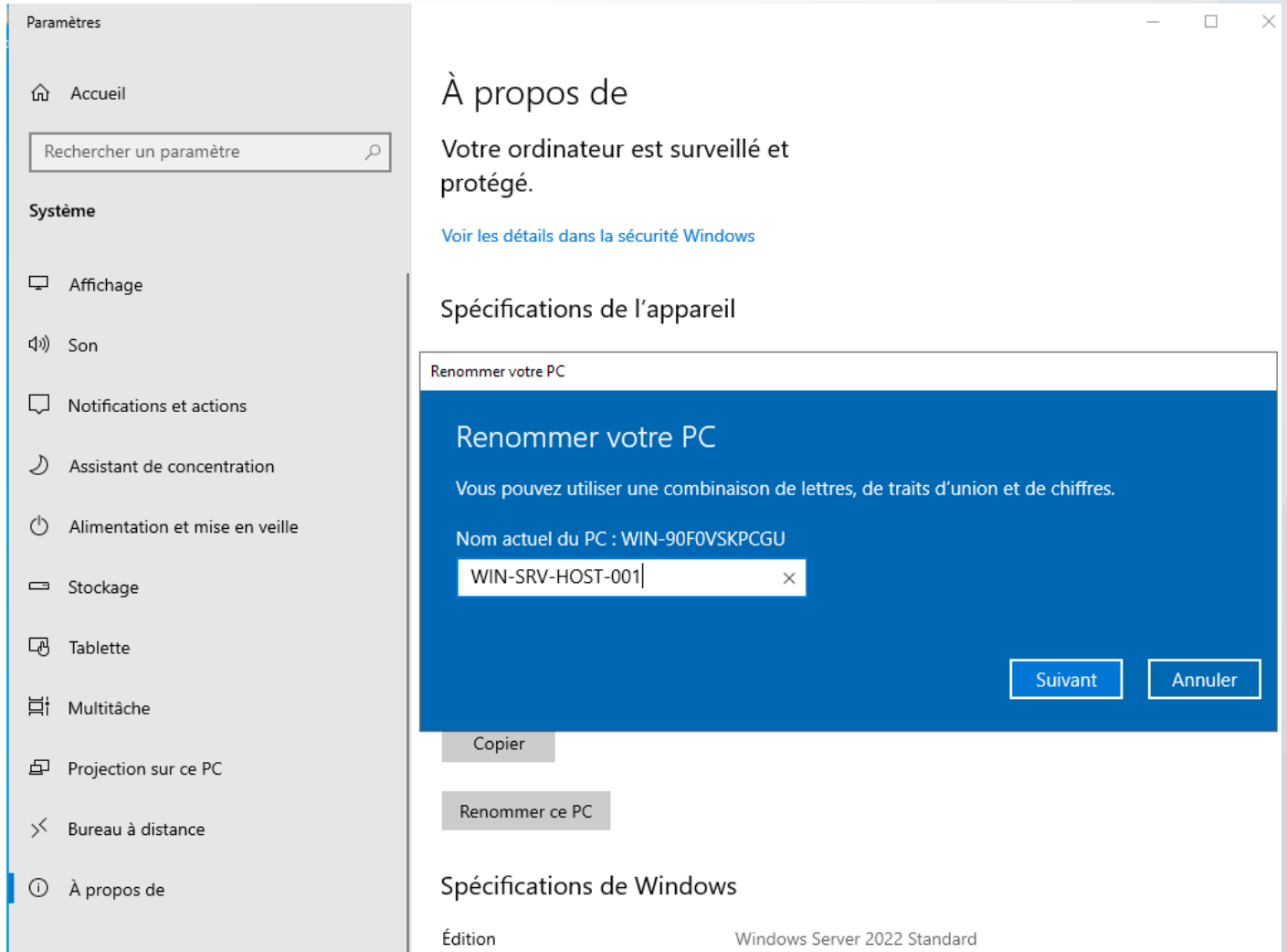


INSTALLATION INITIALE DE WINDOWS SERVER

- Démarrer la VM et installer **Windows Server 2022 Standard**.
- Lors de l'installation, choisir :
 - **Standard (Desktop Experience)** pour bénéficier de l'interface graphique.
 - Créer un mot de passe administrateur fort.

RENOMMER LE SERVEUR

- Aller dans **Paramètres** → **Système** → **À propos de** → **Renommer ce PC**.
- Nommer le serveur : **WIN-SRV-HOST-001**.
- Redémarrer pour appliquer.



The screenshot shows the Windows Settings application. On the left, the 'Paramètres' sidebar is visible with the 'À propos de' (About) option selected. The main content area displays the 'À propos de' (About) page. A dialog box titled 'Renommer votre PC' (Rename your PC) is open, showing the current PC name 'WIN-90F0VSKPCGU' and the new name 'WIN-SRV-HOST-001' entered in the text field. The dialog has 'Suivant' (Next) and 'Annuler' (Cancel) buttons. Below the dialog, there are buttons for 'Copier' (Copy) and 'Renommer ce PC' (Rename this PC). The 'Spécifications de Windows' (Windows specifications) section at the bottom shows the edition as 'Windows Server 2022 Standard'.

RECUPERER LES INFORMATIONS RESEAU DE L'HOTE

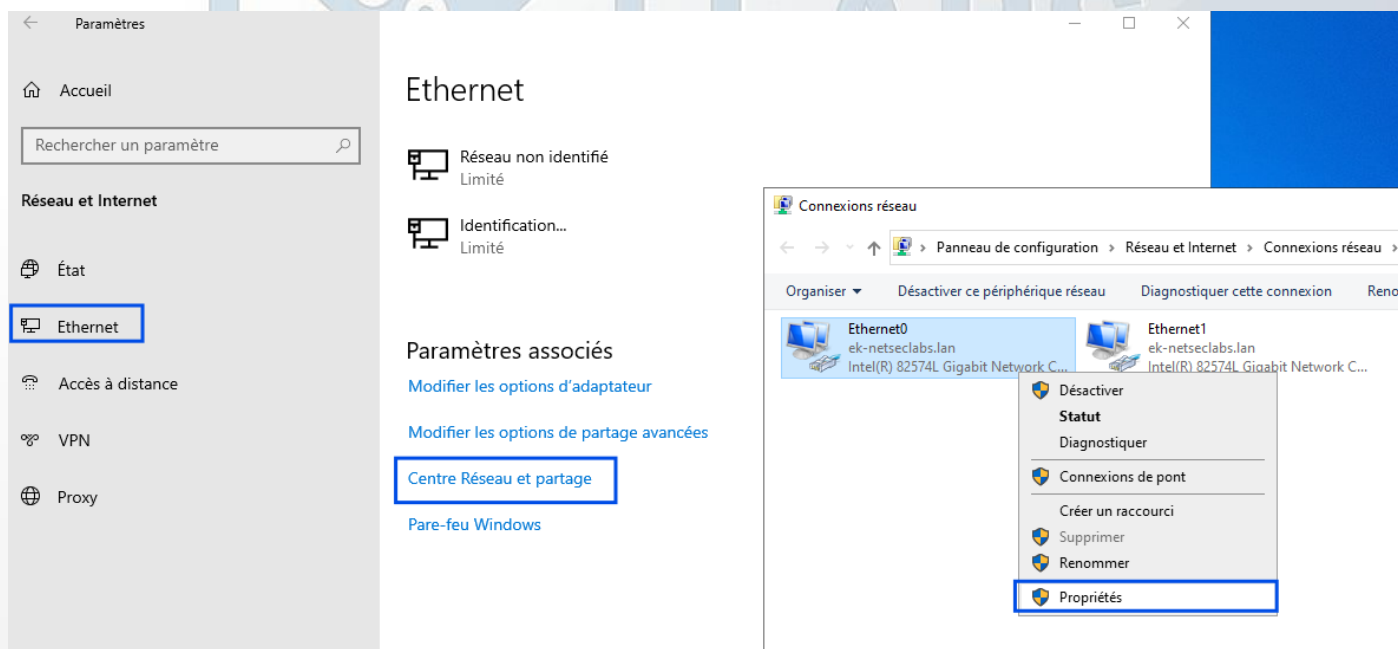
- Sur le PC hôte, lancer ipconfig.
- Noter :
 - Adresse IPv4 hôte : ex. 192.168.1.130.
 - Passerelle par défaut : ex. 192.168.1.254.
 - Masque : 255.255.255.0.

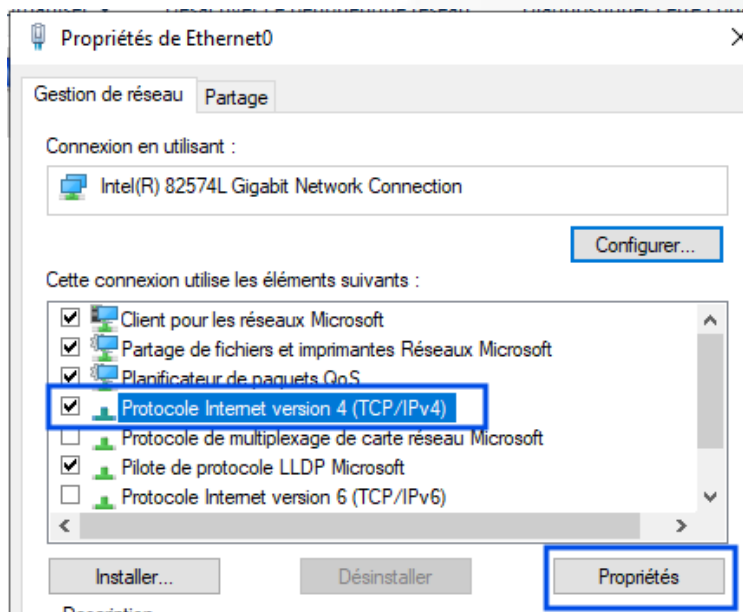
Carte réseau sans fil Wi-Fi :

```
Suffixe DNS propre à la connexion. . . : lan
Adresse IPv6. . . . . : 2001:861:4d00:1320:a208:736:db91:987e
Adresse IPv6 temporaire . . . . . : 2001:861:4d00:1320:cc5b:6b2e:5904:59df
Adresse IPv6 de liaison locale. . . . : fe80::f606:1a04:b519:661c%3
Adresse IPv4. . . . . : 192.168.1.130
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : fe80::22b8:2bff:fe43:1025%3
                                192.168.1.254
```

CONFIGURER LES ADRESSES IP STATIQUES

- Ouvrir **ncpa.cpl** (Connexions réseau).
- Identifier les deux cartes :
 - **Ethernet0 (Bridged)** → accès Internet / administration.
 - **Ethernet1 (Host-Only)** → réseau interne labo.

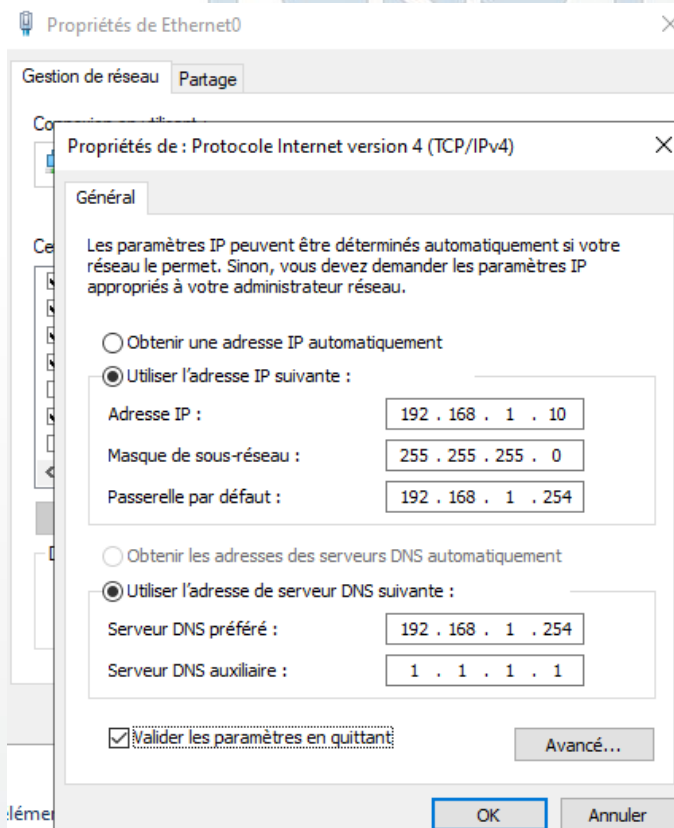




Configurer ainsi :

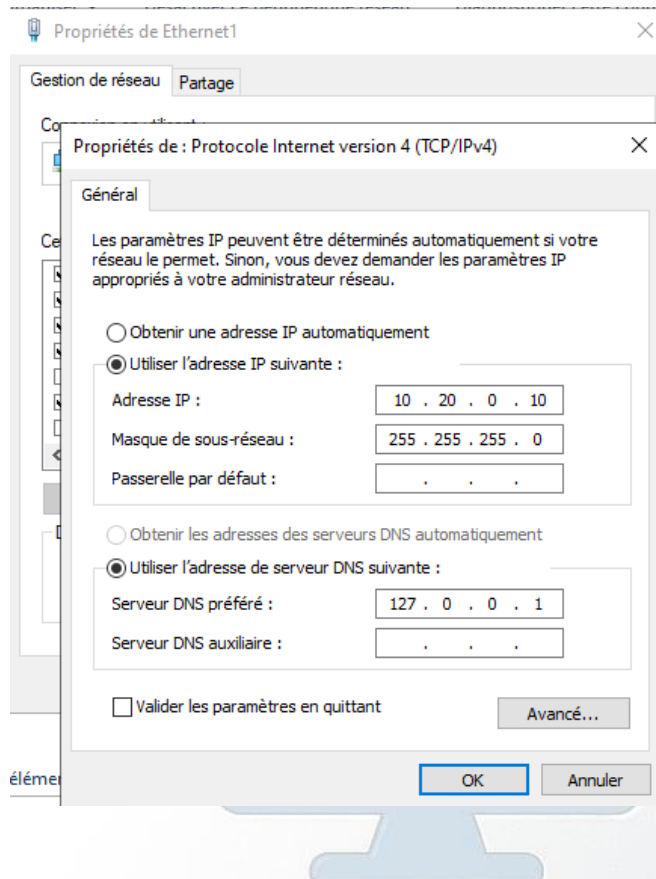
Ethernet0 – Bridged (Management)

- Adresse IP : 192.168.1.10
- Masque : 255.255.255.0
- Passerelle : 192.168.1.254 (la box/routeur)
- DNS préféré : **192.168.1.254** (ou DNS public type 1.1.1.1 pour Internet).



Ethernet1 – Host-Only (Labo AD)

- Adresse IP : 10.20.0.10
- Masque : 255.255.255.0
- Passerelle : *(laisser vide – réseau isolé)*
- DNS préféré : 127.0.0.1 (à utiliser une fois le rôle AD/DNS installé).



EK
NETSEC
LABS

Vérifier la connectivité

- Depuis la VM :
 - Ping la **passerelle** (192.168.1.254) → doit répondre.
 - Ping une IP publique (8.8.8.8) → doit répondre.
 - Tester la résolution DNS (ping google.com) → doit répondre via le DNS de la carte bridged.

CA: Administrateur : Invite de commandes

```
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping 192.168.1.254

Envoi d'une requête 'Ping' 192.168.1.254 avec 32 octets de données :
Réponse de 192.168.1.254 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=11 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=11 ms TTL=64

Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 11ms, Moyenne = 6ms

C:\Users\Administrateur>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=15 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=116
Réponse de 8.8.8.8 : octets=32 temps=12 ms TTL=116

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 15ms, Moyenne = 10ms

C:\Users\Administrateur>ping google.com

Envoi d'une requête 'ping' sur google.com [142.250.179.110] avec 32 octets de données :
Réponse de 142.250.179.110 : octets=32 temps=7 ms TTL=115
Réponse de 142.250.179.110 : octets=32 temps=23 ms TTL=115
Réponse de 142.250.179.110 : octets=32 temps=9 ms TTL=115
Réponse de 142.250.179.110 : octets=32 temps=9 ms TTL=115

Statistiques Ping pour 142.250.179.110:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 23ms, Moyenne = 12ms

C:\Users\Administrateur>
```

INSTALLATION ET CONFIGURATION DES ROLES SUR WIN-SRV-HOST-001

INSTALLATION DES ROLES (PREPARATION)

- Ouvrir le **Gestionnaire de serveur**.
- Cliquer sur **Ajouter des rôles et fonctionnalités**.
- Sélectionner les rôles nécessaires pour l'infrastructure (à configurer plus tard) :
 - **AD DS** (Active Directory Domain Services)
 - **DNS Server**
 - **DHCP Server**
 - **WDS (Windows Deployment Services)**
 - **WSUS (Windows Server Update Services)**
 - **Services de fichiers et de stockage**
 - **IIS (Internet Information Services)** (utilisé par WSUS)
 - **Accès à distance** (VPN/RRAS si besoin plus tard)
- Laisser l'installation se faire, redémarrer si demandé.

👉 Remarque : les rôles sont installés en amont pour **gagner du temps**. La configuration détaillée (DNS, DHCP, WSUS, WDS, GPO, etc.) sera réalisée ultérieurement.

PROMOTION DU SERVEUR EN CONTROLEUR DE DOMAINE

- Dans le **Gestionnaire de serveur**, cliquer sur la notification « Ce serveur doit être promu en contrôleur de domaine ».
- Sélectionner **Ajouter une nouvelle forêt**.
- Nommer la forêt et le domaine racine : **ek-netseclabs.lan**.
- Définir le mot de passe DSRM (Directory Services Restore Mode).
- Laisser les options par défaut pour :
 - Niveau fonctionnel forêt et domaine (**Windows Server 2016 ou plus**).
 - Installation du serveur DNS.
- Vérifier les prérequis et lancer l'installation.
- Redémarrer automatiquement à la fin du processus.

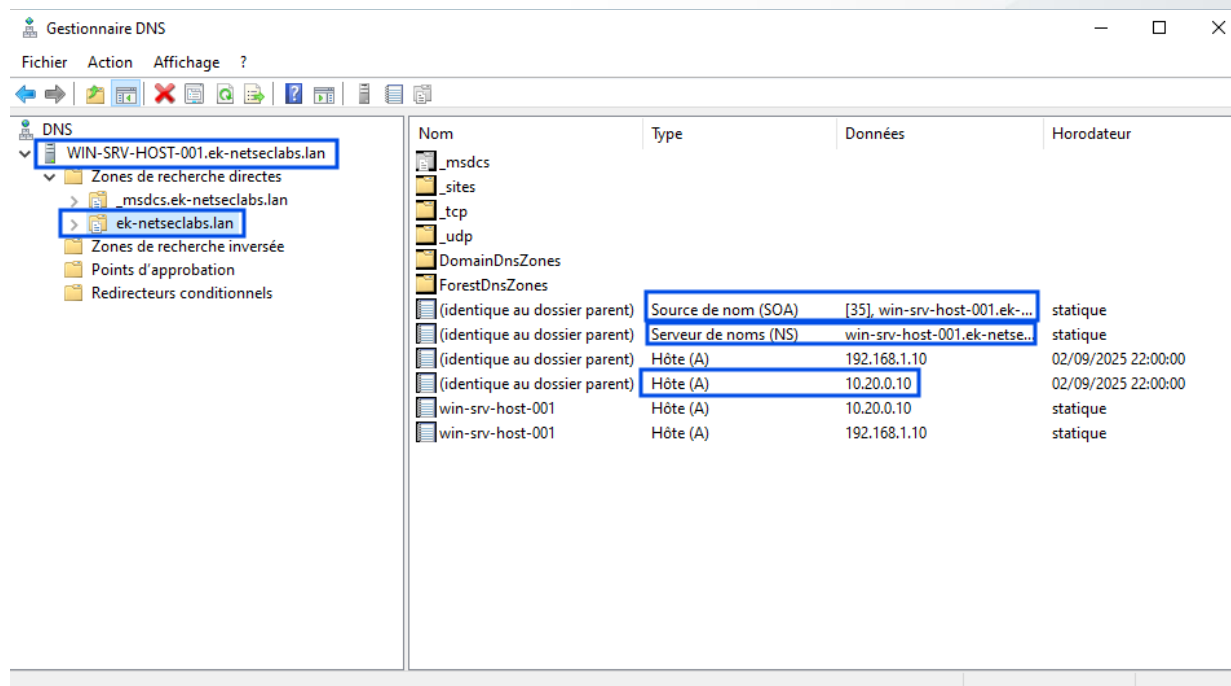
VERIFICATION DU DOMAINE

- Ouvrir **Utilisateurs et ordinateurs Active Directory** (dsa.msc).
- Vérifier la présence du domaine **ek-netseclabs.lan**.
- Confirmer que le contrôleur de domaine est bien enregistré.

CONFIGURATION DU DNS SUR WIN-SRV-HOST-001

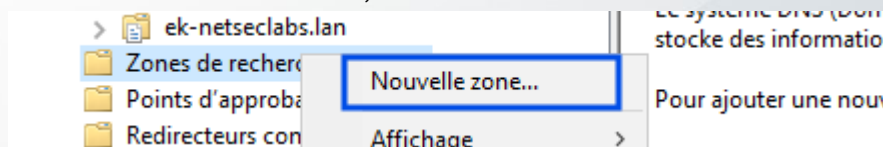
VERIFIER LA ZONE DIRECTE

- Ouvrir **Gestionnaire DNS** (dnsmgmt.msc).
- Déployer le serveur **WIN-SRV-HOST-001**.
- Vérifier que la zone **ek-netseclabs.lan** est présente.
- Vérifier que les enregistrements suivants existent :
 - (A) **DC1** → **10.20.0.10**
 - (NS) **WIN-SRV-HOST-001.ek-netseclabs.lan**
 - (SOA) **Start of Authority**

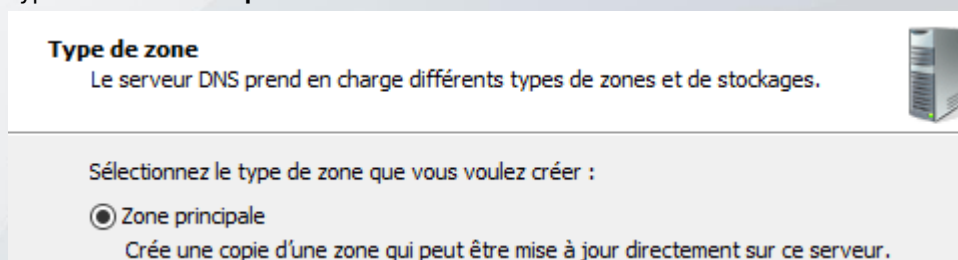


CREER UNE ZONE DE RECHERCHE INVERSEE

- Dans le **Gestionnaire DNS**, clic droit sur **Zones de recherche inversée** → **Nouvelle zone**.



- Suivre l'assistant :
 - Type de zone : **Principale**.



- Réplication : **Vers tous les contrôleurs de domaine de la forêt.**

Étendue de la zone de réplication de Active Directory

Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.



Choisissez la façon dont les données de la zone doivent être répliquées :

- ☐ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : ek-netsec labs.lan
- ☒ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : ek-netsec labs.lan

- ID réseau : 10.20.0 (correspond au réseau Host-Only).

Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

- ☒ ID réseau :

10 .20 .0

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

- ☐ Nom de la zone de recherche inversée :

0.20.10.in-addr.arpa

- Autoriser les mises à jour dynamiques sécurisées.

Mise à niveau dynamique

Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.



Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.

Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

- ☒ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.
- ☐ Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées

- Vérifier que la zone **0.20.10.in-addr.arpa** apparaît.

Gestionnaire DNS

Fichier Action Affichage ?



