



AP2 — PROJET PARCUS

LIVRABLE 2

DOCUMENTATION TECHNIQUE

Plan de tests et documentation technique

GROUPE N°2

KARACELIK Aksel • RODRIGUEZ Maxence • JEANNEY Alexis

BTS SIO (option SISR) — 1re année

CCI Campus Strasbourg

Date limite de remise : 07 juillet 2026

Présentation du projet et du groupe

Le projet PARCUS consiste à mettre en place, pour une petite structure, une infrastructure complète de gestion de parc et d'assistance informatique : un outil de gestion de parc et de tickets (GLPI), une solution de prise en main à distance auto-hébergée (RustDesk), ainsi qu'un annuaire d'authentification centralisé (Windows Server 2025 / Active Directory).

Ce second livrable regroupe la documentation technique du projet, solution par solution : pour chaque lot, la documentation d'installation, la documentation utilisateur destinée aux salariés, puis la documentation d'exploitation destinée aux techniciens — avec les difficultés rencontrées et leurs solutions. Le plan de tests et un glossaire complètent le document.

Répartition des lots

Membre	Lot	Périmètre
RODRIGUEZ Maxence	LOT 1 — RustDesk	Serveur auto-hébergé, clients, prise en main à distance, BitLocker
KARACELIK Aksel	LOT 2 — GLPI	Serveur GLPI, agent d'inventaire, tickets
JEANNEY Alexis	LOT 3 — Windows Server 2025	Active Directory, DHCP, WDS, déploiement de logiciels par GPO

Environnement technique

L'ensemble des services est déployé sur des machines virtuelles reliées au réseau interne du projet, 192.168.137.0/24. Aucun service n'est publié sur Internet : tout fonctionne en environnement local.

Machine	Rôle	Adresse IP
WDS	Serveur de déploiement Windows	192.168.137.2
WEBSRV	GLPI + Apache	192.168.137.3
RUSTDESK	Serveur RustDesk (hbbs + hbbr)	192.168.137.4
Client 1	Poste technicien (prise en main)	192.168.137.11
Client 2	Poste utilisateur (contrôlé à distance)	192.168.137.12

Sommaire

Présentation du projet et du groupe	2
Répartition des lots.....	2
Environnement technique.....	2
Sommaire	3
1. RustDesk — prise en main à distance (LOT 1)	5
1.1. Documentation d'installation — serveur RustDesk auto-hébergé.....	5
1.1.1. De quoi on part	5
1.1.2. Préparer la VM Debian.....	5
1.1.3. Installer Docker	8
1.1.4. Installer le serveur RustDesk	8
1.1.5. Récupérer la clé publique.....	9
1.1.6. Les ports à laisser passer	9
1.1.7. Côté clients (rappel).....	10
1.2. Documentation utilisateur — demander une assistance à distance	10
1.2.1. Étape 1 — Ouvrir RustDesk et trouver vos identifiants.....	10
1.2.2. Étape 2 — Donner ces informations au technicien.....	11
1.2.3. Étape 3 — Laisser le technicien se connecter.....	11
1.2.4. Pendant que le technicien travaille.....	12
1.3. Documentation d'exploitation (technicien) — prise en main à distance.....	12
1.3.1. Configurer un poste client	13
1.3.2. Lancer la connexion	14
1.3.3. Autoriser la prise en main (utilisateur présent)	16
1.3.4. La barre d'outils pendant la session	18
1.3.5. Mettre fin à la session	18
1.3.6. Dépannage courant.....	18
2. GLPI — gestion de parc et assistance (LOT 2)	20
2.1. Documentation d'installation — serveur GLPI et agent d'inventaire	20
2.1.1. Présentation de l'architecture.....	20
2.1.2. Prérequis et installation des composants	20
2.1.3. Configuration de la base de données.....	21
2.1.4. Déploiement de GLPI.....	21
2.1.5. Installation via l'interface web.....	22
2.1.6. Installation du GLPI Agent et ajout d'un équipement à l'inventaire	23
2.1.7. Problèmes rencontrés	25
2.2. Documentation utilisateur — créer et suivre ses tickets.....	27
2.2.1. Créer un ticket par courriel	27
2.2.2. Créer un ticket via le site — connexion au portail Self-Service.....	28
2.2.3. Signaler un incident via le site	28
2.2.4. Suivre l'état de ses tickets.....	30

2.3. Documentation d'exploitation (technicien) — gestion des tickets, collecteur et annuaire	31
2.3.1. Visualisation d'un nouveau ticket	31
2.3.2. Prise en charge du ticket.....	32
2.3.3. Cycle de vie d'un ticket.....	32
2.3.4. Configuration du collecteur de mails	33
2.3.5. Liaison avec l'annuaire d'authentification (LDAPS).....	34
3. Windows Server 2025 — services d'infrastructure (LOT 3)	48
3.1. Documentation d'installation — contrôleur de domaine et services réseau	48
3.1.1. Présentation de l'architecture	48
3.1.2. Configuration de base du serveur (nom et adresse IP)	48
3.1.3. Installation du rôle AD DS	55
3.1.4. Promotion en contrôleur de domaine (parcus.fr)	58
3.1.5. Installation et autorisation du rôle DHCP	60
3.1.6. Création de l'étendue DHCP « UtilisateursParcus »	65
3.1.7. Jonction d'un poste Windows 11 au domaine.....	74
3.1.8. Installation du rôle WDS.....	80
3.1.9. Ajout des images de démarrage et d'installation	87
3.1.10. Mise en place du second serveur (PARCUS-WDSSRV-02)	94
3.1.11. Préparation des postes pour BitLocker (TPM).....	99
3.2. Documentation utilisateur — ouvrir une session sur le domaine	105
3.3. Documentation d'exploitation (technicien) — GPO, images WDS, BitLocker et redondance	106
3.3.1. Déployer un fond d'écran par GPO	106
3.3.2. Préparer une image personnalisée (capture WDS et Sysprep)	113
3.3.3. Déployer un poste par le réseau (démarrage PXE)	115
3.3.4. Redondance DNS : zone secondaire sur le second serveur.....	118
3.3.5. Haute disponibilité DHCP : le basculement	122
3.3.6. Autorité de certification (AD CS).....	128
3.3.7. Chiffrement BitLocker piloté par GPO	131
Plan de tests	157
Tests du LOT 1 — RustDesk.....	157
Tests du LOT 2 — GLPI	157
Tests du LOT 3 — Windows Server 2025.....	159

1. RustDesk — prise en main à distance (LOT 1)

Solution open source de prise en main à distance, auto-hébergée sur notre réseau. Lot réalisé par RODRIGUEZ Maxence.

1.1. Documentation d'installation — serveur RustDesk auto-hébergé

1.1.1. De quoi on part

L'idée est d'héberger nous-mêmes le serveur RustDesk, pour faire de la prise en main à distance entre nos postes sans passer par les serveurs publics de RustDesk. Tout reste chez nous, sur notre réseau.

Le serveur tourne sur une VM Debian. Deux services fonctionnent ensemble, chacun dans un conteneur Docker :

- **hbbs** : le serveur de rendez-vous. C'est lui qui enregistre les identifiants (ID) des postes et qui met deux clients en relation.
- **hbbr** : le relais. Il prend le relais quand la connexion directe entre deux clients ne passe pas (NAT, pare-feu, etc.).

Côté réseau, le serveur a deux cartes. Une carte fixe sur le réseau du projet (192.168.137.0/24), c'est par là que les clients le joignent, et une deuxième carte en DHCP qui lui donne Internet via la box. La deuxième sert uniquement à pouvoir installer Docker.

Le plan d'adressage :

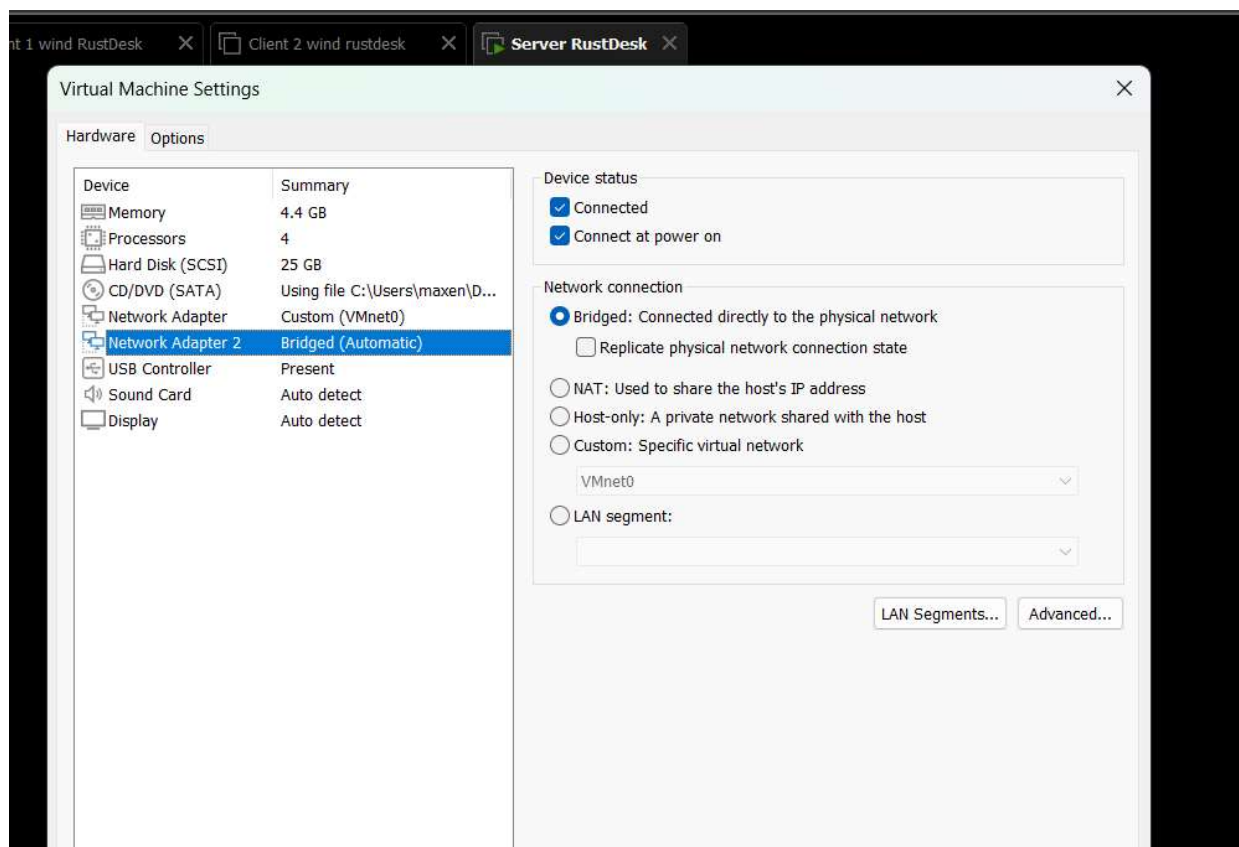
Machine	Rôle	Adresse IP
WDS	Serveur de déploiement Windows	192.168.137.2
WEBSRV	GLPI + Apache	192.168.137.3
RUSTDESK	Serveur RustDesk (hbbs + hbbr)	192.168.137.4
Client 1	Poste depuis lequel on prend la main	192.168.137.11
Client 2	Poste contrôlé à distance	192.168.137.12

1.1.2. Préparer la VM Debian

Les deux cartes réseau. Chaque carte a un rôle précis :

- **ens33** : carte du réseau interne du projet (192.168.137.0/24). C'est par elle que les clients RustDesk joignent le serveur : on lui attribue une IP fixe.
- **ens37** : carte d'accès Internet (via la box), en DHCP. Elle sert uniquement à l'installation de Docker.

Côté VMware, la carte du réseau interne est en mode Bridge, ce qui la place sur le même réseau que les autres machines du projet.



Paramètres VMware de la VM RustDesk : carte réseau en mode Bridge

Configuration dans `/etc/network/interfaces`. Un serveur ne doit pas changer d'adresse, sinon les clients ne le retrouvent plus. On fixe donc `ens33` sur `192.168.137.4` et on laisse `ens37` en DHCP. On ouvre le fichier :

```
sudo nano /etc/network/interfaces
```

On déclare les deux interfaces comme suit (les noms `ens33` / `ens37` peuvent varier selon la machine, à vérifier avec `ip a`) :

```
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
    address 192.168.137.4
    netmask 255.255.255.0

auto ens37
iface ens37 inet dhcp
```

L'interface `ens33` n'a ni passerelle ni DNS : c'est `ens37` (en DHCP) qui fournit la passerelle et l'accès Internet. On applique la configuration :

```
sudo systemctl restart networking
```

```
7pWrkhLaxPyAlu0CTPyFDb1Pcat /etc/network/interfaces rustdesk-server:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
    address 192.168.137.4
    netmask 255.255.255.0

auto ens37
iface ens37 inet dhcp
```

Le fichier `/etc/network/interfaces` : `ens33` en statique, `ens37` en DHCP

Vérification de l'adressage. On contrôle que tout est en place :

```
ip a
```

On doit retrouver 192.168.137.4 sur `ens33`. On voit également `ens37` qui a récupéré une IP en DHCP, et `docker0`, la carte interne de Docker (normale, on n'y touche pas).

```
Debian GNU/Linux 13 rustdesk-server tty1

rustdesk-server login: root
Password:
Linux rustdesk-server 6.12.43+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.43-1 (2025-08-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@rustdesk-server:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:02:3f:dc brd ff:ff:ff:ff:ff:ff
    altnam enp2s1
    altnam enx00c29023fdc
    inet 192.168.137.4/24 brd 192.168.137.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 2a01:e0a:ab6:e150:20c:29ff:fe02:3fdc/64 scope global dynamic mngtmpaddr proto kernel_r
        valid_lft 86201sec preferred_lft 86201sec
    inet6 fe80::20c:29ff:fe02:3fdc/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:02:3f:e6 brd ff:ff:ff:ff:ff:ff
    altnam enp2s5
    altnam enx00c29023fe6
    inet 192.168.1.89/24 brd 192.168.1.255 scope global dynamic noprefixroute ens37
        valid_lft 42936sec preferred_lft 37536sec
    inet6 2a01:e0a:ab6:e150:268:19f:ca0t:3069/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86201sec preferred_lft 86201sec
    inet6 fe80::ec65:4039:7a05:18dc/64 scope link
        valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:58:98:7b:f4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
root@rustdesk-server:~# _
```

ip a : `ens33` bien en 192.168.137.4

Vérification de l'accès Internet. Avant toute installation, on vérifie que la machine sort bien sur Internet (grâce à `ens37`) :

```
ping -c 4 8.8.8.8
```

Si les pings répondent, l'accès est fonctionnel. Sinon, vérifier qu'ens37 a bien récupéré une adresse en DHCP.

```
valid_lft forever preferred_lft forever
root@rustdesk-server:~# ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=10.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=10.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=10.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=10.9 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 10.417/10.573/10.925/0.206 ms
root@rustdesk-server:~#
```

Le ping vers 8.8.8.8 répond : Internet OK

1.1.3. Installer Docker

Les deux services RustDesk tournent dans des conteneurs : il faut donc installer Docker.

```
sudo apt update
sudo apt install -y docker.io
sudo systemctl enable --now docker
```

On vérifie que Docker fonctionne :

```
systemctl status docker
```

La ligne « active (running) » doit apparaître. Le « enabled » signifie que Docker redémarrera automatiquement au démarrage de la VM. Pour quitter cet écran, appuyer sur q.

```
root@rustdesk-server:~# systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
   Active: active (running) since Fri 2026-06-26 15:24:05 CEST; 8min ago
  Invocation: 1ac82f06be4f416db407dbbda3ac1873
    TriggeredBy: ● docker.socket
     Docs: https://docs.docker.com
    Main PID: 932 (dockerd)
      Tasks: 12
     Memory: 113.5M (peak: 115.4M)
        CPU: 1.104s
    CGroup: /system.slice/docker.service
            └─932 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

juin 26 15:24:04 rustdesk-server dockerd[932]: time="2026-06-26T15:24:04.997602179+02:00" level=info msg="Removing stale sandbox 60ae7ce576517db226d5675b6d3b7c"
juin 26 15:24:04 rustdesk-server dockerd[932]: time="2026-06-26T15:24:04.999495502+02:00" level=warning msg="Error (Unable to complete atomic operation, key mo"
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.002307861+02:00" level=info msg="Removing stale sandbox 71ebdfa70bf060bf494e059705e72"
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.002936106+02:00" level=warning msg="Error (Unable to complete atomic operation, key mo"
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.242962401+02:00" level=info msg="Default bridge (docker0) is assigned with an IP address"
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.639166059+02:00" level=info msg="Loading containers: done."
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.660573284+02:00" level=info msg="Docker daemon" commit=411e817 containerd-snapshotter=2"
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.661090464+02:00" level=info msg="Daemon has completed initialization"
juin 26 15:24:05 rustdesk-server dockerd[932]: time="2026-06-26T15:24:05.708589554+02:00" level=info msg="API listen on /run/docker.sock"
juin 26 15:24:05 rustdesk-server systemd[1]: Started docker.service - Docker Application Container Engine.
lines 1-23/23 (END)
```

Docker est actif (running) et activé au démarrage

1.1.4. Installer le serveur RustDesk

On crée d'abord un dossier destiné à contenir les données du serveur (dont la clé générée au premier démarrage), puis on s'y place :

```
mkdir ~/rustdesk
cd ~/rustdesk
```

On lance hbbs (le serveur de rendez-vous) :

```
sudo docker run --name hbbs -v $(pwd):/root -td --net=host \
  --restart unless-stopped rustdesk/rustdesk-server hbbs
```

Puis hbbr (le relais) :

```
sudo docker run --name hbbr -v $(pwd):/root -td --net=host \
  --restart unless-stopped rustdesk/rustdesk-server hbbr
```

Signification des options utilisées :

- **--net=host** : le conteneur utilise directement le réseau de la VM. C'est la configuration recommandée par RustDesk : elle permet la connexion directe entre clients.
- **-v \$(pwd):/root** : on monte le dossier courant dans le conteneur. C'est là que la clé et la base sont stockées ; elles ne sont donc pas perdues si le conteneur est recréé.
- **--restart unless-stopped** : les conteneurs redémarrent automatiquement au démarrage de la VM, sauf s'ils ont été arrêtés volontairement.
- **-td** : le conteneur tourne en arrière-plan.

On vérifie que les deux conteneurs tournent :

```
sudo docker ps
```

Les conteneurs hbbs et hbbr doivent apparaître au statut « Up ».

```
root@rustdesk-server:~# docker ps
CONTAINER ID   IMAGE                  COMMAND                  CREATED        STATUS        PORTS        NAMES
2a7a02035d4a   rustdesk/rustdesk-server "hbbr"                  4 weeks ago   Up 8 minutes               hbbr
cce9cd48c291   rustdesk/rustdesk-server "hbbs"                  4 weeks ago   Up 8 minutes               hbbs
root@rustdesk-server:~# _
```

docker ps : hbbs et hbbr tournent (Up)

1.1.5. Récupérer la clé publique

Au premier démarrage, hbbs génère automatiquement une paire de clés. La clé publique devra être renseignée dans chaque client RustDesk, sans quoi ils refuseront de se connecter au serveur. On l'affiche :

```
cat ~/rustdesk/id_ed25519.pub
```

Attention au copier-coller : la clé s'arrête au signe « = ». Ce qui suit (root@rustdesk-server) est le prompt du terminal et ne fait pas partie de la clé.

```
root@rustdesk-server:~# cat /root/rustdesk/id_ed25519.pub
7pWrkhLaxPyALu0CTPyFDb1PUpPHZoF5W6xxIJYTNZ4=root@rustdesk-server:~#
```

La clé publique du serveur (à coller dans les clients)

1.1.6. Les ports à laisser passer

Pour que les clients puissent joindre le serveur, les ports suivants doivent être ouverts. Sur une Debian sans pare-feu actif, il n'y a rien à faire ; si un pare-feu (ufw) est en place, il faut les autoriser.

Service	Port	Rôle
hbbs	21115 / TCP	Test du type de NAT
hbbs	21116 / TCP + UDP	Enregistrement des ID et mise en relation
hbbr	21117 / TCP	Relais quand la connexion directe ne passe pas
hbbs	21118 / TCP	Client web (optionnel)
hbbr	21119 / TCP	Client web (optionnel)

Avec ufw, les commandes seraient :

```
sudo ufw allow 21115:21119/tcp
sudo ufw allow 21116/udp
```

1.1.7. Côté clients (rappel)

Le serveur est en place. Pour finir, sur chaque poste client (192.168.137.11 et 192.168.137.12), il faut configurer l'application RustDesk pour qu'elle pointe vers notre serveur : dans Paramètres > Réseau > Serveur ID/relais, on met l'IP du serveur (192.168.137.4) dans Serveur ID, et on colle la clé publique récupérée à l'étape 1.1.5. La configuration détaillée des clients et le test de prise en main sont traités dans la documentation d'exploitation (section 1.3).

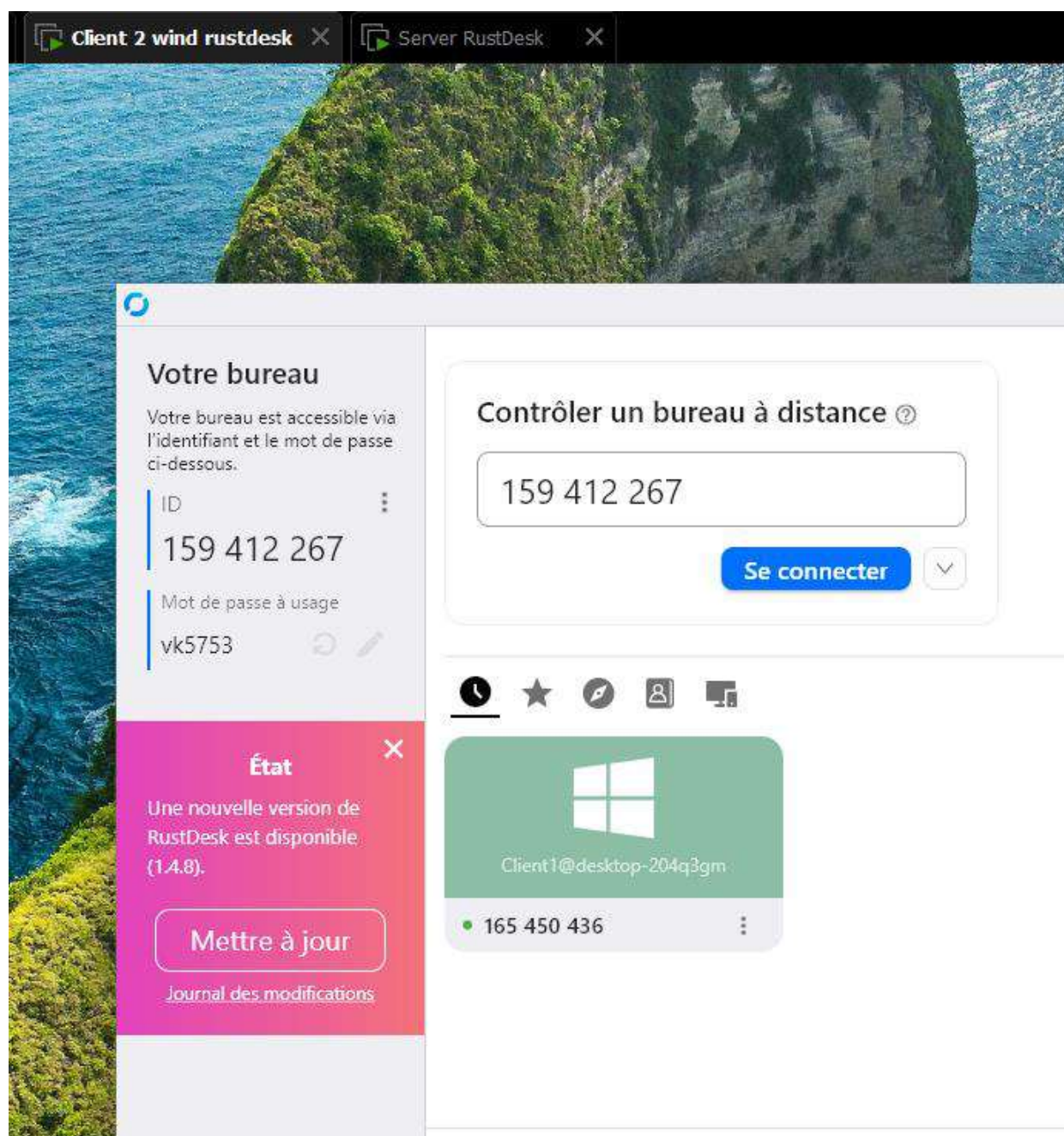
1.2. Documentation utilisateur — demander une assistance à distance

Parfois, plutôt que de se déplacer, un technicien peut vous dépanner directement en prenant la main sur votre ordinateur à distance. Pour cela, on utilise RustDesk, un logiciel déjà installé sur votre poste (la petite icône bleue). Le technicien ne peut jamais se connecter sans votre accord : c'est vous qui ouvrez la porte, à chaque fois.

1.2.1. Étape 1 — Ouvrir RustDesk et trouver vos identifiants

Ouvrez RustDesk. Sur la page d'accueil, à gauche sous « Votre bureau », deux informations vont servir au technicien :

- **L'identifiant (ID)** : la suite de chiffres qui correspond à votre ordinateur.
- **Le mot de passe** : un petit code juste en dessous, qui change de temps en temps.



Votre identifiant et votre mot de passe, sur la page d'accueil

1.2.2. Étape 2 — Donner ces informations au technicien

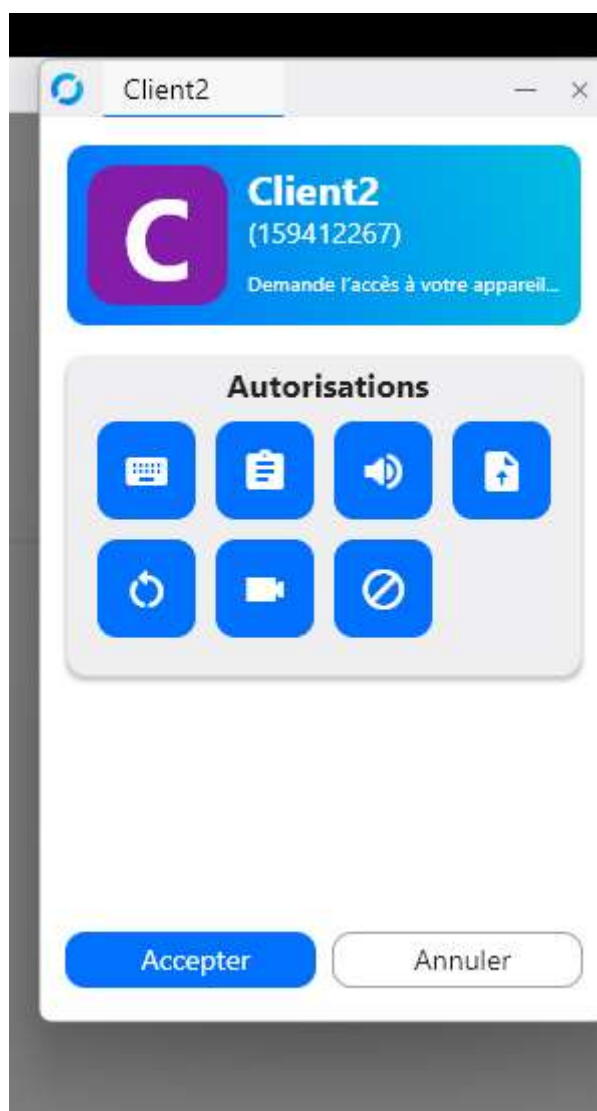
Communiquez votre identifiant au technicien, par téléphone ou par message. Il vous demandera peut-être aussi le mot de passe affiché juste en dessous, selon la façon dont il préfère se connecter.

Ne donnez ces informations qu'à un technicien que vous connaissez, ou que vous avez vous-même appelé. Si quelqu'un vous contacte de nulle part en vous les réclamant, ne donnez rien.

1.2.3. Étape 3 — Laisser le technicien se connecter

Deux cas de figure ; c'est le technicien qui vous dira lequel :

- **Soit vous lui donnez le mot de passe** affiché sur votre écran, et il se connecte avec. Pratique si vous devez vous absenter du poste.
- **Soit vous acceptez sur le moment** : une petite fenêtre s'ouvre sur votre écran pour signaler une demande de connexion : cliquez sur Accepter. C'est le plus sûr, parce que c'est vous qui validez au bon moment.



La fenêtre à accepter pour laisser le technicien entrer

1.2.4. Pendant que le technicien travaille

Une fois connecté, le technicien voit votre écran et peut déplacer la souris et taper au clavier pour régler votre souci. Ce qu'il faut savoir :

- Vous voyez tout ce qu'il fait, en direct.
- Vous n'êtes pas bloqué : vous pouvez reprendre la souris et le clavier quand vous voulez.
- Vous pouvez couper la connexion à tout moment avec le bouton Déconnecter, affiché pendant toute l'intervention.

Les bons réflexes : n'acceptez que si vous attendiez le dépannage et que vous savez qui est en face ; au moindre doute, cliquez sur Annuler et prévenez le service informatique ; pendant l'intervention, évitez de taper vos mots de passe personnels (le technicien voit votre écran) ; à la fin, vérifiez que la fenêtre de connexion s'est bien fermée.

Une question, un doute ? Contactez le service informatique. Dans tous les cas, c'est toujours vous qui décidez de laisser entrer ou non.

1.3. Documentation d'exploitation (technicien) — prise en main à distance

Cette section explique comment utiliser RustDesk au quotidien, côté technicien : configurer un poste pour qu'il passe par notre serveur, puis prendre la main à distance sur un poste, que l'utilisateur soit

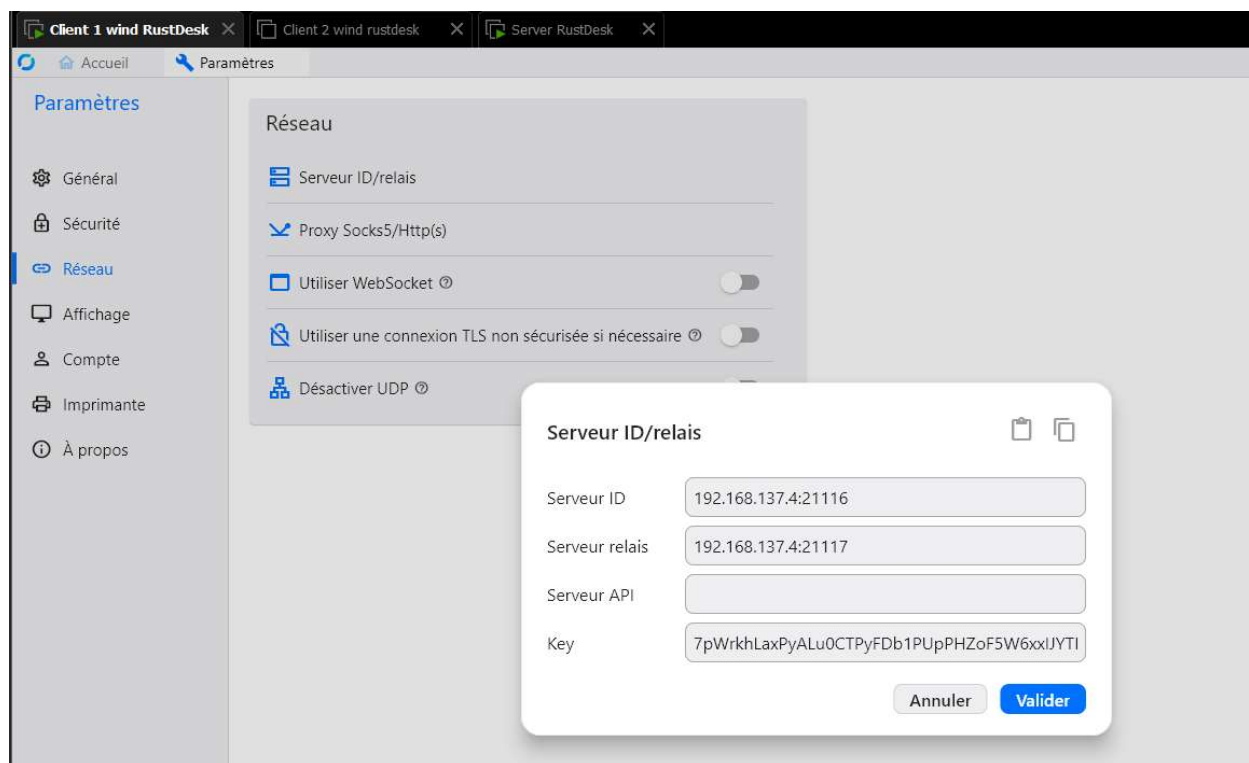
présent ou non. Pour rappel, le serveur RustDesk tourne sur 192.168.137.4 et tous les postes sont sur le réseau 192.168.137.0/24.

1.3.1. Configurer un poste client

Avant de pouvoir prendre la main sur un poste, celui-ci doit avoir l'application RustDesk configurée pour utiliser notre serveur (et non les serveurs publics de RustDesk). C'est à faire une seule fois par poste.

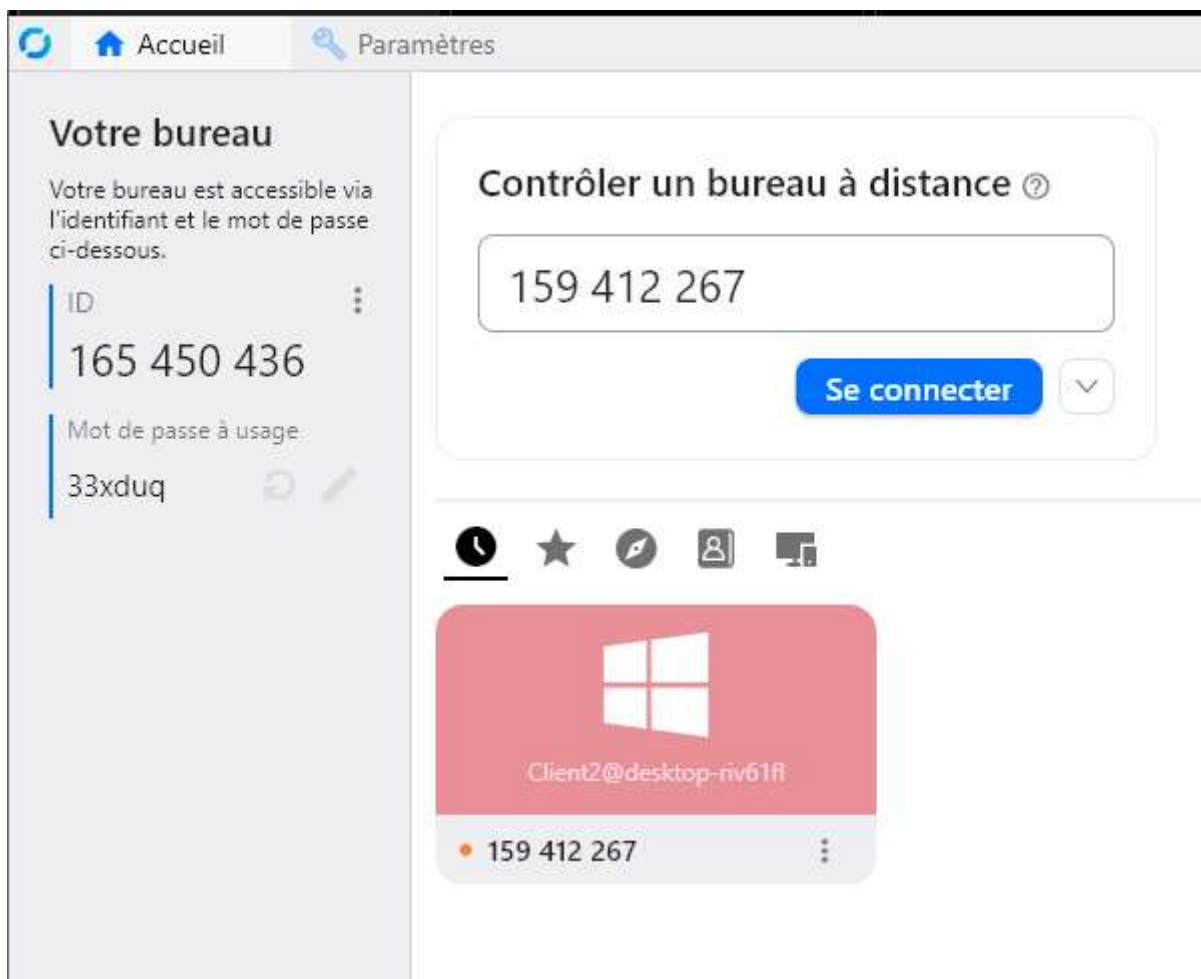
Dans RustDesk, ouvrir les paramètres (les trois points : à côté de l'ID), puis la section Réseau, et cliquer sur Serveur ID/relais :

- Dans **Serveur ID**, renseigner l'adresse du serveur : 192.168.137.4
- Dans **Key**, coller la clé publique du serveur (récupérée à l'installation, section 1.1.5).
- Valider. Le champ Serveur relais se remplit tout seul.



Configuration du serveur ID/relais et de la clé sur un poste client

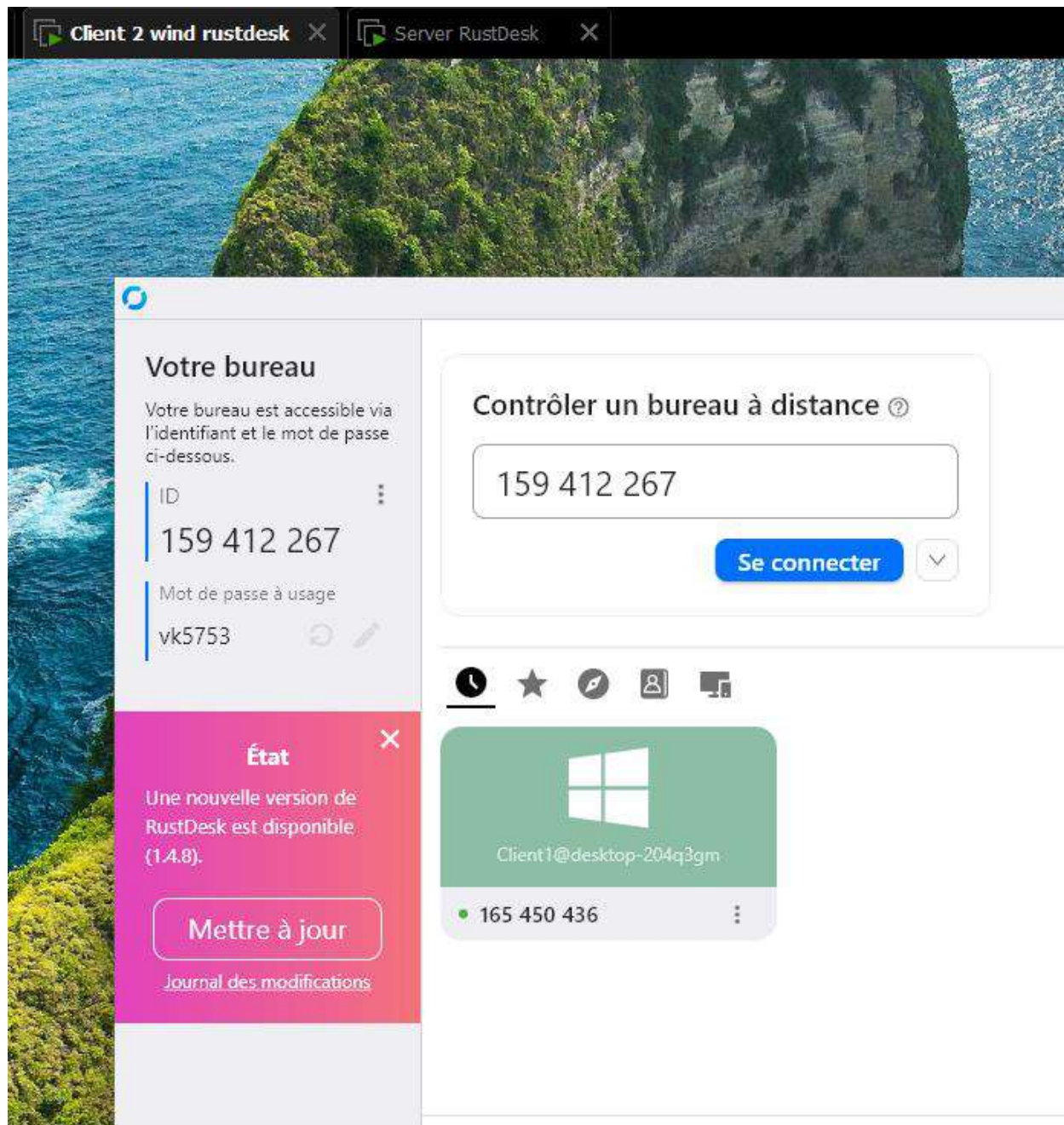
Une fois configuré, chaque poste affiche son propre identifiant RustDesk sur l'écran d'accueil, avec un mot de passe à usage unique. C'est cet identifiant qui sert à joindre le poste pour le contrôler.



Écran d'accueil d'un poste : son identifiant et son mot de passe

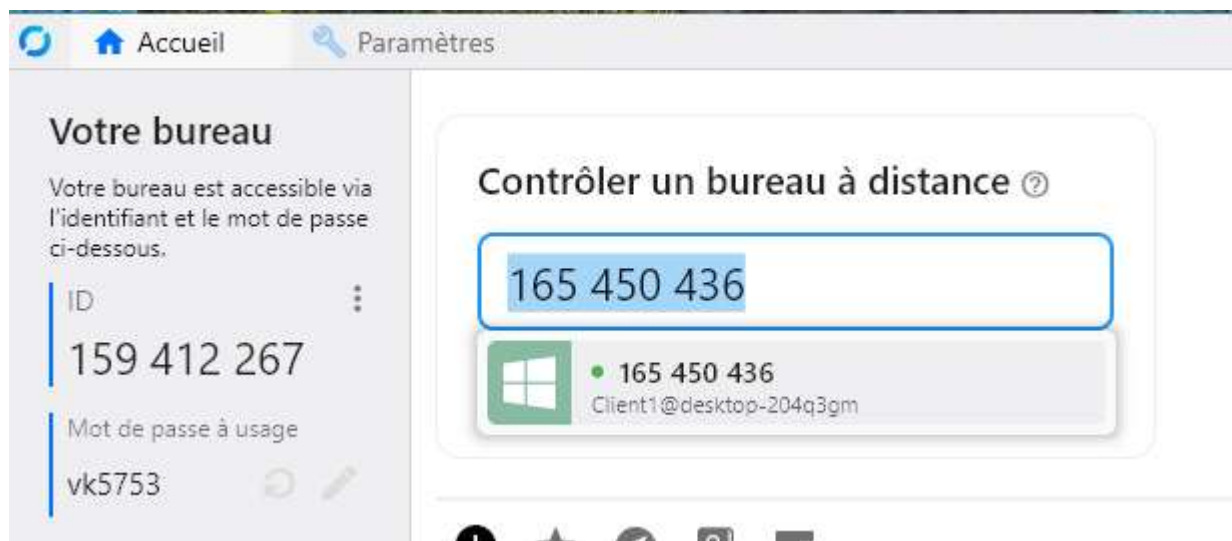
1.3.2. Lancer la connexion

Le technicien a besoin de l'identifiant du poste à dépanner. L'utilisateur le lui communique : il se trouve sur l'écran d'accueil de son RustDesk, sous « Votre bureau ».



Le poste à dépanner communique son identifiant (ici 159 412 267)

Sur le poste du technicien, dans le champ « Contrôler un bureau à distance », saisir l'identifiant du poste distant puis cliquer sur Se connecter.

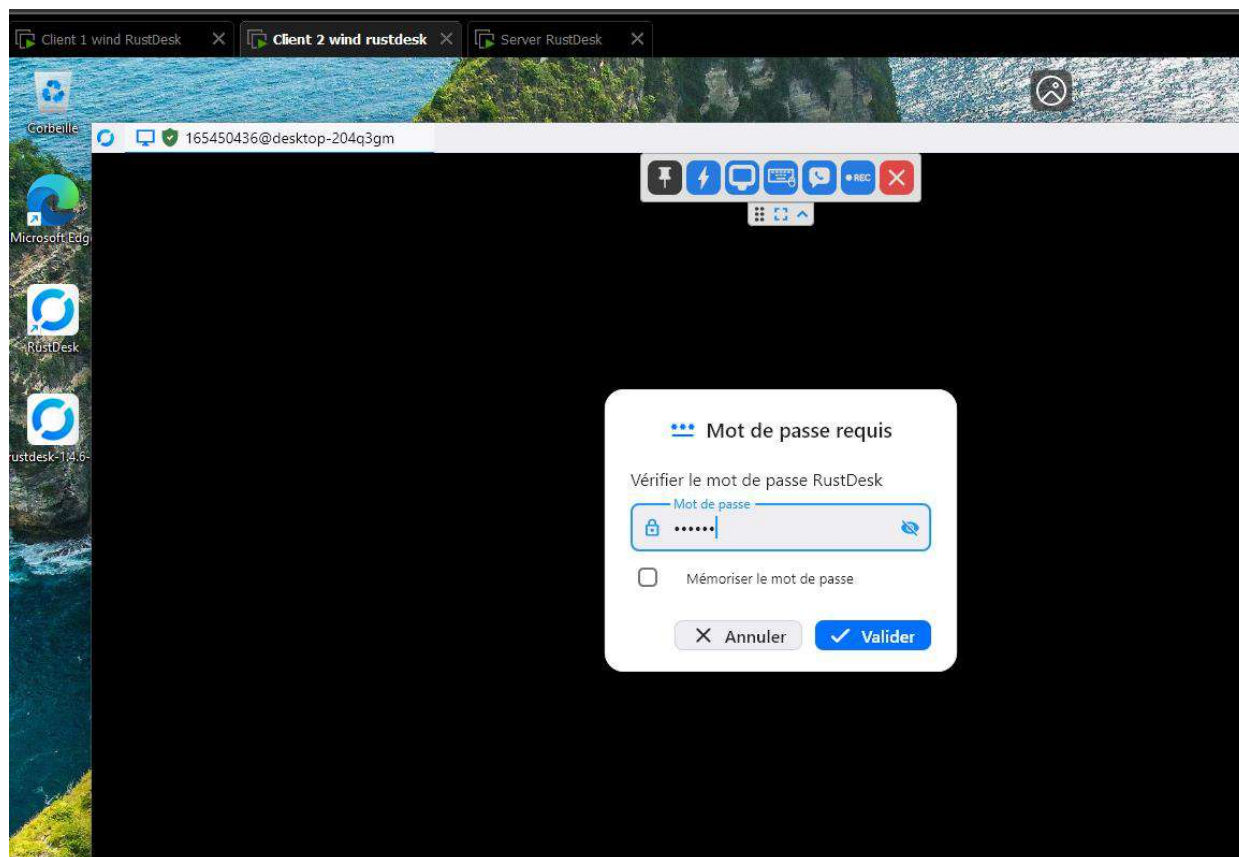


Le technicien saisit l'identifiant du poste à contrôler

1.3.3. Autoriser la prise en main (utilisateur présent)

Quand un utilisateur est devant son poste, il y a deux façons d'autoriser la prise en main. Selon la situation, on utilise l'une ou l'autre.

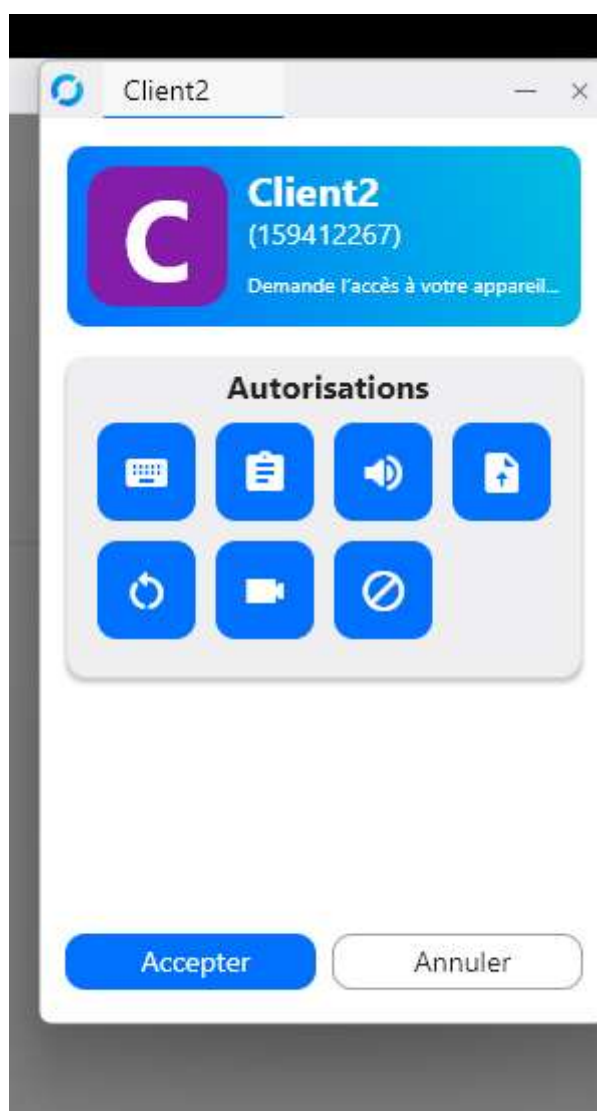
Mode 1 — Par mot de passe. L'utilisateur communique au technicien le mot de passe à usage unique affiché sur son écran d'accueil. Le technicien le saisit dans la fenêtre qui s'ouvre, et la connexion démarre. Pratique quand l'utilisateur ne peut pas rester devant l'écran.



Mode 1 : le technicien saisit le mot de passe communiqué par l'utilisateur

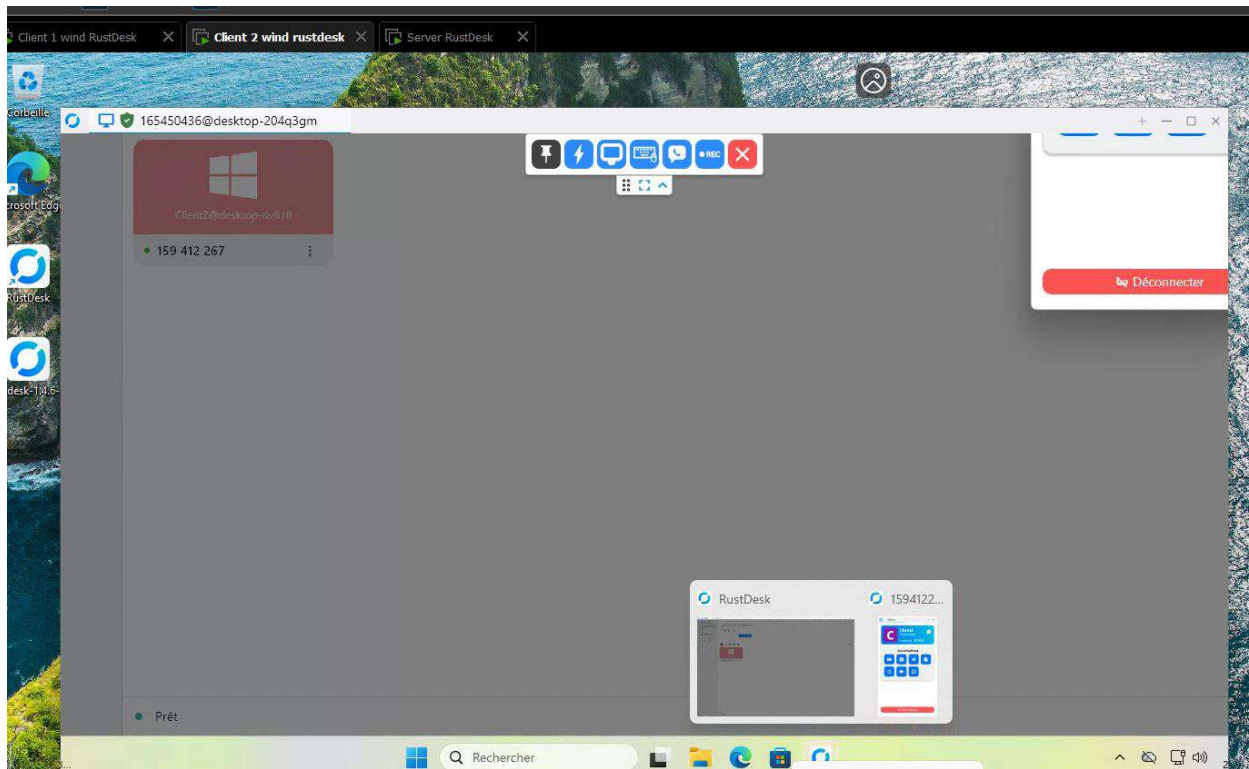
Mode 2 — Par acceptation directe. L'utilisateur n'a pas besoin de donner de mot de passe : une fenêtre apparaît sur son écran, lui indiquant qu'une demande d'accès arrive, et il clique sur Accepter.

Il peut aussi choisir au passage ce qu'il autorise (clavier, presse-papier, son, transfert de fichiers...). C'est le mode le plus sûr quand l'utilisateur est présent, puisque c'est lui qui valide.



Mode 2 : l'utilisateur autorise la prise en main en cliquant sur Accepter

Une fois la connexion acceptée (par l'un ou l'autre mode), la session s'ouvre : le technicien voit l'écran du poste distant et le contrôle comme s'il était devant.



Session de prise en main : l'écran du poste distant s'affiche chez le technicien

1.3.4. La barre d'outils pendant la session

Pendant la prise en main, une barre d'outils est affichée en haut de la session. Elle regroupe les actions utiles :

- **Épingle** : garder la barre affichée en permanence.
- **Actions rapides (éclair)** : envoyer Ctrl+Alt+Suppr, verrouiller la session, redémarrer le poste distant, etc.
- **Affichage (écran)** : choisir l'écran à afficher, régler la qualité d'image et la résolution. C'est ici qu'on baisse la qualité si la connexion rame.
- **Clavier** : changer le mode de saisie clavier.
- **Chat** : discuter par message avec l'utilisateur en face.
- **REC** : enregistrer la session.
- **Croix rouge** : fermer la session et se déconnecter.



La barre d'outils de session RustDesk

1.3.5. Mettre fin à la session

Pour terminer proprement, le technicien clique sur la croix rouge de la barre d'outils (ou ferme la fenêtre de session). Côté utilisateur, la prise en main s'arrête immédiatement, et il peut aussi la couper lui-même à tout moment avec le bouton Déconnecter affiché sur son écran.

1.3.6. Dépannage courant

Les soucis les plus fréquents côté prise en main à distance, et ce qu'il faut vérifier :

Problème	Quoi vérifier
Le client n'affiche pas « prêt » / pastille rouge	Vérifier que l'IP du serveur (192.168.137.4) et la clé sont bien renseignées dans Paramètres > Réseau, et que le poste ping le serveur.
« Clé invalide » ou connexion refusée	La clé publique collée ne correspond pas. La récupérer à nouveau sur le serveur (cat id_ed25519.pub) et la recoller, sans espace ni le prompt.
Le poste distant est introuvable	Le poste contrôlé est éteint, RustDesk fermé, ou pas sur le bon réseau. Vérifier son ipconfig (doit être en 192.168.137.x).
La prise en main est très lente	Réduire la qualité d'image dans la barre d'outils (gestion de l'affichage), ou vérifier la charge réseau.
Le mot de passe ne fonctionne pas	Le mot de passe à usage unique change régulièrement. Demander à l'utilisateur celui affiché à l'instant, ou passer par l'acceptation directe.

2. GLPI — gestion de parc et assistance (LOT 2)

Solution open source de gestion de parc informatique et de tickets d'assistance (ITSM). Lot réalisé par KARACELIK Aksel.

2.1. Documentation d'installation — serveur GLPI et agent d'inventaire

Élément	Détail
Solution	GLPI 11.0.5 (Gestion Libre de Parc Informatique)
Système hôte	Debian 13 (machine virtuelle)
Pile logicielle	Apache2 + PHP 8.4 + MariaDB
Accès	Local — <code>http://ADRESSE_IP/glpi</code>
Agent d'inventaire	GLPI Agent (poste Windows)
Périmètre	LOT 2 du document d'installation de groupe

2.1.1. Présentation de l'architecture

GLPI (Gestion Libre de Parc Informatique) est une solution open source de gestion de parc informatique et d'assistance (ITSM). Dans le cadre du projet PARCUS, le LOT 2 consiste à installer et mettre en service le serveur GLPI ainsi que l'agent d'inventaire permettant la remontée automatique des équipements.