DNS	Nom	Type	État	État DNSSEC
WIN-SRV-HOST-001.ek-netsec labs.lan	0.20.10.in-addr.arpa	Serveur principal intégré à Act...	En cours d'e...	Non signé
Zones de recherche directes				

TESTER LA RESOLUTION DNS

- Ouvrir une invite de commandes sur **DC1**.
- Lancer :

```
nslookup WIN-SRV-HOST-001.ek-netseclabs.lan
nslookup 10.20.0.10
```

```
C:\Users\Administrateur>nslookup WIN-SRV-HOST-001.ek-netseclabs.lan
Serveur : dns.google
Address: 8.8.8.8

*** dns.google ne parvient pas à trouver WIN-SRV-HOST-001.ek-netseclabs.lan : Non-existent domain

C:\Users\Administrateur>nslookup 10.20.0.10
Serveur : dns.google
Address: 8.8.8.8

*** dns.google ne parvient pas à trouver 10.20.0.10 : Non-existent domain

C:\Users\Administrateur>
```

Propriétés de : win-srv-host-001 ? X

Hôte local (A) Sécurité

Hôte (utilise le domaine parent si ce champ est vide) :

win-srv-host-001

Nom de domaine pleinement qualifié (FQDN) :

win-srv-host-001.ek-netseclabs.lan

Adresse IP :

10.20.0.10

☒ Mettre à jour l'enregistrement de pointeur (PTR) associé

Cocher **Mettre à jour enregistrement de pointeur associé (PTR)**

```
C:\Users\Administrateur>nslookup 10.20.0.10
Serveur : localhost
Address: 127.0.0.1

Nom : win-srv-host-001.ek-netseclabs.lan
Address: 10.20.0.10

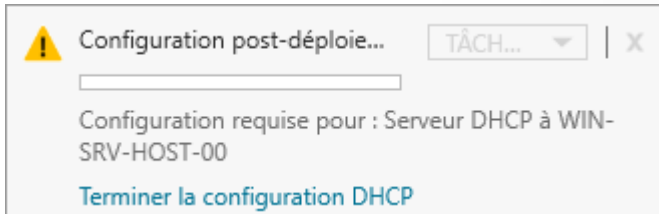
C:\Users\Administrateur>nslookup WIN-SRV-HOST-001.ek-netseclabs.lan
Serveur : localhost
Address: 127.0.0.1

Nom : WIN-SRV-HOST-001.ek-netseclabs.lan
Addresses: 192.168.1.10
           10.20.0.10
```

CONFIGURATION DU DHCP SUR WIN-SRV-HOST-001

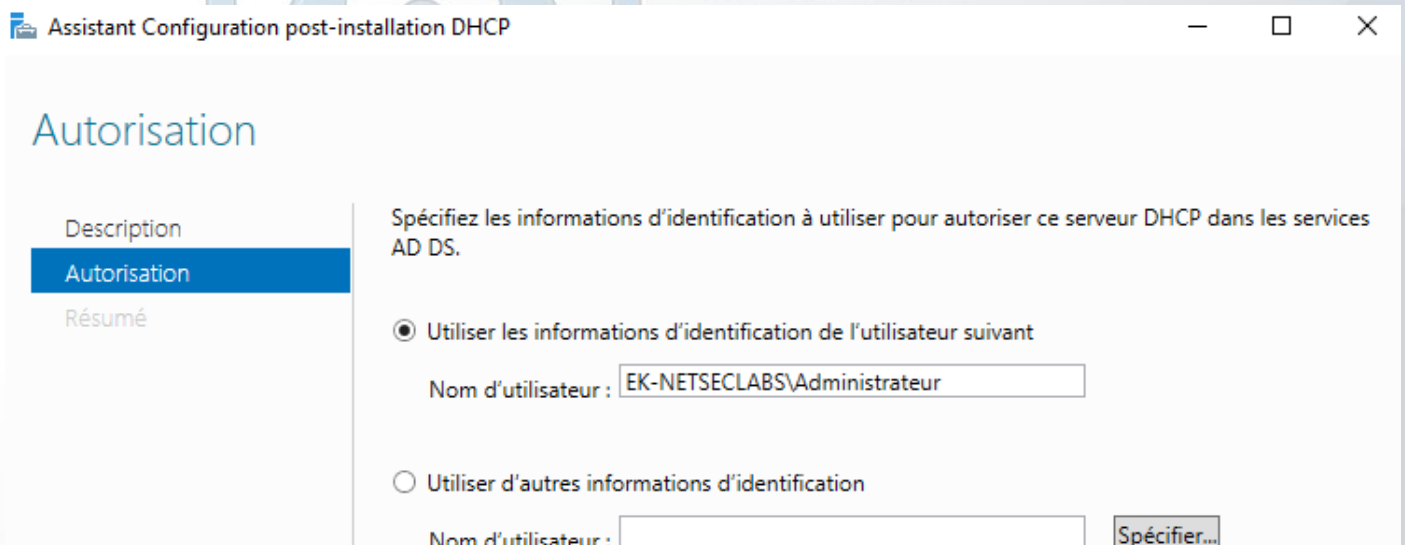
OUVRIR LA NOTIFICATION

- Dans le Gestionnaire de serveur, en haut → notification ⚠.
- Cliquer sur Terminer la configuration DHCP.



ASSISTANT DE POST-DEPLOIEMENT

- Choisir le compte **Administrateur du domaine** (ou un compte équivalent).
- L'assistant va :
 - Créer les groupes de sécurité DHCP (DHCP Administrators, DHCP Users).
 - Autoriser le serveur dans Active Directory.



Résumé

Description

Autorisation

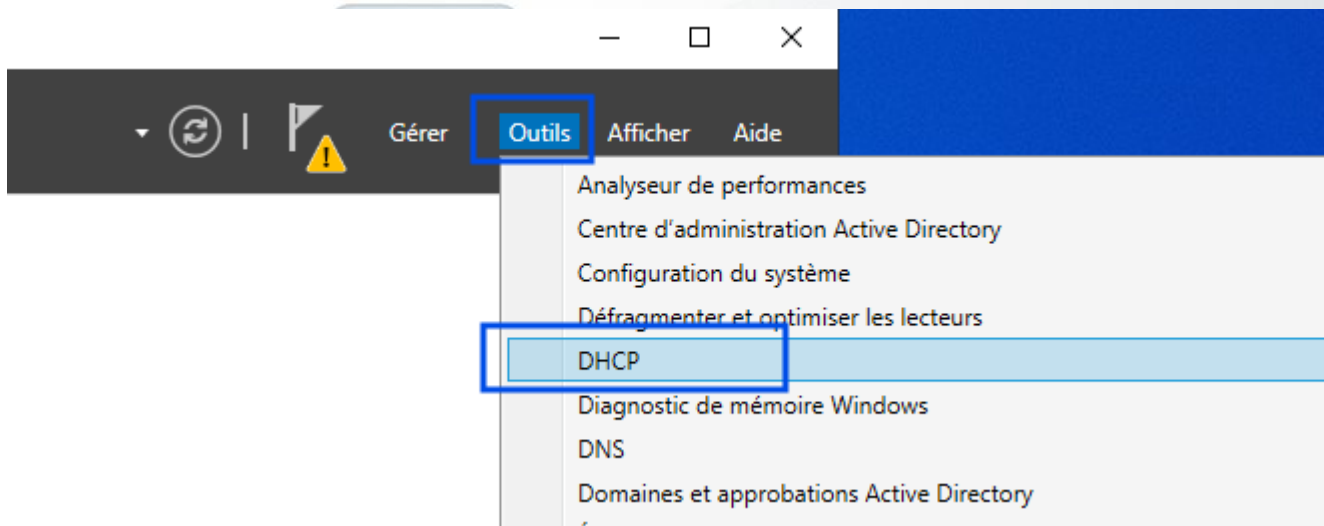
Résumé

L'état des étapes de configuration post-installation est indiqué ci-dessous :

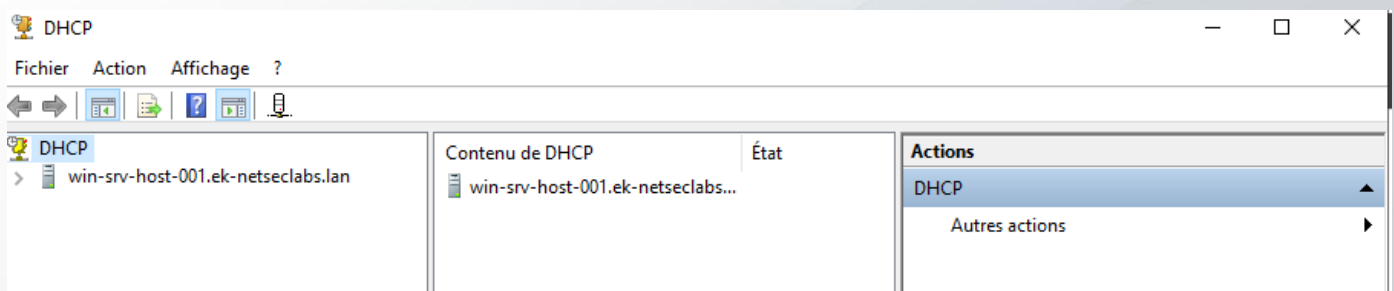
Création des groupes de sécurité	Terminé
Redémarrez le service Serveur DHCP sur l'ordinateur cible pour que les groupes de sécurité soient effectifs.	
Autorisation du serveur DHCP	Terminé

VERIFIER L'AUTORISATION DHCP

- Aller dans **Outils** → **DHCP**.



- Dans la console, le serveur **WIN-SRV-HOST-001.ek-netseclabs.lan** doit être listé sans avertissement rouge.

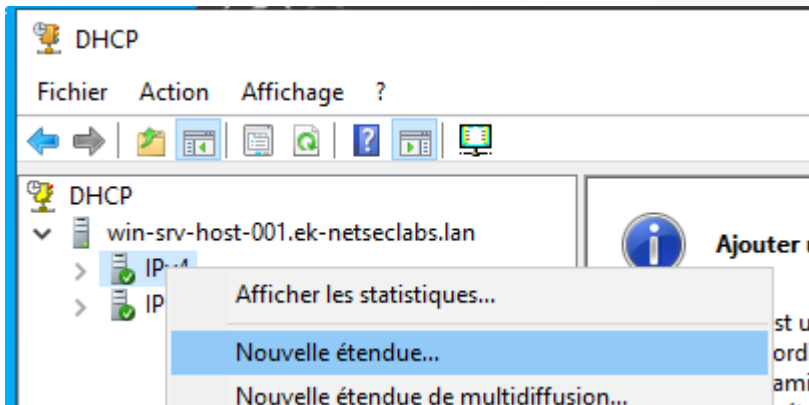


- Si besoin, clic droit sur le serveur → **Autoriser**.

CREATION D'UNE ETENDUE DHCP (SCOPE)

Ouvrir la console DHCP

- Aller dans **Outils → DHCP**.
- Déployer le serveur **WIN-SRV-HOST-001.ek-netseclabs.lan**.
- Clic droit sur **IPv4 → Nouvelle étendue**.



Assistant de nouvelle étendue

- Nom de l'étendue : **LAN_LABO_10.20.0.0**.

Nom de l'étendue
 Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

- Plage d'adresses :
 - Début : 10.20.0.1
 - Fin : 10.20.0.254
 - Masque : 255.255.255.0

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

Définir les exclusions

- Exclure les adresses réservées pour les serveurs et le réseau :
 - 10.20.0.1 – 10.20.0.31 → réservée pour les serveurs et équipements réseau.
 - 10.20.0.224 – 10.20.0.254 → réservée pour tests/administration.

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.



Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : Adresse IP de fin :

Plage d'adresses exclue :

Durée du bail

- Laisser la valeur par défaut : **8 jours**.

Configurer les options DHCP

- Dans l'assistant, renseigner :
 - 003 – Routeur** : (laisser vide si pas de passerelle, ou ajouter plus tard une IP de firewall/routeur VM).
 - 006 – Serveurs DNS** : 10.20.0.10 (DC1), puis 10.20.0.11 (DC2 après installation).
 - 015 – Nom de domaine** : ek-netseclabs.lan.

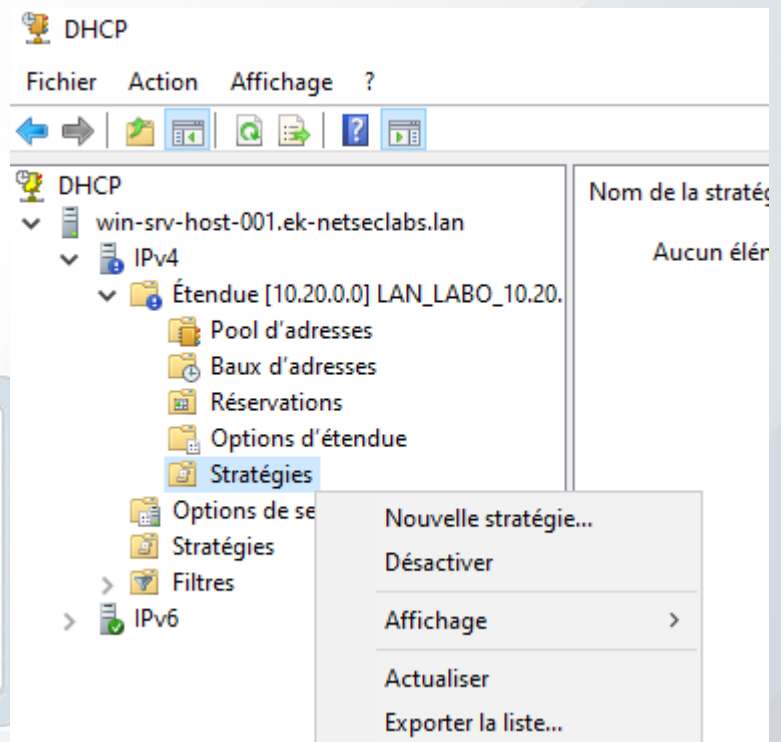
Activer l'étendue

- Finaliser l'assistant.
- Vérifier que l'étendue apparaît sous **IPv4** en état **Active**.

Créer les stratégies par service

- Dans l'étendue, clic droit → **Nouvelle stratégie**.
- Définir des sous-plages pour chaque service :

Service	Plage attribuée
Informatique	10.20.0.32 – 10.20.0.63
Commercial	10.20.0.64 – 10.20.0.95
Marketing	10.20.0.96 – 10.20.0.127
Production	10.20.0.128 – 10.20.0.159
RH	10.20.0.160 – 10.20.0.191
Direction	10.20.0.192 – 10.20.0.223



Pour la version 1.0 du doc, nous n'irons pas plus loin dans cette section, une mise à jour sera mise en place avec un complément.

STRUCTURATION D'ACTIVE DIRECTORY – OU, GROUPES ET UTILISATEURS

CREER L'ARBORESCENCE DES UNITES D'ORGANISATION

- Ouvrir une session PowerShell en **Administrateur de domaine**.
- Exécuter le script 01-create-OU.ps1.

```
# 01-create-OU.ps1 (version stable)
Import-Module ActiveDirectory
$domainDN = "DC=ek-netseclabs,DC=lan"

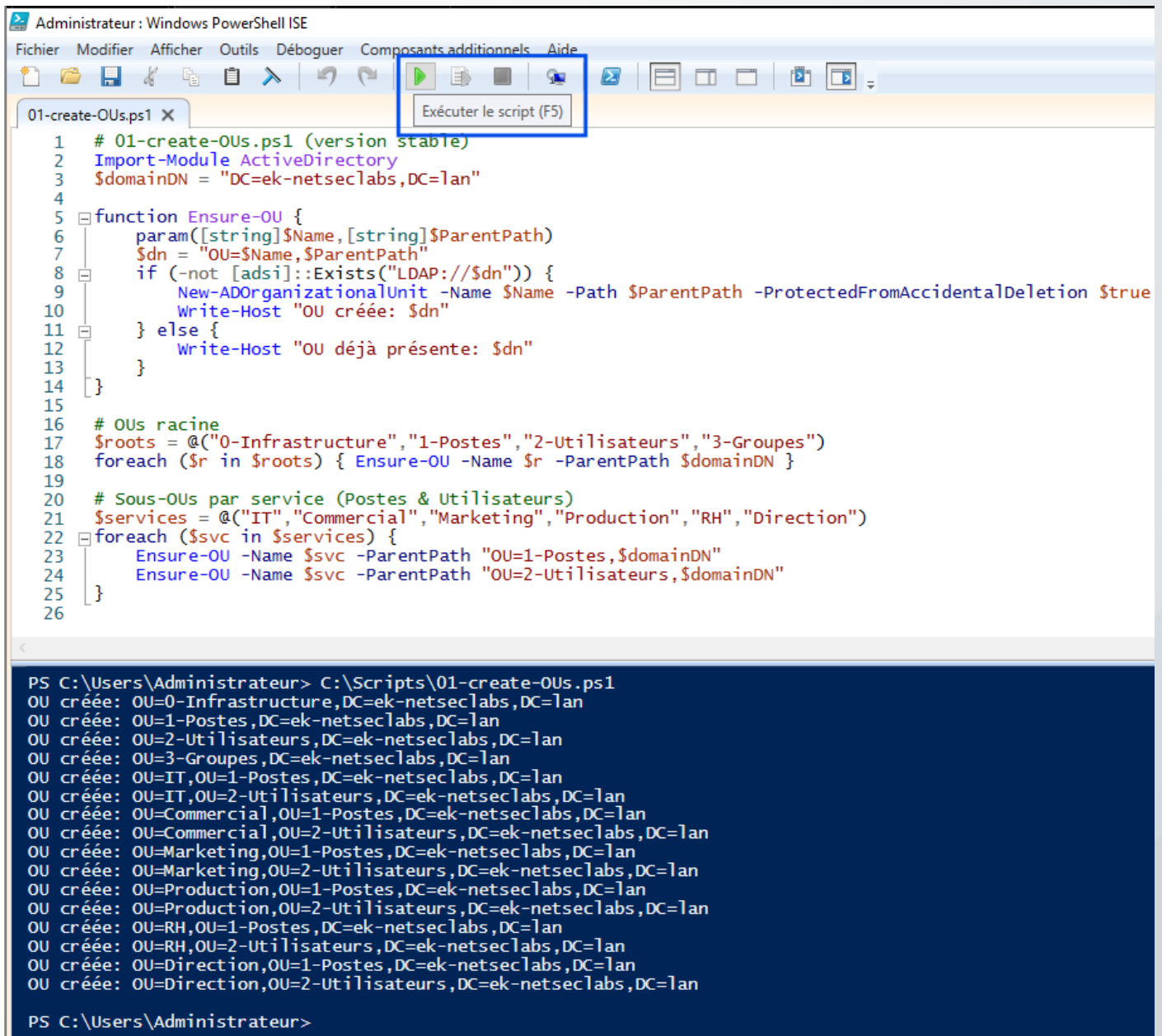
function Ensure-OU {
    param([string]$Name,[string]$ParentPath)
    $dn = "OU=$Name,$ParentPath"
    if (-not [adsisearcher]::Exists("LDAP://$dn")) {
        New-ADOrganizationalUnit -Name $Name -Path $ParentPath -ProtectedFromAccidentalDeletion $true
        Write-Host "OU créée: $dn"
    } else {
        Write-Host "OU déjà présente: $dn"
    }
}

# OUs racine
$roots = @("0-Infrastructure","1-Postes","2-Utilisateurs","3-Groupes")
foreach ($r in $roots) { Ensure-OU -Name $r -ParentPath $domainDN }

# Sous-OUs par service (Postes & Utilisateurs)
$services = @("IT","Commercial","Marketing","Production","RH","Direction")
foreach ($svc in $services) {
    Ensure-OU -Name $svc -ParentPath "OU=1-Postes,$domainDN"
    Ensure-OU -Name $svc -ParentPath "OU=2-Utilisateurs,$domainDN"
}
```

Explications du script

- **Import-Module ActiveDirectory** : sert à charger les commandes nécessaires pour travailler avec Active Directory.
- **\$domainDN** : contient l'adresse racine du domaine (ici « DC=ek-netseclabs,DC=lan »). Toutes les OUs seront créées à partir de ce point.
- **function Ensure-OU** : définit une fonction réutilisable qui permet de créer une OU si elle n'existe pas déjà.
- **param([string]\$Name,[string]\$ParentPath)** : précise que la fonction prend deux paramètres, tous les deux de type texte :
- **\$Name** → le nom de l'OU à créer
- **\$ParentPath** → l'endroit où cette OU doit être placée
- **\$dn = "OU=\$Name,\$ParentPath"** : construit le chemin complet (distinguished name) de l'OU à partir du nom et de son parent.
- **if (-not [adsisearcher]::Exists("LDAP://\$dn"))** : vérifie si l'OU n'existe pas déjà dans Active Directory.
- **New-ADOrganizationalUnit -Name \$Name -Path \$ParentPath -ProtectedFromAccidentalDeletion \$true** : crée l'OU si elle n'existe pas, en la protégeant contre les suppressions accidentelles.
- **Write-Host "OU créée: \$dn"** : affiche un message indiquant que l'OU vient d'être créée.
- **else { Write-Host "OU déjà présente: \$dn" }** : si l'OU existe déjà, affiche un message d'information.
- **\$roots = @("0-Infrastructure","1-Postes","2-Utilisateurs","3-Groupes")** : liste les OUs principales à créer à la racine du domaine.
- **foreach (\$r in \$roots) { ... }** : boucle qui parcourt chaque élément de la liste \$roots et appelle la fonction Ensure-OU pour le créer.
- **\$services = @("IT","Commercial","Marketing","Production","RH","Direction")** : liste des services de l'entreprise qui serviront à créer des sous-OUs.
- **foreach (\$svc in \$services) { ... }** : boucle qui parcourt chaque service et crée deux sous-OUs pour chacun :
- une sous-OU dans « 1-Postes »



The screenshot shows the Windows PowerShell ISE interface. The menu bar includes 'Fichier', 'Modifier', 'Afficher', 'Outils', 'Débugger', 'Composants additionnels', and 'Aide'. The toolbar contains various icons, with a green play button icon highlighted and a tooltip that says 'Exécuter le script (F5)'. The script file is named '01-create-OUs.ps1'. The script content is as follows:

```

1 # 01-create-OUs.ps1 (version stable)
2 Import-Module ActiveDirectory
3 $domainDN = "DC=ek-netsec labs,DC=lan"
4
5 function Ensure-OU {
6     param([string]$Name,[string]$ParentPath)
7     $dn = "OU=$Name,$ParentPath"
8     if (-not [adsi]::Exists("LDAP://$dn")) {
9         New-ADOrganizationalUnit -Name $Name -Path $ParentPath -ProtectedFromAccidentalDeletion $true
10        Write-Host "OU créée: $dn"
11    } else {
12        Write-Host "OU déjà présente: $dn"
13    }
14 }
15
16 # OUs racine
17 $roots = @("0-Infrastructure","1-Postes","2-Utilisateurs","3-Groupes")
18 foreach ($r in $roots) { Ensure-OU -Name $r -ParentPath $domainDN }
19
20 # Sous-OUs par service (Postes & Utilisateurs)
21 $services = @("IT","Commercial","Marketing","Production","RH","Direction")
22 foreach ($svc in $services) {
23     Ensure-OU -Name $svc -ParentPath "OU=1-Postes,$domainDN"
24     Ensure-OU -Name $svc -ParentPath "OU=2-Utilisateurs,$domainDN"
25 }
26

```

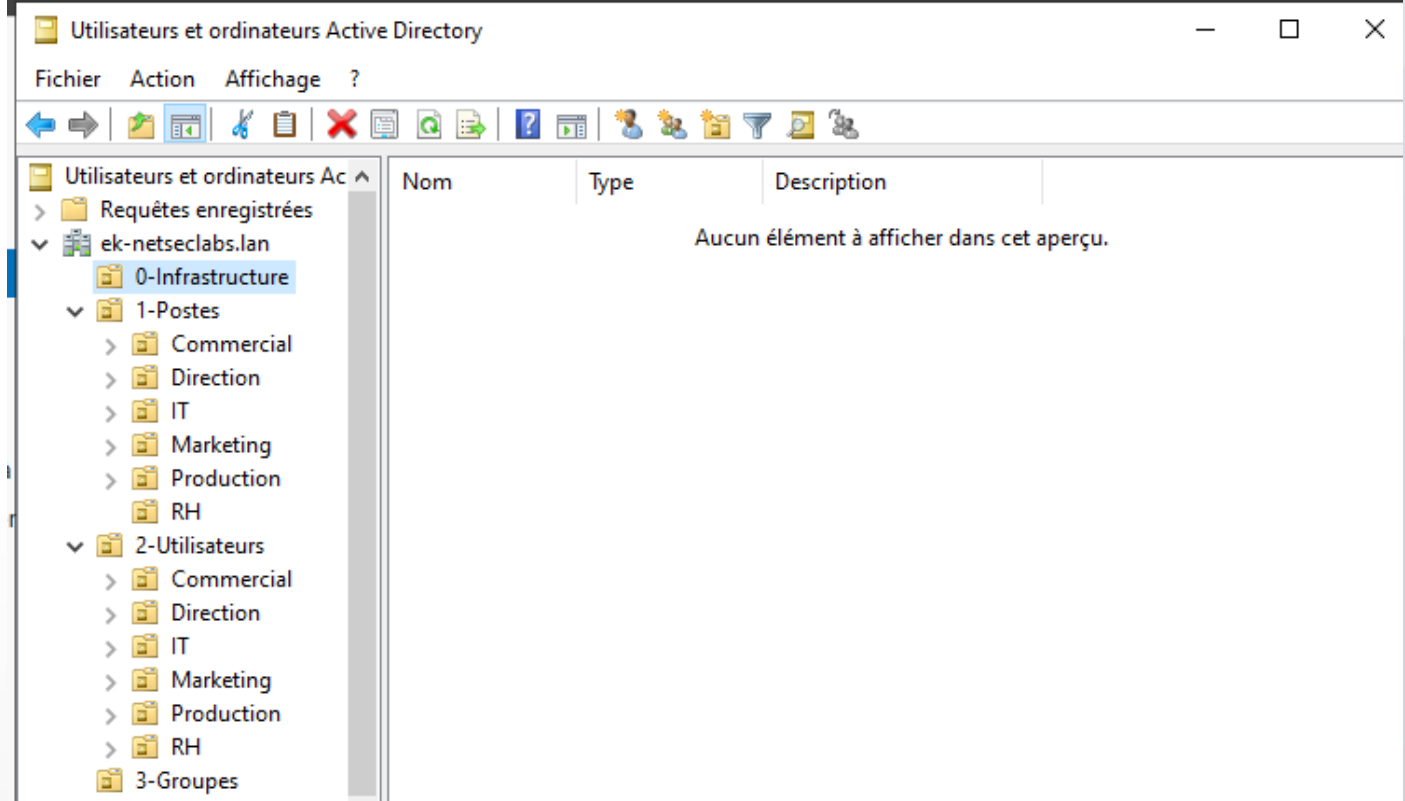
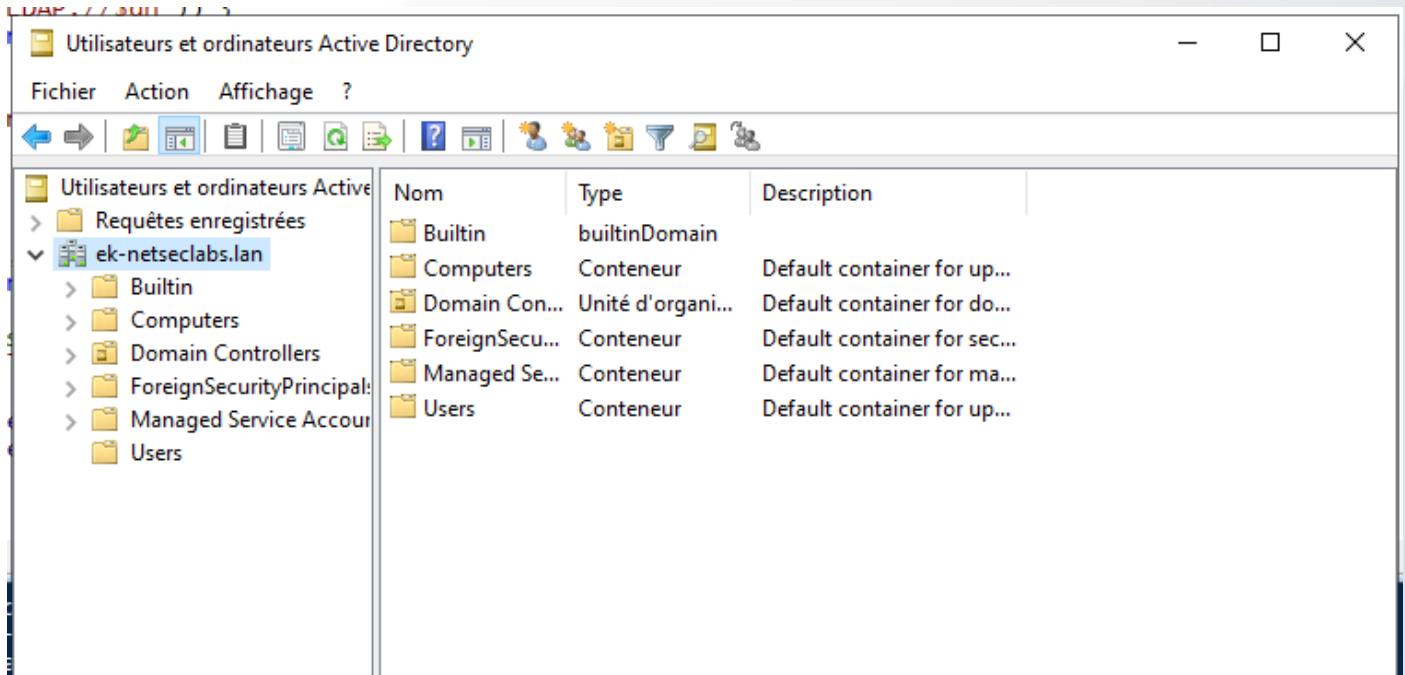
The console output shows the execution of the script, creating the following OUs:

```

PS C:\Users\Administrateur> C:\Scripts\01-create-OUs.ps1
OU créée: OU=0-Infrastructure,DC=ek-netsec labs,DC=lan
OU créée: OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
OU créée: OU=3-Groupes,DC=ek-netsec labs,DC=lan
OU créée: OU=IT,OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=IT,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
OU créée: OU=Commercial,OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=Commercial,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
OU créée: OU=Marketing,OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=Marketing,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
OU créée: OU=Production,OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=Production,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
OU créée: OU=RH,OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=RH,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
OU créée: OU=Direction,OU=1-Postes,DC=ek-netsec labs,DC=lan
OU créée: OU=Direction,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
PS C:\Users\Administrateur>

```

- Vérifier dans la console **Utilisateurs et ordinateurs Active Directory (ADUC)** que l'arborescence est créée :
 - OU racine : *0-Infrastructure, 1-Postes, 2-Utilisateurs, 3-Groupes*.
 - Sous-OU par service : *IT, Commercial, Marketing, Production, RH, Direction*.



CREER LES GROUPES DE SECURITE

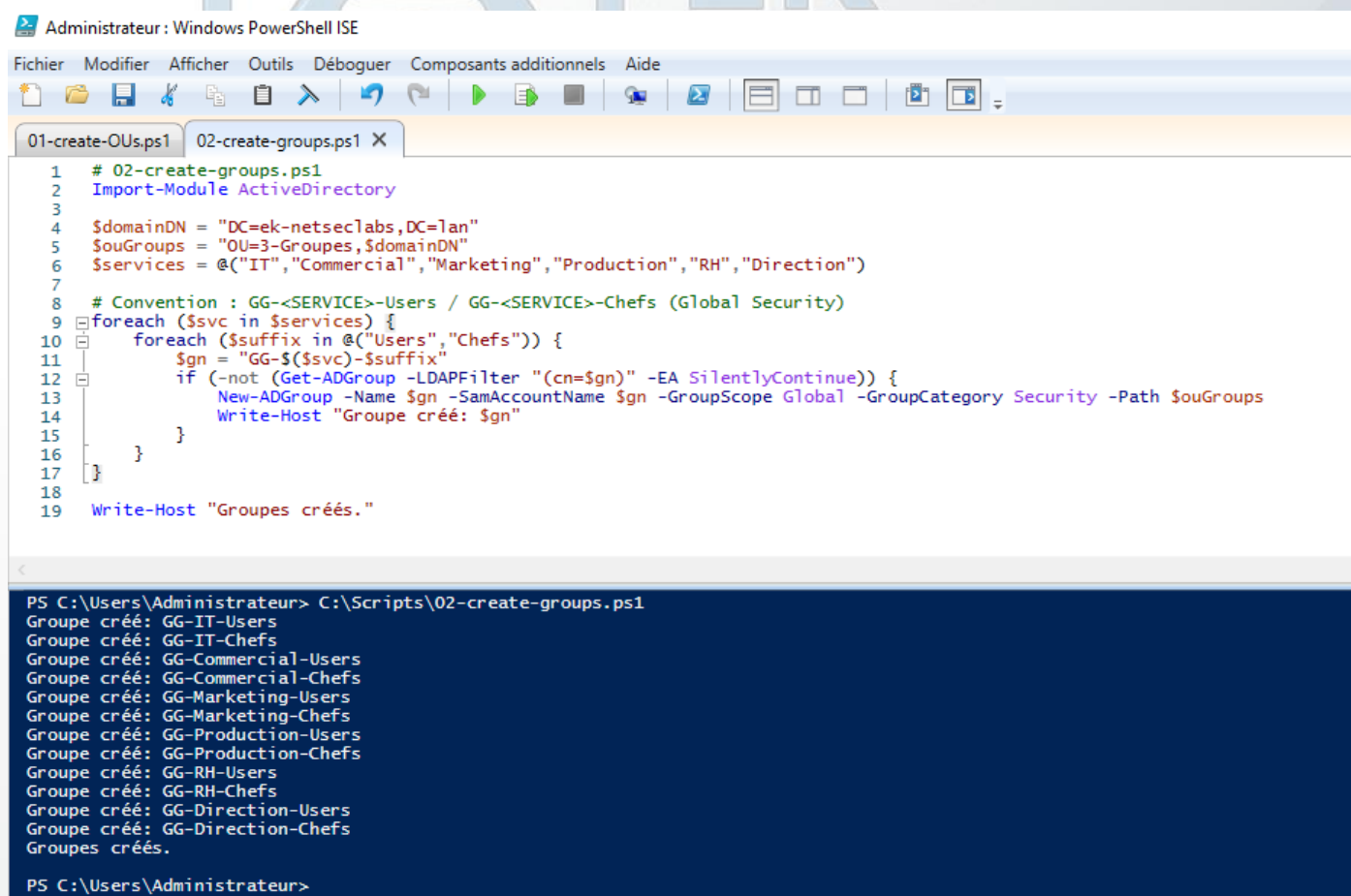
- Exécuter le script 02-create-groups.ps1.

```
# 02-create-groups.ps1
Import-Module ActiveDirectory

$domainDN = "DC=ek-netseclabs,DC=lan"
$ouGroups = "OU=3-Groupes,$domainDN"
$services = @("IT","Commercial","Marketing","Production","RH","Direction")

# Convention : GG-<SERVICE>-Users / GG-<SERVICE>-Chefs (Global Security)
foreach ($svc in $services) {
    foreach ($suffix in @("Users","Chefs")) {
        $sgn = "GG-($svc)-$suffix"
        if (-not (Get-ADGroup -LDAPFilter "(cn=$sgn)" -EA SilentlyContinue)) {
            New-ADGroup -Name $sgn -SamAccountName $sgn -GroupScope Global -GroupCategory Security -Path
            $ouGroups
            Write-Host "Groupe créé: $sgn"
        }
    }
}

Write-Host "Groupes créés."
```



Administrateur : Windows PowerShell ISE

Fichier Modifier Afficher Outils Débugger Composants additionnels Aide

01-create-OU.ps1 02-create-groups.ps1 X

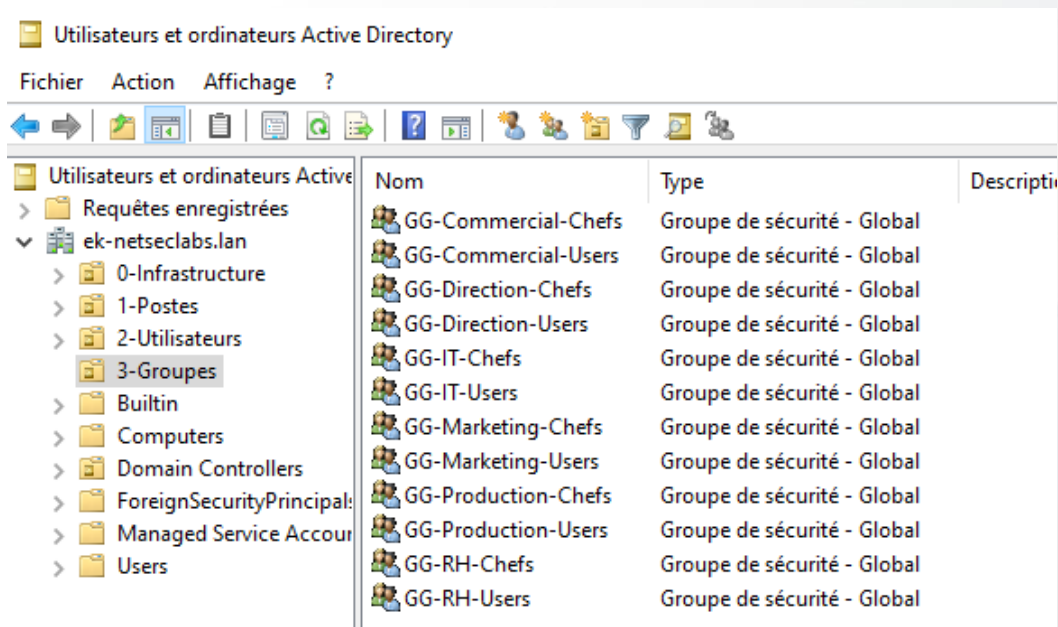
```
1 # 02-create-groups.ps1
2 Import-Module ActiveDirectory
3
4 $domainDN = "DC=ek-netseclabs,DC=lan"
5 $ouGroups = "OU=3-Groupes,$domainDN"
6 $services = @("IT","Commercial","Marketing","Production","RH","Direction")
7
8 # Convention : GG-<SERVICE>-Users / GG-<SERVICE>-Chefs (Global Security)
9 foreach ($svc in $services) {
10     foreach ($suffix in @("Users","Chefs")) {
11         $sgn = "GG-($svc)-$suffix"
12         if (-not (Get-ADGroup -LDAPFilter "(cn=$sgn)" -EA SilentlyContinue)) {
13             New-ADGroup -Name $sgn -SamAccountName $sgn -GroupScope Global -GroupCategory Security -Path $ouGroups
14             Write-Host "Groupe créé: $sgn"
15         }
16     }
17 }
18
19 Write-Host "Groupes créés."
```

PS C:\Users\Administrateur> C:\Scripts\02-create-groups.ps1

Groupe créé: GG-IT-Users
 Groupe créé: GG-IT-Chefs
 Groupe créé: GG-Commercial-Users
 Groupe créé: GG-Commercial-Chefs
 Groupe créé: GG-Marketing-Users
 Groupe créé: GG-Marketing-Chefs
 Groupe créé: GG-Production-Users
 Groupe créé: GG-Production-Chefs
 Groupe créé: GG-RH-Users
 Groupe créé: GG-RH-Chefs
 Groupe créé: GG-Direction-Users
 Groupe créé: GG-Direction-Chefs
 Groupes créés.

PS C:\Users\Administrateur>

- Vérifier dans la console ADUC, sous **OU=3-Groupes**, la création de :
 - GG-<Service>-Users → groupe des utilisateurs standards.
 - GG-<Service>-Chefs → groupe des responsables.



DELEGUER LES DROITS AUX CHEFS DE SERVICE

- Exécuter le script 03-delegate-chefs.ps1.

```
# 03-delegate-chefs.ps1 (ACL .NET, fiable)
Import-Module ActiveDirectory
Add-Type -AssemblyName System.DirectoryServices

$domainDN = (Get-ADDomain).DistinguishedName
$services = "IT","Commercial","Marketing","Production","RH","Direction"

# GUIDs
$userGuid = [Guid]"bf967aba-0de6-11d0-a285-00aa003049e2" # class 'user'
$resetPwdGuid = [Guid]"00299570-246d-11d0-a768-00aa006e0529" # Extended Right: Reset Password
$chgPwdGuid = [Guid]"ab721a53-1e2f-11d0-9819-00aa0040529b" # Extended Right: Change Password

foreach ($svc in $services) {
    $ouDN = "OU=$svc,OU=2-Utilisateurs,$domainDN"
    $grpSam = "GG-$svc-Chefs"

    $ou = Get-ADOrganizationalUnit -Identity $ouDN -EA Stop
    $grp = Get-ADGroup -Identity $grpSam -EA Stop

    $sid = (New-Object System.Security.Principal.SecurityIdentifier($grp.SID.Value))
    $de = New-Object System.DirectoryServices.DirectoryEntry("LDAP://$ouDN")
    $acl = $de.ObjectSecurity

    $inherit = [System.DirectoryServices.ActiveDirectorySecurityInheritance]::Descendants
```

```
# Create/Delete user objects
$aceCreate = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::CreateChild,'Allow',$userGuid,$inherit)
$aceDelete = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::DeleteChild,'Allow',$userGuid,$inherit)

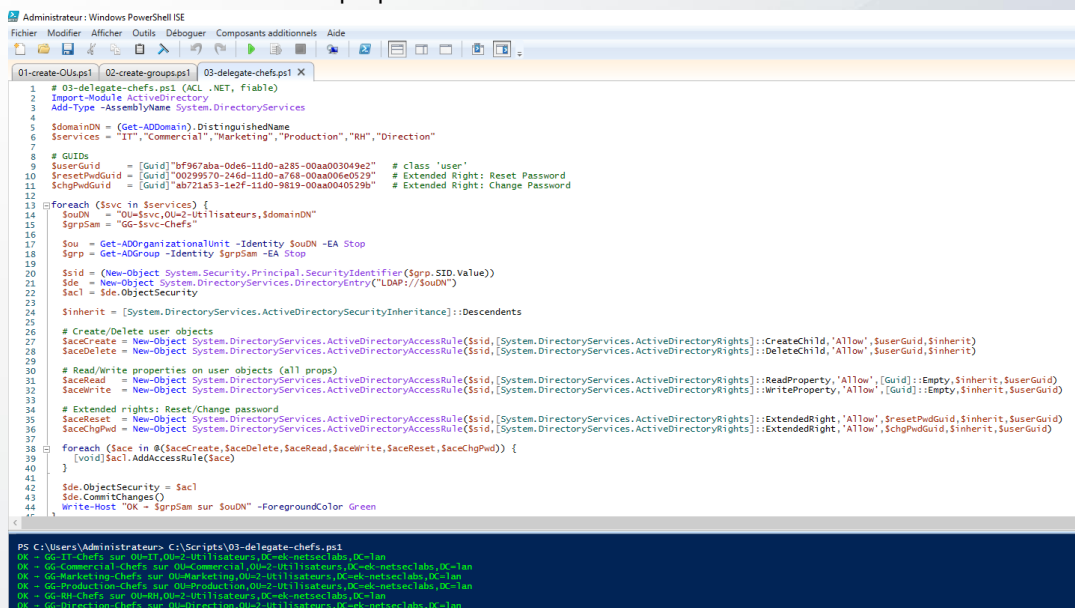
# Read/Write properties on user objects (all props)
$aceRead = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,'Allow',[Guid]::Empty,$inherit,$userGuid)
$aceWrite = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::WriteProperty,'Allow',[Guid]::Empty,$inherit,$userGuid)

# Extended rights: Reset/Change password
$aceReset = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,'Allow',$resetPwdGuid,$inherit,$userGuid)
$aceChgPwd = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,'Allow',$chgPwdGuid,$inherit,$userGuid)

foreach ($ace in @($aceCreate,$aceDelete,$aceRead,$aceWrite,$aceReset,$aceChgPwd)) {
    [void]$acl.AddAccessRule($ace)
}

$de.ObjectSecurity = $acl
$de.CommitChanges()
Write-Host "OK → $grpSam sur $ouDN" -ForegroundColor Green
}
```

- Le script applique les droits suivants au groupe **Chefs** de chaque service, sur l'OU correspondant :
 - Créer des objets utilisateur.
 - Supprimer des objets utilisateur.
 - Modifier les propriétés des utilisateurs.



```
01-create-ous.ps1 | 02-create-groups.ps1 | 03-delegate-chefs.ps1 X
1 # 03-delegate-chefs.ps1 (ACL .NET, fiable)
2 Import-Module ActiveDirectory
3 Add-Type -AssemblyName System.DirectoryServices
4
5 $domainDN = (Get-ADDomain).DistinguishedName
6 $services = "IT","Commercial","Marketing","Production","RH","Direction"
7
8 # GUIDs
9 $userGuid = [Guid]"bf967aba-0de6-11d0-a285-00aa003049e2" # class 'user'
10 $resetPwdGuid = [Guid]"00299970-246d-11d0-a768-00aa006029b" # Extended Right: Reset Password
11 $chgPwdGuid = [Guid]"0b724833-1e2f-11d0-9819-00aa006029b" # Extended Right: Change Password
12
13 foreach ($svc in $services) {
14     $ouDN = "OU=$svc,OU=2-utilisateurs,$domainDN"
15     $grpSam = "GG-$svc-Chefs"
16
17     $ou = Get-ADOrganizationalUnit -Identity $ouDN -EA Stop
18     $grp = Get-ADGroup -Identity $grpSam -EA Stop
19
20     $sid = (New-Object System.Security.Principal.SecurityIdentifier($grp.SID.Value))
21     $de = New-Object System.DirectoryServices.DirectoryEntry("LDAP://$ouDN")
22     $acl = $de.ObjectSecurity
23
24     $inherit = [System.DirectoryServices.ActiveDirectorySecurityInheritance]::Descendants
25
26     # Create/Delete user objects
27     $aceCreate = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::CreateChild,'Allow',$userGuid,$inherit)
28     $aceDelete = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::DeleteChild,'Allow',$userGuid,$inherit)
29
30     # Read/Write properties on user objects (all props)
31     $aceRead = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,'Allow',[Guid]::Empty,$inherit,$userGuid)
32     $aceWrite = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::WriteProperty,'Allow',[Guid]::Empty,$inherit,$userGuid)
33
34     # Extended rights: Reset/Change password
35     $aceReset = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,'Allow',$resetPwdGuid,$inherit,$userGuid)
36     $aceChgPwd = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($sid,[System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,'Allow',$chgPwdGuid,$inherit,$userGuid)
37
38     foreach ($ace in @($aceCreate,$aceDelete,$aceRead,$aceWrite,$aceReset,$aceChgPwd)) {
39         [void]$acl.AddAccessRule($ace)
40     }
41
42     $de.ObjectSecurity = $acl
43     $de.CommitChanges()
44     Write-Host "OK → $grpSam sur $ouDN" -ForegroundColor Green
45 }
```

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage

Propriétés de : IT

Général Géré par Objet Sécurité COM+ Éditeur d'a

Noms de groupes ou d'utilisateurs :

- Système
- GG-IT-Chefs (EK-NETSECLABS\GG-IT-Chefs)
- Admins du domaine (EK-NETSECLABS\Admins du domaine)
- Administrateurs de l'entreprise (EK-NETSECLABS\Administrateurs de l'entreprise)
- Administrateurs clés (EK-NETSECLABS\Administrateurs clés)

Autorisations pour GG-IT-Chefs

- Contrôle total
- Lire
- Écrire
- Créer tous les objets enfants
- Supprimer tous les objets enfants

Pour les autorisations spéciales et les paramètres avancés, cliquez sur le lien ci-dessous.

[Informations sur le contrôle d'accès et les autorisations](#)

OK Annuler

Propriétaire : Admins du domaine (EK-NETSECLABS\Admins du domaine) [Modifier](#)

Autorisations Audit Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'autorisations :

Type	Principal	Accès	Hérité de	S'applique à
Refuser	Tout le monde	Spéciale	Aucun	Cet objet uniquement
Autoriser	GG-IT-Chefs (EK-NETSECLABS\GG-IT-...	Modifier le mot de pas...	Aucun	Objets Utilisateur des...
Autoriser	GG-IT-Chefs (EK-NETSECLABS\GG-IT-...	Réinitialiser le mot de ...	Aucun	Objets Utilisateur des...
Autoriser	GG-IT-Chefs (EK-NETSECLABS\GG-IT-...	Créer/supprimer les o...	Aucun	Les objets descendan...
Autoriser	GG-IT-Chefs (EK-NETSECLABS\GG-IT-...	Lecture/Écriture de to...	Aucun	Objets Utilisateur des...
Autoriser	Opérateurs de compte (EK-NETSECLA...	Créer/supprimer les o...	Aucun	Cet objet uniquemen...
Autoriser	Opérateurs de compte (EK-NETSECLA...	Créer/supprimer les o...	Aucun	Cet objet uniquemen...
Autoriser	Opérateurs de compte (EK-NETSECLA...	Créer/supprimer les o...	Aucun	Cet objet uniquemen...

Ajouter Supprimer Modifier Paramètres par défaut

Désactiver l'héritage

OK Annuler Appliquer



EK NETSEC LABS

PREPARER LE FICHIER CSV DES UTILISATEURS

- Créer un fichier users.csv contenant les colonnes :
GivenName, Surname, SamAccountName, UPN, Department, Title, IsChef, Password.
- Ajouter 5 utilisateurs par service (dont 1 chef).