Le serveur est hébergé sur une machine virtuelle Debian 13 reposant sur une pile LAMP (Linux, Apache2, PHP, MariaDB). L'ensemble fonctionne en environnement strictement local : GLPI est accessible uniquement depuis le réseau interne et n'est pas publié sur Internet.

Postes clients	Réseau local	Serveur GLPI
Windows + GLPI Agent	LAN interne (192.168.137.0/24)	VM Debian 13

Le rôle de chaque composant est le suivant :

Composant	Rôle
Debian 13	Système d'exploitation hôte de la VM
Apache2	Serveur web qui publie l'application GLPI
PHP 8.4	Interpréteur exécutant le code de GLPI
MariaDB	Base de données stockant le parc, les tickets, etc.
GLPI 11.0.5	Application de gestion de parc et d'assistance
GLPI Agent	Agent installé sur les postes pour l'inventaire automatique

2.1.2. Prérequis et installation des composants

GLPI 11 nécessite au minimum PHP 8.2. Debian 13 fournit nativement PHP 8.4, compatible. La procédure suit la documentation officielle GLPI (help.glpi-project.org).

Mise à jour du système :

```
sudo apt update && sudo apt upgrade -y
```

Installation de la pile LAMP et des extensions PHP. On installe Apache2, PHP et l'ensemble des extensions requises par GLPI, puis le serveur de base de données MariaDB :

```
sudo apt install -y apache2 libapache2-mod-php \  
  php php-{apcu,cli,common,curl,gd,imap,ldap,mysql,xmldrpc,xml,\  
  mbstring,bcmath,intl,zip,bz2} php-soap  
  
sudo apt install -y mariadb-server
```

Attention — extension php-imap : cette extension est nécessaire au collecteur de mails (transformation des emails en tickets), traité dans la documentation d'exploitation (2.3). Sur Debian 13, ce paquet n'est plus présent dans les dépôts par défaut : si la vérification des prérequis le signale absent, il faut l'ajouter par une méthode complémentaire (voir 2.1.7, Problèmes rencontrés). Vérification :

```
php -m | grep imap
```

2.1.3. Configuration de la base de données

Sécurisation de MariaDB et fuseaux horaires. MariaDB est livré sans mot de passe root. On lance l'assistant de sécurisation, puis on importe les fuseaux horaires utilisés par GLPI :

```
sudo mysql_secure_installation  
sudo mysql_tzinfo_to_sql /usr/share/zoneinfo | sudo mysql mysql
```

Réponses recommandées à l'assistant : définir un mot de passe root, supprimer les utilisateurs anonymes, interdire la connexion root distante, supprimer la base de test, recharger les privilèges.

Création de la base et de l'utilisateur GLPI :

```
sudo mysql -u root -p
```

Puis, dans l'invite MariaDB :

```
CREATE DATABASE glpi;  
CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'VotreMotDePasse';  
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';  
GRANT SELECT ON mysql.time_zone_name TO 'glpi'@'localhost';  
FLUSH PRIVILEGES;  
EXIT;
```

Le compte glpi est celui utilisé par l'application pour lire et écrire dans sa base. Le mot de passe est documenté dans le dossier technique mais ne doit jamais être publié dans un dépôt public.

2.1.4. Déploiement de GLPI

Téléchargement et extraction. On télécharge la dernière archive stable de GLPI 11 depuis le dépôt officiel GitHub (11.0.5 au moment de notre installation) et on l'extrait dans la racine web d'Apache :

```
cd /var/www/html
```

```
sudo wget https://github.com/glpi-project/glpi/releases/download/11.0.5/glpi-11.0.5.tgz
sudo tar -xvzf glpi-11.0.5.tgz
```

Permissions des fichiers. On attribue le dossier à l'utilisateur du service web pour qu'Apache puisse lire et écrire les fichiers nécessaires :

```
sudo chown -R www-data:www-data /var/www/html/glpi
sudo chmod -R 755 /var/www/html/glpi
```

Accès à GLPI via Apache. GLPI est servi par le site Apache par défaut, qui publie le contenu de /var/www/html. GLPI étant extrait dans /var/www/html/glpi, il est accessible localement à l'adresse `http://ADRESSE_IP_DU_SERVEUR/glpi`. On active le module de réécriture d'URL et on redémarre Apache :

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

2.1.5. Installation via l'interface web

On ouvre un navigateur sur l'adresse locale du serveur (`http://ADRESSE_IP/glpi`). L'assistant d'installation se lance automatiquement :

- **Choix de la langue** : sélectionner Français, puis OK.
- **Licence** : cocher l'acceptation de la licence, puis Continuer.
- **Démarrage** : cliquer sur Installer (nouvelle installation).
- **Vérification des prérequis** : tout doit être validé. En cas d'erreur, corriger puis Réessayer.
- **Connexion à la base** : Serveur = localhost, Utilisateur = glpi, Mot de passe = celui défini, puis Continuer.
- **Sélection de la base** : choisir la base glpi, puis Continuer.
- **Fin** : GLPI initialise la base ; cliquer sur Utiliser GLPI.

Comptes par défaut créés à l'installation :

Identifiant	Mot de passe	Profil
glpi	glpi	Super-Administrateur
tech	tech	Technicien
normal	normal	Utilisateur normal
post-only	postonly	Utilisateur simple (post-only)

Sécurisation après installation. À la première connexion (glpi/glpi), GLPI signale la présence du dossier d'installation et des comptes par défaut. On corrige immédiatement :

```
sudo rm -rf /var/www/html/glpi/install/
```

À faire impérativement : supprimer le dossier d'installation puis actualiser GLPI (l'alerte doit disparaître) ; modifier le mot de passe de tous les comptes par défaut (glpi, tech, normal, post-only) ; désactiver les comptes par défaut non utilisés.

Vérification du fonctionnement. Depuis un navigateur du réseau local, l'accès à `http://ADRESSE_IP/glpi` doit afficher la page de connexion, puis le tableau de bord après authentification. Cela confirme que la chaîne Apache + PHP + MariaDB fonctionne.

2.1.6. Installation du GLPI Agent et ajout d'un équipement à l'inventaire

GLPI seul stocke les informations du parc mais ne les collecte pas automatiquement. Le GLPI Agent, installé sur chaque poste à inventorier, scanne la machine (matériel, logiciels, système, réseau) et envoie ces données au serveur, qui crée ou met à jour automatiquement la fiche de l'équipement.

Le GLPI Agent est le successeur de FusionInventory (même base de code). L'inventaire est intégré nativement à GLPI depuis la version 10 : aucun composant supplémentaire n'est requis côté serveur, seulement l'activation de la fonctionnalité.

Étape 1 — Activer l'inventaire côté serveur GLPI.

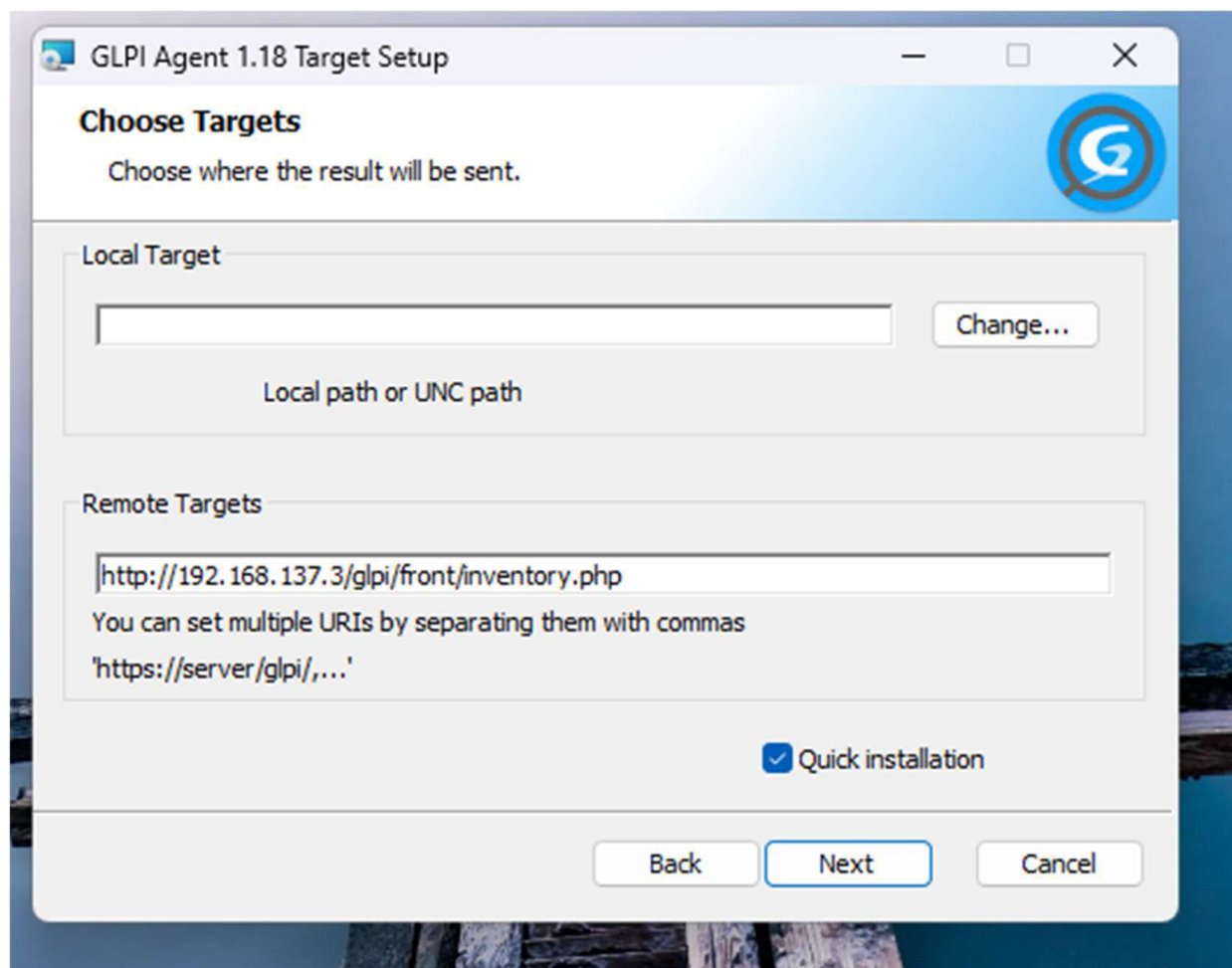
- Aller dans Administration puis Inventaire.
- Cocher la case Activer l'inventaire.
- Enregistrer.

Le serveur écoute alors les inventaires sur l'URL : `http://IP_DU_SERVEUR/front/inventory.php`

Étape 2 — Télécharger et installer l'agent sur le poste.

Sur le poste client à inventorier (ici Windows), télécharger la dernière version stable du GLPI Agent depuis le dépôt officiel (github.com/glpi-project/glpi-agent/releases), au format Windows Installer (.msi), en version x64. Installation via l'assistant graphique :

- Écran d'accueil : cliquer sur Next.
- Accepter le contrat de licence, puis Next.
- Conserver (ou adapter) le chemin d'installation, puis Next.
- Type d'installation : choisir Typical.
- Écran « Choose Targets » : renseigner l'URL du serveur GLPI dans le champ Remote Targets (et non dans Local Target) : `http://192.168.137.3/glpi/front/inventory.php`, puis Next.
- Options SSL : en environnement de test local, cocher Disable SSL check, puis Next.
- Mode d'exécution : choisir l'exécution en tant que service (As a Windows service) et cocher Run inventory immediately after installation.
- Terminer l'installation.



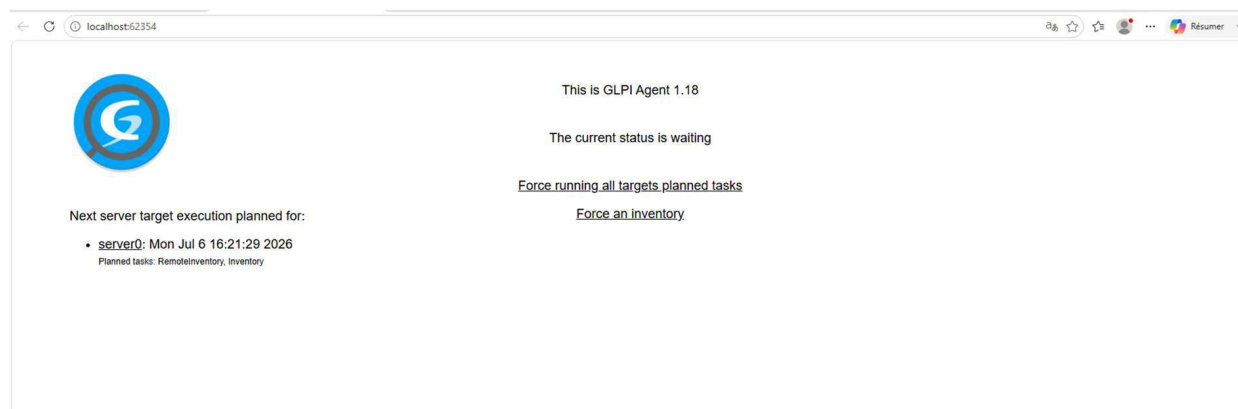
Écran « Choose Targets » : l'URL du serveur GLPI dans le champ Remote Targets

Installation silencieuse (alternative en ligne de commande). L'agent peut aussi être déployé sans interface, utile pour un déploiement de masse. L'option RUNNOW=1 force un inventaire immédiatement après l'installation :

```
msiexec /quiet /i GLPI-Agent-x.x_x64.msi ^
  RUNNOW=1 ^
  SERVER="http://IP_DU_SERVEUR/front/inventory.php"
```

Étape 3 — Forcer et vérifier la remontée d'inventaire.

Pour déclencher un premier inventaire sans attendre le passage planifié, ouvrir l'interface locale de l'agent sur le poste (<http://127.0.0.1:62354>) et cliquer sur « Force an inventory ».



Interface locale de l'agent (localhost:62354) : bouton « Force an inventory »

Côté serveur, on vérifie ensuite dans Parc > Ordinateurs : la machine cliente apparaît avec ses caractéristiques (modèle, système, processeur, RAM, disques, logiciels). On peut aussi contrôler dans Administration > Inventaire (ou Agents) la présence de l'agent et la date du dernier inventaire.

NOM	STATUT	FABRICANT	NUMÉRO DE SÉRIE	TYPE	MODÈLE	SYSTÈME D'EXPLOITATION - NOM	LIEU	DERNIÈRE MODIFICATION	COMPOSANTS - PROCESSEUR
DESKTOP-GG2OGNE		VMware, Inc.	VMware-56 4d 2d da bb ba 4e e6-ce f8 68 02 d2 4d 6e 34	VMware	VMware20,1	Microsoft Windows 11 Professionnel		2026-07-06 13:24	Intel(R) Core(TM) i7-10850H CPU @ 2.70GHz

Le poste remonté automatiquement dans Parc > Ordinateurs

2.1.7. Problèmes rencontrés

Accès réseau de la VM Debian (résolution DNS).

Lors de la configuration du serveur GLPI, la VM Debian ne parvenait pas à joindre le réseau, empêchant les tests de connectivité et le téléchargement des paquets. Symptôme observé :

```
ping google.com
-> Echec temporaire dans la resolution du nom
ping 8.8.8.8
-> connect: Le reseau n'est pas accessible
```

Cause : la carte réseau ajoutée à la VM n'était pas active (aucune adresse IP ni passerelle attribuées).

Résolution : identification de l'interface, activation et obtention d'une adresse en DHCP :

```
ip a
sudo ip link set ens33 up
sudo dhclient ens33
```

Configuration permanente dans le fichier des interfaces :

```
sudo nano /etc/network/interfaces

auto ens33
iface ens33 inet dhcp

sudo systemctl restart networking
```

En cas de réseau accessible mais sans résolution de nom, on force des serveurs DNS publics :

```
echo 'nameserver 8.8.8.8' | sudo tee /etc/resolv.conf
echo 'nameserver 8.8.4.4' | sudo tee -a /etc/resolv.conf
```

Note — hyperviseur : vérifier que la carte réseau de la VM est en mode NAT ou Bridge dans VMware. En mode Host-only, la VM n'a pas accès au réseau étendu.

Absence de remontée d'inventaire (GLPI Agent).

Si un poste équipé de l'agent n'apparaît pas dans le parc :

- Vérifier que l'URL du serveur est correcte et joignable depuis le poste (réseau, pare-feu).
- Vérifier que l'inventaire est bien activé côté serveur (Administration puis Inventaire).
- Consulter le journal de l'agent : C:\ProgramData\GLPI-Agent\glpi-agent.log

L'agent tente de créer un dossier au lieu d'envoyer l'inventaire.

Pendant l'installation de l'agent, si l'URL du serveur est renseignée dans le champ du dossier d'installation (Local Target) au lieu du champ Remote Targets, l'installateur essaie de créer un dossier nommé d'après l'URL et échoue avec « An error occurred while attempting to create the directory ». Il faut annuler, relancer l'installation et saisir l'URL uniquement dans le champ Remote Targets.

LDAPS injoignable — « No route to host » sur le port 636.

Lors du premier test de l'annuaire, GLPI bloquait à l'étape « Flux TCP » avec le message « No route to host (ERREUR: 113) vers 192.168.137.2 sur le port 636 ». La VM Debian n'atteignait pas le contrôleur de domaine. Diagnostic depuis la Debian :

```
ping -c4 192.168.137.2      # les deux VM se voient-elles ?
nc -zv 192.168.137.2 636    # le port LDAPS est-il ouvert ?
```

Deux causes à écarter : les cartes réseau des deux VM doivent être sur le même mode dans VMware (Bridge des deux côtés) pour qu'elles se voient ; et le pare-feu du contrôleur de domaine doit autoriser le port 636 en entrée. Le cas échéant, ouvrir le port sur le DC (PowerShell administrateur) :

```
New-NetFirewallRule -DisplayName "LDAPS 636" `
  -Direction Inbound -Protocol TCP -LocalPort 636 -Action Allow
```

Extension php-imap absente des dépôts Debian 13.

L'extension php-imap est requise par le collecteur de mails de GLPI (transformation des courriels en tickets, voir 2.3.4). Sur Debian 13, ce paquet n'est plus présent dans les dépôts par défaut : la vérification des prérequis de GLPI le signale absent.

Contournement : l'extension doit être ajoutée par une méthode complémentaire (dépôt PHP tiers ou installation via PECL), puis Apache redémarré. Vérification de la présence de l'extension :

```
php -m | grep imap
```

Une fois l'extension chargée, le collecteur configuré sur la boîte de support (relevé IMAP) transforme correctement les courriels entrants en tickets.

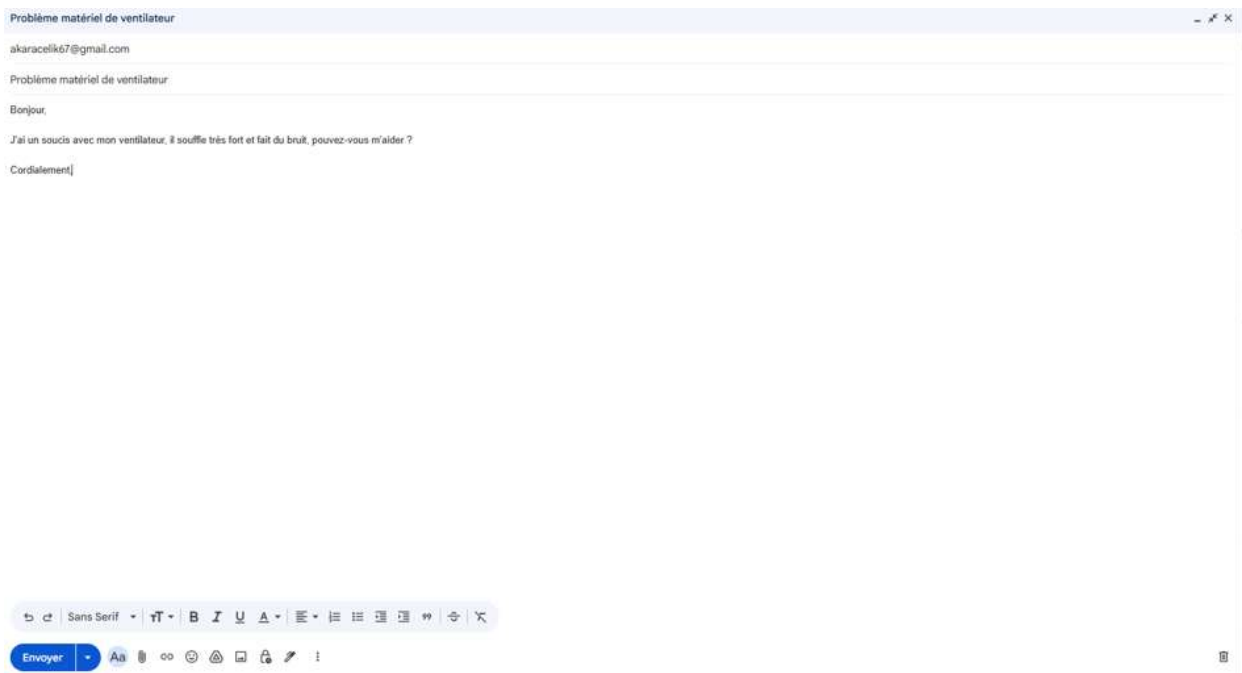
2.2. Documentation utilisateur — créer et suivre ses tickets

Cette partie s'adresse aux salariés de l'entreprise : comment ouvrir un ticket auprès du support, par mail ou depuis le portail GLPI, et comment suivre sa demande.

2.2.1. Créer un ticket par courriel

Envoyer un mail au support.

Envoyer un mail à l'adresse du support : akaracelik67@gmail.com. L'objet du mail devient le titre du ticket, le corps du message en devient la description.



Rédaction du mail adressé au support

Le ticket est créé automatiquement.

Après l'envoi, GLPI crée le ticket automatiquement. Il apparaît dans la liste, au statut « Nouveau ».

ID	TITRE	STATUT	DERNIERE MODIFICATION	DATE D'OUVERTURE	PRIORITE	DEMANDEUR - DEMANDEUR	ATTRIBUE À - TECHNICIEN	CATÉGORIE	TTR
13	Problème matériel de ventilateur	Nouveau	2026-06-26 13:38	2026-06-26 13:38	Moyenne	akaracelik67@gmail.com			
3	Bonjour, j'ai un soucis avec mon PC il démarre plus	En attente	2026-06-26 13:21	2026-06-26 13:15	Moyenne	post-only			
2	Problème active directory	Nouveau	2026-06-05 13:31	2026-06-05 13:30	Moyenne	mdrcoo278@gmail.com			
1	PROBLEME IT	Nouveau	2026-06-05 12:37	2026-06-05 12:37	Moyenne	akaracelik67@gmail.com			

At the bottom of the table, there is a pagination bar showing "20" items per page and "De 1 à 4 sur 4 lignes".

Le ticket créé automatiquement apparaît dans la liste, au statut « Nouveau »

Dans le ticket, le champ « Source de la demande » indique « E-Mail ».

Détail du ticket : le champ « Source de la demande » indique « E-Mail »

2.2.2. Créer un ticket via le site — connexion au portail Self-Service

L'interface Self-Service est la vue simplifiée proposée aux utilisateurs ne faisant pas partie de l'équipe informatique. Elle permet de créer une demande, de la suivre et de consulter la base de connaissances, sans accès aux fonctions d'administration.

Après connexion avec ses identifiants, l'utilisateur arrive sur la page d'accueil du portail. Le profil actif (« Self-Service ») et l'entité de rattachement sont affichés en haut à droite. La page présente plusieurs tuiles correspondant aux actions disponibles :

- **Parcourir les articles d'aide** : consulter la FAQ et la base de connaissances avant d'ouvrir un ticket.
- **Signaler un incident** : déclarer un dysfonctionnement (panne, erreur, matériel défaillant).
- **Demander un service** : formuler une demande non liée à une panne (accès, logiciel, matériel).
- **Créer un ticket** : accéder au catalogue de services et choisir un formulaire.
- **Voir vos tickets** : consulter la liste de ses demandes et leur état d'avancement.
- **Faire une réservation** : réserver un actif (salle, matériel) pour une date donnée.

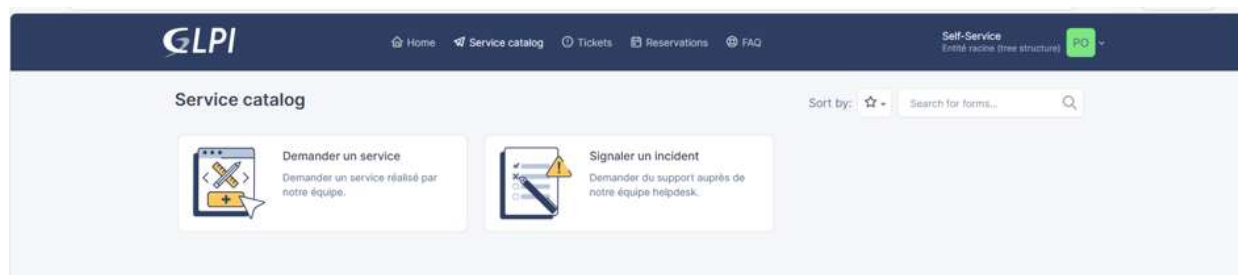


Page d'accueil de l'interface Self-Service

Incident ou demande de service ? Un incident correspond à quelque chose qui ne fonctionne plus (ex. « mon PC ne démarre plus »). Une demande de service correspond à un besoin nouveau (ex. « j'ai besoin d'un accès à un logiciel »). Ce choix oriente le ticket vers le bon circuit de traitement.

2.2.3. Signaler un incident via le site

Sur la page d'accueil, cliquer sur la tuile « Signaler un incident ». Le catalogue de services s'affiche : cliquer à nouveau sur « Signaler un incident ».



Catalogue de services : choix entre « Demander un service » et « Signaler un incident »

Le formulaire de signalement s'ouvre alors ; il regroupe les informations nécessaires au technicien pour qualifier et traiter la demande :

- **Titre** : résumé court et explicite du problème.
- **Description (obligatoire)** : explication détaillée : symptômes, message d'erreur, contexte d'apparition.
- **Urgence** : niveau d'urgence ressenti par l'utilisateur ; il participe au calcul de la priorité du ticket.
- **Catégorie** : type d'incident (matériel, réseau, logiciel...), utile pour le routage vers la bonne équipe.
- **Matériels de l'utilisateur** : permet d'associer l'incident à un équipement de l'inventaire (poste, imprimante...).
- **Observateurs** : personnes à tenir informées du suivi du ticket sans en être le demandeur.
- **Lieu** : localisation concernée (bâtiment, bureau, site).
- **Pièces jointes** : fichiers ou captures d'écran (2 Mio maximum par fichier) illustrant le problème.

Une fois les champs renseignés, valider le formulaire. GLPI crée le ticket, lui attribue automatiquement un numéro et le place au statut « Nouveau ». Le ticket est alors visible par l'équipe support.

The screenshot shows the 'Signaler un incident' form in GLPI. The form is titled 'Signaler un incident' and has a dark blue header with the GLPI logo and navigation links: Home, Service catalog, Tickets, Reservations, and FAQ. On the right, there is a 'Self-Service' section with a 'PO' button. The form fields are: Urgence (dropdown), Category (dropdown), Matériels de l'utilisateur (dropdown), Observers (text input), Location (dropdown), Titre (text input), and Description (rich text editor). Below the description is an Attachments section with a file upload area and a button 'Choisir un fichier'.

Formulaire « Signaler un incident »

Conseils pour un ticket efficace : un titre clair et une description précise accélèrent le traitement. Indiquer le message d'erreur exact, le moment d'apparition du problème et les actions déjà tentées évite des allers-retours avec le technicien.

2.2.4. Suivre l'état de ses tickets

Depuis la page d'accueil, cliquer sur la tuile « Voir vos tickets » (ou sur l'entrée « Tickets » du menu supérieur).



Accès au suivi via la tuile « Voir vos tickets »

La liste des demandes s'affiche. Chaque ligne récapitule l'essentiel :

- **ID** : numéro unique du ticket.
- **Title (Titre)** : intitulé saisi lors de la création.
- **Status (Statut)** : état d'avancement du ticket (ex. « Pending » / En attente).
- **Last update (Dernière mise à jour)** : date du dernier événement sur le ticket.
- **Opening date (Date d'ouverture)** : date de création du ticket.