Exemple

users.csv

GivenName;Surname;SamAccountName;Department;Password;Title;IsChef;UPN

Alice;Durand;alice.durand;IT;P@ssw0rd!123;Technicien;false;

Brahim;Morel;brahim.morel;IT;P@ssw0rd!123;Technicien;false;

Chloe;Martin;chloe.martin;IT;P@ssw0rd!123;Technicien;false;

David;Leroy;david.leroy;IT;P@ssw0rd!123;Technicien;false;

Ethan;Bernard;ethan.bernard;IT;P@ssw0rd!123;Chef;true;

Fatou;Robert;fatou.robert;Commercial;P@ssw0rd!123;Commercial;false;

Gilles;Petit;gilles.petit;Commercial;P@ssw0rd!123;Commercial;false;

Hana;Dubois;hana.dubois;Commercial;P@ssw0rd!123;Commercial;false;

Ilian;Fontaine;ilian.fontaine;Commercial;P@ssw0rd!123;Commercial;false;

Jade;Lucas;jade.lucas;Commercial;P@ssw0rd!123;Chef;true;

Karim;Garcia;karim.garcia;Marketing;P@ssw0rd!123;Marketing;false;

Lina;Rousseau;lina.rousseau;Marketing;P@ssw0rd!123;Marketing;false;

Mehdi;Faure;mehdi.faure;Marketing;P@ssw0rd!123;Marketing;false;

Nina;Chevalier;nina.chevalier;Marketing;P@ssw0rd!123;Marketing;false;

Omar;Perez;omar.perez;Marketing;P@ssw0rd!123;Chef;true;

Aya;Lemaire;aya.lemaire;Production;P@ssw0rd!123;Operateur;false;

Boris;Guillot;boris.guillot;Production;P@ssw0rd!123;Operateur;false;

Camille;Adam;camille.adam;Production;P@ssw0rd!123;Operateur;false;

Diane;Noel;diane.noel;Production;P@ssw0rd!123;Operateur;false;

Eliot;Blanc;eliot.blanc;Production;P@ssw0rd!123;Chef;true;

Rita;Gauthier;rita.gauthier;RH;P@ssw0rd!123;Gestionnaire;false;

Sami;Legrand;sami.legrand;RH;P@ssw0rd!123;Gestionnaire;false;

Tara;Marchand;tara.marchand;RH;P@ssw0rd!123;Gestionnaire;false;

Ugo;Perrot;ugo.perrot;RH;P@ssw0rd!123;Gestionnaire;false;

Valerie;Colin;valerie.colin;RH;P@ssw0rd!123;Chef;true;

Wassim;Renard;wassim.renard;Direction;P@ssw0rd!123;Assistant;false;

Xavier;Schmitt;xavier.schmitt;Direction;P@ssw0rd!123;Assistant;false;

Yasmin;Poulain;yasmin.poulain;Direction;P@ssw0rd!123;Assistant;false;

Ziad;Bonneau;ziad.bonneau;Direction;P@ssw0rd!123;Assistant;false;

Amine;Charvet;amine.charvet;Direction;P@ssw0rd!123;Chef;true;

IMPORTER LES UTILISATEURS

- Exécuter le script 04-import-users.ps1.

```
# 04-import-users.ps1
Import-Module ActiveDirectory

$csvPath = 'C:\Scripts\fichierCSV\users.csv'
$delim = ',' # si ton CSV est en virgule, mets $delim=';'

$domainDN = 'DC=ek-netseclabs,DC=lan'
$baseOU = "OU=2-Utilisateurs,$domainDN"

if (!(Test-Path $csvPath)) { throw "CSV introuvable: $csvPath" }
$users = Import-Csv -Path $csvPath -Delimiter $delim

foreach ($u in $users) {
    # validations minimales
    foreach ($k in 'GivenName','Surname','SamAccountName','Department','Password') {
        if ([string]::IsNullOrEmpty($u.$k)) { Write-Warning "Champ '$k' vide → $($u | ConvertTo-Json -Compress)"; continue 2 }
    }

    $ouDN = "OU= $($u.Department),$baseOU"
    if (-not (Get-ADOrganizationalUnit -Identity $ouDN -EA SilentlyContinue)) {
        Write-Warning "OU inexistante: $ouDN → $($u.SamAccountName) ignoré"; continue
    }

    $sam = $u.SamAccountName.Trim()
    $name = "$($u.GivenName.Trim()) $($u.Surname.Trim())"
    $upn = if ($u.UPN) { $u.UPN.Trim() } else { "$sam@ek-netseclabs.lan" }
    $pwd = ConvertTo-SecureString $u.Password -AsPlainText -Force

    $exists = Get-ADUser -Filter "SamAccountName -eq '$sam'" -EA SilentlyContinue
    if (-not $exists) {
        New-ADUser -Name $name -GivenName $u.GivenName -Surname $u.Surname `
            -SamAccountName $sam -UserPrincipalName $upn `
            -Department $u.Department -Title $u.Title `
            -Path $ouDN -AccountPassword $pwd -Enabled $true -ChangePasswordAtLogon $true
        Write-Host "Créé: $sam → $ouDN"
    } else {
        Set-ADUser -Identity $sam -Department $u.Department -Title $u.Title
        Set-ADAccountPassword -Identity $sam -NewPassword $pwd -Reset
        Enable-ADAccount -Identity $sam
        Write-Host "MAJ: $sam"
    }
}

# Groupes
$grpUsers = "GG- $($u.Department)-Users"
if (Get-ADGroup -Identity $grpUsers -EA SilentlyContinue) {
    Add-ADGroupMember -Identity $grpUsers -Members $sam -EA SilentlyContinue
}
if ($u.IsChef -match '^(true|1|yes)$') {
    $grpChefs = "GG- $($u.Department)-Chefs"
    if (Get-ADGroup -Identity $grpChefs -EA SilentlyContinue) {
        Add-ADGroupMember -Identity $grpChefs -Members $sam -EA SilentlyContinue
    }
}
}

Write-Host "Import terminé."
```

```

Administrateur : Windows PowerShell ISE
Fichier Modifier Afficher Outils Débugger Composants additionnels Aide

01-create-OUs.ps1 02-create-groups.ps1 03-delegate-chefs.ps1 04-import-users.ps1 X

1 # 04-import-users.ps1
2 Import-Module ActiveDirectory
3
4 $csvPath = 'C:\Scripts\fichierCSV\users.csv'
5 $delim = ';' # si ton CSV est en virgule, mets $delim=','
6
7 $domainDN = 'DC=ek-netsec labs,DC=lan'
8 $baseOU = "OU=2-Utilisateurs,$domainDN"
9
10 if (!(Test-Path $csvPath)) { throw "CSV introuvable: $csvPath" }
11 $users = Import-Csv -Path $csvPath -Delimiter $delim
12
13 foreach ($u in $users) {
14     # validations minimales
15     foreach ($k in 'GivenName','Surname','SamAccountName','Department','Password') {
16         if ([string]::IsNullOrEmpty($u.$k)) { Write-Warning "Champ '$k' vide → $($u | ConvertTo-Json -Compress)"; continue 2 }
17     }
18
19     $ouDN = "OU= $($u.Department), $baseOU"
20     if (-not (Get-ADOrganizationalUnit -Identity $ouDN -EA SilentlyContinue)) {
21         Write-Warning "OU inexistante: $ouDN → $($u.SamAccountName) ignoré"; continue
22     }
23
24     $sam = $u.SamAccountName.Trim()
25     $name = "$($u.GivenName.Trim()) $($u.Surname.Trim())"
26     $upn = if ($u.UPN) { $u.UPN.Trim() } else { "$sam@ek-netsec labs.lan" }
27     $pwd = ConvertTo-SecureString $u.Password -AsPlainText -Force
28
29     Create-User -Name $name -SamAccountName $sam -Password $pwd -Department $u.Department -Organization $u.Department -OU $ouDN
30 }
31
32 PS C:\Users\Administrateur>

```

Crée: nana.dubois → OU=Commercial,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: ilian.Fontaine → OU=Commercial,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: jade.lucas → OU=Commercial,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: karim.garcia → OU=Marketing,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: lina.rousseau → OU=Marketing,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: mehdi.fauve → OU=Marketing,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: nina.chevalier → OU=Marketing,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: omar.perez → OU=Marketing,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: aya.lemaire → OU=Production,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: boris.guillot → OU=Production,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: camille.adam → OU=Production,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: diane.noel → OU=Production,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: eliot.blanc → OU=Production,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: rita.gauthier → OU=RH,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: sami.legrand → OU=RH,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: tara.marchand → OU=RH,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: ugo.perrot → OU=RH,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: valerie.colin → OU=RH,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: wassim.renard → OU=Direction,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: xavier.schmitt → OU=Direction,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: yasmin.poulain → OU=Direction,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: ziad.bonneau → OU=Direction,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Crée: amine.charvet → OU=Direction,OU=2-Utilisateurs,DC=ek-netsec labs,DC=lan
 Import terminé.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

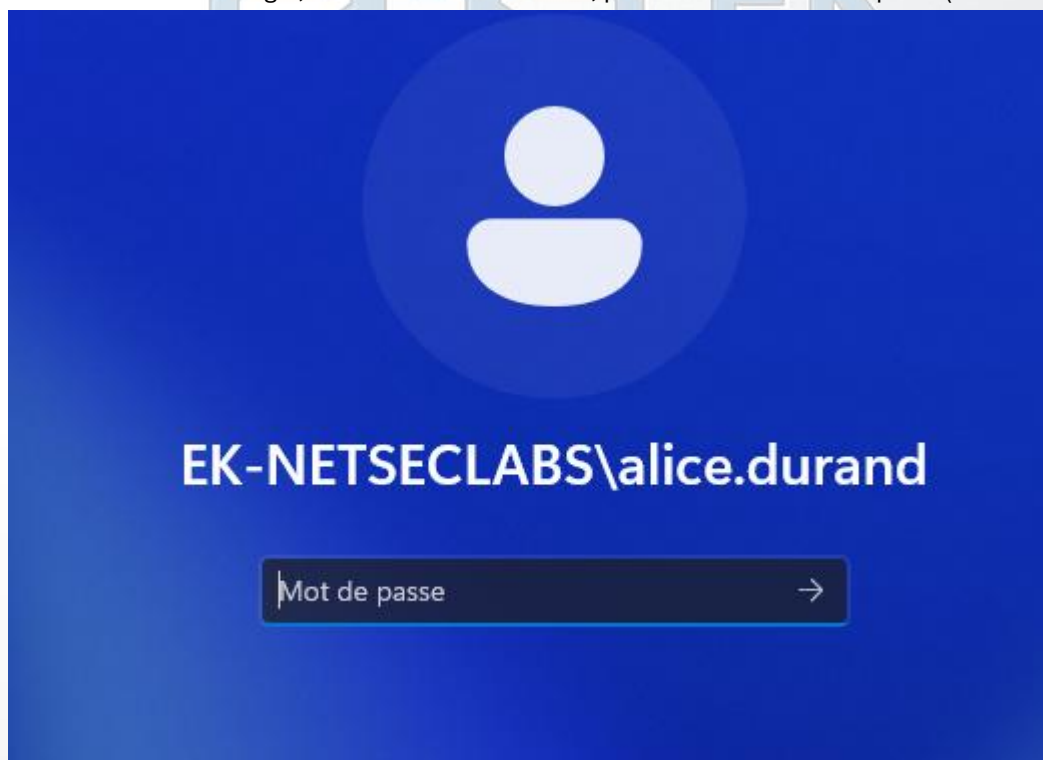
	Nom	Type	Descript
Utilisateurs et ordinateurs Active Directory			
Requêtes enregistrées			
ek-netsec labs.lan			
0-Infrastructure			
1-Postes			
2-Utilisateurs			
Commercial	Alice Durand	Utilisateur	
Direction	Brahim Morel	Utilisateur	
IT	Chloe Martin	Utilisateur	
Marketing	David Leroy	Utilisateur	
Production	Ethan Bernard	Utilisateur	
RH			
3-Groupes			
Built-in			

PARTIE GPO (FOND D'ECRAN)

INSTALLER UNE VM CLIENTE POUR LES TESTS

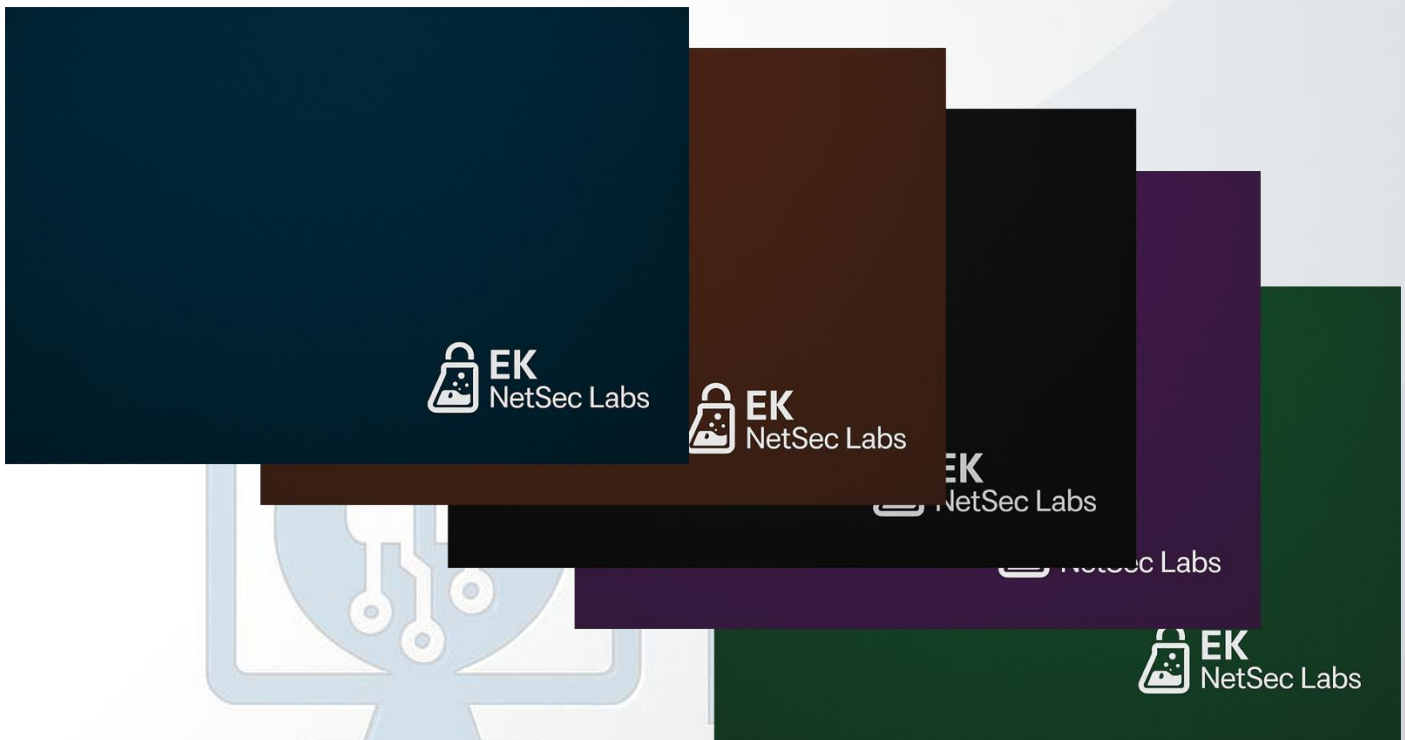
Étapes pour ajouter un poste Windows 10/11 au domaine

- Connecter la VM au réseau **Host-Only (VMnet2)** pour qu'elle parle au DC.
- Vérifier la config IP → ipconfig /all
 - IP dans la plage DHCP 10.20.0.x
 - DNS = l'IP de ton DC (ex. 10.20.0.10).
- Renommer le PC (ex. WIN-CLIENT-01).
 - **Paramètres** → **Système** → **À propos** → **Renommer ce PC (paramètres avancés)**.
 - Redémarrer.
- Joindre le domaine :
 - Win + R → taper sysdm.cpl → onglet **Nom de l'ordinateur** → **Modifier....**
 - Sélectionner **Domaine**.
 - Entrer : ek-netseclabs.lan.
- Entrer les identifiants d'un **Administrateur du domaine** (ex. Administrateur).
- Message "Bienvenue dans le domaine ek-netseclabs.lan" → Redémarrer.
- À l'écran de login, choisir **Autre utilisateur**, puis tester avec un compte IT (ex. alice.durand).

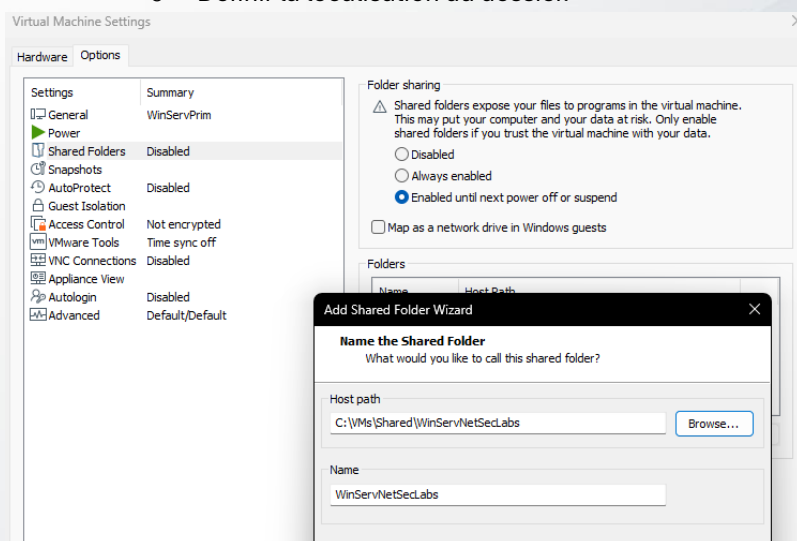


CREER UN DOSSIER PARTAGE POUR LES GPO

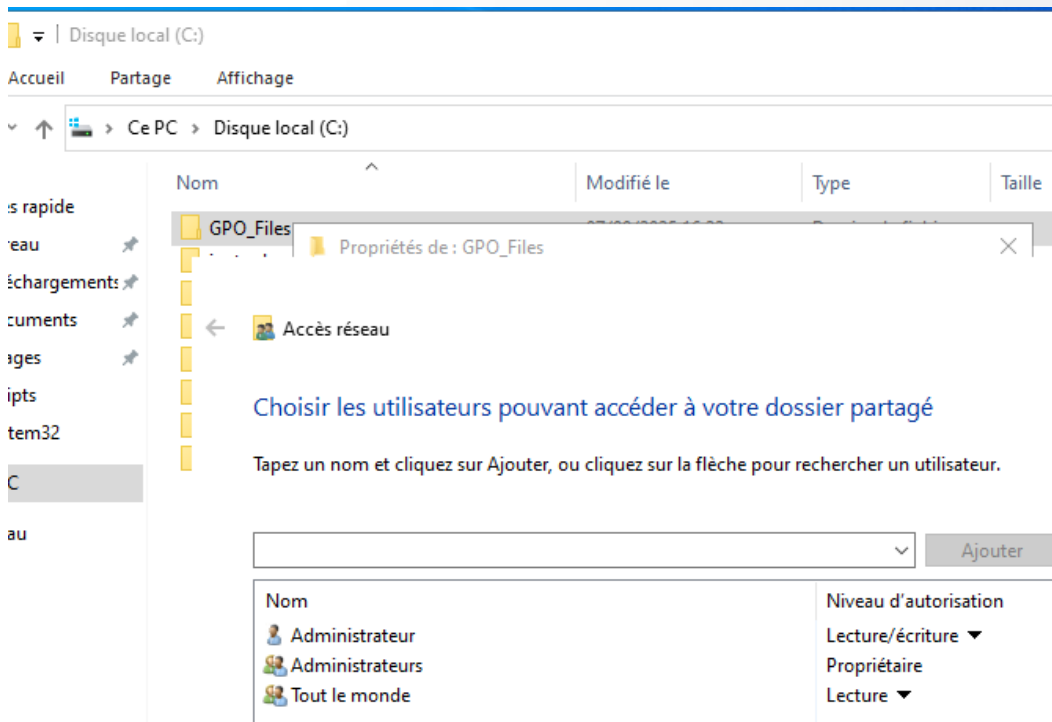
- Création de fond d'écran avec un code couleur par groupe
 - **IT** → ● Bleu
 - **Commercial** → ● Orange
 - **Marketing** → ● Violet
 - **Production** → ⚙ Gris anthracite
 - **RH** → ● Vert
 - **Direction** → ● Noir avec doré



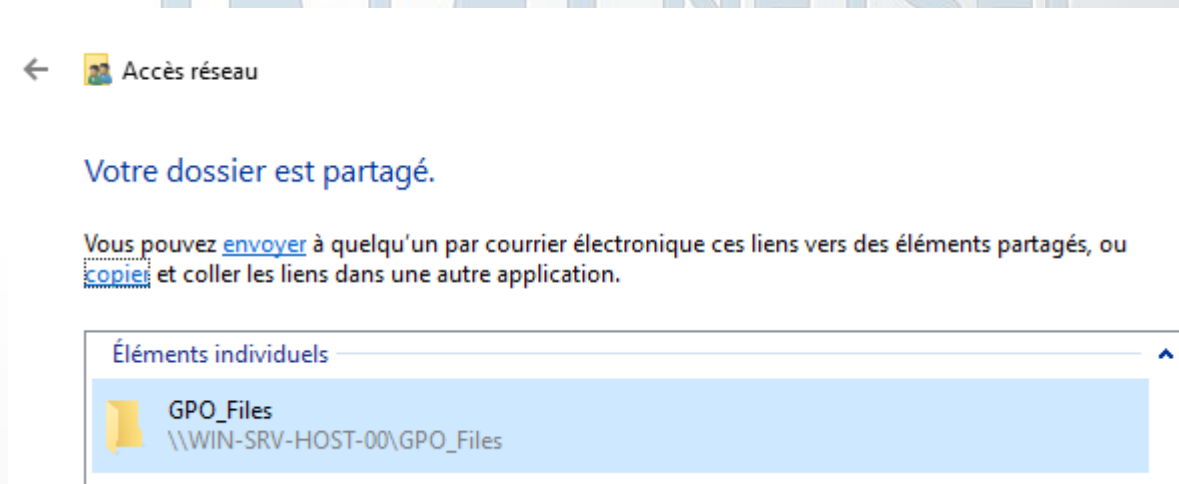
- Créer un dossier partager entre le pc hôte et le serveur pour transférer les fichiers.
 - Ouvrir les paramètres de la VM.
 - Sélectionner l'onglet option.
 - Activer le partage de dossier.
 - Définir la localisation du dossier.



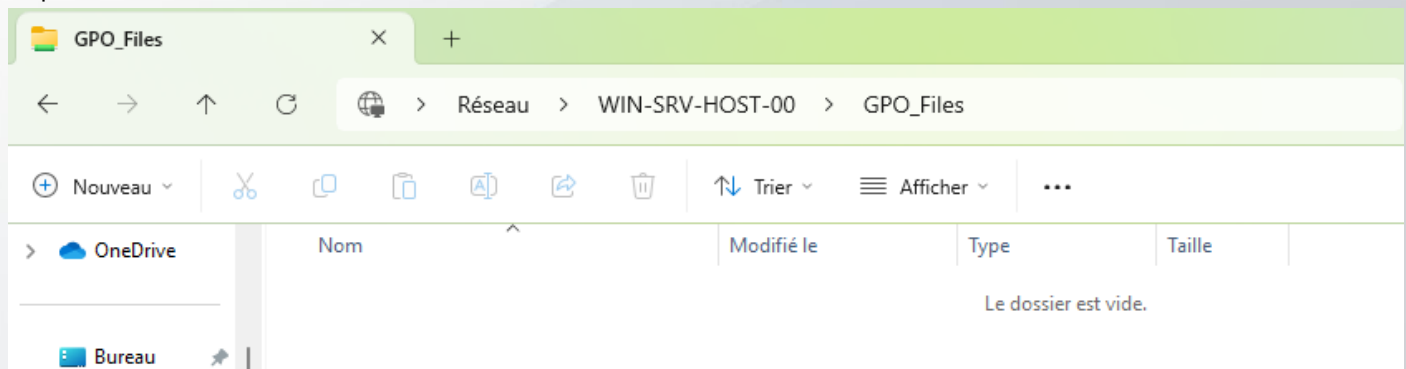
- Créer un dossier GPO_Files dans C:\ sur **WIN-SRV-HOST-001**.
- Partager le dossier en lecture pour **Tout le monde**.



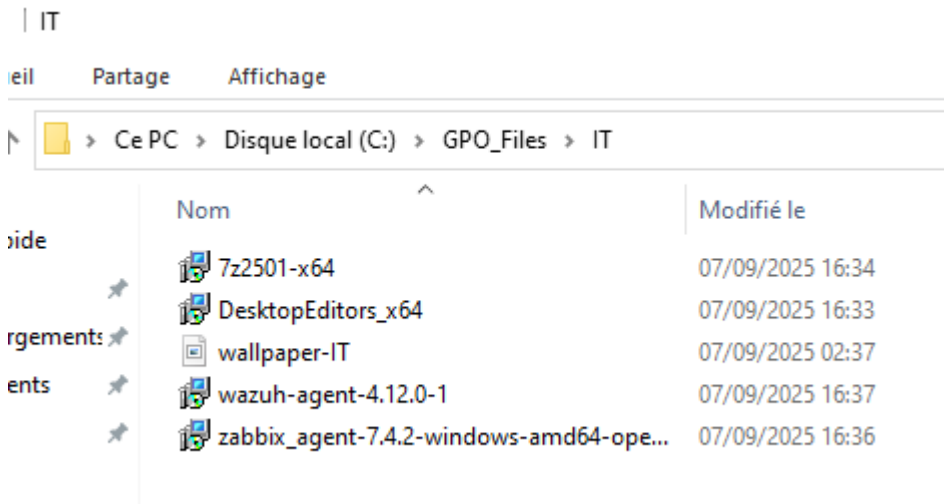
- Le rendre accessible via chemin UNC : \\WIN-SRV-HOST-001\GPO_Files.



Depuis l'Host client :

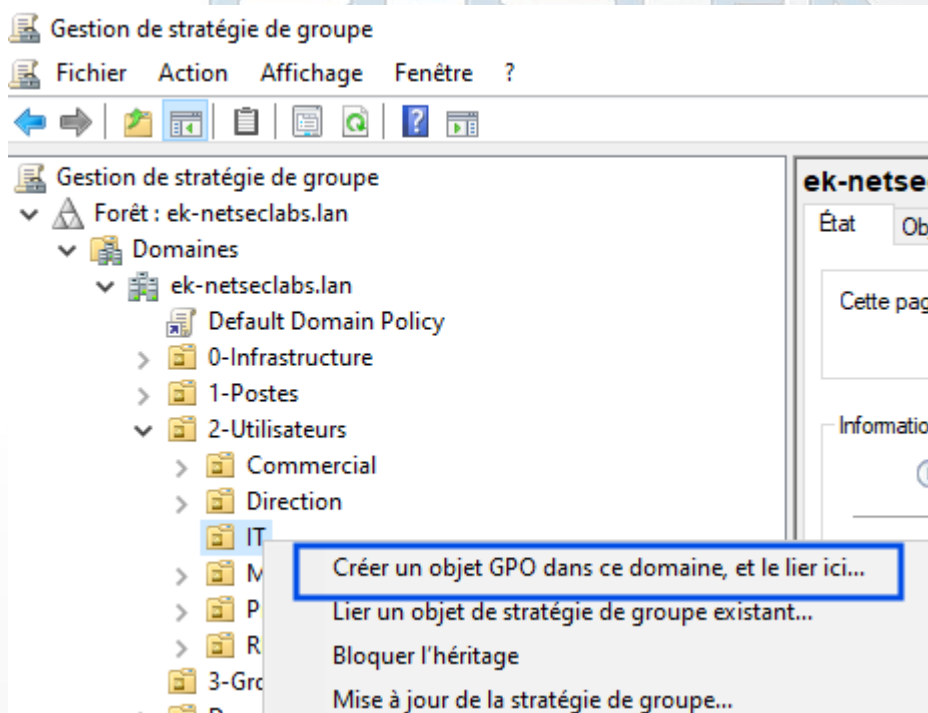


- Y copier :
 - Le fond d'écran du service IT (wallpaper-IT.bmp).
 - Les MSI nécessaires (ex. 7-Zip, OnlyOffice, Agents : Wazuh, Zabbix).



3. Créer la GPO de fond d'écran pour l'IT

- Ouvrir la **Console de gestion des stratégies de groupe (GPMC)**.
- Clic droit sur le domaine → **Créer un objet GPO**.



- Nommer : GPO-IT-FondEcran.
- Lier la GPO à l'OU : OU=IT,OU=2-Utilisateurs,DC=ek-netseclabs,DC=lan.
- Éditer la GPO :
 - Aller dans **Configuration utilisateur → Stratégies → Paramètres Windows → Paramètres du Bureau → Papier peint du Bureau**.

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie GPO-IT-FondEcran- [WIN-SRV-HOST-001.EK-NETSECLAB]

- Configuration ordinateur
 - Stratégies
 - Préférences
 - Configuration utilisateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Scripts (ouverture/fermeture de session)
 - Paramètres de sécurité
 - Redirection de dossiers
 - QoS basée sur la stratégie
 - Modèles d'administration : définitions de stratégies (filtrées)
 - Bureau
 - Active Directory
 - Bureau
 - Composants Windows
 - Dossiers partagés
 - Menu Démarrer et barre des tâches
 - Panneau de configuration
 - Réseau
 - Système
 - Tous les paramètres

Paramètre

- Activer Active Desktop
- Désactiver Active Desktop
- Interdire les modifications
- Papier peint du Bureau
- Empêcher l'ajout d'éléments
- Empêcher la fermeture de la session
- Empêcher la suppression de fichiers
- Empêcher la modification de fichiers
- Désactiver tous les paramètres
- Ajouter/supprimer des paramètres
- N'autoriser que les paramètres

Modifier

Paramètre

- Filtre activé
- Options des filtres...
- Réappliquer le filtre
- Toutes les tâches
- Aide

Papier peint du Bureau

Modifier le paramètre de stratégie

Configuration requise :
Au minimum Windows 2000

Description :
Spécifie l'image d'arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.

Ce paramètre vous permet de spécifier le papier peint du Bureau des utilisateurs et empêche ces derniers de modifier l'image ou sa présentation. Le papier peint spécifié peut être enregistré dans un fichier de type bitmap (*.bmp) ou JPEG (*.jpg).

Pour utiliser ce paramètre, entrez le chemin d'accès complet et le nom du fichier contenant le papier peint. Vous pouvez taper un chemin d'accès local, tel que C:\windows\web\wallpaper\home.jpg

- Activer la stratégie.
- Indiquer : \\WIN-SRV-HOST-001\GPO_Files\wallpaper-IT.bmp.

Papier peint du Bureau

Papier peint du Bureau

Paramètre précédent

☐ Non configuré

☒ Activé

☐ Désactivé

Commentaire :

Pris en charge sur : Au minimum Windows 2000

Options :

Nom du papier peint :

HOST-00\GPO_Files\IT\wallpaper-IT.bmp

Exemple : avec un chemin local :
C:\windows\web\wallpaper\home.jpg

Aide :

Spécifie l'image d'arrière-plan (le « papier peint ») affichée sur le Bureau des utilisateurs.

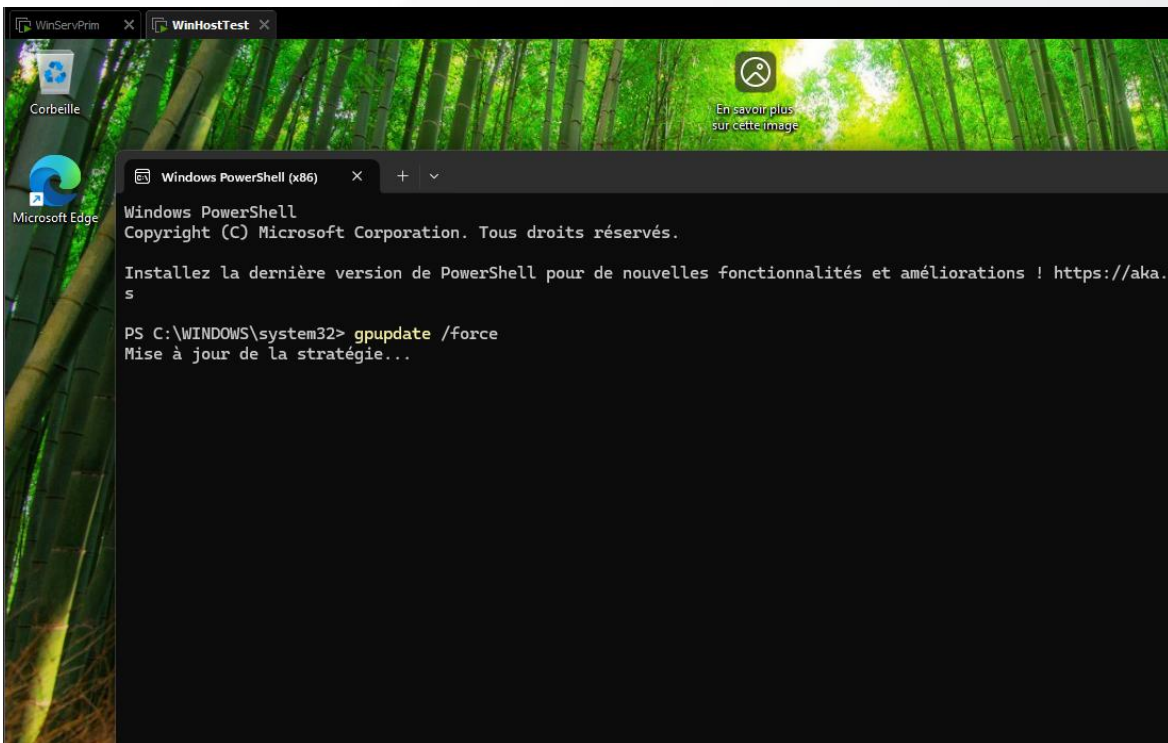
Ce paramètre vous permet de spécifier le papier peint du Bureau des utilisateurs et empêche ces derniers de modifier l'image ou sa présentation. Le papier peint spécifié peut être enregistré dans un fichier de type bitmap (*.bmp) ou JPEG (*.jpg).

- Choisir style : Ajuster.

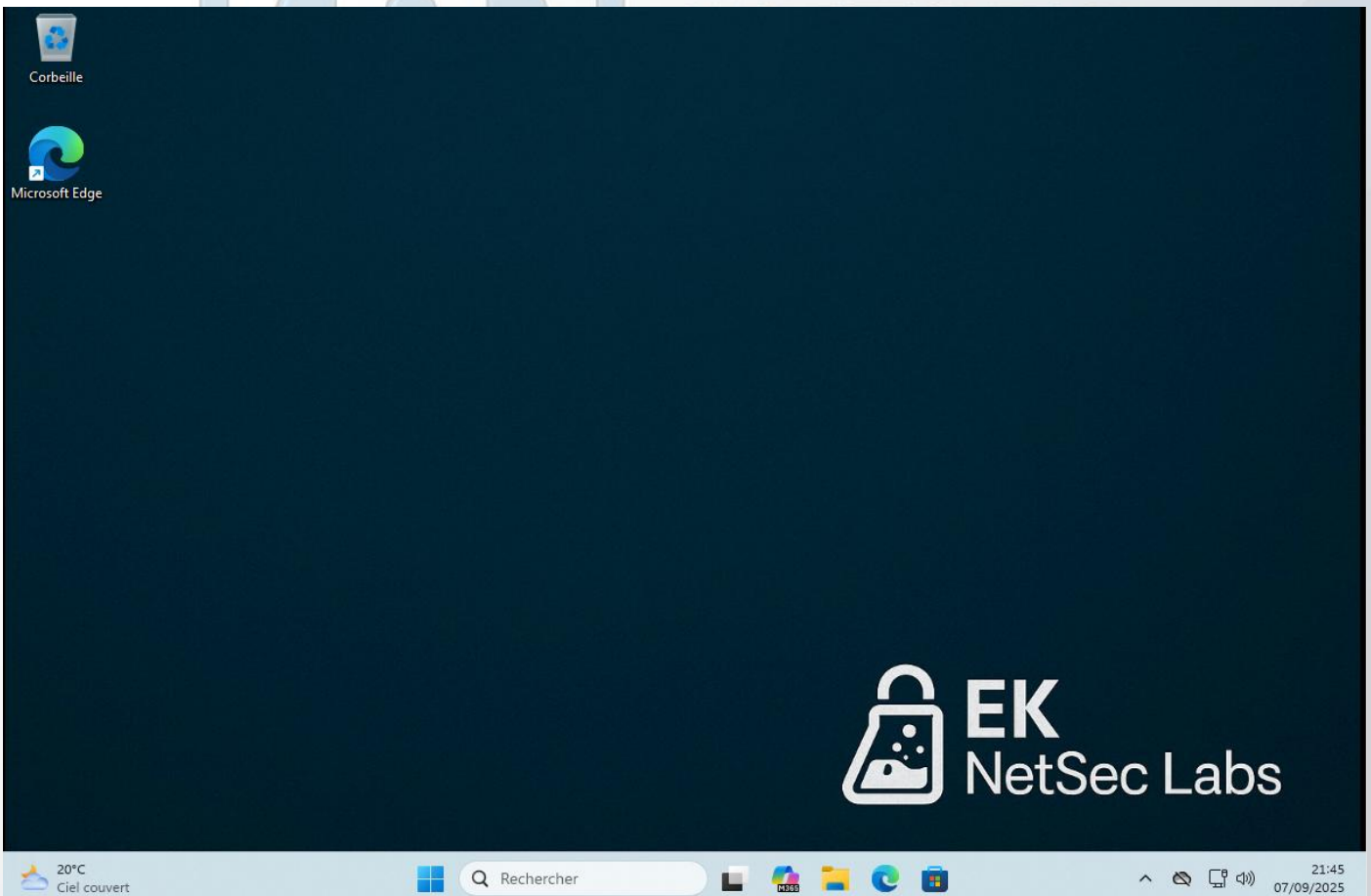
4. Forcer et tester la GPO

- Sur le client WIN-CLIENT-01, ouvrir une session avec un utilisateur IT.
- Dans un terminal, lancer :

```
gpupdate /force
```



- Vérifier que le fond d'écran s'applique.
- Si besoin, redémarrer le poste.



Vérification et diagnostic

- Vérifier les GPO appliquées :

```
gpresult /r
```

- Confirmer que GPO-IT-FondEcran est listée.

```
Stratégie de groupe appliquée depuis : WIN-SRV-HOST-001.ek-netseclabs.lan
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : EK-NETSECLABS
Type de domaine : Windows 2008 ou supérieur
```

```
Objets Stratégie de groupe appliqués
```

```
-----
GPO-IT-FondEcran-
```

```
Les objets stratégie de groupe n'ont pas été appliqués
car ils ont été refusés
```

```
-----
Stratégie de groupe locale
Filtrage : Non appliqué (vide)
```

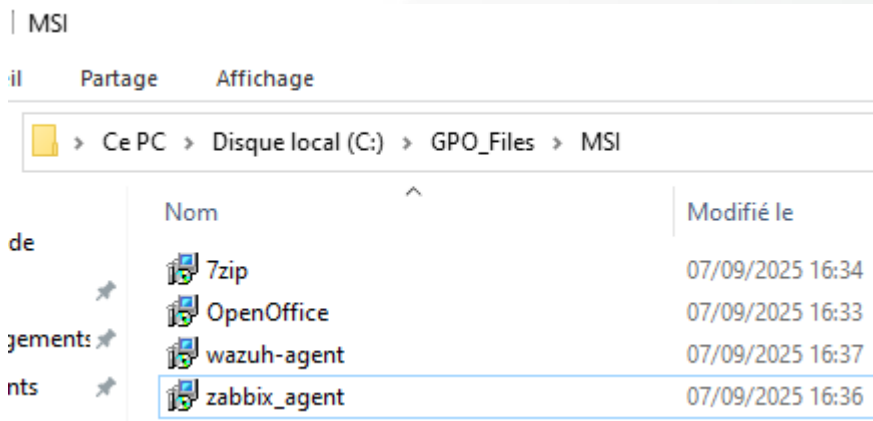
```
L'utilisateur fait partie des groupes de sécurité suivants
```

```
-----
Utilisateurs du domaine
Tout le monde
Utilisateurs
INTERACTIF
OUVERTURE DE SESSION DE CONSOLE
Utilisateurs authentifiés
Cette organisation
LOCAL
GG-IT-Users
Identité déclarée par une autorité d'authentification
Niveau obligatoire moyen
```

PARTIE GPO (DEPLOIEMENT LOGICIELS & AGENTS)

PREPARER LES FICHIERS MSI

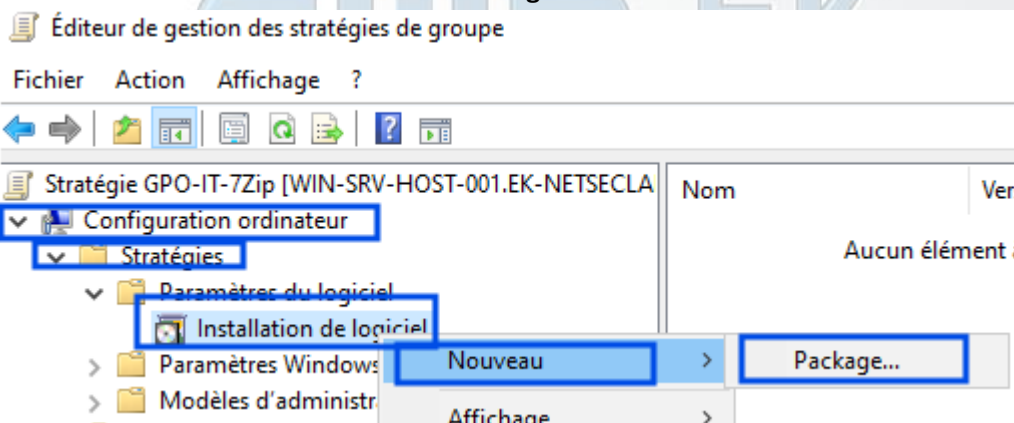
- Créer un dossier dédié dans le partage :
\\WIN-SRV-HOST-00\GPO_Files\MSI
- Copier les fichiers suivants :
 - 7zip.msi
 - openoffice.msi
 - zabbix_agent.msi
 - wazuh_agent.msi



Déploiement logiciel par service

Service IT → 7-Zip

1. Dans **GPMC**, créer une GPO : GPO-IT-7Zip.
2. Lier cette GPO à l'OU **IT**.
3. Éditer la GPO :
 - **Configuration ordinateur** → **Stratégies** → **Paramètres logiciels** → **Installation de logiciels**.
 - Clic droit → **Nouveau** → **Package**.



- Sélectionner : \\WIN-SRV-HOST-001\GPO_Files\MSI\7zip.msi.
- Mode : **Attribué**.

3. Déploiement des agents de monitoring

Zabbix Agent

1. Créer une GPO GPO-IT-ZabbixAgent.
2. Lier à l'OU **IT** (ou à toutes les OU si l'agent doit être universel).
3. Ajouter le package : \\WIN-SRV-HOST-001\GPO_Files\MSI\zabbix_agent.msi.
4. Mode : **Assigné**.

Wazuh Agent

1. Créer une GPO GPO-IT-WazuhAgent.
2. Lier à l'OU **IT** (ou global si voulu).
3. Ajouter le package MSI : wazuh_agent.msi.
4. Mode : **Assigné**.
5. Script de configuration possible via GPO de **Démarrage ordinateur**.

4. Tester le déploiement

- Redémarrer un client joint au domaine (ex. WIN-CLIENT-01).

- Vérifier que les logiciels et agents s'installent automatiquement.
- Commande utile :
- `gpresult /r`

Il se peut que la stratégie de groupe concernant l'installation des applications et des agents ne remonte pas. Dans ce cas il faut :

1. Vérifier l'emplacement des machines dans l'AD

- Ouvrir **Utilisateurs et ordinateurs Active Directory (ADUC)**.
- Déplacer les postes clients dans l'OU correspondante :
Exemple : 1-Postes > IT > WIN-CLIENT-0001.

2. Lier la GPO à l'OU des ordinateurs

- Dans la **Gestion des stratégies de groupe (GPMC)**.
- Sélectionner l'OU 1-Postes > IT.
- Lier la GPO de déploiement logiciel (ex. GPO-IT-7Zip).
Les GPO de logiciels doivent être liées aux **OU d'ordinateurs** et non aux OU des utilisateurs.

3. Configurer le filtrage de sécurité de la GPO

- Dans la GPMC, sélectionner la GPO.
- Onglet **Délégation** → **Avancé**.
- Ajouter le groupe **Ordinateurs du domaine** s'il n'est pas présent.
- Cocher les autorisations :
 - **Lecture**
 - **Appliquer la stratégie de groupe**

4. Forcer l'application sur le client

- Redémarrer le poste client.
- Forcer une mise à jour des stratégies :

```
gpupdate /force  
gpresult /r
```

- Vérifier que la GPO apparaît dans **Configuration ordinateur** → **Stratégies appliquées**.

5. Validation

- Après redémarrage, le logiciel (ex. 7-Zip) est automatiquement installé sur le poste client.
- Vérifier dans *Programmes et fonctionnalités* que l'application est présente.

MISE EN PLACE DE WSUS

INSTALLATION DU ROLE WSUS

- Accéder au **Gestionnaire de serveur** → **Ajouter des rôles et fonctionnalités**.
- Sélectionner **Windows Server Update Services**.
- Ajouter les rôles et fonctionnalités nécessaires (IIS inclus automatiquement).
- Valider et installer.

CONFIGURATION POST-INSTALLATION

- Ouvrir la console **WSUS**.
- Lancer l'**Assistant de configuration WSUS**.
 - Synchronisation avec **Microsoft Update**.



Choisir le serveur en amont

Indiquez le serveur en amont à partir duquel le contenu doit être synchronisé

Avant de commencer
Programme d'amélioration
de Microsoft Update

Choisir le serveur en amont

Définir le serveur proxy

Choisir les langues

Choisir les produits

Choisir les classifications

Configurer la planification
de la synchronisation



Vous pouvez choisir le serveur en amont à partir duquel votre serveur doit synchroniser les mises à jour.

☒ Synchroniser à partir de Microsoft Update

☐ Synchroniser à partir d'un autre serveur Windows Server Update Services

Nom du serveur :

Numéro du port :

- Se connecter au serveur en amont -> Démarrer la connexion



Assistant de configuration de Windows Server Update Services:WIN-SRV-HOST-00



Se connecter au serveur en amont

Téléchargez les informations de mise à jour à partir de Microsoft Update

Avant de commencer
Programme d'amélioration
de Microsoft Update

Choisir le serveur en amont

Définir le serveur proxy

Choisir les langues

Choisir les produits

Choisir les classifications

Configurer la planification
de la synchronisation

Terminé

Étapes suivantes



Pour configurer Windows Server Update Services sur les écrans suivants, nous devons appliquer vos paramètres de serveur en amont et de serveur proxy, et synchroniser les informations relatives aux mises à jour disponibles.

Les informations à télécharger comprennent :

les types de mises à jour disponibles ;
les produits qui peuvent être mis à jour ;
les langues disponibles.

Cliquez sur **Démarrer la connexion** pour enregistrer et télécharger les informations relative au serveur en amont et au serveur proxy. Ce processus peut prendre plusieurs minutes selon la vitesse de votre connexion.

Démarrer la connexion

Agrêter la connexion

- Choisir les langues (laisser *français* + *anglais*).
- Choisir les produits (Windows).



Choisir les produits

Sélectionnez les produits Microsoft à mettre à jour

Avant de commencer
Programme d'amélioration
de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification
de la synchronisation
Terminé
Étapes suivantes



Vous pouvez indiquer les produits pour lesquels vous souhaitez des mises à jour.

Produits :

- ☐ Kernel Updates
- ☒ Windows
 - ☒ Azure Stack HCI
 - ☒ Gestionnaire de serveur Windows – Programme d'installation dynamique
 - ☒ Microsoft Defender Antivirus
 - ☒ Microsoft Defender for Endpoint
 - ☒ Microsoft Edge
 - ☒ Microsoft Server operating system-21H2
 - ☒ Microsoft Server Operating System-22H2
 - ☒ Microsoft Server Operating System-23H2
 - ☒ Microsoft Server Operating System-24H2
 - ☒ Mise à jour de sélection du navigateur UE - Pour l'Europe uniquement
 - ☒ OOBE ZDP

- Choisir les classifications (Mises à jour critiques, Sécurité, Définitions...).



Choisir les classifications

Sélectionnez les classifications à télécharger

Avant de commencer
Programme d'amélioration
de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification
de la synchronisation
Terminé
Étapes suivantes



Vous pouvez indiquer la classification de mises à jour à synchroniser.

Classifications :

- ☒ Toutes les classifications
- ☐ Ensemble de mises à jour
- ☐ Feature Pack
- ☒ Jeux de pilotes
- ☒ Mise à jour critique
- ☒ Mise à jour de la sécurité
- ☐ Mise à jour
- ☒ Mises à jour de définitions
- ☒ Outil
- ☒ Pilote
- ☐ Service Pack
- ☒ Upgrades

Toutes les classifications, y compris celles ajoutées ultérieurement.

- Planifier la synchronisation (ex. 1 fois par jour).



Définir la planification de la synchronisation

Configurez ce paramètre lorsque ce serveur est synchronisé avec Microsoft Update

Avant de commencer
Programme d'amélioration
e Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification
e la synchronisation
Terminé
Tapes suivantes



Vous pouvez synchroniser les mises à jour manuellement ou définir une planification pour une synchronisation quotidienne automatique.

☐ Synchroniser manuellement

☒ Synchroniser automatiquement

Première synchronisation : 21:16:00

Synchronisations par jour : 1

Lors de la planification d'une synchronisation quotidienne à partir de Microsoft Update, notez que l'heure de début effective sera décalée d'une trentaine de minutes au maximum par rapport à celle indiquée.

< Précédent

Suivant >

Terminer

Annuler

Mettre à jour les services

Fichier Action Affichage Fenêtre ?

Update Services

WIN-SRV-HOST-00

Services WSUS (Windows Server Update Services)

Ce composant logiciel enfichable permet de déployer de manière fiable et rapide les dernières mises à jour sur les ordinateurs. Pour établir une connexion à un serveur distant, cliquez sur Se connecter au serveur dans le menu Action.