Des filtres et tris (« Filtered by Status », « Sorted by Last update ») permettent d'organiser l'affichage. En cliquant sur un ticket, l'utilisateur accède au détail : il peut lire les réponses du technicien, ajouter un suivi (complément d'information) ou valider la solution proposée.

ID	TITLE	STATUS	LAST UPDATE	OPENING DATE
3	Bonjour, J'ai un soucis avec mon PC il démarre plus	Pending	2026-06-26 13:21	2026-06-26 13:15

Liste des tickets de l'utilisateur et leur statut

2.3. Documentation d'exploitation (technicien) — gestion des tickets, collecteur et annuaire

Cette section décrit le cycle de vie d'un ticket d'assistance dans GLPI, depuis sa création par un utilisateur jusqu'à sa prise en charge par un technicien du service informatique. Elle concerne deux publics :

- **l'utilisateur final** (salarié de l'entreprise), qui dispose de l'interface simplifiée Self-Service pour signaler un incident et suivre l'avancement de sa demande (voir la documentation utilisateur, section 2.2) ;
- **le technicien du support** (profil Technicien), qui réceptionne les tickets, les attribue et en assure le traitement.

À propos des comptes utilisés dans ce document : les captures présentées illustrent le parcours avec deux comptes de démonstration : un compte à droits restreints (profil Self-Service, icône « PO ») côté utilisateur, et un compte à profil Technicien (icône « TE ») côté support. Dans un environnement de production, chaque salarié dispose de son propre compte nominatif.

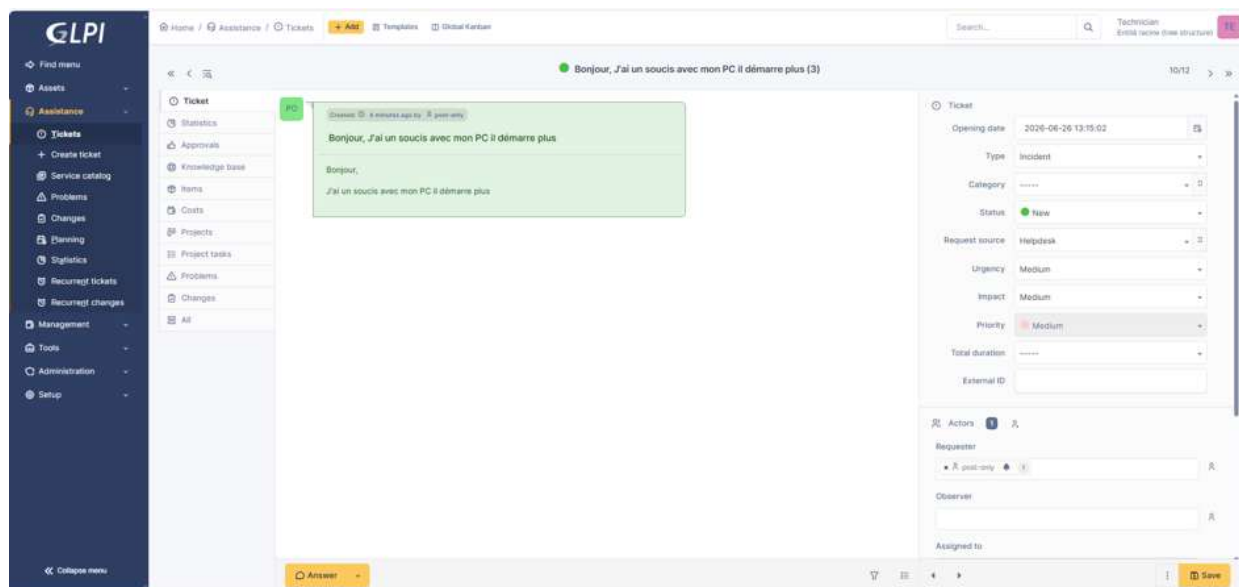
Le technicien dispose de l'interface complète de GLPI. Les tickets créés par les utilisateurs (via le portail Self-Service ou par mail) y apparaissent automatiquement et peuvent être attribués, traités puis clôturés.

2.3.1. Visualisation d'un nouveau ticket

Le technicien se connecte avec un compte à profil Technicien. Le ticket apparaît dans le menu Assistance > Tickets, au statut « Nouveau » (New). En l'ouvrant, il accède à l'ensemble des informations saisies par l'utilisateur.

L'écran se compose de trois zones :

- **Menu de gauche** : navigation dans GLPI (Assistance, Parc, Gestion, Outils, Administration...).
- **Zone centrale** : le message du demandeur et l'historique des échanges ; le bouton « Answer » (Répondre) permet d'ajouter un suivi ou une solution.
- **Panneau de droite** : les caractéristiques du ticket : date d'ouverture, type (Incident), catégorie, statut, source (Helpdesk), urgence, impact, priorité, et les acteurs (Demandeur, Observateur, Attribué à).



Vue technicien d'un ticket nouvellement reçu

2.3.2. Prise en charge du ticket

La prise en charge consiste à s'attribuer le ticket, à en faire évoluer le statut puis à répondre à l'utilisateur. Le déroulé type est le suivant :

- Ouvrir le ticket depuis la liste Assistance > Tickets.
- S'attribuer le ticket : dans le panneau « Acteurs », renseigner le technicien dans le champ « **Attribué à** ».
- Faire évoluer le statut de « **Nouveau** » vers « **En cours (attribué)** » pour indiquer que le traitement a commencé.
- Répondre au demandeur via le bouton « **Answer** » : ajouter un suivi (question, information) ou une solution.
- Si une information manque, passer le statut à « **En attente** » (Pending) : c'est l'état que l'utilisateur voit alors côté Self-Service.
- Enregistrer les modifications avec le bouton « **Save** ».

Lorsque le problème est résolu, le technicien passe le ticket en « Résolu » avec une description de la solution. L'utilisateur peut alors valider, ce qui clôture définitivement le ticket (« Clos »).

2.3.3. Cycle de vie d'un ticket

Un ticket suit un enchaînement de statuts, de sa création à sa clôture. Le tableau ci-dessous récapitule les états possibles ainsi que leur correspondance entre l'interface française et l'interface anglaise.

Statut (GLPI FR)	Libellé EN	Signification
Nouveau	New	Ticket créé par l'utilisateur, en attente d'un technicien.
En cours (attribué)	Processing (assigned)	Un technicien a pris le ticket en charge.
En cours (planifié)	Processing (planned)	Une intervention a été programmée à une date donnée.
En attente	Pending	Traitement suspendu, souvent en attente d'une réponse de l'utilisateur.

Statut (GLPI FR)	Libellé EN	Signification
Résolu	Solved	Une solution a été proposée, en attente de validation.
Clos	Closed	Ticket terminé, validé et archivé.

Schématiquement, le parcours nominal est : Nouveau → En cours (attribué) → éventuellement En attente → Résolu → Clos.

2.3.4. Configuration du collecteur de mails

Le collecteur de mails permet de transformer automatiquement les courriels reçus sur la boîte de support en tickets GLPI : l'objet du mail devient le titre du ticket, le corps devient la description (côté salarié, la marche à suivre est décrite en section 2.2.1). La boîte de support du projet est akaracelik67@gmail.com, relevée en IMAP.

Prérequis : l'extension php-imap.

Le collecteur repose sur l'extension PHP imap. On vérifie qu'elle est bien chargée sur le serveur :

```
php -m | grep imap
```

La ligne « imap » doit être retournée. Sur Debian 13, le paquet n'est plus dans les dépôts par défaut : voir 2.1.7 (Problèmes rencontrés) pour la méthode d'installation.

Préparer la boîte Gmail : mot de passe d'application.

Gmail n'accepte pas le mot de passe habituel du compte pour une connexion IMAP par une application tierce : il faut générer un mot de passe d'application, dédié à GLPI.

- Sur le compte Google (myaccount.google.com), aller dans Sécurité et activer la validation en deux étapes (indispensable, sinon l'option n'apparaît pas).
- Toujours dans Sécurité, ouvrir « Mots de passe des applications ».
- Créer une entrée (ex. « GLPI ») : Google génère un mot de passe de 16 caractères, à copier immédiatement (il n'est affiché qu'une fois).

C'est ce mot de passe de 16 caractères, et non celui du compte, qui sera renseigné dans GLPI.

Créer le collecteur dans GLPI.

Dans GLPI, aller dans Configuration > Collecteurs, puis Ajouter. Renseigner :

- **Nom** : l'adresse de la boîte de support, akaracelik67@gmail.com (ce champ sert aussi d'adresse de réponse).
- **Actif** : Oui.
- **Serveur de messagerie** : imap.gmail.com
- **Options de connexion** : IMAP, SSL, port 993, dossier INBOX.
- La chaîne de connexion générée est : {imap.gmail.com:993/imap/ssl}INBOX
- **Identifiant** : akaracelik67@gmail.com
- **Mot de passe** : le mot de passe d'application généré à l'étape précédente.
- **Taille maximale des pièces jointes** : 2 Mio, en cohérence avec la limite du portail.
- **Entité de destination** : l'entité racine du projet.

Enregistrer. Le bouton « Tester » de la fiche doit confirmer que la connexion à la boîte réussit.

Le relevé automatique (action mailgate).

La boîte n'est pas relevée en continu : c'est l'action automatique mailgate qui interroge le collecteur à intervalle régulier. Dans Configuration > Actions automatiques, ouvrir mailgate et vérifier :

- **Fréquence d'exécution** : toutes les 10 minutes (valeur retenue pour le projet).
- **Statut** : Programmé.
- **Mode d'exécution** : GLPI (l'action tourne au fil des visites de l'interface) ; en production, le mode CLI avec une tâche cron est recommandé.

Pour tester sans attendre le prochain passage, cliquer sur « Exécuter » directement dans la fiche de l'action : les mails en attente sont relevés immédiatement.

Test de bout en bout.

- Envoyer un mail à akaracelik67@gmail.com depuis une boîte quelconque, avec un objet et un corps de test.
- Forcer l'exécution de mailgate (ou attendre le prochain relevé).
- Vérifier dans Assistance > Tickets : un ticket est créé, titre = objet du mail, description = corps du mail, champ « Source de la demande » = E-Mail.

Si l'expéditeur correspond à un utilisateur connu de GLPI (adresse renseignée sur sa fiche, par exemple importée depuis l'annuaire), le ticket lui est automatiquement rattaché comme demandeur.

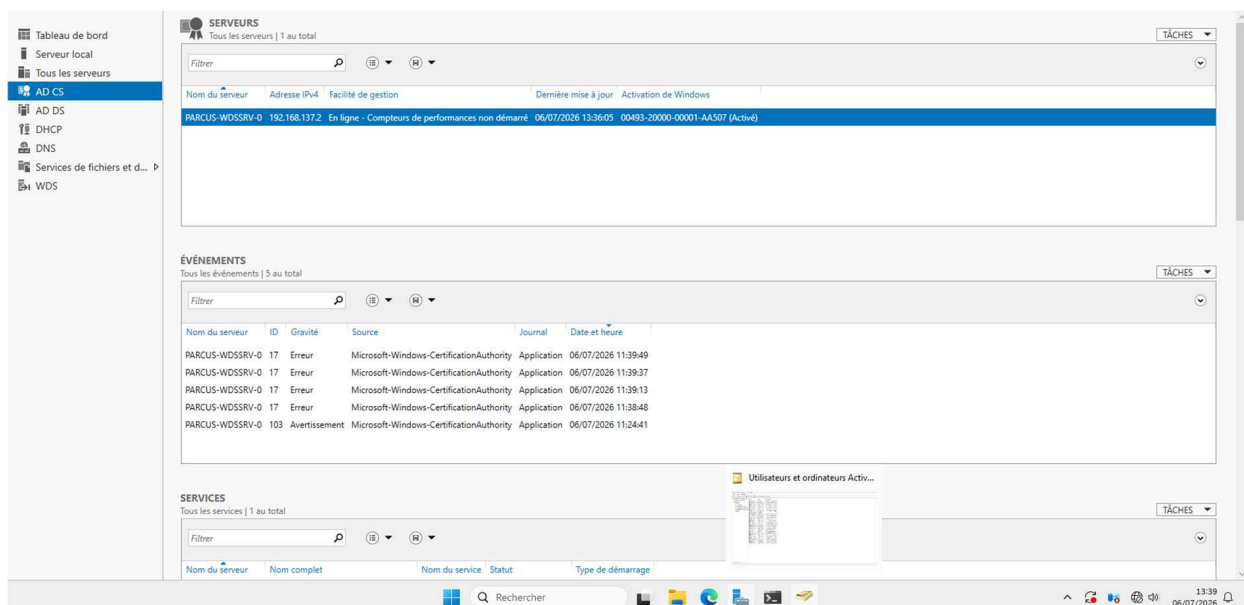
2.3.5. Liaison avec l'annuaire d'authentification (LDAPS)

Les salariés se connectent à GLPI avec leur compte Active Directory : il n'y a plus de comptes locaux GLPI à créer et à maintenir, et un mot de passe unique suffit pour la session Windows et le portail d'assistance. La liaison se fait en LDAPS (LDAP sur SSL, port 636) plutôt qu'en LDAP simple (port 389), afin que les mots de passe ne transitent jamais en clair sur le réseau.

Environnement du projet : le contrôleur de domaine est PARCUS-WDSSRV-01 (192.168.137.2), le domaine parcus.fr, et le serveur GLPI est la VM Debian 192.168.137.3.

Étape 1 — Installer le rôle AD CS sur le contrôleur de domaine.

LDAPS exige que le contrôleur de domaine présente un certificat serveur. On installe pour cela le rôle AD CS (Services de certificats Active Directory) : dans le Gestionnaire de serveur, Gérer > Ajouter des rôles et fonctionnalités.



Le Gestionnaire de serveur du contrôleur de domaine : le rôle AD CS apparaît après installation

Dans l'assistant, on sélectionne le serveur de destination (PARCUS-WDSSRV-01.parcus.fr) :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
PARCUS-WDSSRV-01.parcus.fr

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
PARCUS-WDSSRV-01.pa...	192.168.137.1	Microsoft Windows Server 2025 Standard Evaluation

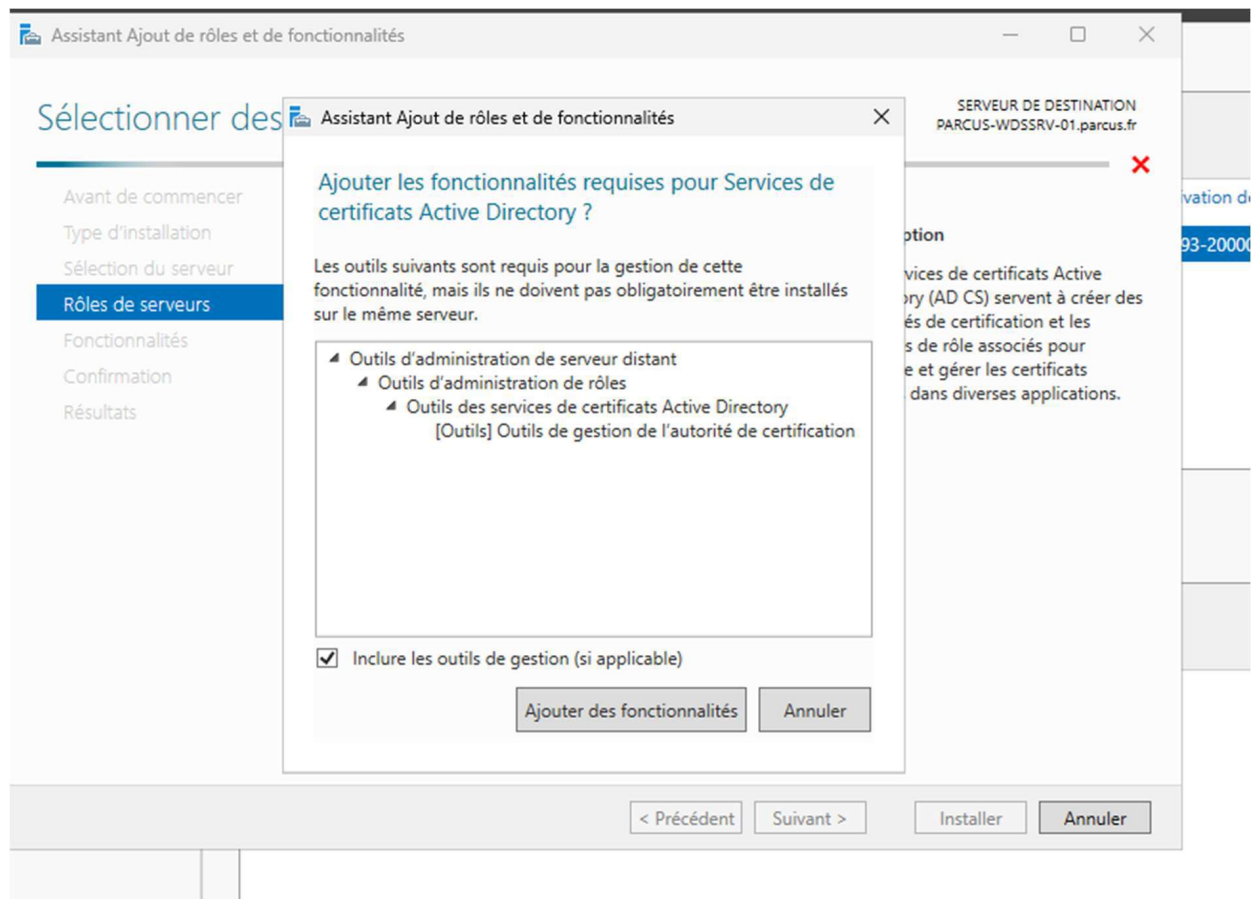
1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

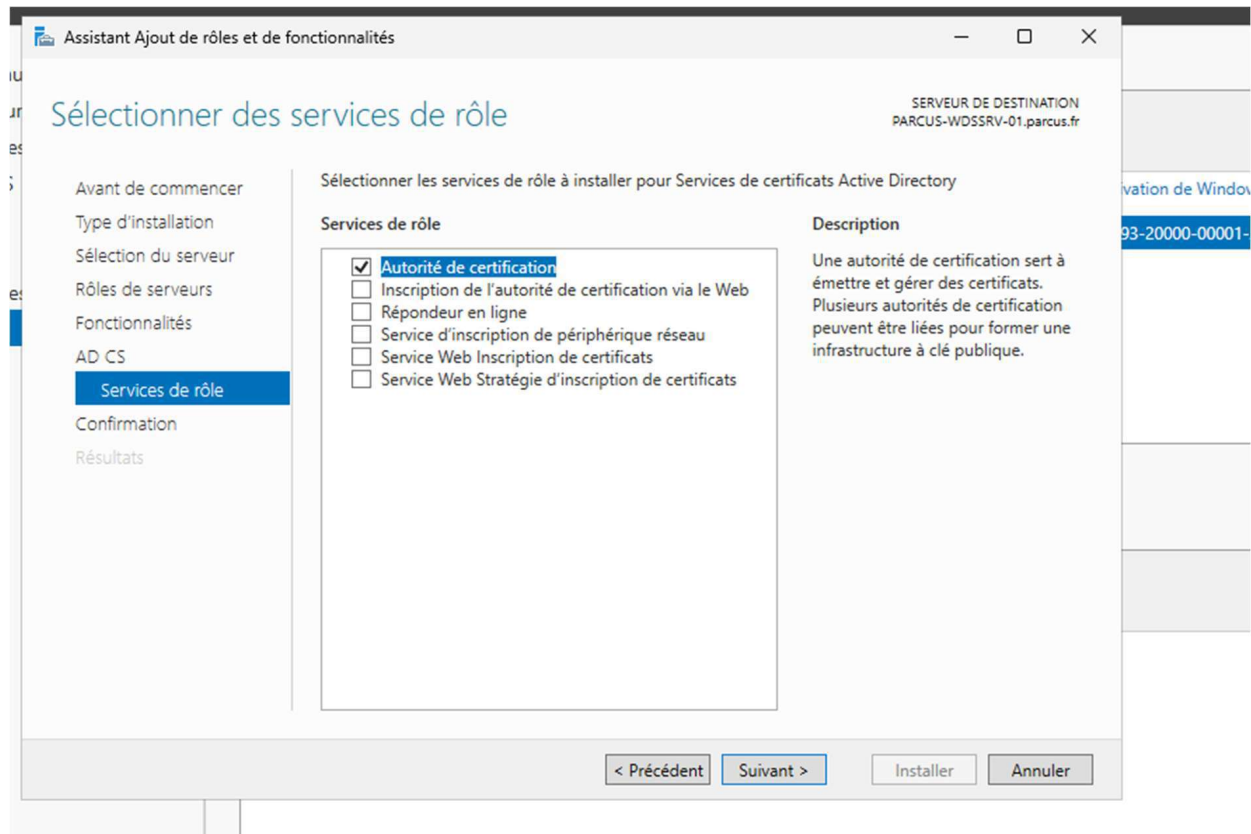
Assistant Ajout de rôles : sélection du serveur de destination

Au moment de cocher le rôle Services de certificats Active Directory, l'assistant propose d'ajouter les outils de gestion associés : cliquer sur Ajouter des fonctionnalités.



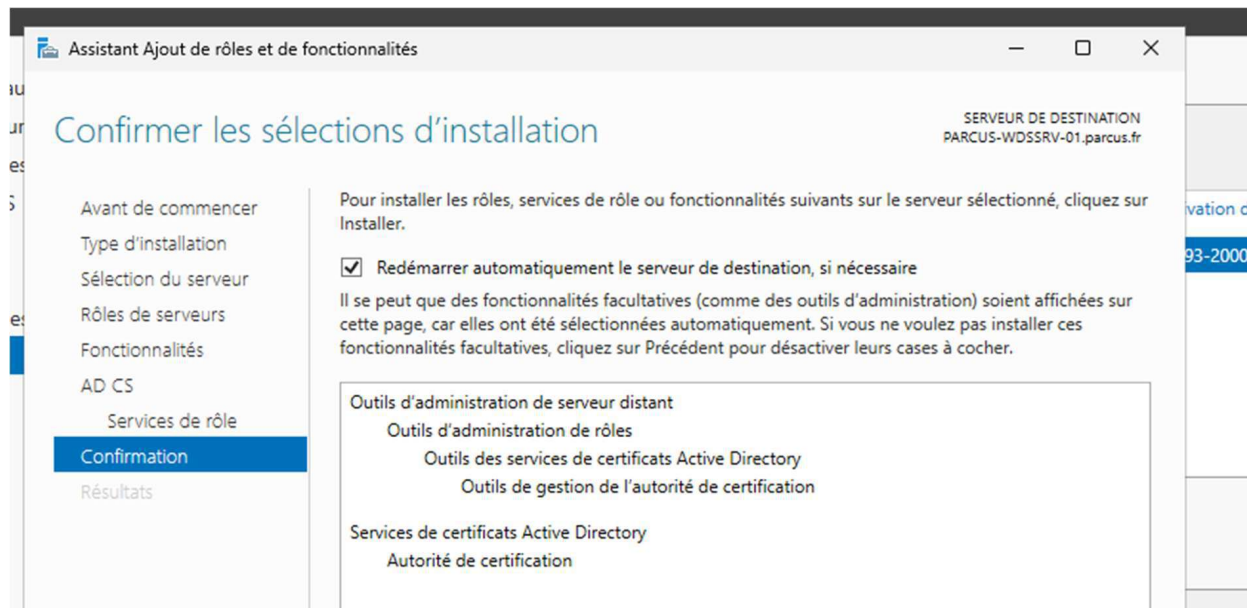
Ajout des fonctionnalités requises pour AD CS (outils de gestion de l'autorité de certification)

Dans Services de rôle, seul « Autorité de certification » est nécessaire :



Services de rôle : seule l'Autorité de certification est cochée

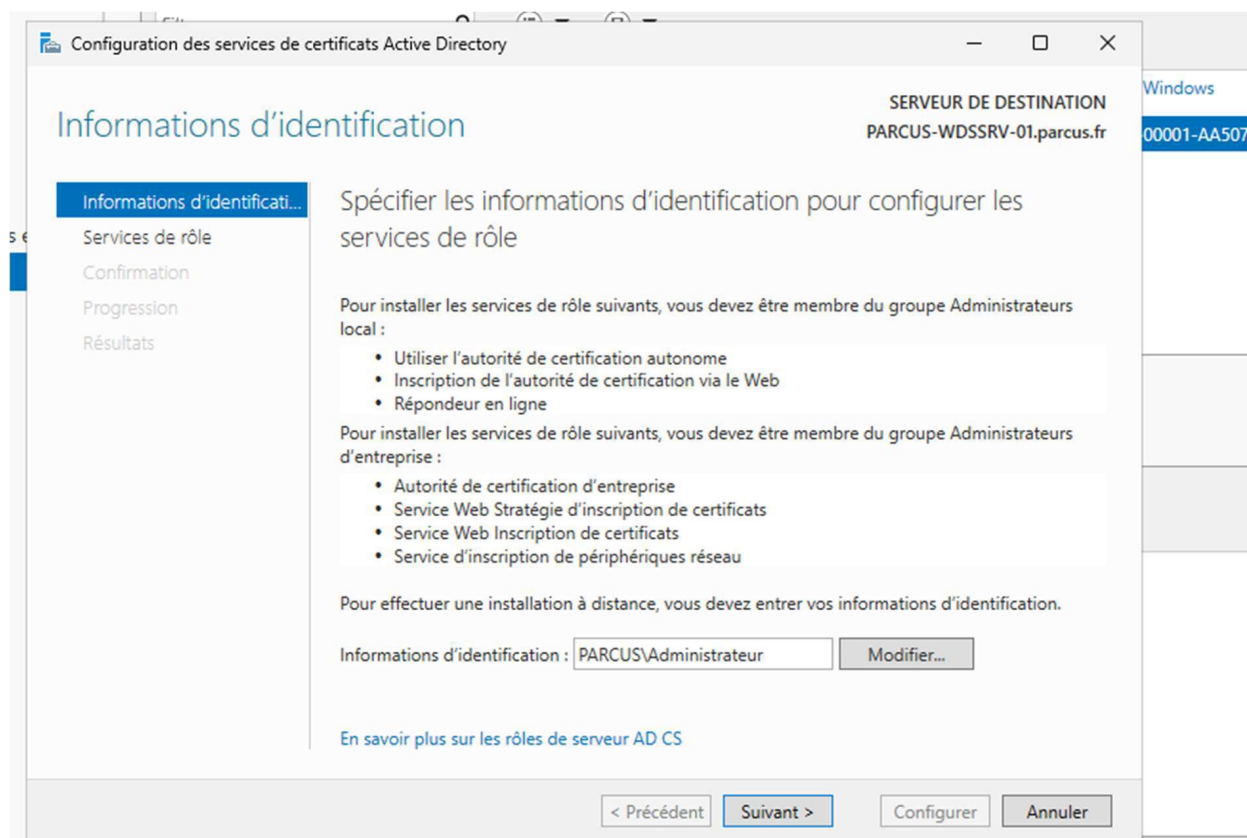
On confirme et on lance l'installation (l'option de redémarrage automatique peut être cochée) :



Confirmation des sélections et installation du rôle

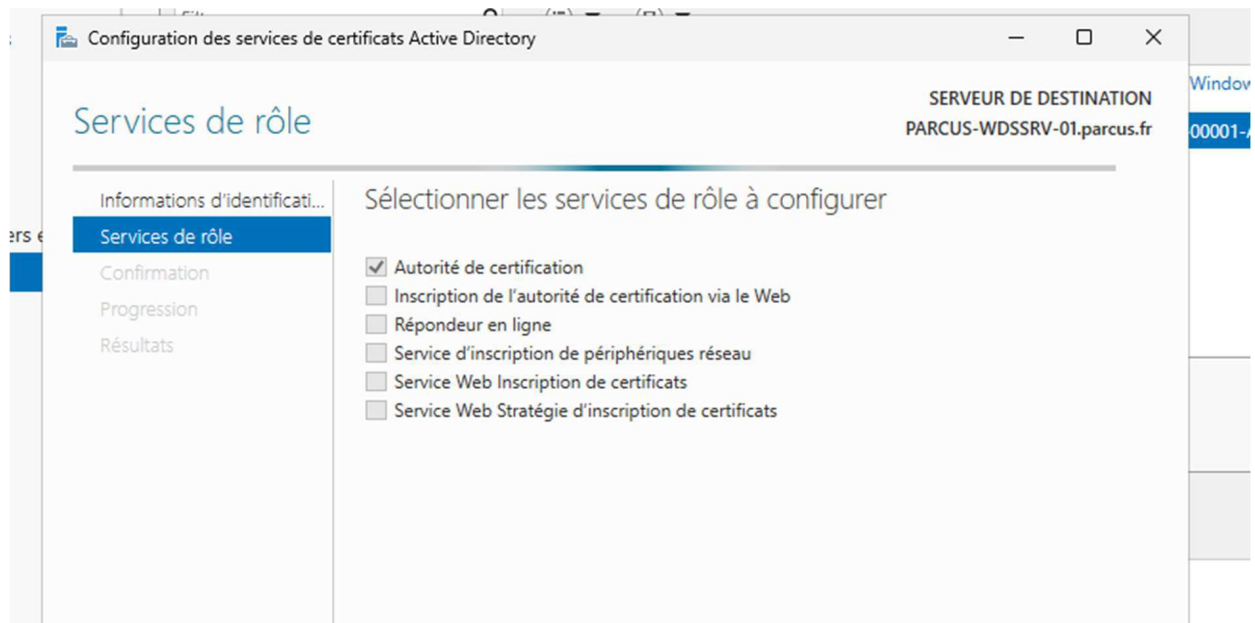
Étape 2 — Configurer l'autorité de certification (post-déploiement).