Serveurs gérés à partir de cette console

WIN-SRV-HOST-00

État d'ordinateur WIN-SRV-HOST-00

Ordinateurs avec des erreurs :	0
Ordinateurs nécessitant des mises à jour :	0
Ordinateurs installés/non applicables :	0

État de mise à jour WIN-SRV-HOST-00

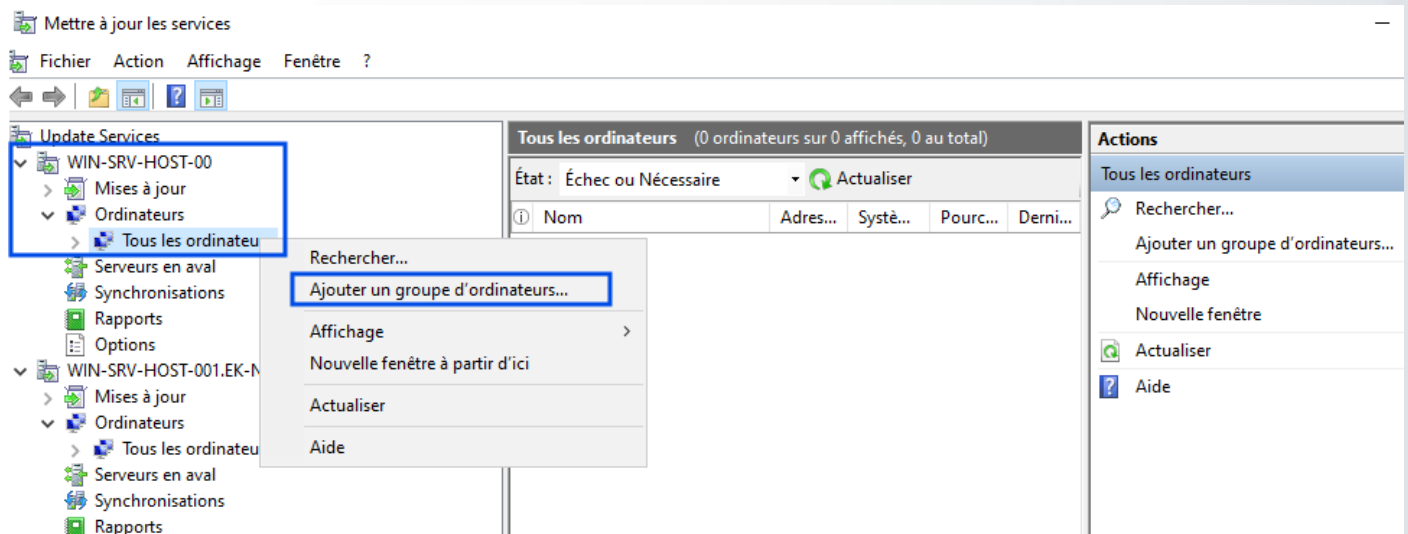
Mises à jour avec des erreurs :	0
Mises à jour requises par des ordinateurs :	0
Mises à jour installées/non applicables :	0

Actions

- Update Services
- Connexion au serveur...
- Affichage
- Nouvelle fenêtre
- Actualiser
- Aide

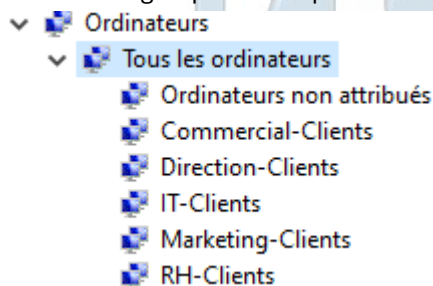
CREATION DES GROUPES WSUS

- Dans la console WSUS → créer des groupes cibles :



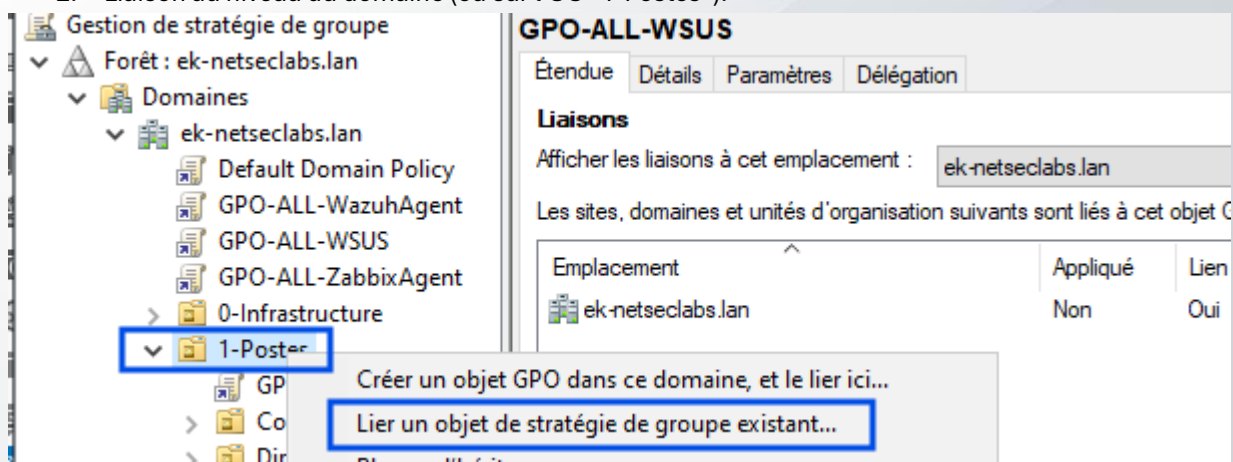
- IT-Clients
- Commercial-Clients
- RH-Clients
- etc.

- Ces groupes correspondent aux OU dans AD.



4. Configuration GPO pour WSUS

- Dans **GPMP**, créer une GPO (ex. GPO-ALL-WSUS).
- Liaison au niveau du domaine (ou sur l'OU "1-Postes").



Sélectionner un objet GPO

Rechercher dans ce domaine :

ek-netsedabs.lan

Objets de stratégie de groupe :

Nom
Default Domain Controllers Policy
Default Domain Policy
GPO-ALL-WazuhAgent
GPO-ALL-WSUS
GPO-ALL-ZabbixAgent
GPO-IT-7Zip
GPO-IT-FondEcran
GPO-IT-FondEcran-
GPO-IT-OpenOffice

3. Modifier la GPO :

- **Configuration ordinateur → Stratégies → Modèles d'administration → Composants Windows → Windows Update.**
- Activer :
 - **Spécifier l'emplacement intranet du service de mise à jour Microsoft :**
 - http://WIN-SRV-HOST-00:8530
 - http://WIN-SRV-HOST-00:8530

Spécifier l'emplacement intranet du service de mise à jour Microsoft

Spécifier l'emplacement intranet du service de mise à jour Microsoft

Paramètre précédent Paramètre suivant

☐ Non configuré ☒ Activé ☐ Désactivé

Commentaire :

Pris en charge sur : Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de Windows

Options :

Configurer le service de Mise à jour pour la détection des mises à jour : http://WIN-SRV-HOST-00:8530

Configurer le serveur intranet de statistiques : http://WIN-SRV-HOST-00:8530

Définir le serveur de téléchargement alternatif : (exemple: https://IntranetUpd01)

☐ Télécharger les fichiers sans URL dans les métadonnées si un serveur de téléchargement alternatif est défini.

☐ Ne pas appliquer l'épingle de certificat TLS du client Windows Update pour la détection des mises à jour.

Aide :

Spécifie l'emplacement du service de mise à jour automatique.

Ce paramètre recherche des mises à jour.

Pour utiliser ce paramètre, spécifiez un serveur de téléchargement alternatif.

- **Configuration du mode de mise à jour automatique → 4 (téléchargement auto + installation planifiée).**
- **Planifier l'installation** (ex. tous les jours à 12h).

Configuration du service Mises à jour automatiques

Configuration du service Mises à jour automatiques

Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :
☒ Activé
☐ Désactivé

Pris en charge sur : Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3
Option 7 uniquement prise en charge sur les serveurs ou au moins édition Windows Server 2016

Options : Aide :

Configuration de la mise à jour automatique :

4 - Téléchargement automatique et planification des installations

Les paramètres suivants ne sont nécessaires et ne s'appliquent que si l'option 4 est sélectionnée

☐ Installer durant la maintenance automatique

Jour de l'installation planifiée : 0 - Tous les jours

Heure de l'installation planifiée : 12:00

Si vous avez sélectionné « 4 - Téléchargement automatique et planification des installations » jour de l'installation planifiée et que vous avez spécifié une planification, vous pouvez également limiter l'exécution des mises à jour de manière hebdomadaire, bihebdomadaire ou mensuelle, à des options ci-dessous :

☒ Chaque semaine

☐ Première semaine du mois

☐ Deuxième semaine du mois

☐ Troisième semaine du mois

☐ Quatrième semaine du mois

☐ Installer les mises à jour d'autres produits Microsoft

Indique si l'ordinateur doit recevoir les mises à jour de sécurité et d'autres téléchargements importants via le service Mises à jour automatiques de Windows.

Remarque : cette stratégie ne s'applique pas à Windows RT.

Ce paramètre de stratégie vous permet de spécifier si les mises à jour automatiques sont activées sur cet ordinateur. Si le service est activé, vous devez sélectionner l'une des quatre options du paramètre de stratégie de groupe :

2 = Avertir avant de télécharger et d'installer des mises à jour.

Lorsque Windows trouve des mises à jour s'appliquant à l'ordinateur, un message indique à l'utilisateur que des mises à jour sont prêtes pour le téléchargement. Après avoir accédé à Windows Update, les utilisateurs peuvent télécharger et installer les mises à jour disponibles.

3 = (Valeur par défaut) Télécharger automatiquement les mises à jour et avertir l'utilisateur lorsqu'elles sont prêtes pour l'installation

Windows trouve des mises à jour s'appliquant à votre ordinateur et les télécharge en tâche de fond (l'utilisateur n'est ni averti ni interrompu au cours du processus). Une fois les téléchargements terminés, un message indique aux utilisateurs que les mises à jour sont prêtes à être installées. Après avoir accédé à Windows Update, les utilisateurs peuvent les installer.

4 = Télécharger automatiquement les mises à jour et les installer selon la planification spécifiée.

5. Validation côté client

- Sur WIN-CLIENT-0001 :
 - Forcer une mise à jour des stratégies :

```
gpupdate /force
```

Depuis une invite **cmd** (pas PowerShell) en admin :

```
usoclient StartScan
usoclient StartDownload
usoclient StartInstall
usoclient RefreshSettings
```

⚠ Ne donne pas de retour console, mais ça force bien la détection et l'envoi vers WSUS.

Mettre à jour les services

Fichier Action Affichage Fenêtre ?

Update Services

- WIN-SRV-HOST-00
 - Mises à jour
 - Ordinateurs
 - Tous les ordinateurs
 - Ordinateurs non attribués
 - Commercial-Clients
 - Direction-Clients
 - IT-Clients
 - Marketing-Clients
 - RH-Clients
 - Serveurs en aval
 - Synchronisations
 - Rapports
 - Options

Tous les ordinateurs (1 ordinateurs sur 1 affichés, 1 au total)

État : Toutes Actualiser

Nom	Adresse IP	Système d'exploitati...	Pourcentage install...	Dernier rapport d'état
win-srv-host-001.ek-netseclabs.lan	fe80:f55d:2387:7f2d:7...	Windows Server 2022 ...	100%	11/09/2025 17:48

win-srv-host-001.ek-netseclabs.lan

État

- Mises à jour avec des erreurs : 0
- Mises à jour nécessaires : 0
- Mises à jour installées/non applicables : 85694
- Mises à jour sans état : 0

Appartenance au groupe : Tous les ordinateurs, Ordinateurs non attribués

SE : Windows Server 2022 Standard

Langue SE : fr-FR

Service Pack : Aucun

Adresse IP : fe80:f55d:2387:7f2d:7f11%9



EK
NETSEC
LABS

MISE EN PLACE DE LA REDONDANCE AD/DNS/DHCP

PREPARER LA VM WIN-SRV-HOST-2

- Créer une nouvelle VM sous VMware.
- Allouer **4–8 Go RAM, 2–4 CPU, 40 Go disque**.
- Ajouter **1 carte réseau en Bridged (VMnet0)**.
- Installer **Windows Server 2022 Standard**.
- Renommer la machine :
 - WIN-SRV-HOST-002
- Attribuer une IP fixe :
 - IP : 192.168.1.11
 - Masque : 255.255.255.0
 - Passerelle : 192.168.1.254
 - DNS préféré : 192.168.1.10 (DC1)
 - DNS auxiliaire : 127.0.0.1 (sera utile après répllication)

JOINDRE LA MACHINE AU DOMAINE

- Tester la connexion entre les hôtes
 - ping 192.168.1.10
 - ping win-srv-host-001.ek-netseclabs.lan
 - nslookup win-srv-host-001.ek-netseclabs.lan

```
C:\Users\Administrateur>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>ping win-srv-host-001.ek-netseclabs.lan

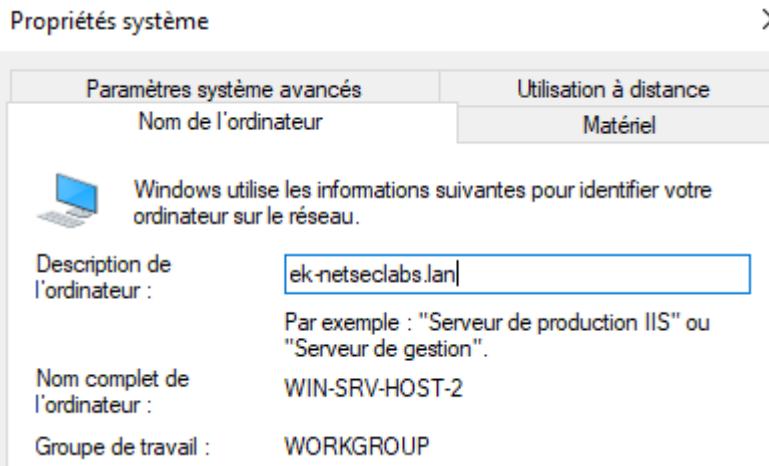
Envoi d'une requête 'ping' sur win-srv-host-001.ek-netseclabs.lan [192.168.1.10] avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>nslookup win-srv-host-001.ek-netseclabs.lan
Serveur :    Unknown
Address:  192.168.1.10

Nom :      win-srv-host-001.ek-netseclabs.lan
Addresses: 2001:861:4d00:1320:735f:2187:fee4:9175
           192.168.1.10
           10.20.0.10
```

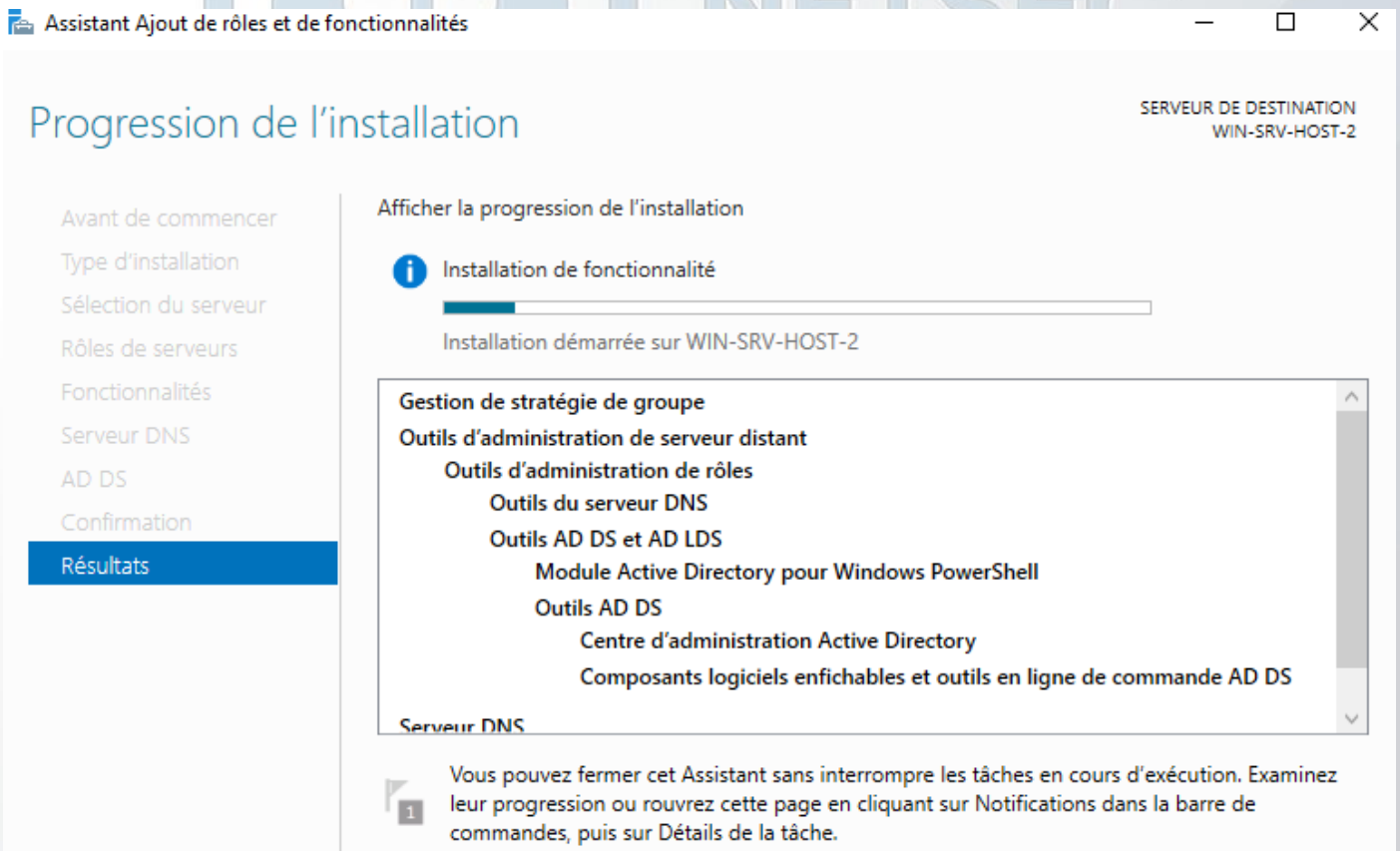
- Ouvrir **Paramètres > Système > À propos de > Renommer ce PC (domaine)**.
- Rejoindre le domaine :
 - ek-netseclabs.lan



- Redémarrer la VM.

PROMOUVOIR EN CONTROLEUR DE DOMAINE SECONDAIRE

- Depuis le **Gestionnaire de serveur** → Ajouter rôles et fonctionnalités.
- Installer :
 - **AD DS**
 - **DNS Server**



- Une fois installé → **Promouvoir ce serveur en contrôleur de domaine**.

- Choisir :
 - Ajouter un contrôleur de domaine à un domaine existant.
 - Domaine : ek-netseclabs.lan.
 - Fournir des identifiants admin du domaine.

Sélectionner l'opération de déploiement

☒ Ajouter un contrôleur de domaine à un domaine existant

☐ Ajouter un nouveau domaine à une forêt existante

☐ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine :

Fournir les informations d'identification pour effectuer cette opération

- Cocher : **Catalogue global (GC).**
- Ne pas cocher **Serveur DNS en lecture seule.**

Options du contrôleur de domaine

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Spécifier les capacités du contrôleur de domaine et les informations sur le site

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Nom du site :

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

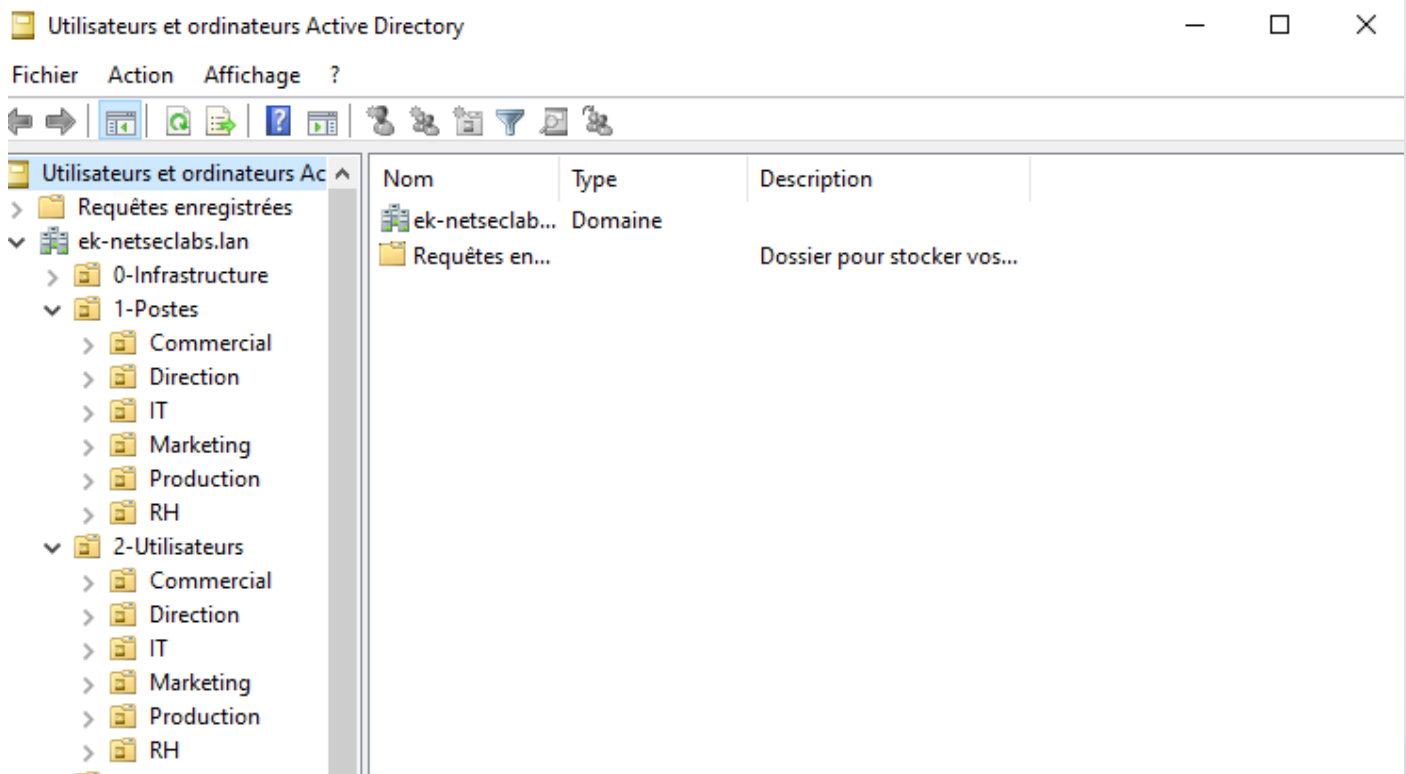
Mot de passe :

Confirmer le mot de passe :

- Terminer et redémarrer.

VERIFIER LA REPLICATION AD & DNS

- Sur DC2 : ouvrir **Utilisateurs et ordinateurs Active Directory** → vérifier que les OU et comptes sont présents.



- Tester réplcation :

```
repadmin /replsummary
repadmin /showrepl
```

```
C:\Users\Administrateur.EK-NETSECLABS>repadmin /replsummary
Heure de début du résumé de la réplcation : 2025-09-11 20:41:04

Début de la collecte des données pour le résumé de la réplcation ;
cette opération peut prendre un certain temps :
.....

DSA source                différence max    nb échecs %%    erreur
WIN-SRV-HOST-00           02m:59s         0 / 5          0

DSA de destination        différence max    nb échecs %%    erreur
WIN-SRV-HOST-2           02m:59s         0 / 5          0
```

```
C:\Users\Administrateur.EK-NETSECLABS>repadmin /showrepl

Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Default-First-Site-Name\WIN-SRV-HOST-2
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : f9c4c250-04b2-4d63-84b7-8e285be49731
ID de l'invocation DSA : 51ef0fac-e48e-4b8b-9fd2-90ed25493de6

=== INSTANCES VOISINES ENTRANTES =====

DC=ek-netseclabs,DC=lan
  Default-First-Site-Name\WIN-SRV-HOST-00 via RPC
  GUID de l'objet DSA : 7450d1b3-7bf3-448f-aeb3-86ce63b59911
  La dernière tentative, le 2025-09-11 20:38:05, a réussi.

CN=Configuration,DC=ek-netseclabs,DC=lan
  Default-First-Site-Name\WIN-SRV-HOST-00 via RPC
  GUID de l'objet DSA : 7450d1b3-7bf3-448f-aeb3-86ce63b59911
  La dernière tentative, le 2025-09-11 20:38:05, a réussi.

CN=Schema,CN=Configuration,DC=ek-netseclabs,DC=lan
  Default-First-Site-Name\WIN-SRV-HOST-00 via RPC
  GUID de l'objet DSA : 7450d1b3-7bf3-448f-aeb3-86ce63b59911
  La dernière tentative, le 2025-09-11 20:38:05, a réussi.

DC=DomainDnsZones,DC=ek-netseclabs,DC=lan
  Default-First-Site-Name\WIN-SRV-HOST-00 via RPC
  GUID de l'objet DSA : 7450d1b3-7bf3-448f-aeb3-86ce63b59911
  La dernière tentative, le 2025-09-11 20:38:05, a réussi.

DC=ForestDnsZones,DC=ek-netseclabs,DC=lan
  Default-First-Site-Name\WIN-SRV-HOST-00 via RPC
  GUID de l'objet DSA : 7450d1b3-7bf3-448f-aeb3-86ce63b59911
  La dernière tentative, le 2025-09-11 20:38:05, a réussi.
```

- Tester DNS :

```
nslookup win-srv-host-001.ek-netseclabs.lan
nslookup win-srv-host-002.ek-netseclabs.lan
```

```
C:\Users\Administrateur.EK-NETSECLABS>nslookup win-srv-host-001.ek-netseclabs.lan
Serveur : localhost
Address: 127.0.0.1

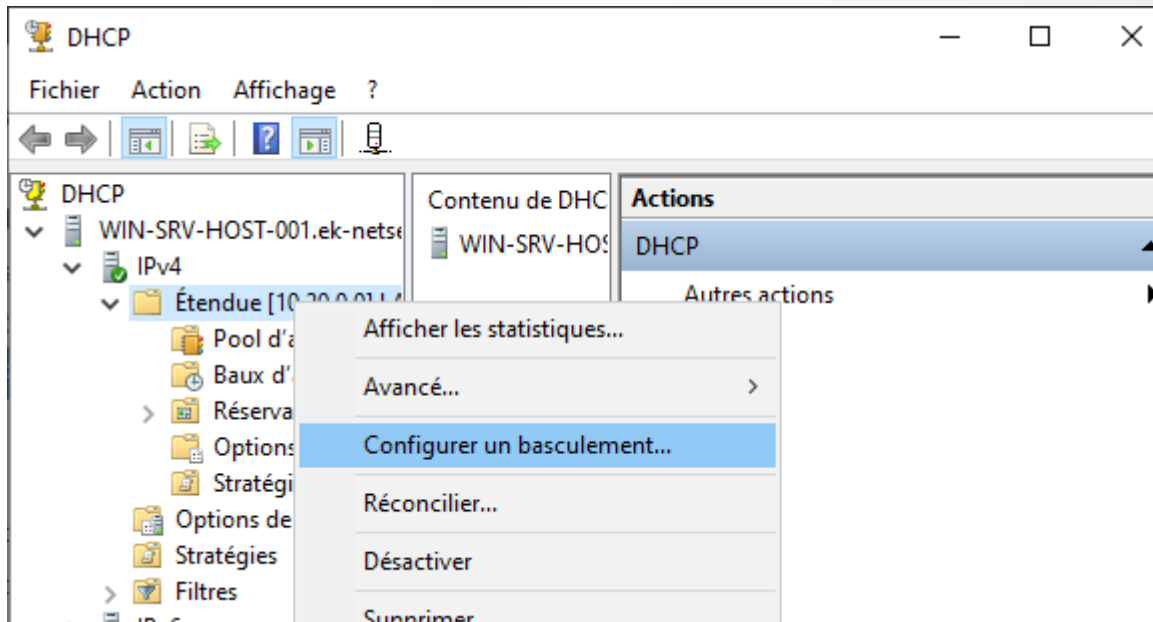
Nom : win-srv-host-001.ek-netseclabs.lan
Addresses: 2001:861:4d00:1320:735f:2187:fee4:9175
          192.168.1.10
          10.20.0.10

C:\Users\Administrateur.EK-NETSECLABS>nslookup win-srv-host-001.ek-netseclabs.lan
Serveur : localhost
Address: 127.0.0.1

Nom : win-srv-host-001.ek-netseclabs.lan
Addresses: 2001:861:4d00:1320:735f:2187:fee4:9175
          10.20.0.10
          192.168.1.10
```

MISE EN PLACE DU DHCP EN REDONDANCE (FAILOVER)

- Ouvrir la console **DHCP Manager** sur WIN-SRV-HOST-001.
- Cliquer droit sur l'étendue DHCP à répliquer.
- Sélectionner **Configurer le basculement (Failover)**.