L'installation du rôle ne suffit pas : il faut lancer la configuration post-déploiement (bannière d'avertissement du Gestionnaire de serveur > « Configurer les services de certificats Active Directory »). L'assistant demande d'abord les informations d'identification : renseigner un compte administrateur du domaine (PARCUS\Administrateur).



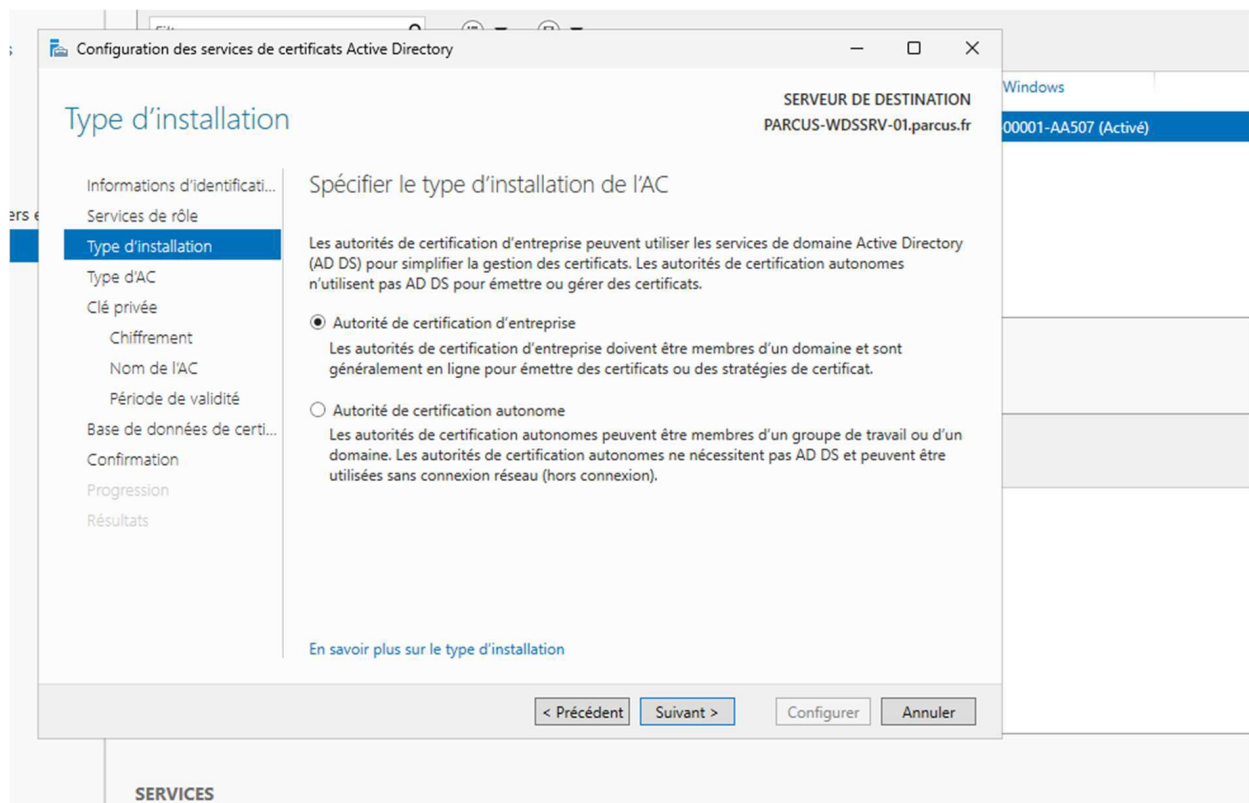
Configuration AD CS : informations d'identification (PARCUS\Administrateur)

Sélectionner le service de rôle « Autorité de certification » à configurer :



Sélection du service de rôle à configurer

Le type d'installation est le choix décisif pour LDAPS : sélectionner « Autorité de certification d'entreprise ». Une CA d'entreprise s'appuie sur AD DS, ce qui permet au contrôleur de domaine de s'inscrire automatiquement pour un certificat d'authentification serveur.



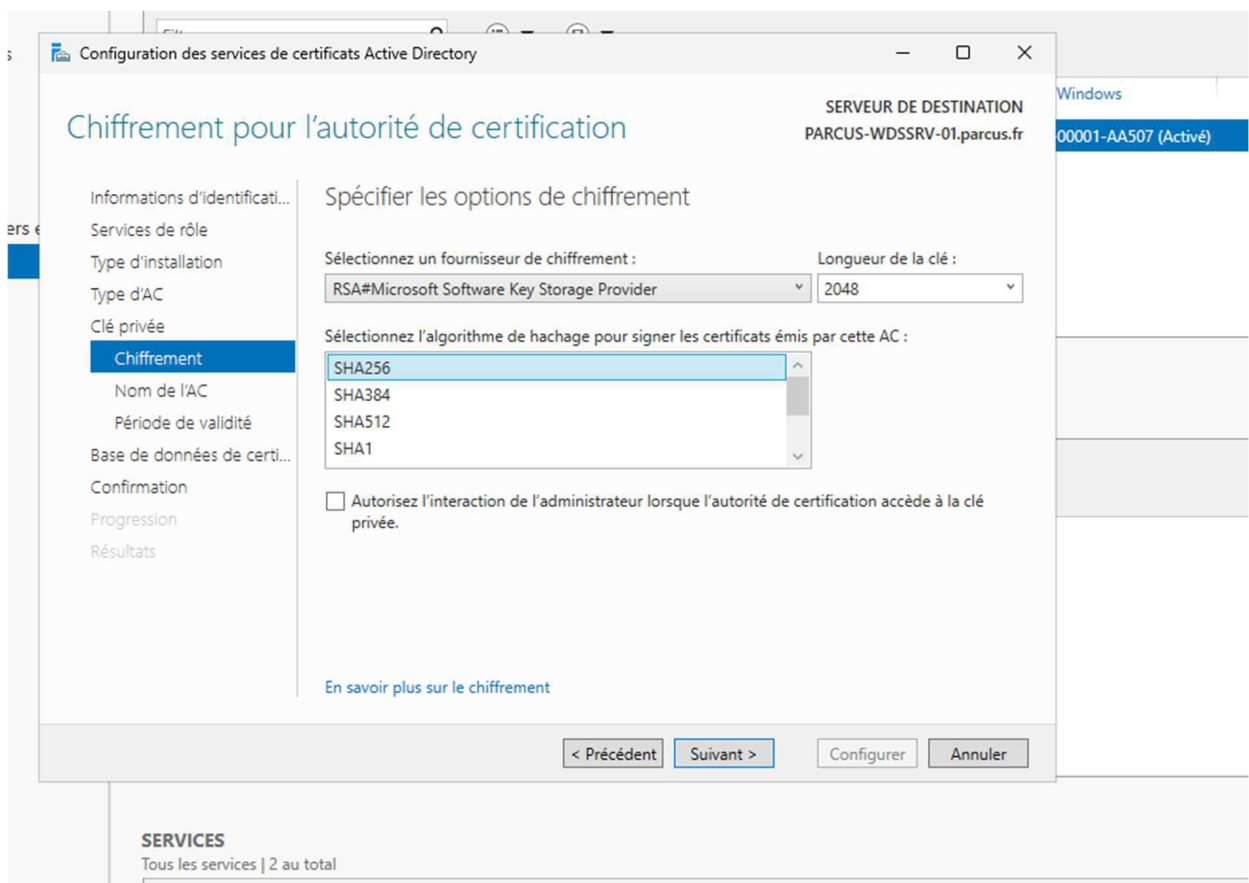
Type d'installation : Autorité de certification d'entreprise

Type d'AC : « Autorité de certification racine » (première autorité de la hiérarchie PKI) :



Type d'autorité de certification : racine

Options de chiffrement : conserver les valeurs par défaut (RSA 2048, hachage SHA256) :



Options de chiffrement de la CA : RSA 2048 / SHA256

Le nom proposé pour l'AC est conservé (parcus-PARCUS-WDSSRV-0-CA, suffixe DC=parcus,DC=fr), puis période de validité par défaut (5 ans) et chemins de base de données par défaut. Cliquer sur Configurer : « Configuration réussie ».

rs Configuration des services de certificats Active Directory

Nom de l'autorité de certification

SERVEUR DE DESTINATION
PARCUS-WDSSRV-01.parcus.fr

Window
00001-A

Informations d'identification...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :
parcus-PARCUS-WDSSRV-0-CA

Suffixe du nom unique :
DC=parcus,DC=fr

Aperçu du nom unique :
CN=parcus-PARCUS-WDSSRV-0-CA,DC=parcus,DC=fr

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Nom de l'autorité de certification : parcus-PARCUS-WDSSRV-0-CA

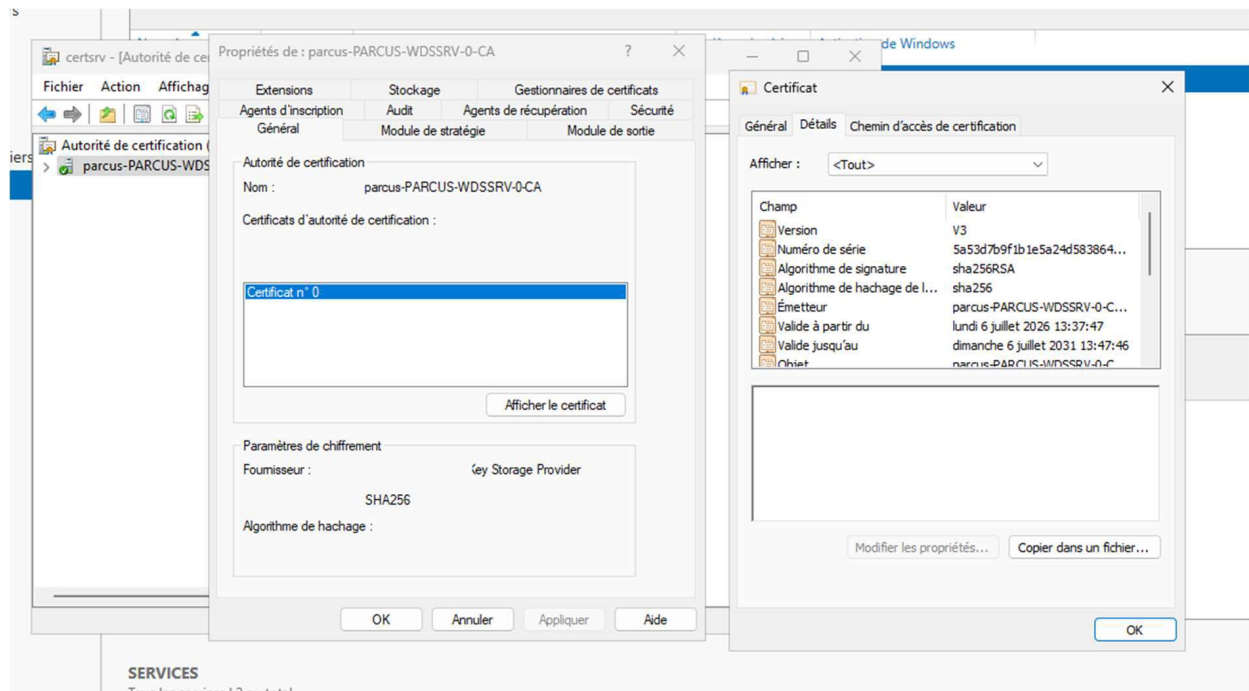
Après la configuration, on force l'inscription du certificat puis on redémarre le serveur :

```
certutil -pulse  
gpupdate /force
```

On vérifie ensuite que LDAPS répond avec l'outil ldp.exe (Connexion > Connexion, serveur PARCUS-WDSSRV-01.parcus.fr, port 636, case SSL cochée) : l'affichage du RootDSE confirme que LDAPS fonctionne.

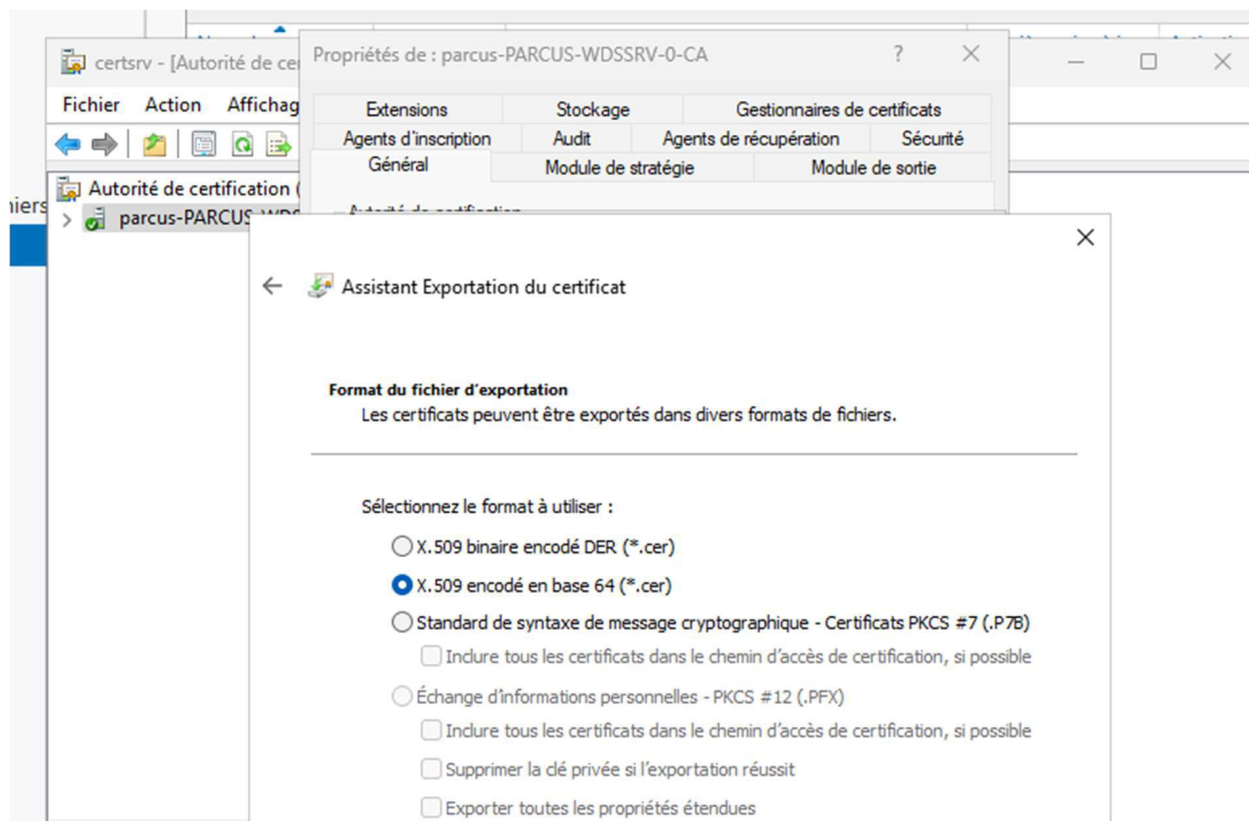
Étape 3 — Exporter le certificat de l'autorité.

C'est ce certificat que le serveur GLPI devra approuver. Dans la console Autorité de certification (Outils > Autorité de certification), clic droit sur la CA parcus-PARCUS-WDSSRV-0-CA > Propriétés > Général > Afficher le certificat > onglet Détails > Copier dans un fichier.

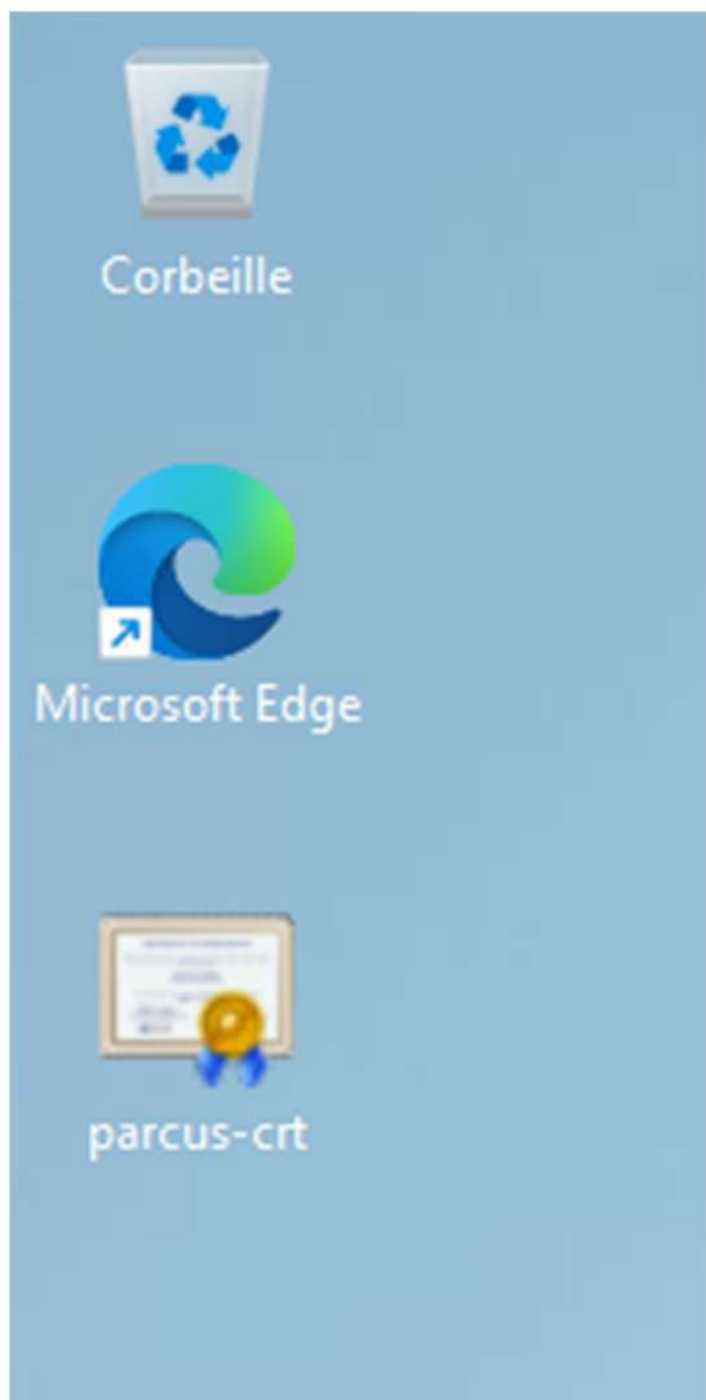


Propriétés de la CA : affichage du certificat de l'autorité

Dans l'assistant d'exportation, choisir le format X.509 encodé en Base 64 (.CER) et enregistrer le fichier (ca-parcus.cer) :



Export du certificat au format X.509 encodé en Base 64 (.cer)

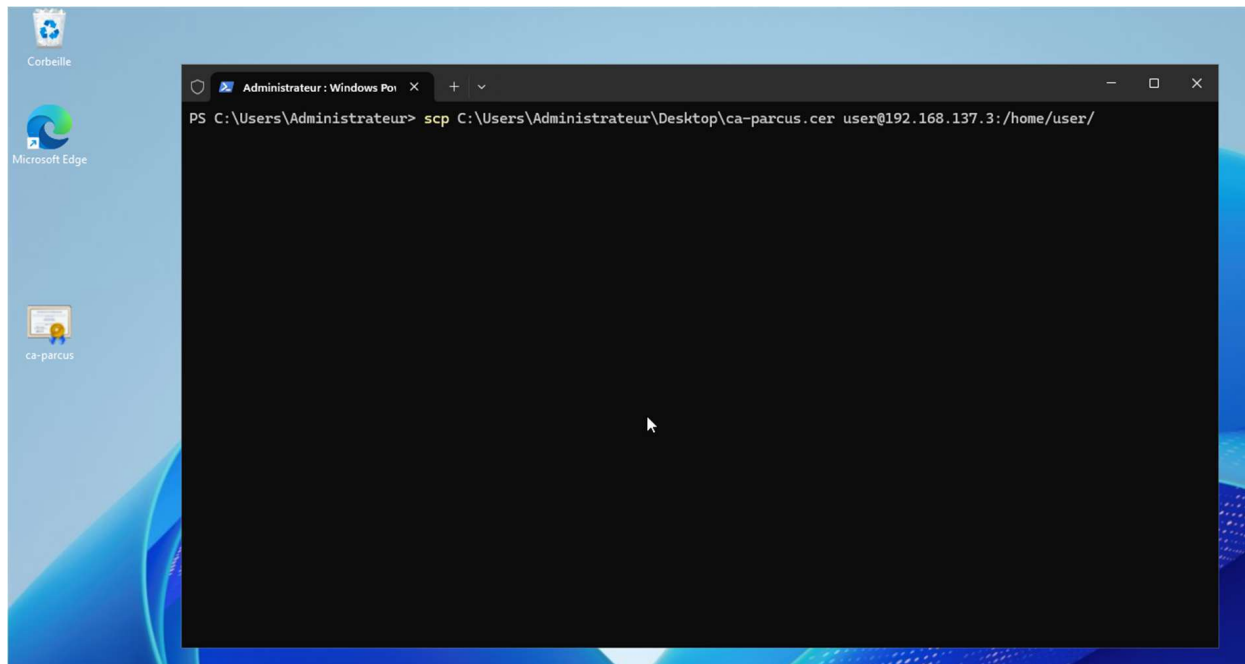


Le certificat exporté (ca-parcus) sur le bureau du serveur

Étape 4 — Transférer le certificat sur le serveur GLPI.

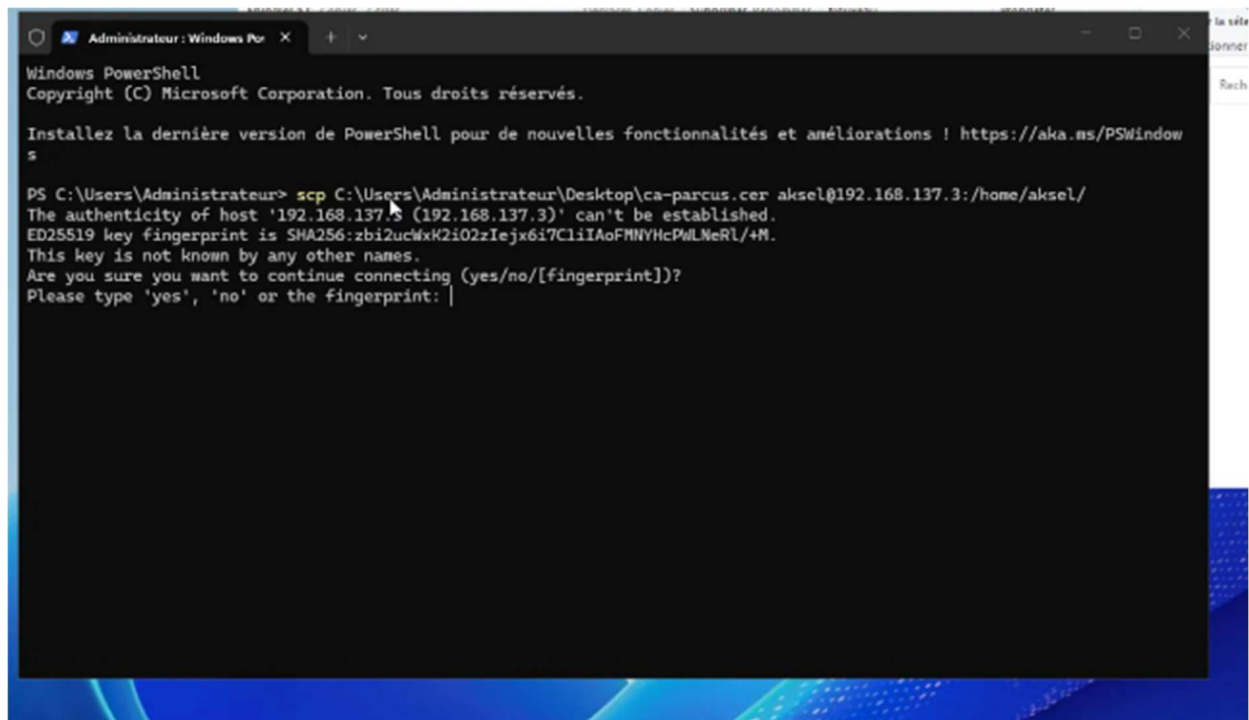
Le fichier est transféré vers la VM Debian par scp, directement depuis PowerShell sur le serveur Windows :

```
scp C:\Users\Administrateur\Desktop\ca-parcus.cer user@192.168.137.3:/home/user/
```



Transfert du certificat par scp depuis PowerShell

À la première connexion, scp demande de confirmer l'empreinte du serveur SSH (taper yes), puis le mot de passe de l'utilisateur Debian (la saisie est invisible, c'est normal) :



Première connexion SSH : confirmation de l'empreinte du serveur (yes)

```

Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\Administrateur> scp C:\Users\Administrateur\Desktop\ca-parcus.cer aksel@192.168.137.3:/home/aksel/
The authenticity of host '192.168.137.3 (192.168.137.3)' can't be established.
ED25519 key fingerprint is SHA256:zbi2ucWxK2i02zIejx6i7C1iIAoFMNYHcPWLNeRL/+H.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Please type 'yes', 'no' or the fingerprint:
Warning: Permanently added '192.168.137.3' (ED25519) to the list of known hosts.
aksel@192.168.137.3's password:
Permission denied, please try again.
aksel@192.168.137.3's password:
Connection closed by 192.168.137.3 port 22
C:\WINDOWS\System32\OpenSSH\scp.exe: Connection closed
PS C:\Users\Administrateur> scp C:\Users\Administrateur\Desktop\ca-parcus.cer aksel@192.168.137.3:/home/aksel/
aksel@192.168.137.3's password:
Permission denied, please try again.
aksel@192.168.137.3's password:

```

Saisie du mot de passe de l'utilisateur Debian pour le transfert

Étape 5 — Faire confiance au certificat côté serveur GLPI.

Sur la VM Debian, on ajoute le certificat aux certificats de confiance du système, on met à jour le magasin, puis on redémarre Apache :

```

sudo cp /home/user/ca-parcus.cer /usr/local/share/ca-certificates/ca-parcus.crt
sudo update-ca-certificates
sudo systemctl restart apache2

```

La commande doit indiquer « 1 added ». Sans cette étape, la connexion LDAPS échoue avec une erreur de certificat. Le serveur GLPI doit également pouvoir résoudre le nom du contrôleur de domaine (DNS pointant vers 192.168.137.2, ou entrée dans /etc/hosts).

```

user@debianNG:~$ sudo cp /home/user/ca-parcus.cer /usr/local/share/ca-certificates/ca-parcus.crt
sudo update-ca-certificates
sudo systemctl restart apache2
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt, it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
user@debianNG:~$

```

update-ca-certificates sur la Debian : « 1 added, 0 removed; done. »

Étape 6 — Déclarer l'annuaire dans GLPI.

Dans GLPI, aller dans Configuration > Authentification > Annuaire LDAP, puis Ajouter. Les valeurs retenues pour le projet sont :

- **Nom** : Parcus
- **Serveur** : ldaps://192.168.137.2
- **Port** : 636
- **BaseDN** : DC=parcus,DC=fr — le point de départ des recherches dans l'annuaire.
- **DN du compte (connexions non anonymes)** :
CN=Administrateur,CN=Users,DC=parcus,DC=fr
- **Mot de passe du compte** : celui du compte utilisé pour lire l'annuaire.