- Ajouter le serveur partenaire WIN-SRV-HOST-002.
- Choisir le mode de basculement :
 - **Équilibrage de charge (Load balance)** → répartir les baux IP entre les deux serveurs (50/50 par défaut).

Configurer un basculement

Créer une relation de basculement



Créer une relation de basculement avec le partenaire WIN-SRV-HOST-2

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode :

Pourcentage d'équilibrage de charge

Serveur local : %

Serveur partenaire : %

☐ Intervalle de basculement d'état : minutes

☒ Activer l'authentification du message

Secret partagé :

< Précédent

Suivant >

Annuler

- **Secours (Hot standby)** → laisser un serveur principal et basculer sur le second uniquement en cas de panne.
- **Valider** les paramètres de répllication et **appliquer** la configuration.
- **Vérifier** que l'étendue DHCP est bien visible et active sur WIN-SRV-HOST-002.

DHCP

Fichier Action Affichage ?



DHCP

WIN-SRV-HOST-2.ek-netseclabs.lan

IPv4

Étendue [10.20.0.0] LAN_LABO_10.20.0.0

Pool d'adresses

Baux d'adresses

> Réservations

Options d'étendue

Contenu de l'étendue

Pool d'adresses

Baux d'adresses

Réservations

Options d'étendue

Stratégies

ÉTAPES DE VERIFICATION

- **Éteindre** temporairement WIN-SRV-HOST-001.
- **Allumer** un client et **forcer** le renouvellement d'adresse IP avec la commande :

```
ipconfig /renew
```

- **Vérifier** que le client reçoit bien une adresse IP depuis WIN-SRV-HOST-002.
- **Relancer** WIN-SRV-HOST-001 et **confirmer** que la répartition ou la reprise fonctionne correctement.

MISE EN PLACE DE DNSSEC

PREPARER L'ENVIRONNEMENT DNSSEC

- Vérifier que les rôles **DNS** sont installés sur WIN-SRV-HOST-001 et WIN-SRV-HOST-002.
- Ouvrir la console **DNS Manager** sur WIN-SRV-HOST-001.
- Localiser la zone de ton domaine :
 - ek-netseclabs.lan

SIGNER LA ZONE DNS

- Clic droit sur la zone → **Signer la zone....**

Gestionnaire de serveur

Gestionnaire DNS

Fichier Action Affichage ?

DNS

WIN-SRV-HOST-001.ek-netseclabs.lan

Zones de recherche directes

_msdcs.ek-netseclabs.lan

ek-netseclabs.lan

Mettre à jour un fichier de données du serveur

Charger à nouveau

Nouvel hôte (A ou AAAA)...

Nouvel alias (CNAME)...

Nouveau serveur de messagerie (MX)...

Nouveau domaine...

Nouvelle délégation...

Nouveaux enregistrements...

DNSSEC

Toutes les tâches

Affichage

Supprimer

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
Source de nom (SOA)	[71], win-srv-host-001.ek-...	statique	
Serveur de noms (NS)	win-srv-host-001.ek-netse...	statique	
Hôte (A)	10.20.1.11	11/09/2025 20:00:00	
Hôte (A)	10.20.0.10	13/09/2025 03:00:00	
Hôte (A)	192.168.1.10	13/09/2025 03:00:00	
Hôte (A)	192.168.1.11	11/09/2025 20:00:00	
DNSSEC	Signer la zone	07/09/2025 22:00:00	
	Supprimer la signature de la zone	statique	
	Propriétés	statique	11/09/2025 21:00:00

- Suivre l'assistant :
 - Utiliser les paramètres par défaut (clé KSK + ZSK générées automatiquement).

Assistant Signature de zone

Options de signature

Le serveur DNS prend en charge trois options de signature.



Choisissez l'une des options disponibles pour signer la zone :

☐ Personnalisez les paramètres de signature de zone.

Signe la zone avec un jeu de paramètres de signature de zone.

☐ Signer la zone à l'aide des paramètres d'une zone existante.

Signe la zone à l'aide des paramètres d'une zone signée existante.

Nom de la zone :

☒ Utiliser les paramètres pour signer la zone.

Signe la zone à l'aide des paramètres par défaut.

- **Algorithme recommandé** : RSA/SHA-256.
 - **Durée de vie de la clé** : laisser par défaut (peut être ajustée selon la politique de sécurité).
- Terminer → la zone est signée.

Gestionnaire DNS

Fichier Action Affichage ?

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[89], win-srv-host-001.ek-...	statique
(identique au dossier parent)	Serveur de noms (NS)	win-srv-host-2.ek-netsecl...	statique
(identique au dossier parent)	Serveur de noms (NS)	win-srv-host-001.ek-netse...	statique
(identique au dossier parent)	Hôte (A)	192.168.1.10	02/09/2025 22:00:00
(identique au dossier parent)	Hôte (A)	10.20.0.10	02/09/2025 22:00:00
(identique au dossier parent)	Hôte (A)	10.20.1.11	11/09/2025 20:00:00
(identique au dossier parent)	Hôte (A)	192.168.1.11	11/09/2025 20:00:00
(identique au dossier parent)	RR Signature (RRSIG)	[A][Inception(UTC): 13/09/...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[NS][Inception(UTC): 13/0...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[SOA][Inception(UTC): 13/...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[DNSKEY][Inception(UTC):...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[DNSKEY][Inception(UTC):...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[NSEC3PARAM][Inception...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	Next Secure 3 Parameter...	[SHA-1][0][50][40C020218...	statique
05vp1r46hgcni5mjmd8jjov3...	RR Signature (RRSIG)	[NSEC3][Inception(UTC): 1...	statique
05vp1r46hgcni5mjmd8jjov3...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
150465h29a5d8pc389vkiok...	RR Signature (RRSIG)	[NSEC3][Inception(UTC): 1...	statique
150465h29a5d8pc389vkiok...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
16cubi2ket1f6cnek8n173d...	RR Signature (RRSIG)	[NSEC3][Inception(UTC): 1...	statique

Gestionnaire DNS

Fichier Action Affichage ?

DNS

- WIN-SRV-HOST-2.ek-netsec
 - Zones de recherche directe
 - _msdcs.ek-netseclabs
 - ek-netseclabs.lan
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Zones de recherche inverses
 - Points d'approbation
 - Redirecteurs conditionnels

Nom	Type	Données	Horo
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[90], win-srv-host-2.ek-ne...	statiq
(identique au dossier parent)	Serveur de noms (NS)	win-srv-host-2.ek-netsecl...	statiq
(identique au dossier parent)	Serveur de noms (NS)	win-srv-host-001.ek-netse...	statiq
(identique au dossier parent)	Hôte (A)	192.168.1.10	02/09
(identique au dossier parent)	Hôte (A)	10.20.0.10	02/09
(identique au dossier parent)	Hôte (A)	10.20.1.11	11/09
(identique au dossier parent)	Hôte (A)	192.168.1.11	11/09
(identique au dossier parent)	RR Signature (RRSIG)	[DNSKEY][Inception(UTC):...	statiq
(identique au dossier parent)	RR Signature (RRSIG)	[DNSKEY][Inception(UTC):...	statiq
(identique au dossier parent)	RR Signature (RRSIG)	[A][Inception(UTC): 13/09/...	statiq
(identique au dossier parent)	RR Signature (RRSIG)	[NS][Inception(UTC): 13/0...	statiq
(identique au dossier parent)	RR Signature (RRSIG)	[NSEC3PARAM][Inception...	statiq
(identique au dossier parent)	RR Signature (RRSIG)	[SOA][Inception(UTC): 13/...	statiq

REPLICATION SUR LE SECOND DC

- La signature DNSSEC est stockée dans Active Directory → elle est automatiquement répliquée sur WIN-SRV-HOST-002.
- Vérifier la présence des enregistrements DNSSEC dans la zone depuis DC2.

CONFIGURER UNE GPO POUR APPLIQUER DNSSEC SUR LES POSTES CLIENTS

- Ouvrir la **console de gestion des stratégies de groupe (GPMC)**.
- Créer une nouvelle GPO (ex. GPO-ALL-DNSSEC).
- Lier la GPO sur l'OU **1-Postes** (ou directement au domaine si tu veux l'appliquer partout).
- Modifier la GPO :
 - Aller dans :
 - Configuration ordinateur
 - Stratégies
 - Paramètres Windows
 - Paramètres de sécurité
 - Stratégies de résolution de noms
- Ajouter une **Nouvelle stratégie de résolution de noms**.
- Indiquer le domaine :

ek-netseclabs.lan

- Activer DNSSEC dans cette règle

- Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Stratégie GPO-ALL-DNSSEC [WIN-SRV-HOST-001.EI]

- Configuration ordinateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Stratégie de résolution de noms
 - Scripts (démarrage/arrêt)
 - Paramètres de sécurité
 - QoS basée sur la stratégie
 - Modèles d'administration : définitions de
 - Préférences
 - Configuration utilisateur

Stratégie de résolution de noms

Vue d'ensemble

La table de stratégie de résolution de noms stocke les paramètres de configuration de la sécurité DNS (DNSSEC) et de DirectAccess sur les ordinateurs clients DNS. Vous pouvez utiliser cette page pour créer ou modifier des règles qui servent à élaborer des stratégies pouvant être appliquées à une unité d'organisation Active Directory.

[En savoir plus sur DNSSEC sur le Web](#)

Description

La stratégie de résolution de noms est l'objet de stratégie de groupe qui contient les informations de stratégie figurant dans la table de stratégie de résolution de noms.

Créer des règles

À quelle partie de l'espace de noms s'applique cette règle ?

Suffixe

Autorité de certification : (Facultatif)

DNSSEC Paramètres DNS pour DirectAccess Serveur DNS générique Codage

☒ Activer DNSSEC dans cette règle

Paramètres DNSSEC

Validation :

☒ Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS

IPsec :

☐ Utiliser IPsec dans les communications entre le client DNS et le serveur DNS

Type de chiffrement :

```
PS C:\WINDOWS\system32> Resolve-DnsName ek-netseclabs.lan
```

Name	Type	TTL	Section	IPAddress
ek-netseclabs.lan	A	600	Answer	192.168.1.10
ek-netseclabs.lan	A	600	Answer	10.20.0.10
ek-netseclabs.lan	A	600	Answer	10.20.1.11
ek-netseclabs.lan	A	600	Answer	192.168.1.11

```
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> Resolve-DnsName ek-netseclabs.lan
```

Name	Type	TTL	Section	IPAddress
ek-netseclabs.lan	AAAA	600	Answer	2a0d:e487:39f:565b:9594:7a9:f03a:9b72
ek-netseclabs.lan	A	600	Answer	10.20.0.10
ek-netseclabs.lan	A	600	Answer	192.168.1.10
ek-netseclabs.lan	A	600	Answer	192.168.1.11
ek-netseclabs.lan	A	600	Answer	10.20.1.11

```
Name       : ek-netseclabs.lan
QueryType  : RRSIG
TTL        : 600
Section    : Answer
TypeCovered : AAAA
Algorithm  : 8
LabelCount : 2
OriginalTtl : 600
Expiration : 23/09/2025 10:37:49
Signed     : 13/09/2025 09:37:49
Signer     : ek-netseclabs.lan
Signature  : {34, 204, 37, 26...}
```

SECURISATION DU SERVICE DHCP

AFFICHER LES BAUX D'ADRESSES ACTIFS

- Ouvrir le **Gestionnaire DHCP** depuis le serveur.
- Naviguer dans :
IPv4 → Baux d'adresses.
- Vérifier que la machine cliente (WIN-CLIENT-0001) possède bien une adresse IP délivrée par le serveur DHCP.

 DHCP

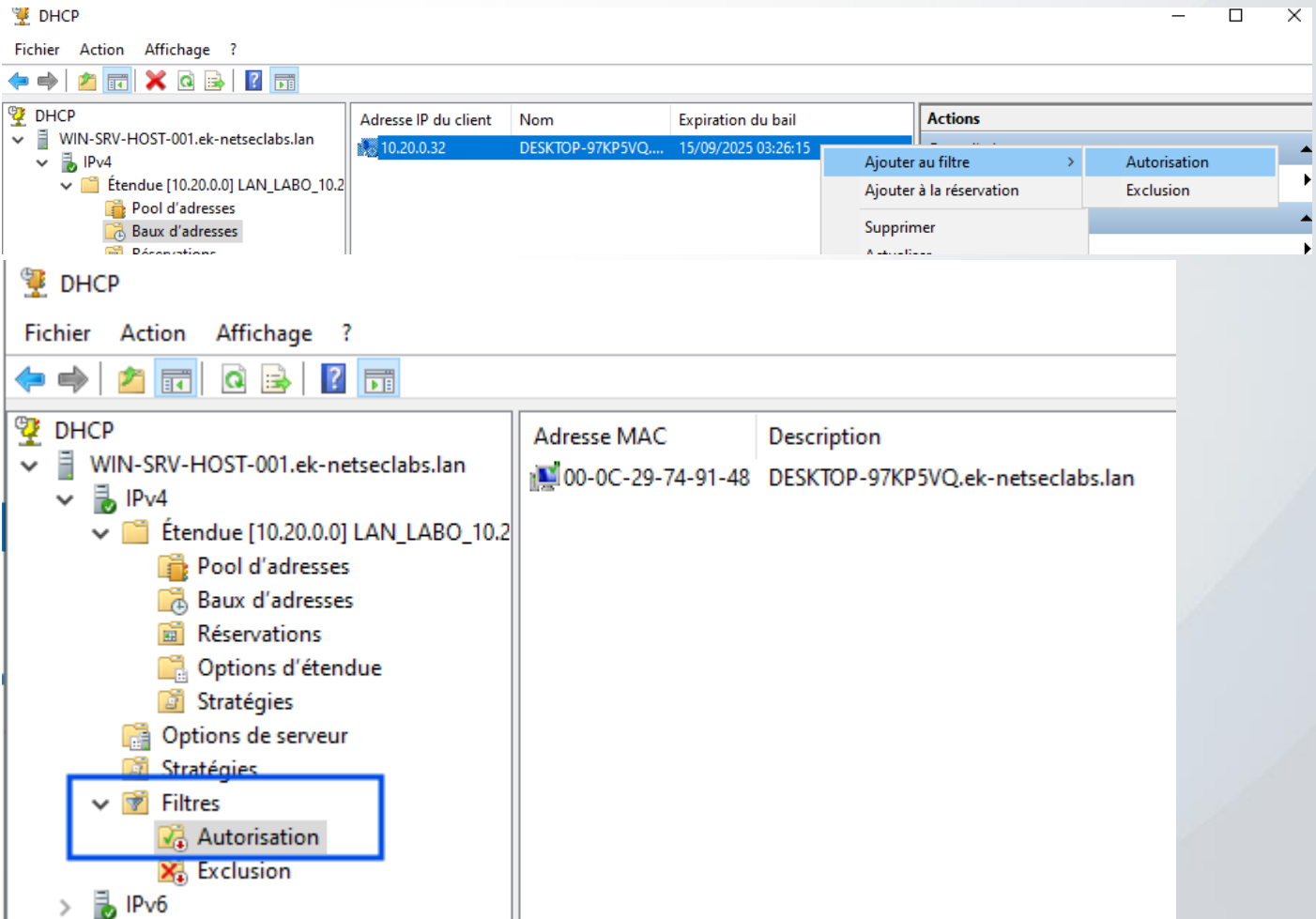
Fichier Action Affichage ?



DHCP	Adresse IP du client	Nom	Expiration du bail
- WIN-SRV-HOST-001.ek-netseclabs.lan - IPv4 - Étendue [10.20.0.0] LAN_LABO_10.2 - Pool d'adresses - Baux d'adresses - Réservations - Options d'étendue - Stratégies	10.20.0.32	DESKTOP-97KP5VQ....	15/09/2025 03:26:15

AUTORISER UN HOTE SPECIFIQUE

- Aller dans
 - IPv4 → Filtrage → Autoriser.
- Ajouter l'adresse MAC de la machine cliente dans la liste des hôtes autorisés.



The top screenshot shows the DHCP console with the 'Actions' menu open for the IP address 10.20.0.32. The 'Autorisation' option is highlighted. The bottom screenshot shows the DHCP console with the 'Filtres' folder expanded in the left pane, and the 'Autorisation' option selected.

1. Vérifier l'attribution IP

- Sur la machine cliente, exécuter :

```
ipconfig /release
ipconfig /renew
```

```
C:\Users\alice.durand>ipconfig /renew
```

Configuration IP de Windows

Carte Ethernet Ethernet0 :

```
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::1fd6:7186:aa95:40f2%8
Adresse IPv4. . . . . : 10.20.0.50
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 10.20.0.10
```

Carte Ethernet Ethernet1 :

```
Suffixe DNS propre à la connexion. . . . : lan
Adresse IPv6. . . . . : 2001:861:4d00:1320:7863:e781:8758:78b
Adresse IPv6 temporaire . . . . . : 2001:861:4d00:1320:49b7:8879:1c95:f4d7
Adresse IPv6 de liaison locale. . . . . : fe80::b495:2a5d:4aa2:75d0%13
Adresse IPv4. . . . . : 192.168.1.60
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : fe80::22b8:2bff:fe43:1025%13
                                192.168.1.254
```

- Déplacer vers la liste d'exclusion et vérifier de nouveau l'attribution de l'adresse IP

 DHCP

Fichier Action Affichage ?



 DHCP

WIN-SRV-HOST-001.ek-netseclabs.lan
 IPv4
 Étendue [10.20.0.0] LAN_LABO_10.2
 Pool d'adresses
 Baux d'adresses

Adresse MAC	Description
00-0C-29-74-91-48	DESKTOP-97KP5VQ.ek-netseclabs.lan
Modifier un filtre Déplacer vers la liste d'exclusion Supprimer	

```
C:\Users\alice.durand>ipconfig /renew
```

Configuration IP de Windows

L'attribution de l'adresse ip ne se fait pas.

DEPLOIEMENT PXE (WDS + MDT)

Objectif

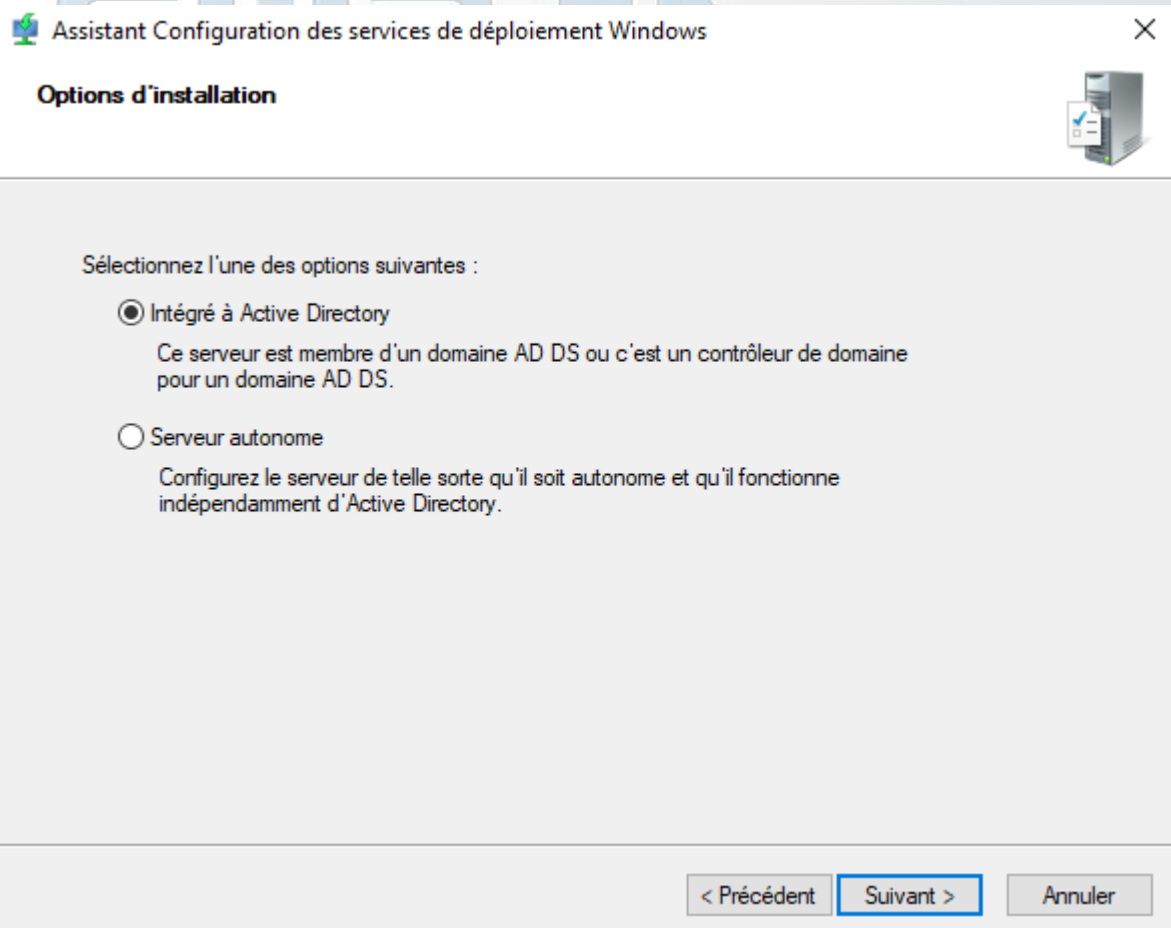
Mettre en place un service PXE permettant le déploiement automatisé de systèmes d'exploitation Windows sur les postes clients via le réseau.