- **Filtre de connexion :**
(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
— filtre Active Directory qui ne remonte que les utilisateurs actifs (le dernier terme exclut les comptes désactivés).
- **Champ de l'identifiant :** samaccountname — les salariés se connectent avec leur identifiant de session Windows.
- **Champ de synchronisation :** objectguid

Fiche de configuration de l'annuaire LDAP dans GLPI

Étape 7 — Tester la connexion.

Sur la fiche de l'annuaire, onglet Tester : GLPI déroule cinq contrôles, qui doivent tous passer au vert : flux TCP vers 192.168.137.2:636, Base DN, URI LDAP, connexion bind (authentification) et recherche d'entrées.

Test LDAP : les cinq étapes réussies (flux TCP, Base DN, URI, bind, recherche)

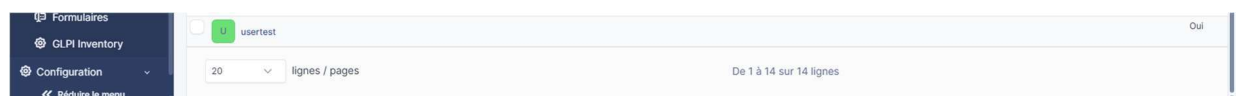
Étape 8 — Créer un utilisateur dans l'annuaire et l'importer.

Côté Windows Server, dans « Utilisateurs et ordinateurs Active Directory », on crée les comptes des salariés (ici un compte de test usertest) :

Création d'un utilisateur dans Active Directory : fiche du compte usertest

Fiche de l'utilisateur usertest dans Active Directory (suite)

Côté GLPI, deux fonctionnements se complètent : l'import manuel (Administration > Utilisateurs > Liaison annuaire LDAP > Importation de nouveaux utilisateurs) et l'import à la volée (un salarié présent dans l'AD est créé automatiquement à sa première connexion). Dans les deux cas, le profil « Self-Service » est affecté par défaut (voir section 2.2) ; les techniciens reçoivent le profil Technicien manuellement.

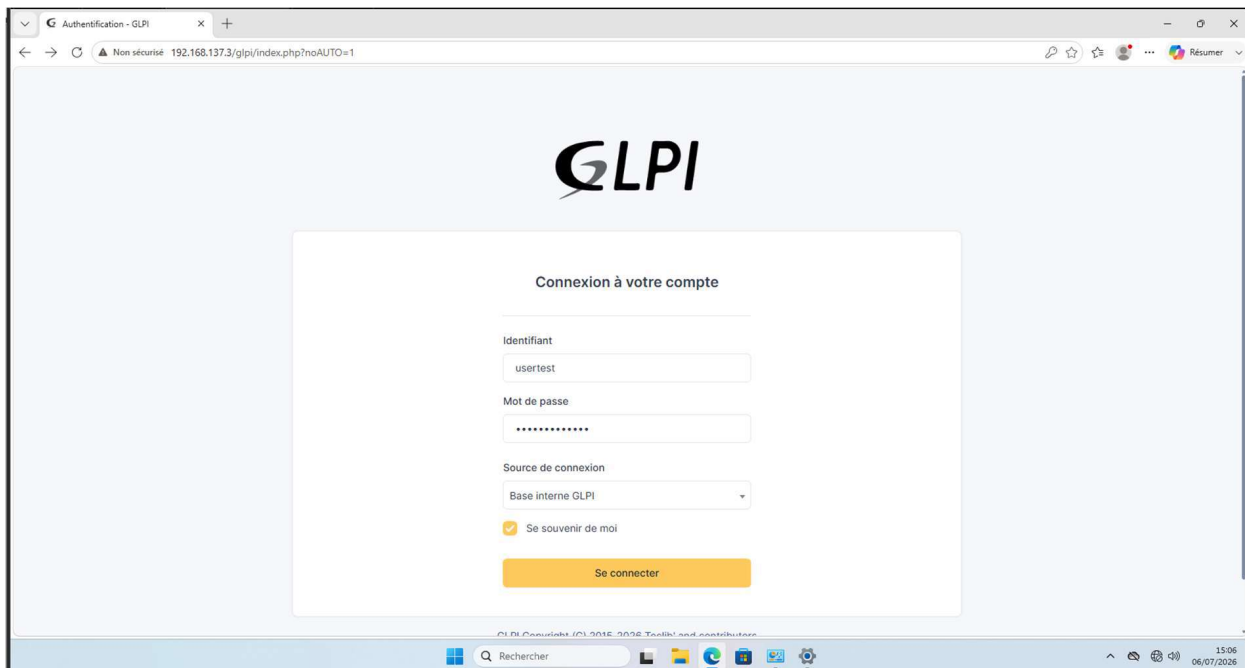


L'utilisateur usertest importé apparaît dans la liste des utilisateurs GLPI

Étape 9 — Vérification : connexion et premier ticket.

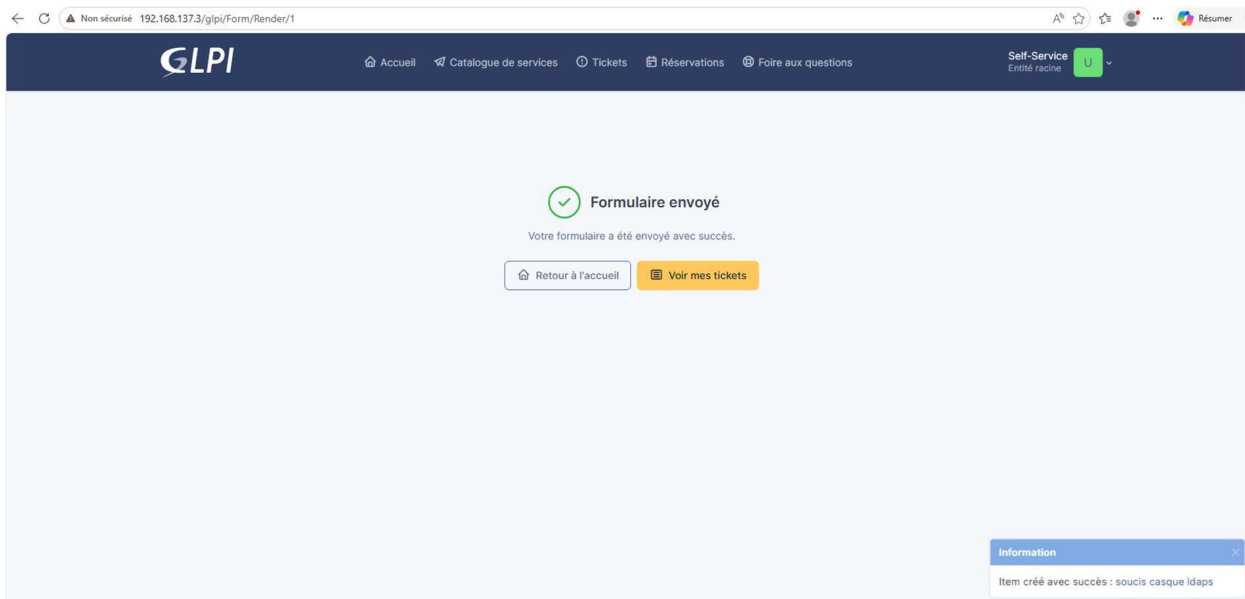
On ouvre une session GLPI avec le compte du domaine (identifiant usertest + mot de passe AD). La session s'ouvre sur le portail Self-Service : l'authentification centralisée est fonctionnelle. À

chaque connexion, GLPI vérifie le mot de passe directement auprès du contrôleur de domaine : un compte désactivé dans l'AD ne peut plus se connecter à GLPI.

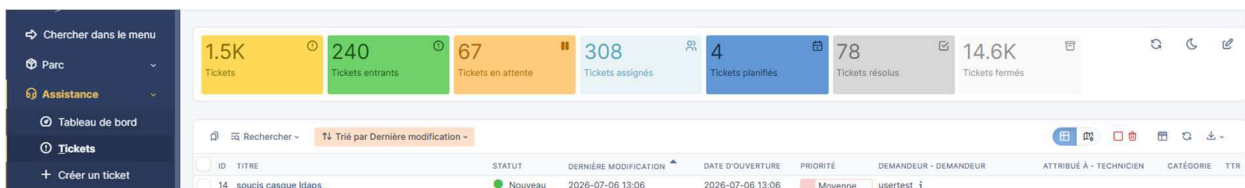


Connexion à GLPI avec le compte Active Directory usertest

Pour valider le parcours de bout en bout, l'utilisateur crée un premier ticket depuis le portail :



Le formulaire de ticket envoyé avec succès depuis le portail Self-Service



Le ticket créé par usertest apparaît dans la liste des tickets côté technicien

3. Windows Server 2025 — services d'infrastructure (LOT 3)

Lot réalisé par JEANNEY Alexis : annuaire Active Directory (domaine parcus.fr), services DNS et DHCP, déploiement de postes par le réseau avec WDS, stratégies de groupe (GPO), chiffrement BitLocker des postes avec sauvegarde des clés de récupération dans l'annuaire, puis un second serveur de redondance portant la zone DNS secondaire, le basculement DHCP et l'autorité de certification (AD CS).

3.1. Documentation d'installation — contrôleur de domaine et services réseau

3.1.1. Présentation de l'architecture

Le LOT 3 met en place le cœur de l'infrastructure PARCUS : un domaine Active Directory nommé parcus.fr, hébergé sur un serveur Windows Server 2025. Ce serveur cumule les rôles AD DS (annuaire), DNS (résolution de noms), DHCP (attribution des adresses IP) et WDS (déploiement de Windows par le réseau). Un second serveur Windows Server 2025 vient ensuite en secours : il héberge une copie de la zone DNS, participe au basculement DHCP et porte l'autorité de certification (AD CS) utilisée notamment pour le LDAPS du LOT 2.

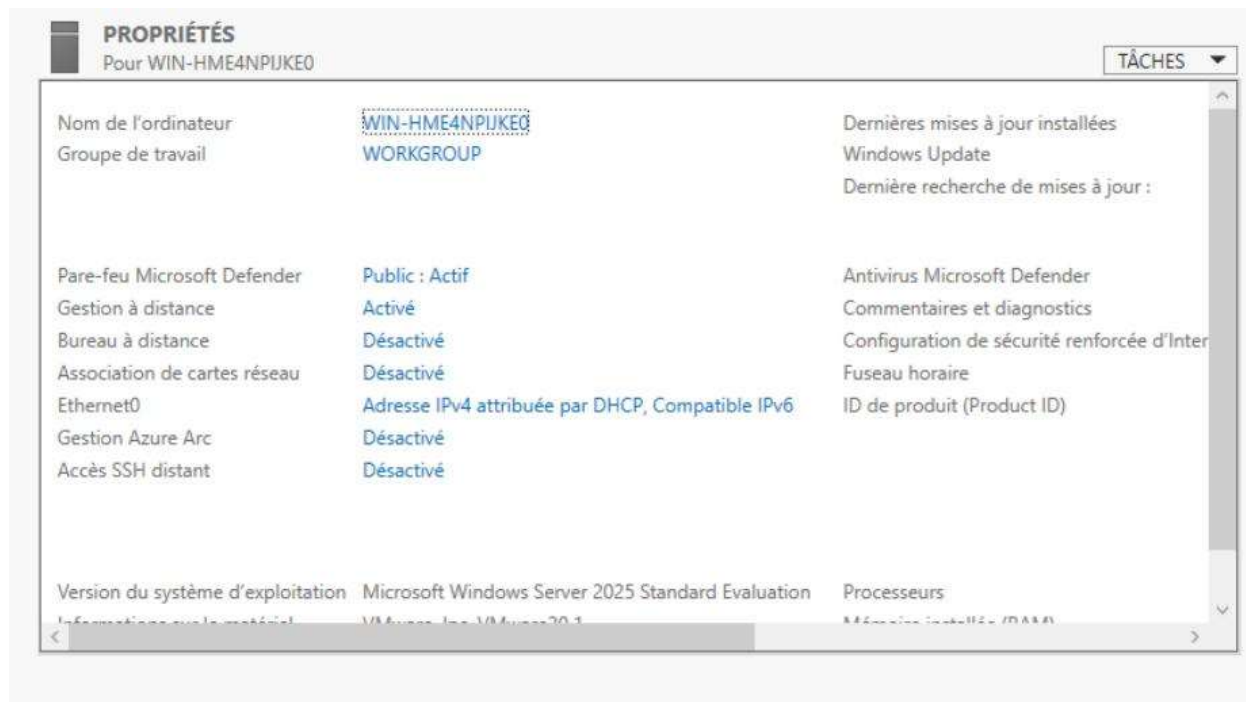
Machine	Adresse IP	Rôles
PARCUS-WDSSRV-01	192.168.137.1 /24	Contrôleur de domaine (AD DS), DNS, DHCP, WDS, GPO
PARCUS-WDSSRV-02	192.168.137.2 /24	DNS secondaire, DHCP en basculement, AD CS
VM-TEST2	DHCP (192.168.137.15)	Poste client Windows 11 Pro 25H2, joint au domaine
DESKTOP-204Q3GM / DESKTOP-RIV61FL	DHCP	Postes clients Windows 11 (clients RustDesk du LOT 1), joints au domaine, chiffrés BitLocker

Remarque sur le nom : le nom NetBIOS d'une machine Windows est limité à 15 caractères. « PARCUS-WDSSRV-01 » en fait 16, le premier serveur apparaît donc « PARCUS-WDSSRV-0 » dans certaines fenêtres (partages, console GPO). Son nom DNS complet reste bien parcus-wdssrv-01.parcus.fr.

Tout fonctionne en réseau local sur 192.168.137.0/24, sans passerelle : les serveurs n'ont pas besoin d'accès Internet pour rendre ces services.

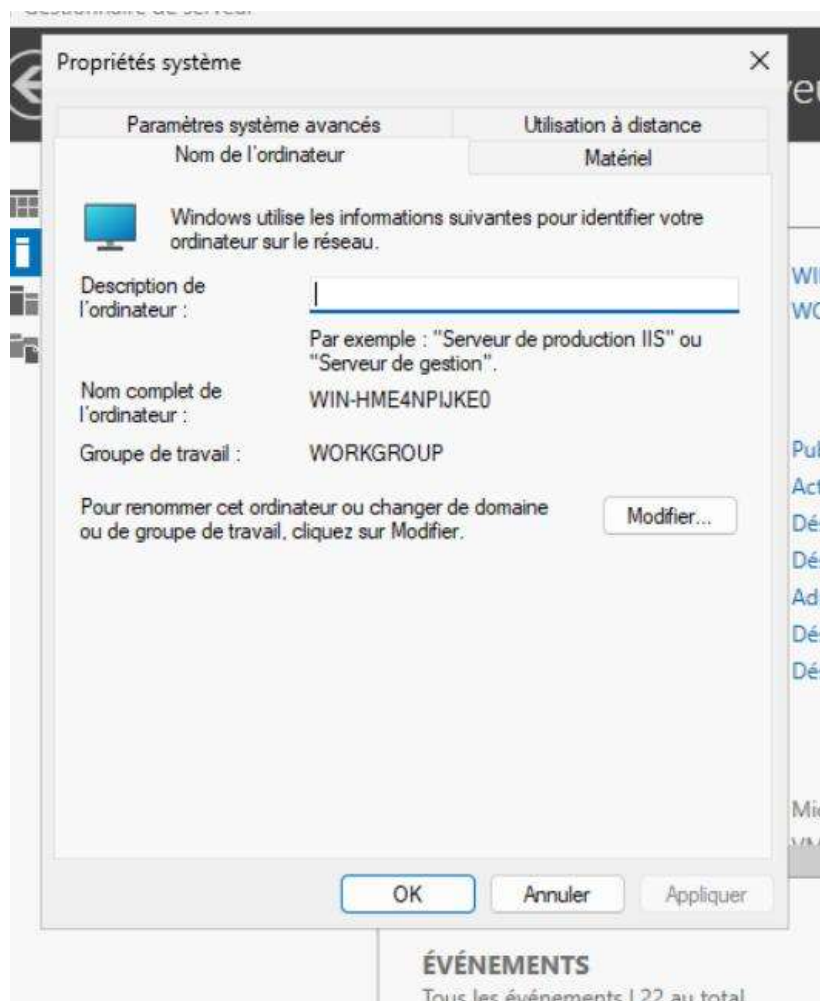
3.1.2. Configuration de base du serveur (nom et adresse IP)

À la fin de l'installation de Windows Server 2025, la machine porte un nom généré aléatoirement (ici WIN-HME4NPUKE0) et récupère son adresse en DHCP. Avant d'installer le moindre rôle, on fixe ces deux éléments : un contrôleur de domaine ne doit jamais changer de nom ni d'adresse.



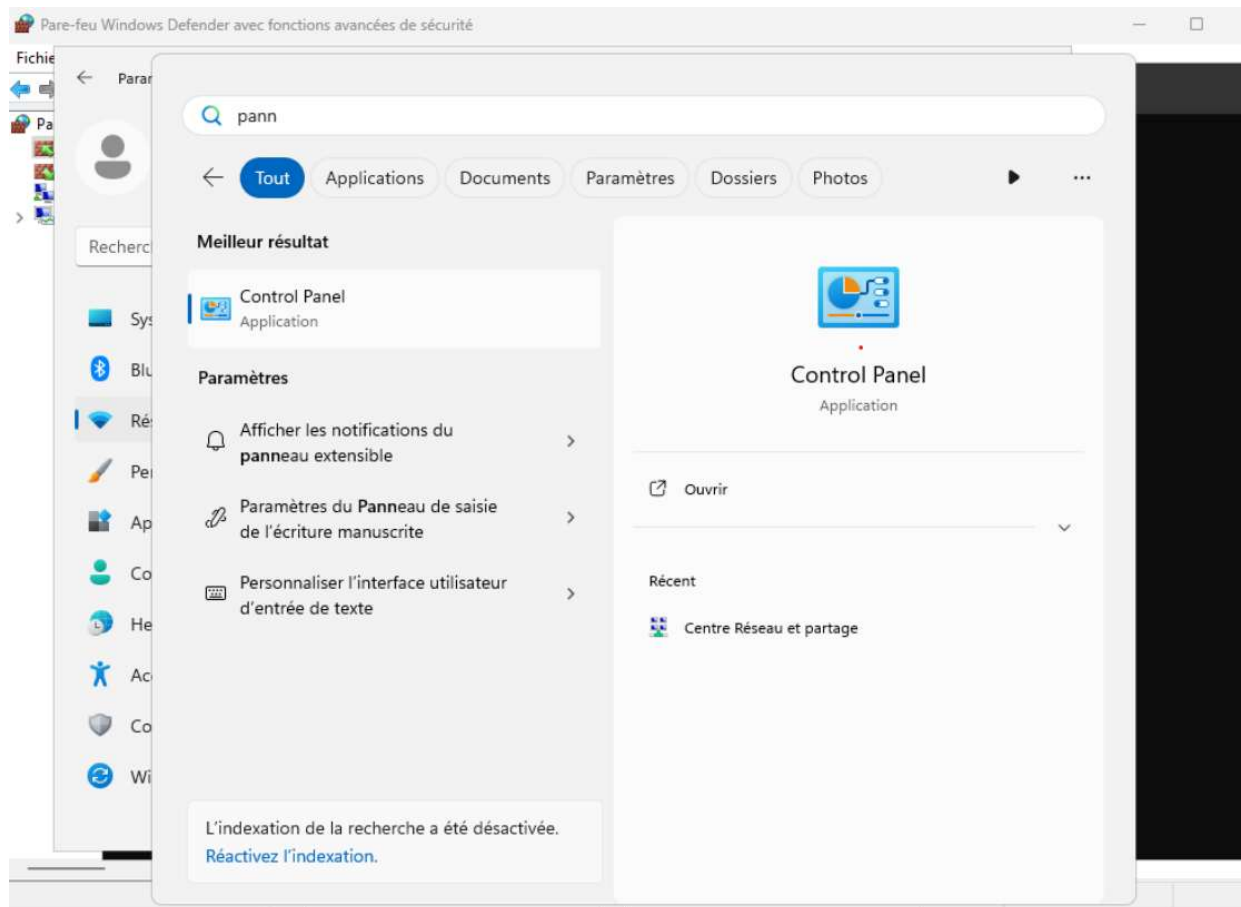
État initial du serveur dans le Gestionnaire de serveur : nom aléatoire, groupe de travail WORKGROUP, adresse en DHCP

Renommage. Dans le Gestionnaire de serveur, on clique sur le nom de l'ordinateur pour ouvrir les Propriétés système, puis sur Modifier... : on saisit le nouveau nom PARCUS-WDSSRV-01 et on redémarre pour appliquer.

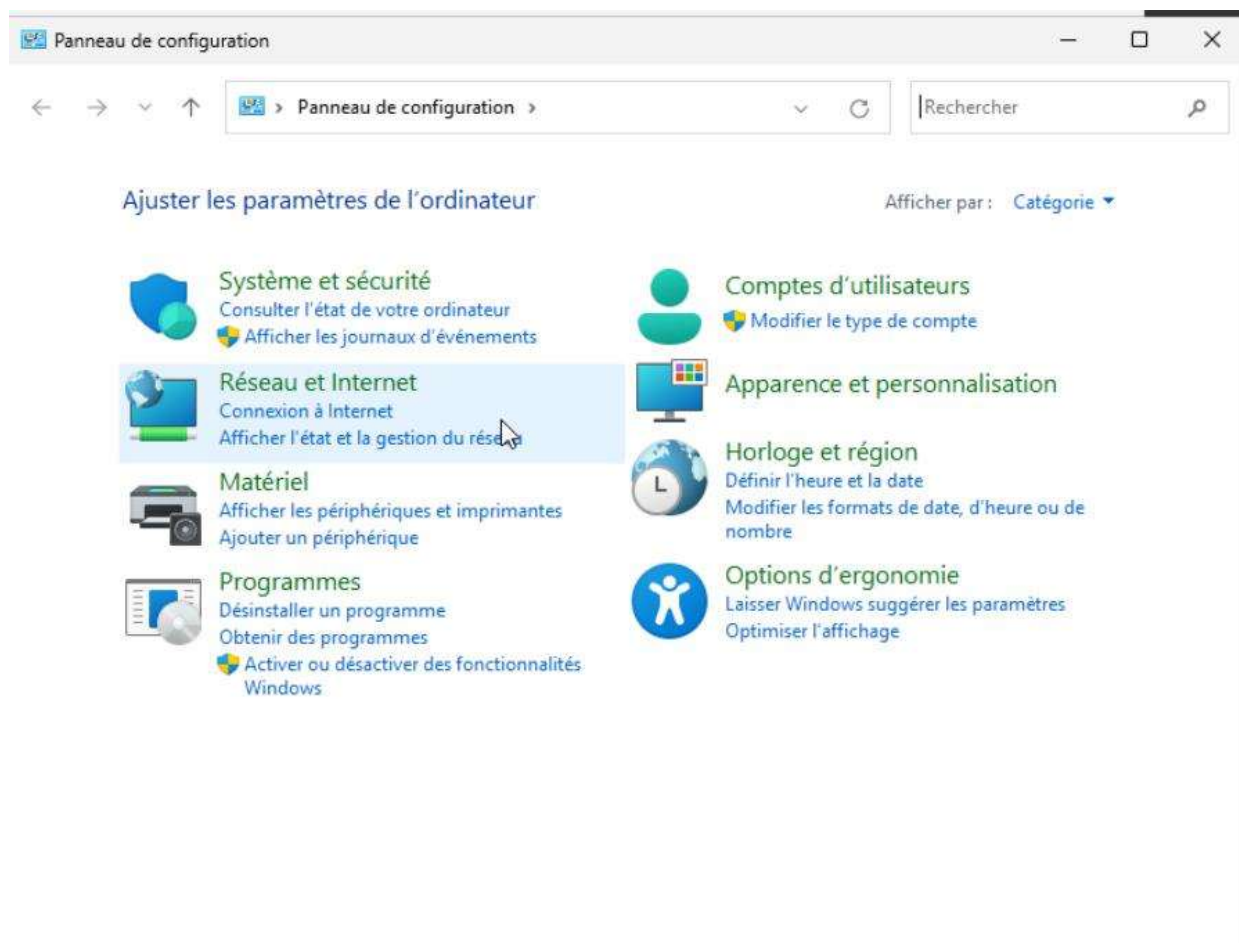


Propriétés système : le bouton Modifier... permet de renommer la machine avant de la promouvoir

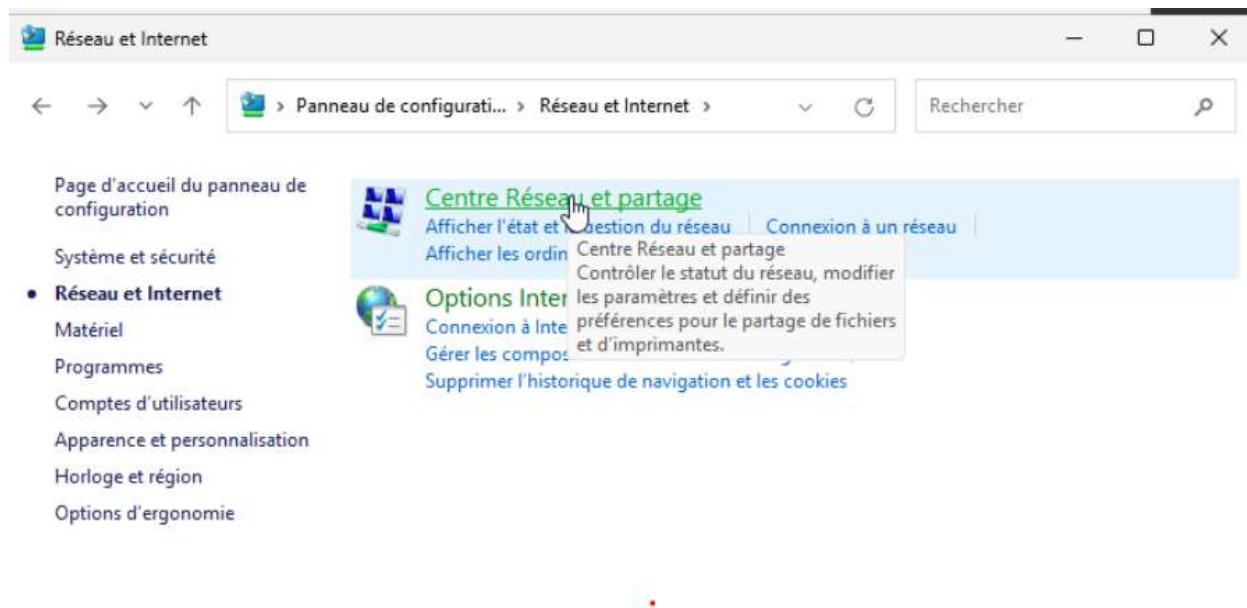
Adresse IP fixe. On passe par le Panneau de configuration (recherche Windows), rubrique Réseau et Internet, puis Centre Réseau et partage.



Recherche du Panneau de configuration depuis le menu Démarrer

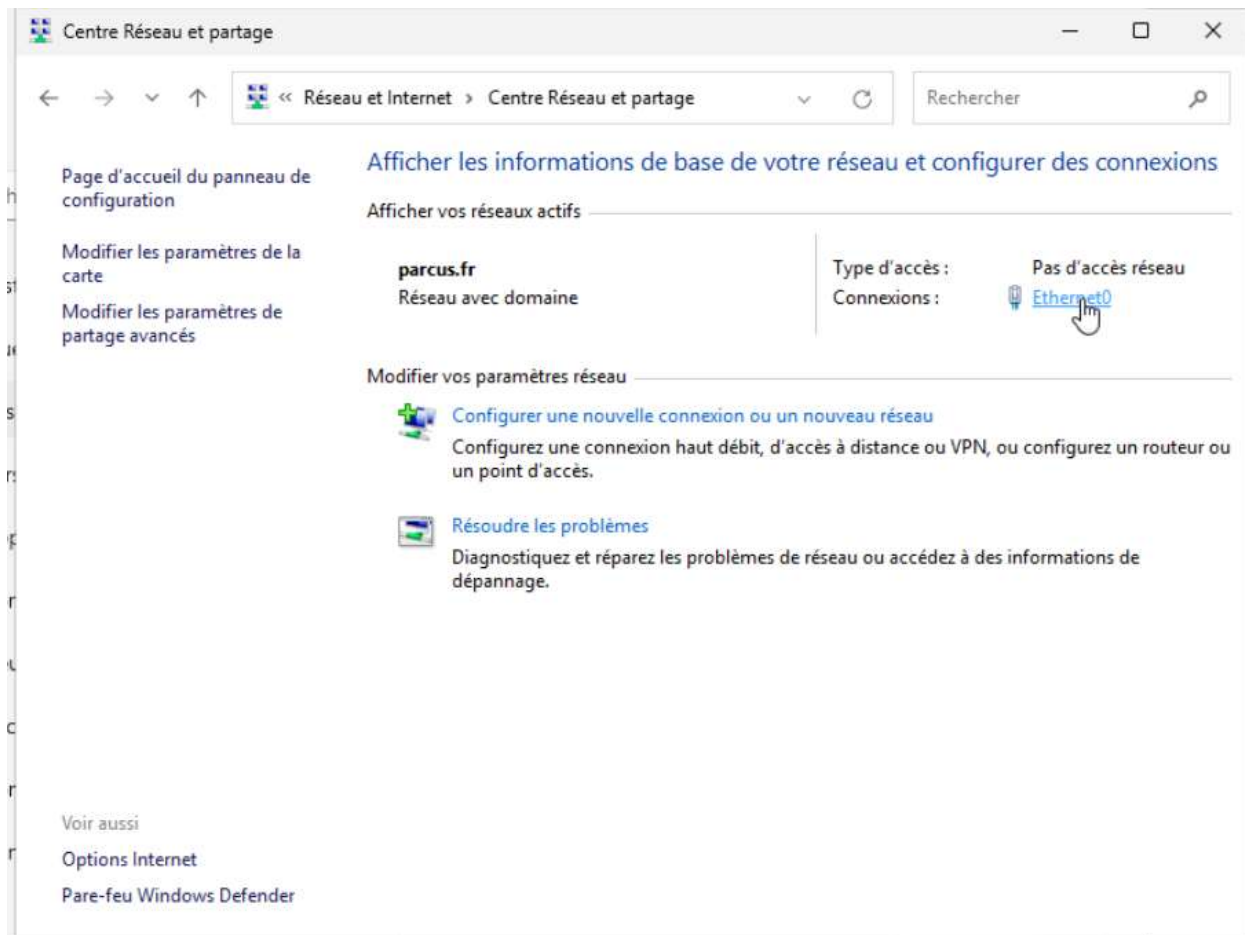


Panneau de configuration : on ouvre la rubrique Réseau et Internet

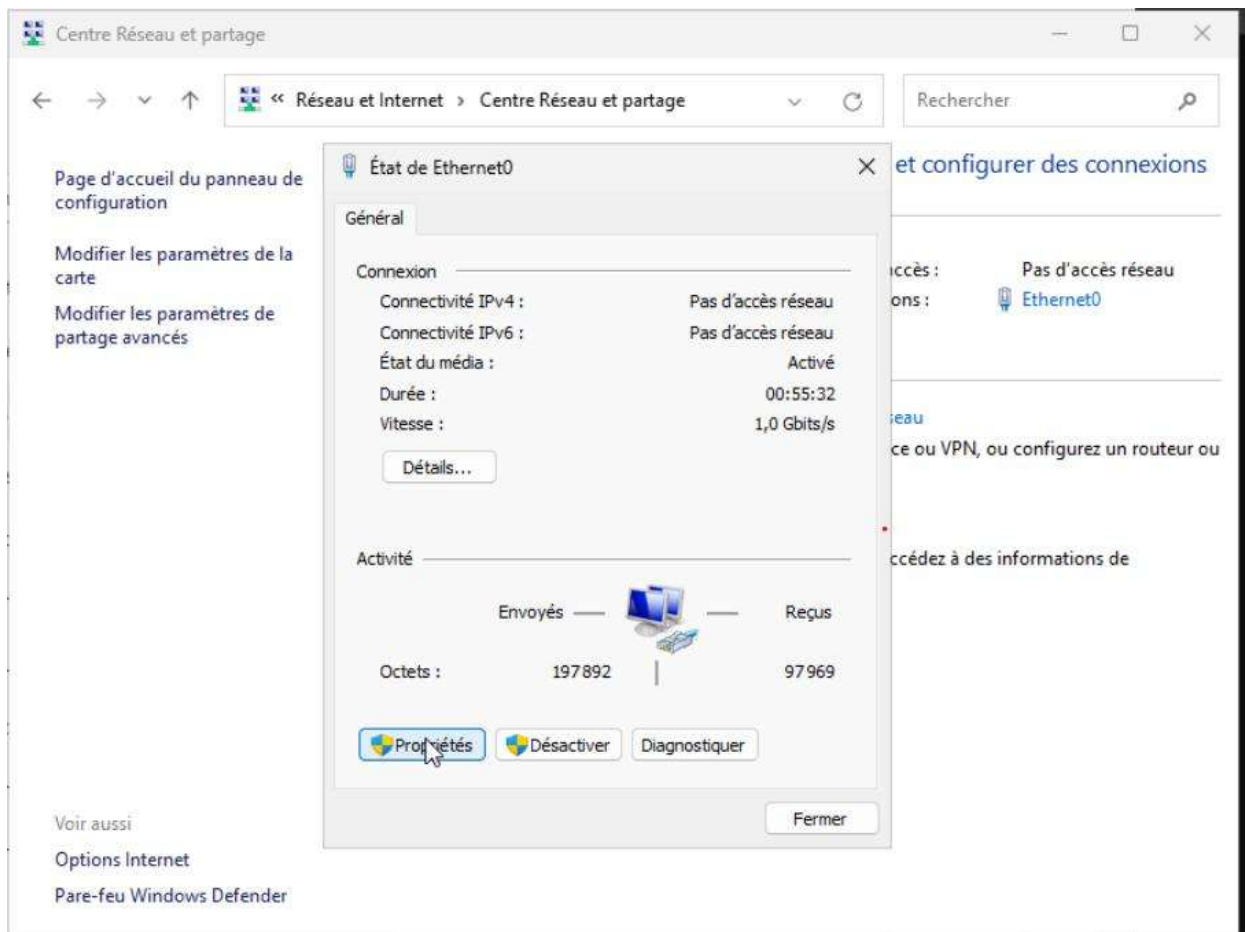


Réseau et Internet : accès au Centre Réseau et partage

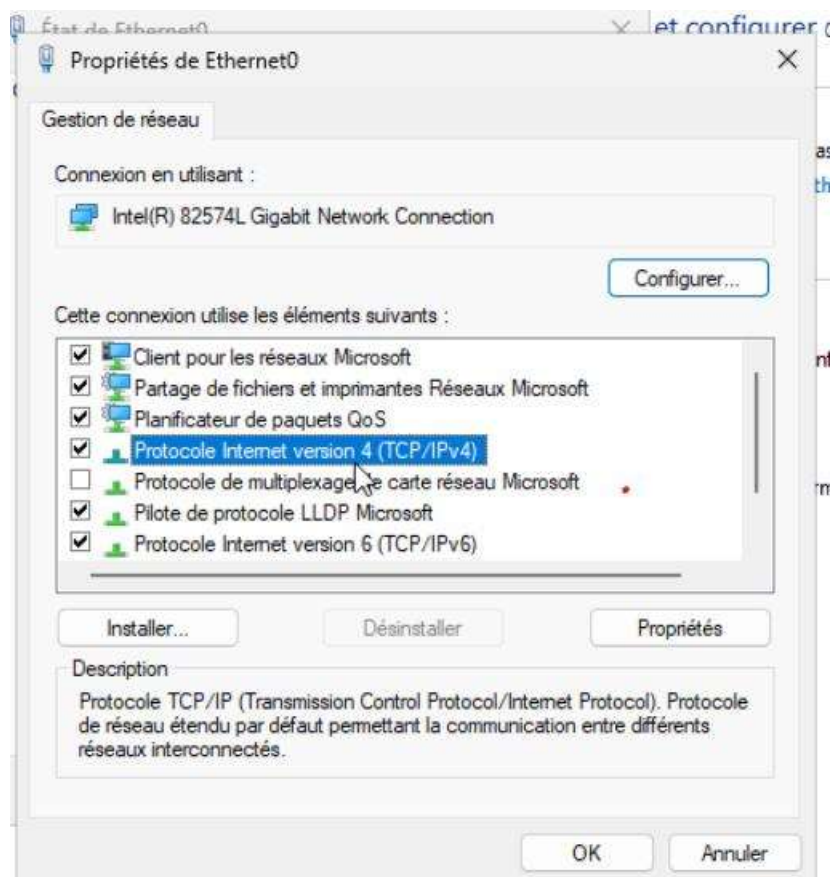
Dans le Centre Réseau et partage, on clique sur la connexion Ethernet0, puis sur Propriétés, et on ouvre le Protocole Internet version 4 (TCP/IPv4).



Centre Réseau et partage : la carte Ethernet0 du serveur

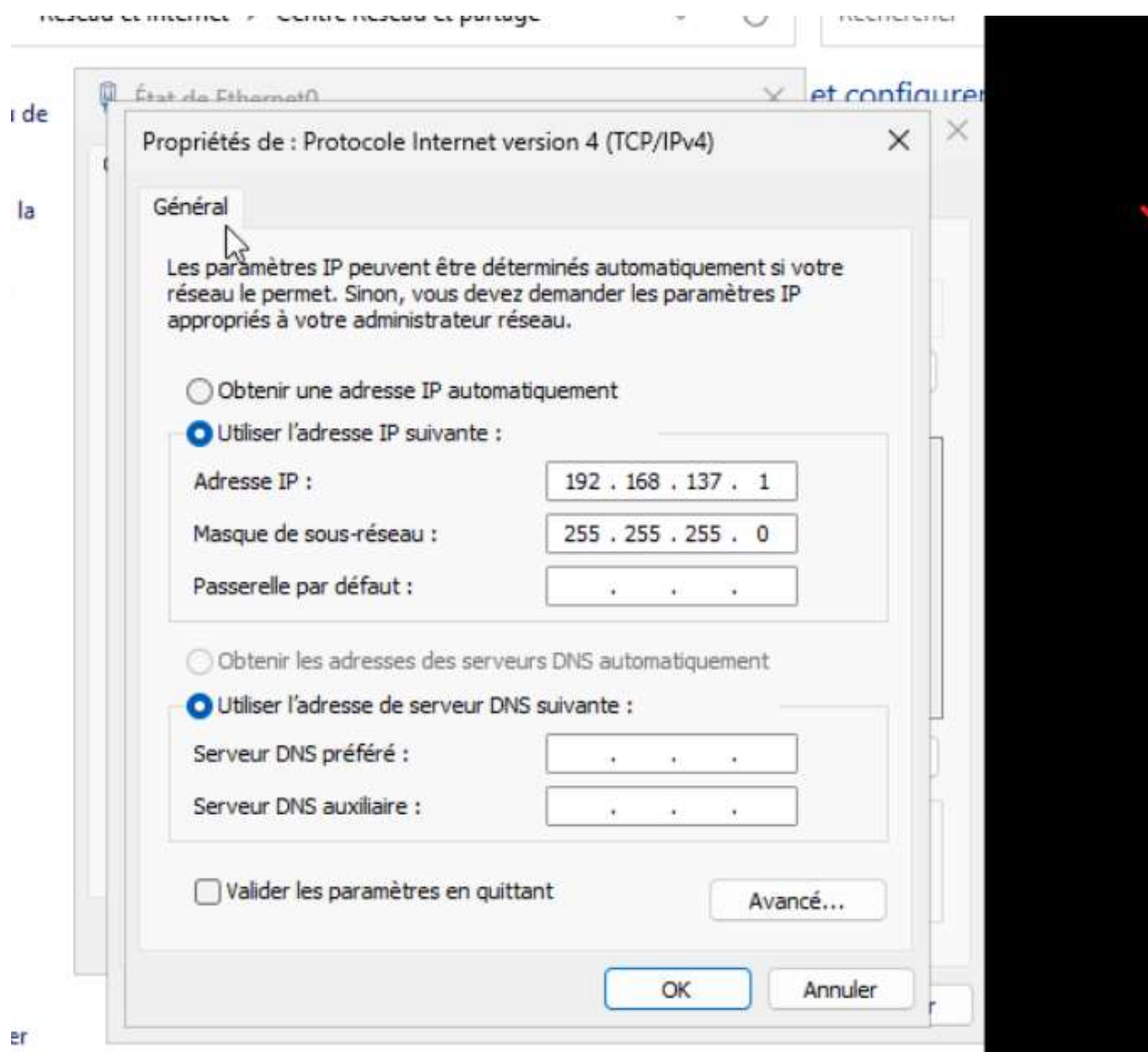


État de Ethernet0 : le bouton Propriétés donne accès à la configuration de la carte



Propriétés de Ethernet0 : on sélectionne Protocole Internet version 4 (TCP/IPv4)

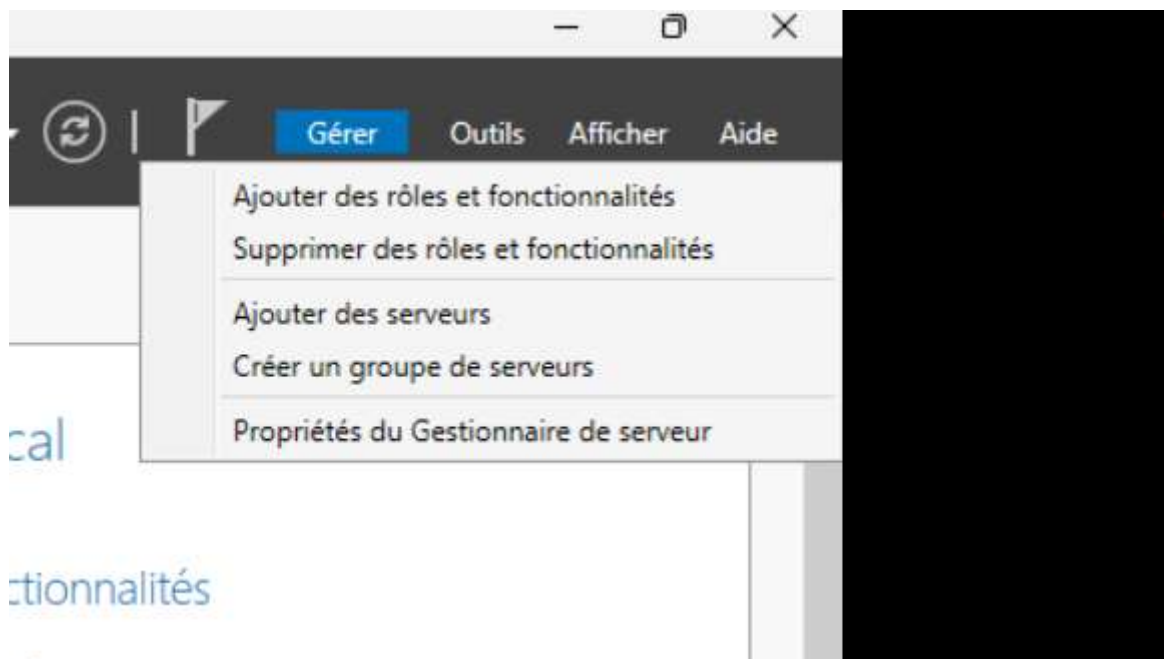
On attribue au serveur l'adresse 192.168.137.1 avec le masque 255.255.255.0. Pas de passerelle : le réseau est purement local. Le DNS sera ajusté automatiquement lors de la promotion en contrôleur de domaine.



Adresse statique du premier serveur : 192.168.137.1 /24, sans passerelle

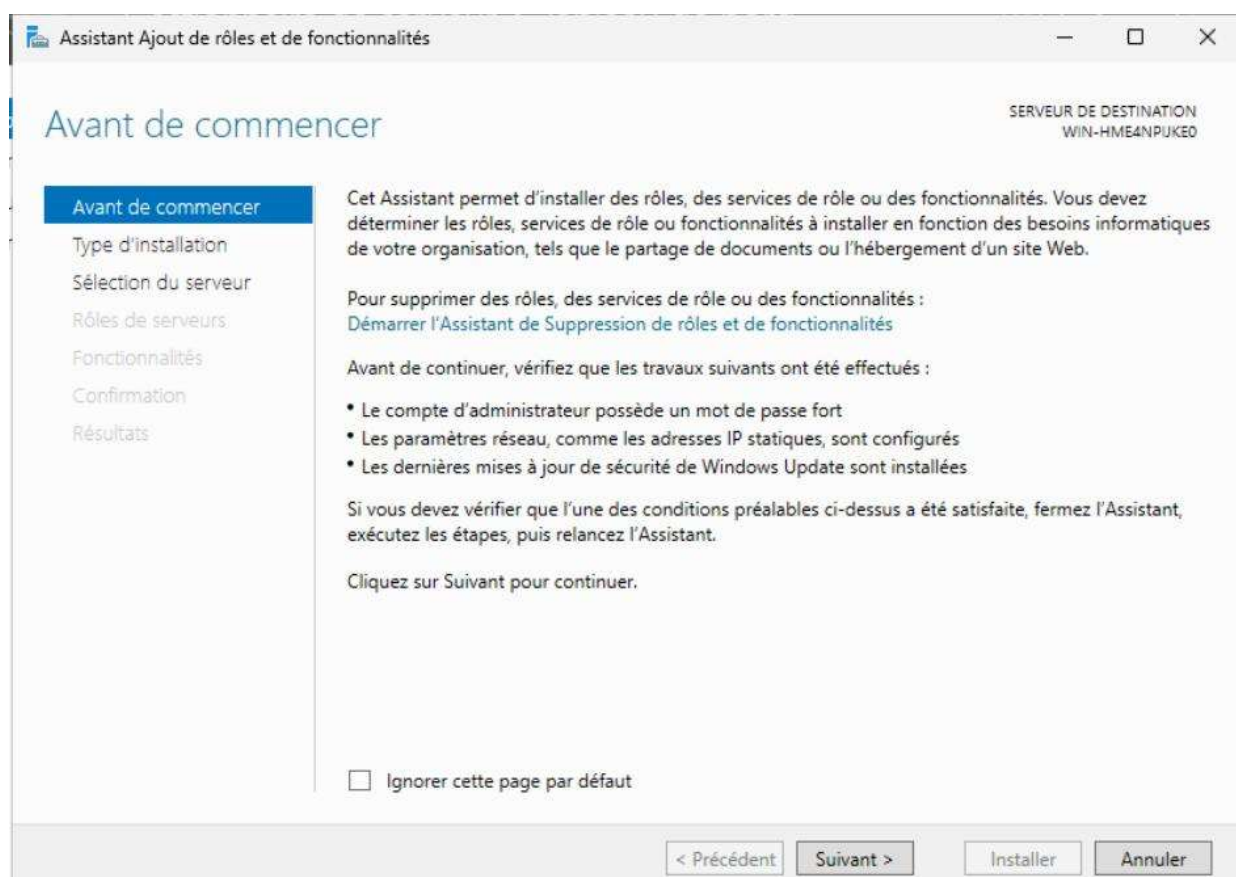
3.1.3. Installation du rôle AD DS

L'installation des rôles se fait depuis le Gestionnaire de serveur, menu Gérer, entrée Ajouter des rôles et fonctionnalités.



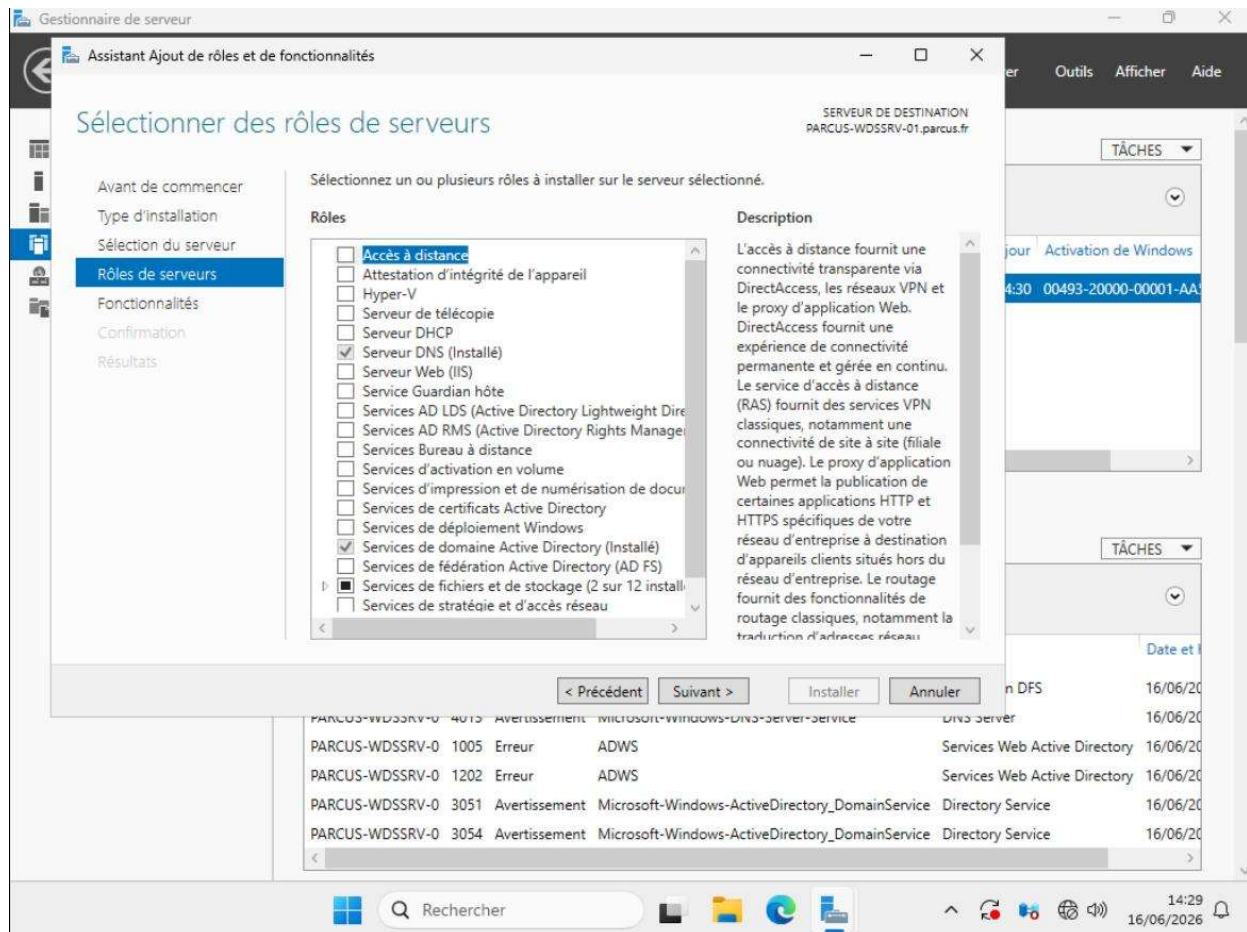
Menu Gérer du Gestionnaire de serveur : Ajouter des rôles et fonctionnalités

L'assistant rappelle les prérequis avant de commencer : mot de passe administrateur fort, adresse IP statique configurée, mises à jour installées. C'est justement ce qu'on vient de faire à l'étape précédente.



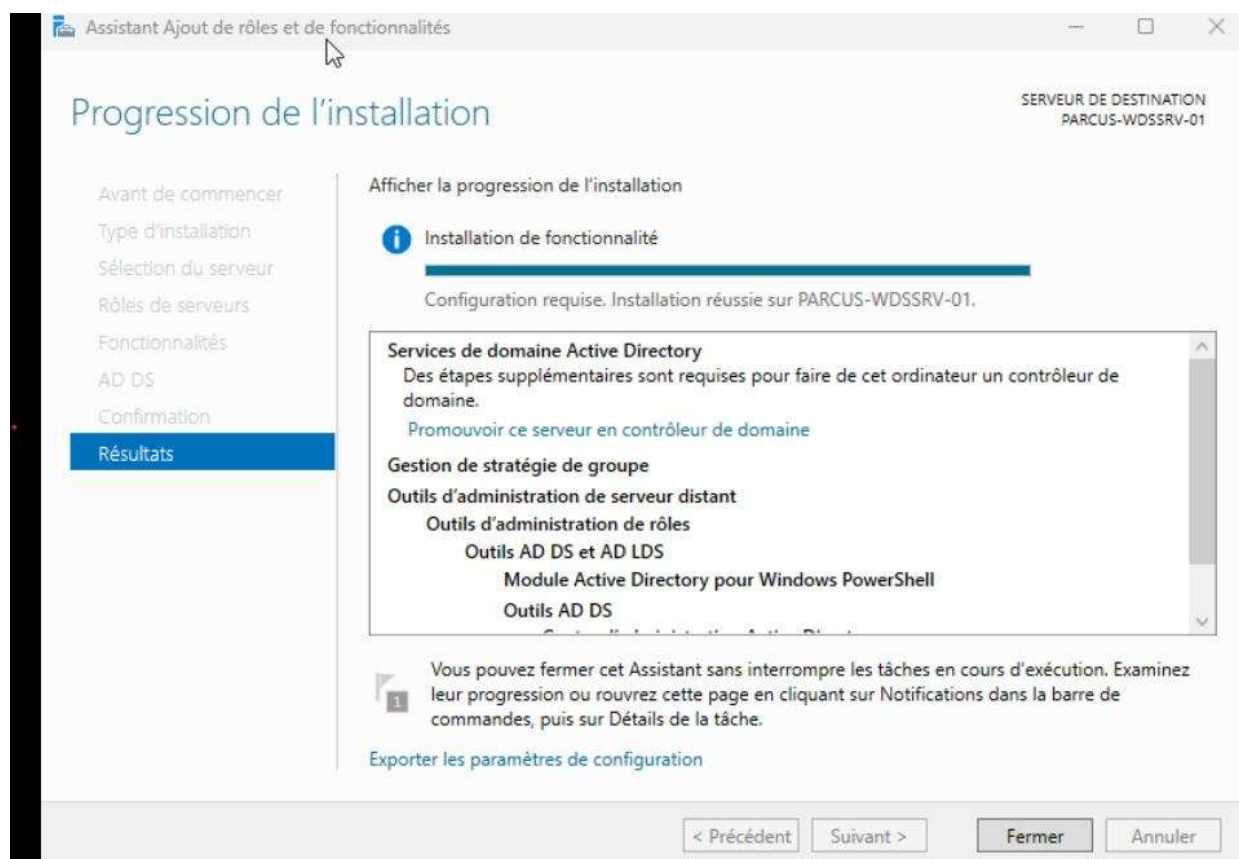
Page « Avant de commencer » de l'assistant Ajout de rôles et de fonctionnalités

On choisit une installation basée sur un rôle, on sélectionne le serveur local, puis on coche Services de domaine Active Directory dans la liste des rôles. Le rôle Serveur DNS est installé dans la foulée : un contrôleur de domaine a besoin d'un DNS qui connaît le domaine.



Sélection des rôles : Services de domaine Active Directory et Serveur DNS

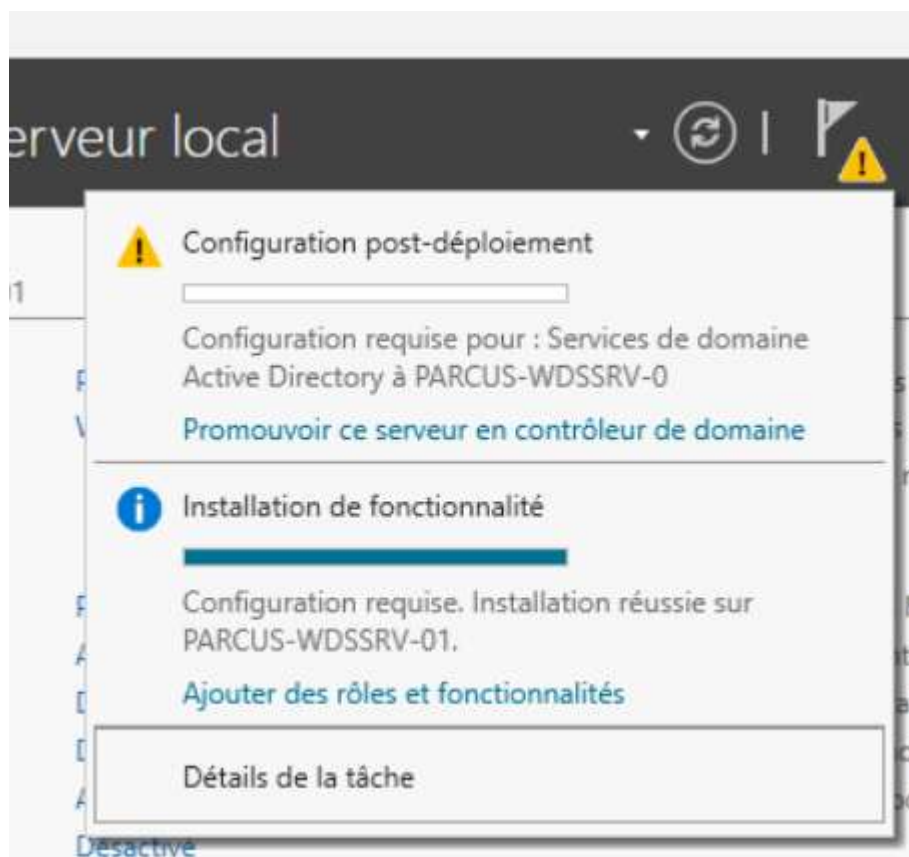
Une fois l'installation terminée, l'assistant signale que des étapes supplémentaires sont nécessaires et propose directement le lien « Promouvoir ce serveur en contrôleur de domaine ».