INSTALLER LE ROLE WDS

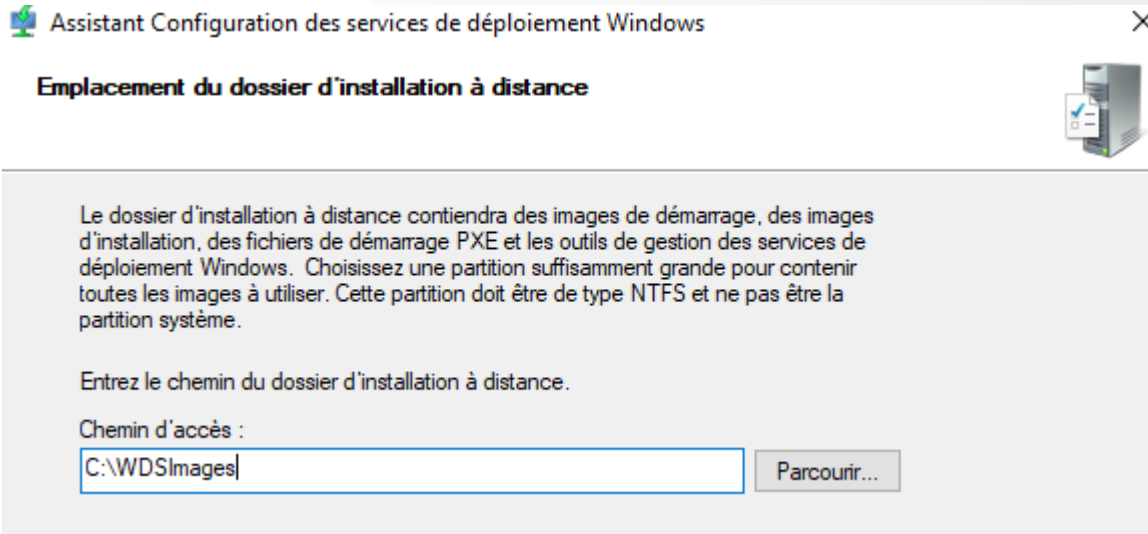
- Ouvrir **Server Manager** → *Ajouter des rôles et fonctionnalités*.
- Sélectionner **Services de déploiement Windows (WDS)**.
- Inclure les sous-rôles **Serveur de déploiement** et **Serveur de transport**.
- Lancer l'installation.

CONFIGURER WDS

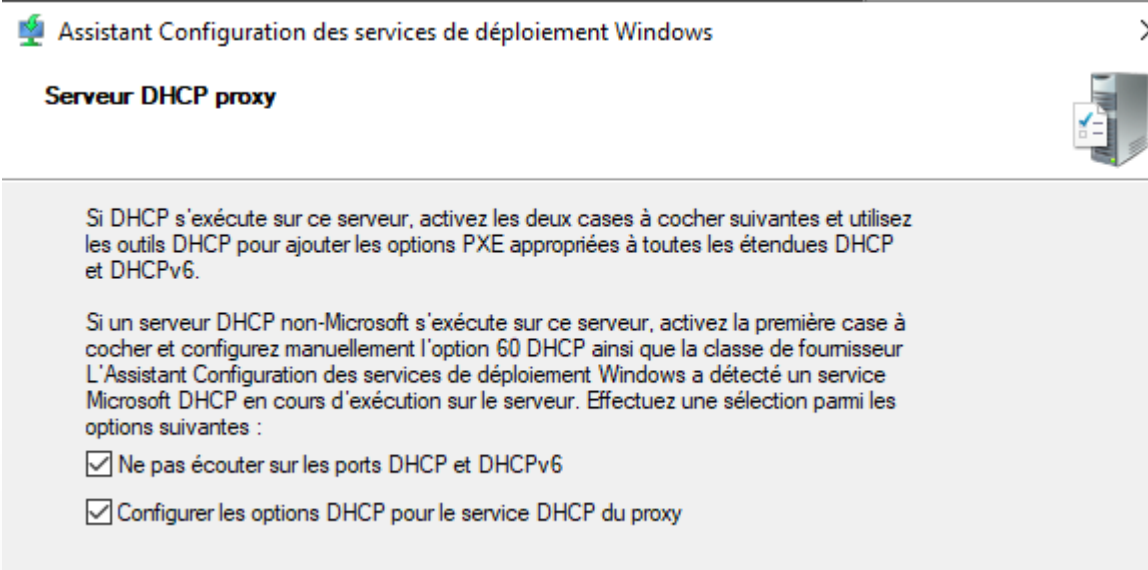
- Ouvrir la console **WDS**.
- Lors de l'assistant de configuration, choisir :
Intégré à Active Directory → recommandé, car le serveur fait partie du domaine ek-netseclabs.lan.



- Choisir un répertoire de stockage pour les images (D:\WDSImages).



- Cocher : **Ne pas écouter sur les ports DHCP et DHCPv6**
(permet d'éviter un conflit car DHCP est déjà installé sur le serveur).
- Cocher : **Configurer les options DHCP pour le service DHCP du proxy**
(WDS configurera automatiquement les options nécessaires pour PXE → option 60 "PXEClient").



- Sélectionner l'option **Répondre aux clients connus et inconnus** pour autoriser le boot PXE des machines.

Assistant Configuration des services de déploiement Windows

Paramètres initiaux du serveur PXE

Vous pouvez utiliser ces paramètres pour définir les ordinateurs clients auquel ce serveur doit répondre. Les clients connus sont les clients qui ont été préinstallés. Lorsque l'ordinateur physique effectue un démarrage PXE, le système d'exploitation s'installe selon les paramètres que vous avez définis.

Sélectionnez une des options suivantes :

☐ Ne répondre à aucun ordinateur client

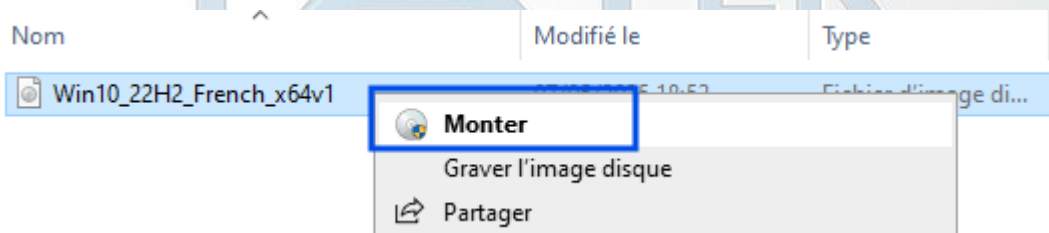
☐ Répondre uniquement aux ordinateurs clients connus

☒ Répondre à tous les ordinateurs clients (connus et inconnus)

☐ Exiger l'approbation administrateur pour les ordinateurs inconnus. Si vous utilisez cette option, approuvez les ordinateurs avec le nœud Périphériques en attente du composant logiciel enfichable. Les ordinateurs approuvés seront ajoutés à la liste des clients préinstallés.

3. Ajouter les images d'installation et de démarrage

- Monter l'ISO d'installation de Windows Server / Windows 10/11.



- Depuis la console WDS → Images de démarrage → Ajouter → sélectionner boot.wim.

Services de déploiement Windows

Fichier Action Affichage ?

Services de déploiement Windows

- Serveurs
 - WIN-SRV-HOST-2.ek-netsecclabs.l
 - Images d'installation
 - Images de démarrage**
 - Périphériques en attente
 - Transmission par multidiffusion
 - Pilotes
 - Périphériques de préinstallation Active

Images de démarrage

Nom de l'image	Architecture	État	Taille décompressée	Date	Version du système d'exploit
Microsoft Win...	x64	En li...	1932 Mo	14/0...	10.0.19041

Assistant Ajout d'images

Fichier image

Entrez l'emplacement du fichier image Windows contenant les images à ajouter.

Emplacement du fichier :

E:\sources\boot.wim

Parcourir...

Remarque : les images d'installation et de démarrage par défaut (Boot.wim et Install.wim) sont présentes sur le DVD d'installation dans le dossier \Sources.

- Depuis la console WDS → Images d'installation → Ajouter → sélectionner install.wim.

The screenshot shows the Windows Deployment Services (WDS) console on the left and the 'Assistant Ajout d'images' (Add Image Assistant) window on the right.

WDS Console:

- Tree view: Services de déploiement Windows > Serveurs > WIN-SRV-HOST-2.ek-netseclabs.l > Images d'installation
- Right pane: 'Images d'installation' showing a list of images. 'Windows 10 Pro Education N' is selected.
- Bottom pane: 'ImageGroup1' showing 1 image(s) d'installation.

Assistant Ajout d'images:

- Section: Fichier image
- Text: 'Entrez l'emplacement du fichier image Windows contenant les images à ajouter.'
- Field: 'Emplacement du fichier : E:\sources\install.wim' with a 'Parcourir...' button.
- Remark: 'Remarque : les images d'installation et de démarrage par défaut (Boot.wim et Install.wim) sont présentes sur le DVD d'installation dans le dossier \Sources.'

Nom de l'image	Architecture	État	Taille décompressée	Date	Version du système d'exploitation
Windows 10 P...	x64	En li...	14051 Mo	14/0...	10.0.19041

INSTALLER ET CONFIGURER MDT (MICROSOFT DEPLOYMENT TOOLKIT)

- Télécharger et installer **MDT** sur le serveur.

The screenshot shows the Microsoft Deployment Toolkit (MDT) download page. The browser address bar shows the URL: <https://www.microsoft.com/en-us/download/details.aspx?id=54259&msocid=187a9583e2546869247583e4e3cc697a>.

Microsoft Deployment Toolkit (MDT)

The Microsoft Deployment Toolkit (MDT) is for Windows operating system deployment.

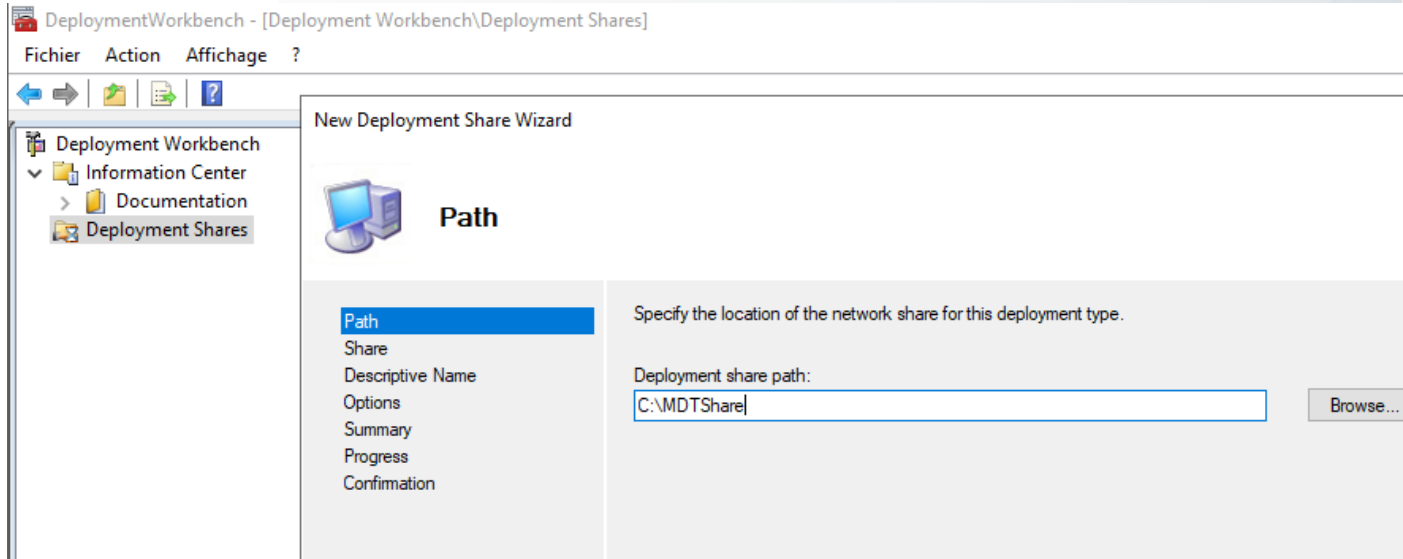
Important! Selecting a language below will dynamically change the complete page content to that language.

Select language: English (dropdown menu) [Download button]

Importer le système d'exploitation

- Ouvrir **Deployment Workbench**.

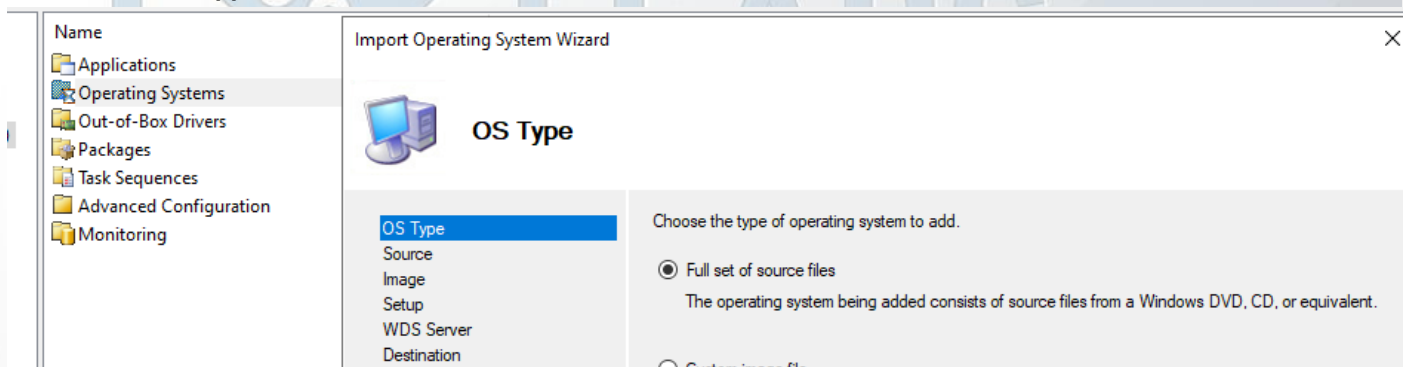
- Naviguer vers **Deployment Shares** → **MDT Deployment Share (C:\MDTShare)** → **Operating Systems**.



- Clic droit → **Import Operating System**.
- Choisir le type d'importation :
 - **Full set of source files** si l'on dispose de l'ISO complet de Windows.
- Donner un nom explicite à l'OS (ex. *Windows 10 Entreprise x64*).

Importer les applications

- Aller dans **Applications**.
- Clic droit → **New Application**.



- Choisir le type d'application :
 - **Application with source files** → pour les .msi (ex : 7zip.msi).
 - **Application without source files** → pour les scripts (PowerShell, batch).
 - **Application bundle** → pour regrouper plusieurs applis en un seul package.

New Application Wizard



Application Type

Application Type

Details

Source

Destination

Command Details

Summary

Specify the type of application to add.

☒ Application with source files

Copy the source files for this application to the deployment share, which will be used for installing the application.

- Renseigner le nom (ex. *7-Zip* ou *OpenOffice*) et terminer l'assistant.

New Application Wizard



Command Details

Application Type

Details

Source

Destination

Command Details

Summary

Progress

Confirmation

Specify the quiet install command line and working directory needed to install this application.

Command line:

`msiexec /i openoffice.msi /quiet /norestart`

Working directory:

`.\Applications\OpenOffice`

Importer les pilotes (optionnel mais recommandé)

- Aller dans **Out-of-Box Drivers**.
- Clic droit → **Import Drivers**.
- Sélectionner le dossier contenant les pilotes au format .inf.
- Les drivers réseau/chipset sont prioritaires pour que le boot PXE fonctionne sur du matériel physique.

Ajouter les mises à jour (optionnel)

- Aller dans **Packages**.
- Importer les correctifs, packs de langues ou mises à jour nécessaires.
- Cette étape peut être ignorée si un serveur WSUS est déjà déployé.

Créer une séquence de tâches

- Aller dans **Task Sequences**.
- Clic droit → **New Task Sequence**.
- Définir un ID (ex. TS-Win10-IT) et un nom explicite (ex. *Déploiement Windows 10 IT*).

- ▼ MDT Deployment Share (C:\MDTShare)
 - > Applications
 - > Operating Systems
 - > Out-of-Box Drivers
 - > Packages
 - > Task Sequences
 - > Advanced Configuration
 - > Monitoring



General Settings

General Settings

- Select Template
- Select OS
- Specify Product Key
- OS Settings
- Admin Password
- Summary
- Progress
- Confirmation

Specify general information about this task sequence. The task sequence ID is used internally as part of the deployment process. The task sequence name and comments are displayed by the deployment wizard.

Task sequence ID:

Task sequence name:

- Choisir le modèle **Standard Client Task Sequence**.
- Sélectionner l'OS importé.

New Task Sequence Wizard



OS Settings

- General Settings
- Select Template
- Select OS
- Specify Product Key
- OS Settings
- Admin Password
- Summary
- Progress
- Confirmation

Specify settings about this task sequence. These settings will be used for all deployments of this task sequence, unless overridden during the deployment process using the wizard or a rule.

Full Name:

Organization:

Internet Explorer Home Page:

- Renseigner le mot de passe Administrateur local.



Admin Password

- General Settings
- Select Template
- Select OS
- Specify Product Key
- OS Settings
- Admin Password
- Summary
- Progress
- Confirmation

Specify the local Administrator password for this task sequence.

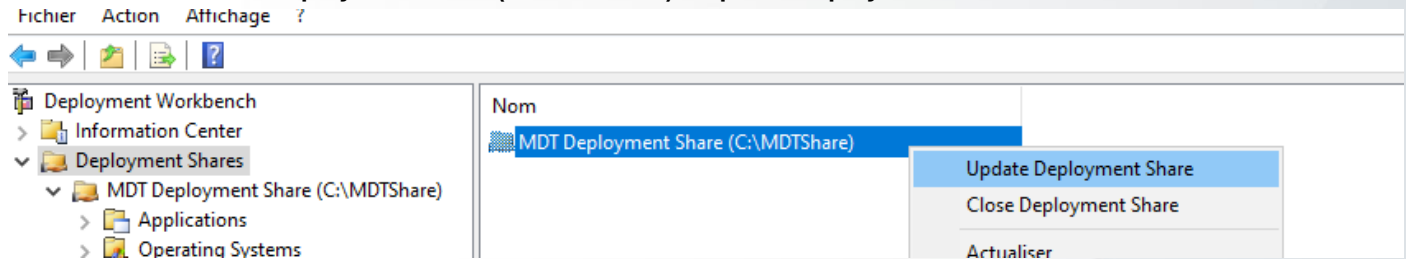
- ☒ Use the specified local Administrator password.

Administrator Password:

Please confirm Administrator Password:

Générer l'image de démarrage

- Aller sur **Deployment Shares**.
- Clic droit sur **MDT Deployment Share (C:\MDTShare)** → **Update Deployment Share**.



Correction des erreurs liées aux images WIM dans MDT

Lors de la configuration de **Microsoft Deployment Toolkit (MDT)**, une erreur peut apparaître lors de la génération des images de démarrage (WIM) :

Unable to open the specified WIM file
System.IO.DirectoryNotFoundException

Cause

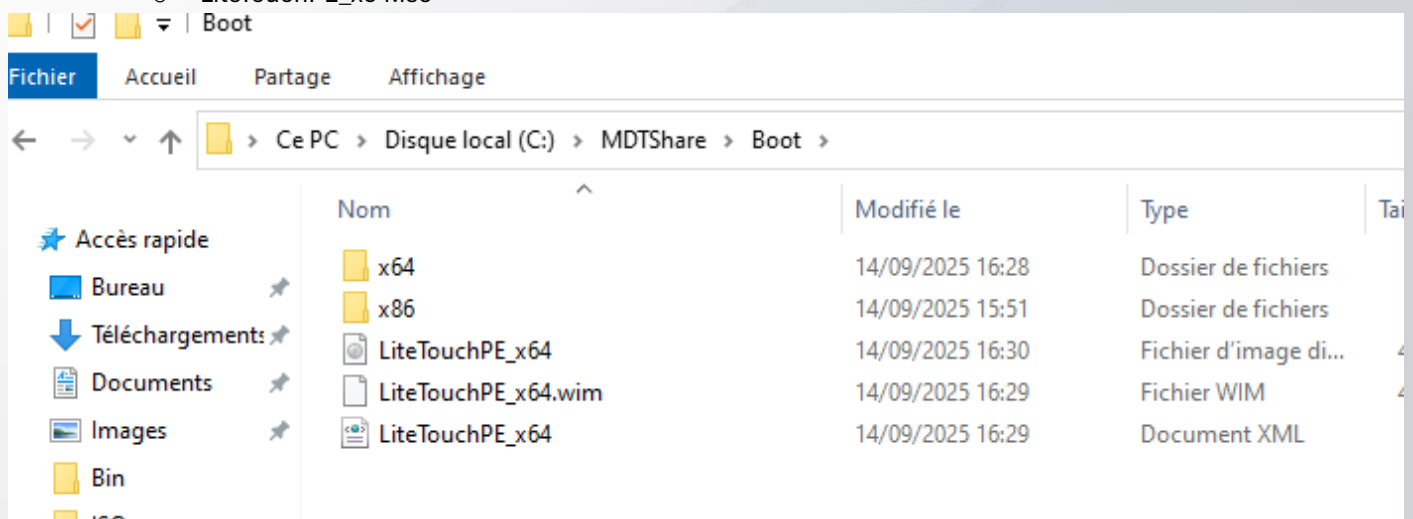
- Par défaut, MDT tente de générer des images de démarrage **x86** et **amd64**.
- Si seuls les binaires **Windows ADK / WinPE (amd64)** sont installés, MDT ne trouve pas les fichiers nécessaires pour **x86**, ce qui provoque l'erreur.

Solution

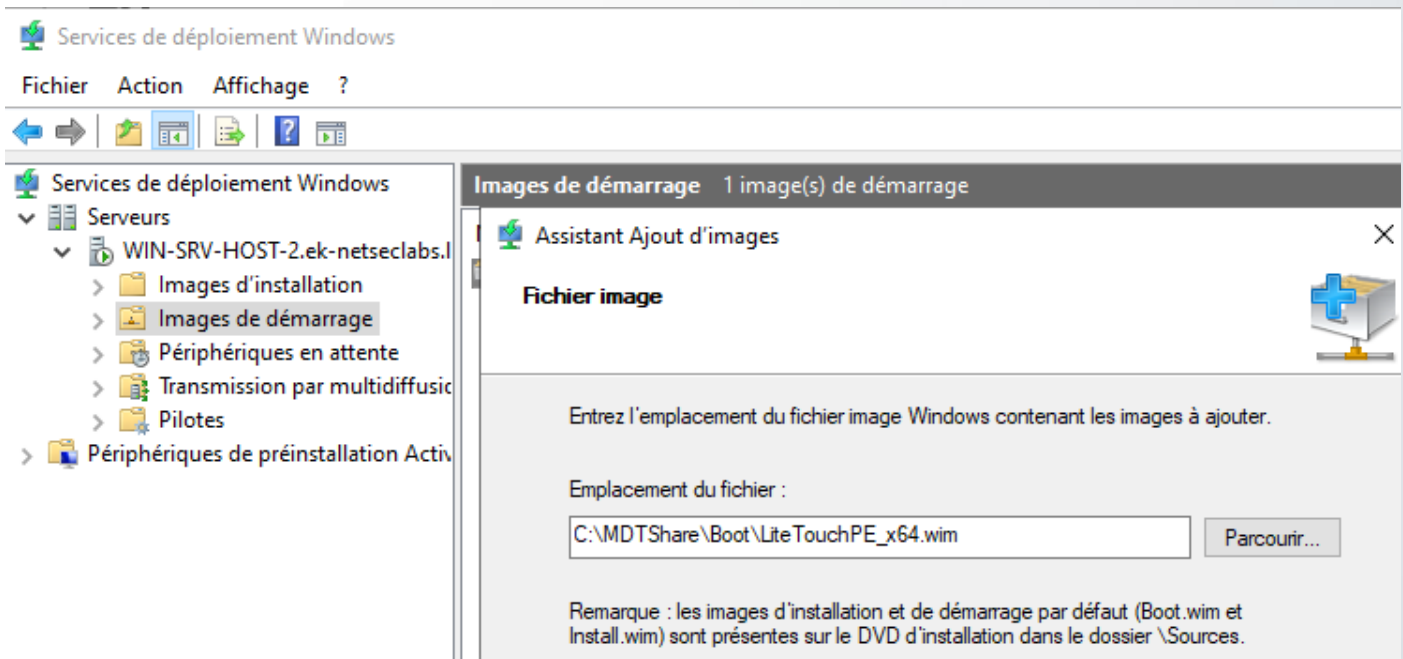
1. Ouvrir **Deployment Workbench**.
2. Clic droit sur **MDT Deployment Share** → **Properties**.
3. Onglet **General** → **décocher** :
 - "Generate a Lite Touch Windows PE x86 boot image"
4. Onglet **Windows PE** :
 - Ne laisser actif que **amd64**.
5. Relancer un **Update Deployment Share**.

Résultat : MDT ne génère que l'image de boot **amd64**, compatible avec ton environnement → plus d'erreurs WIM.

- Cela génère dans C:\MDTShare\Boot\ :
 - LiteTouchPE_x64.wim
 - LiteTouchPE_x64.iso



- Importer le fichier **LiteTouchPE_x64.wim** dans **WDS** :
 - Dans **Boot Images** → clic droit → **Add Boot Image**.



DEMARRAGE PXE

- Configurer les postes clients pour démarrer sur le réseau (**PXE boot**).
- Au démarrage, WDS charge le **LiteTouchPE_x64.wim**.
- L'assistant MDT s'exécute et propose la séquence de tâches.
- L'installation de Windows + Applications se lance automatiquement.

En cours de production... à suivre !