Fin de l'installation du rôle AD DS : le lien de promotion apparaît dans les résultats

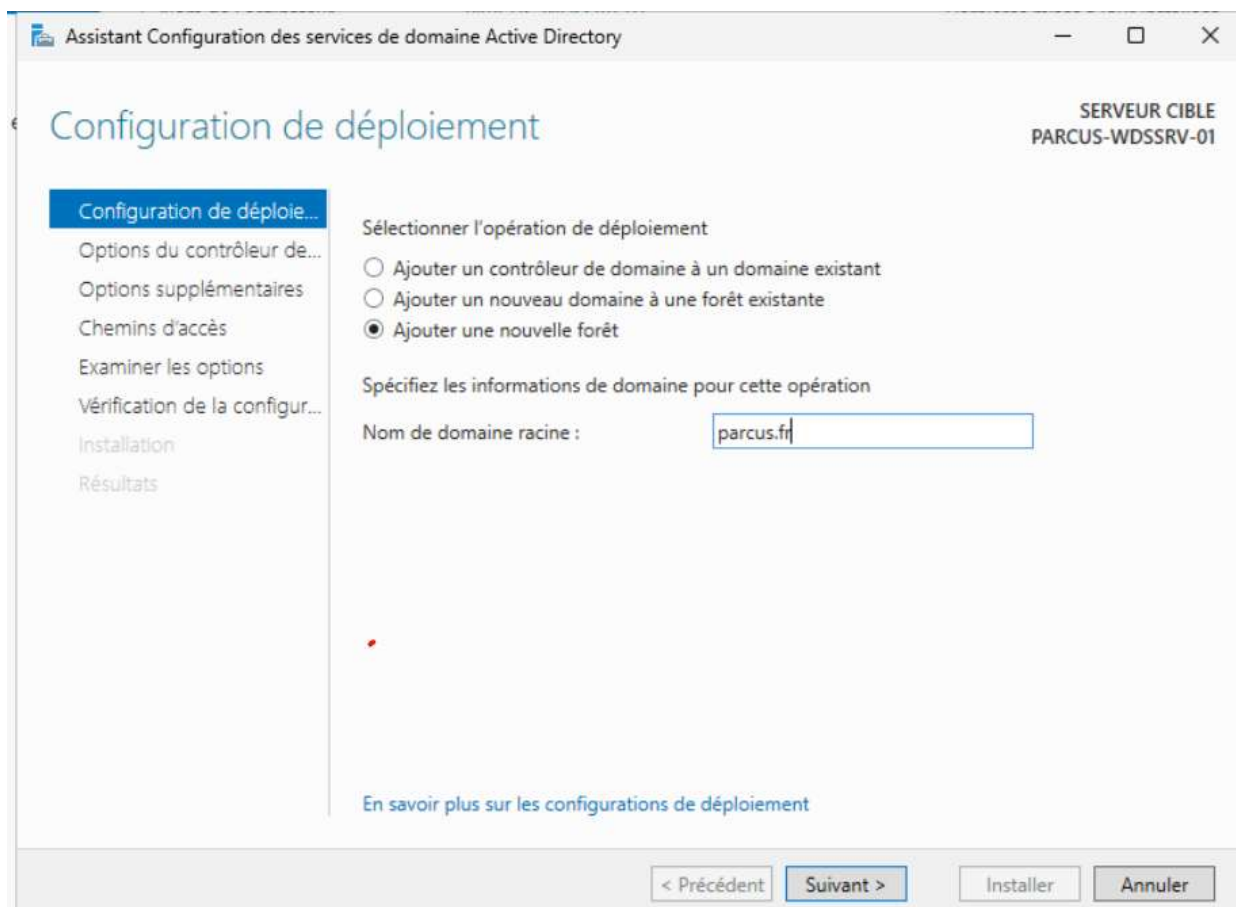
3.1.4. Promotion en contrôleur de domaine (parcus.fr)

La notification de configuration post-déploiement (drapeau jaune en haut du Gestionnaire de serveur) reste disponible tant que la promotion n'a pas été faite.



Notification post-déploiement : promotion du serveur en contrôleur de domaine

Comme il s'agit du tout premier contrôleur, on choisit Ajouter une nouvelle forêt et on saisit le nom de domaine racine : parcus.fr.



Configuration de déploiement : création de la forêt parcus.fr

Sur la page suivante, on garde le niveau fonctionnel Windows Server 2025 pour la forêt et le domaine, on laisse cochés Serveur DNS et Catalogue global, et on définit le mot de passe du mode de restauration des services d'annuaire (DSRM). Ce mot de passe sert uniquement en cas de réparation de l'annuaire : on le conserve précieusement à part.

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE
PARCUS-WDSSRV-01

Options du contrôleur de domaine

Configuration de déploiement...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration...
Installation
Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2025

Niveau fonctionnel du domaine : Windows Server 2025

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Dgmain Name System)
☒ Catalogue global (GC)
☐ Contrôleur de domaine en lecture seule (RODC)

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

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

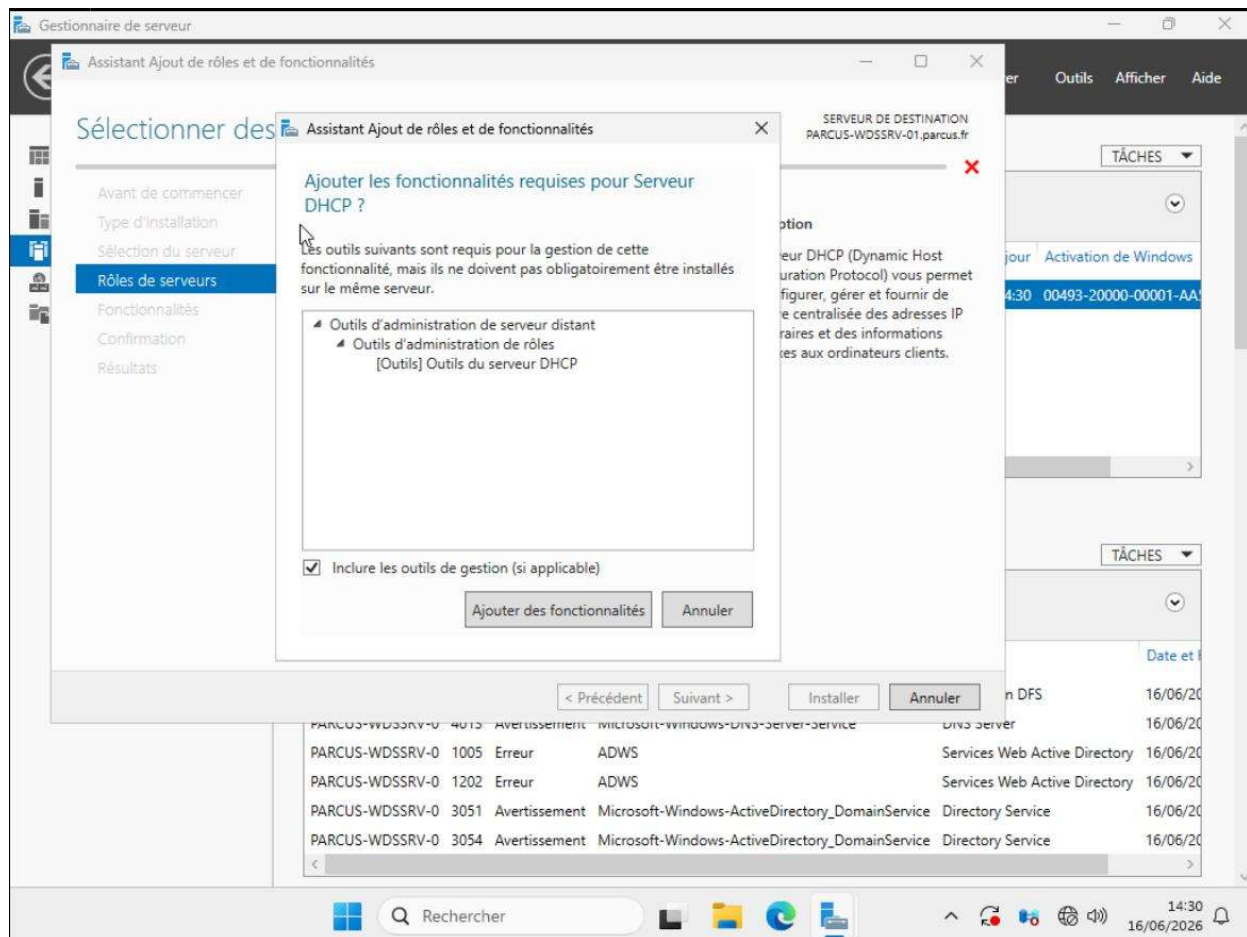
< Précédent Suivant > Installer Annuler

Options du contrôleur de domaine : niveaux fonctionnels, DNS, catalogue global et mot de passe DSRM

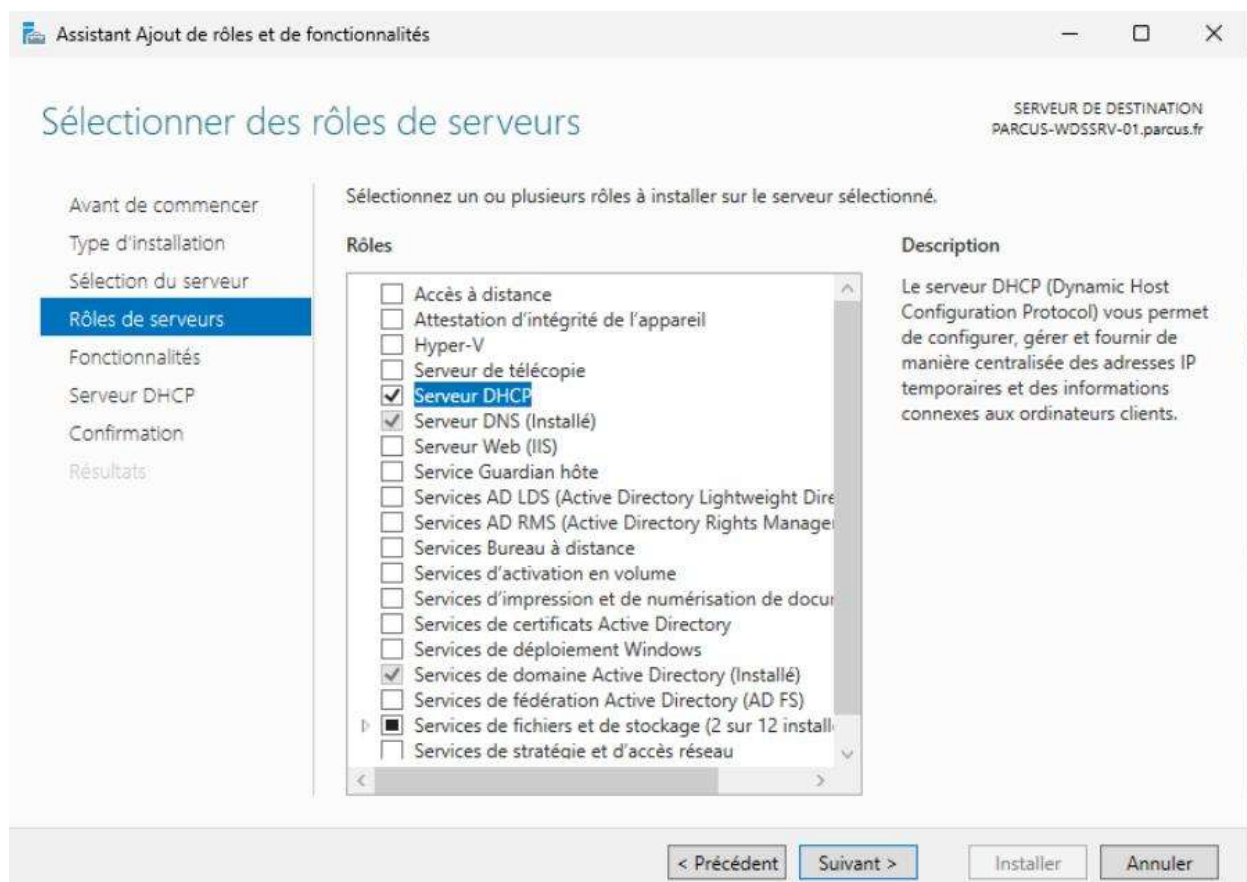
L'assistant vérifie ensuite la configuration puis installe l'annuaire ; le serveur redémarre tout seul. À la reconnexion, on ouvre la session avec le compte PARCUS\Administrateur : le domaine existe.

3.1.5. Installation et autorisation du rôle DHCP

On relance l'assistant d'ajout de rôles et on coche cette fois Serveur DHCP. L'assistant propose d'ajouter les outils d'administration qui vont avec : on accepte.

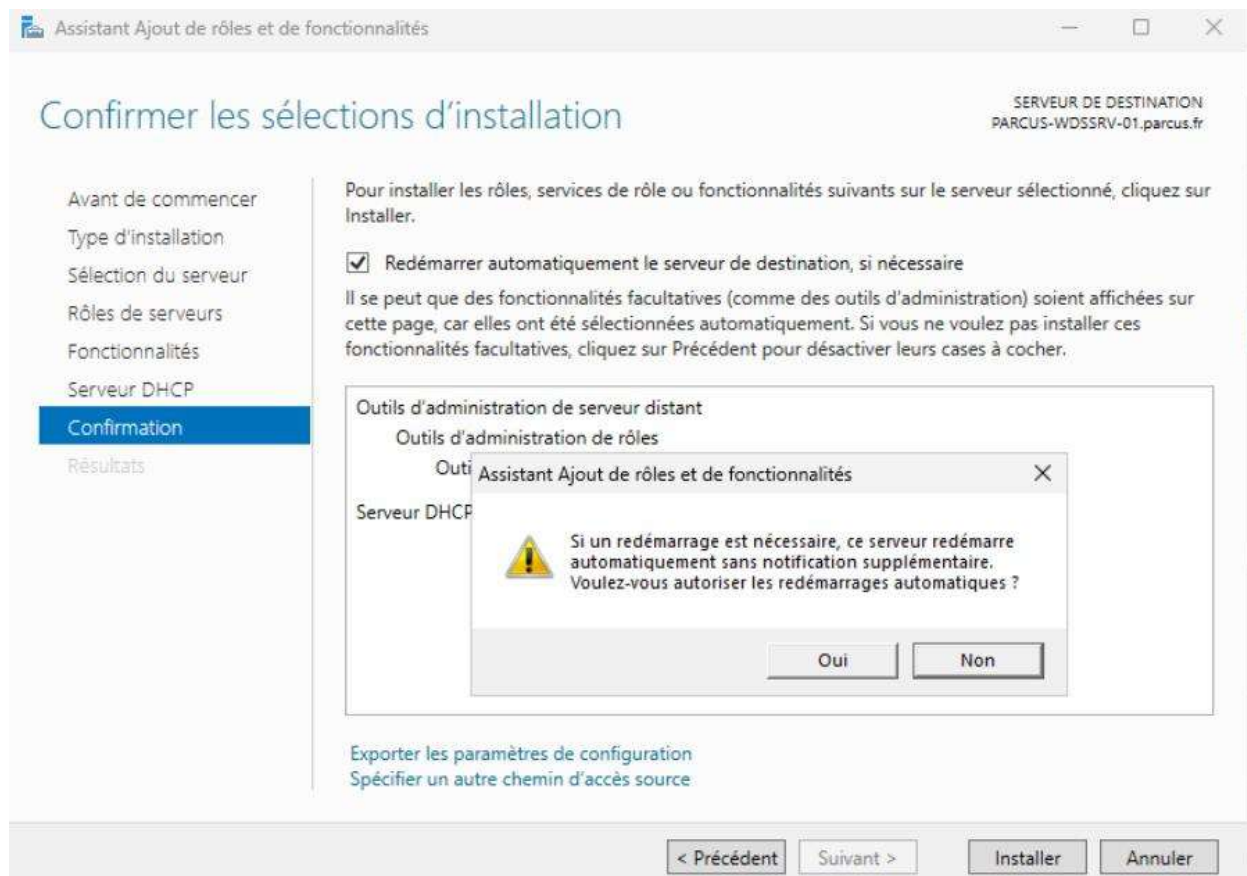


Fonctionnalités requises pour le rôle Serveur DHCP : on ajoute les outils de gestion

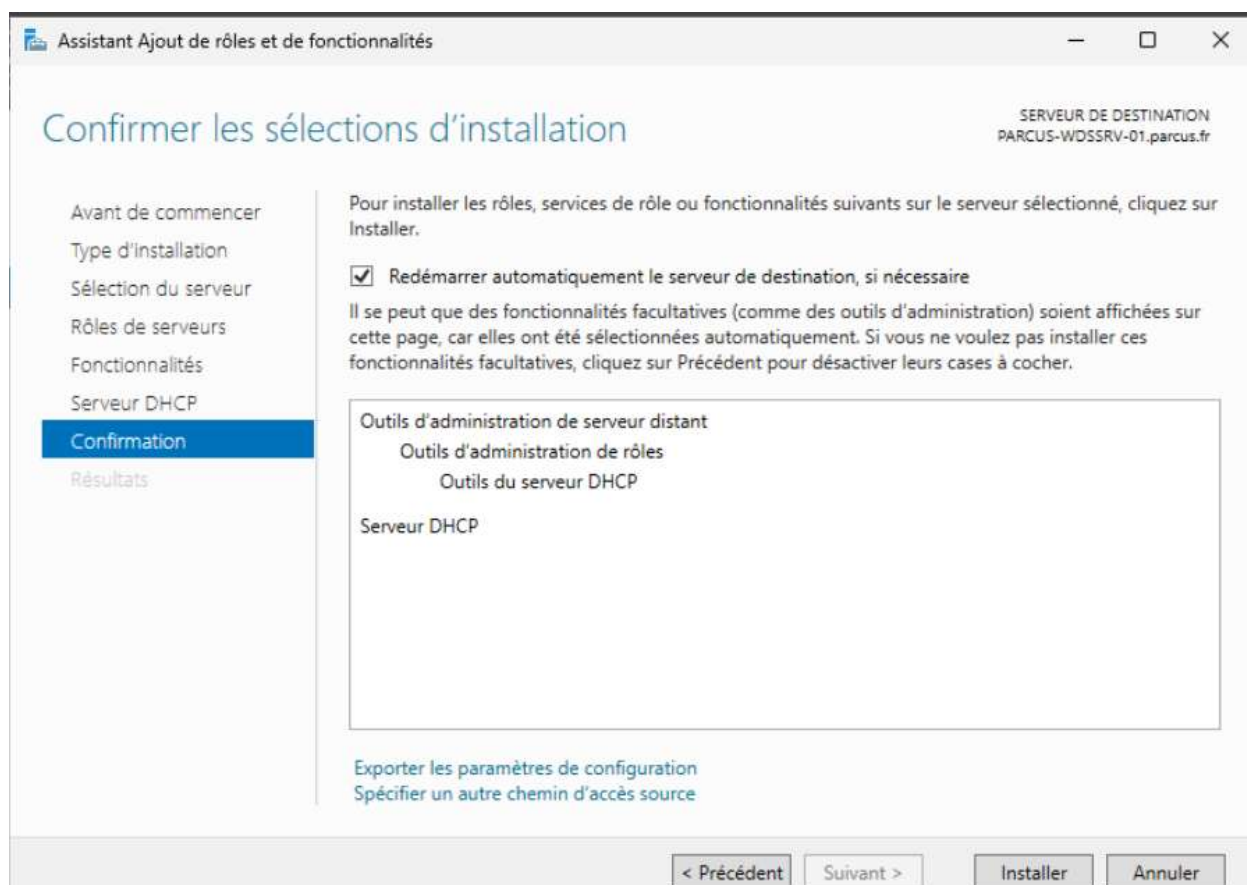


Sélection du rôle Serveur DHCP (AD DS et DNS apparaissent déjà installés)

Sur l'écran de confirmation, on coche « Redémarrer automatiquement le serveur de destination, si nécessaire » ; Windows demande de valider ce choix.

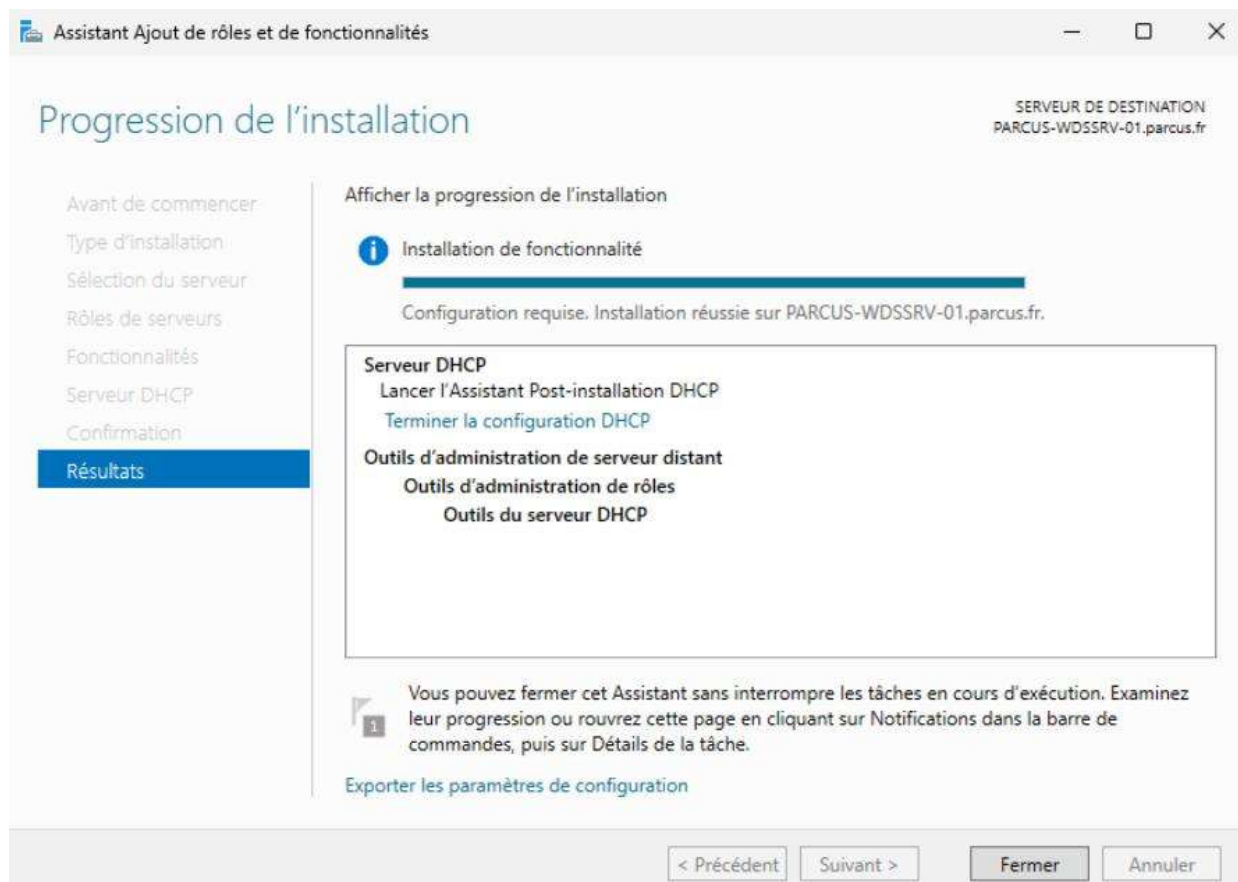


Confirmation de l'installation : autorisation des redémarrages automatiques

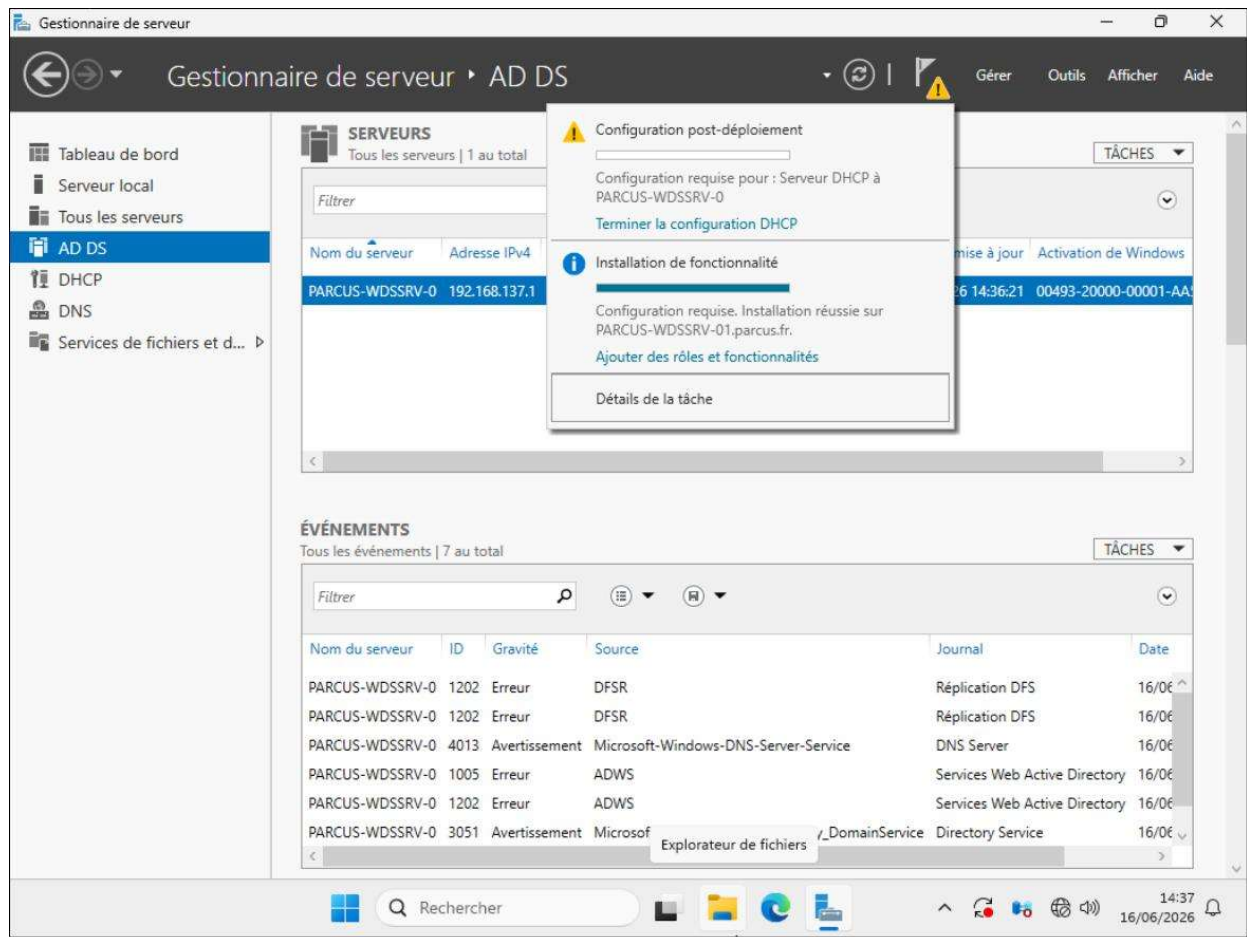


Récapitulatif de l'installation du serveur DHCP et de ses outils

À la fin de l'installation, un lien « Terminer la configuration DHCP » apparaît : il lance un petit assistant de post-installation.



Fin d'installation du rôle DHCP : lancement de l'assistant post-installation



La notification « Terminer la configuration DHCP » reste visible dans le Gestionnaire de serveur

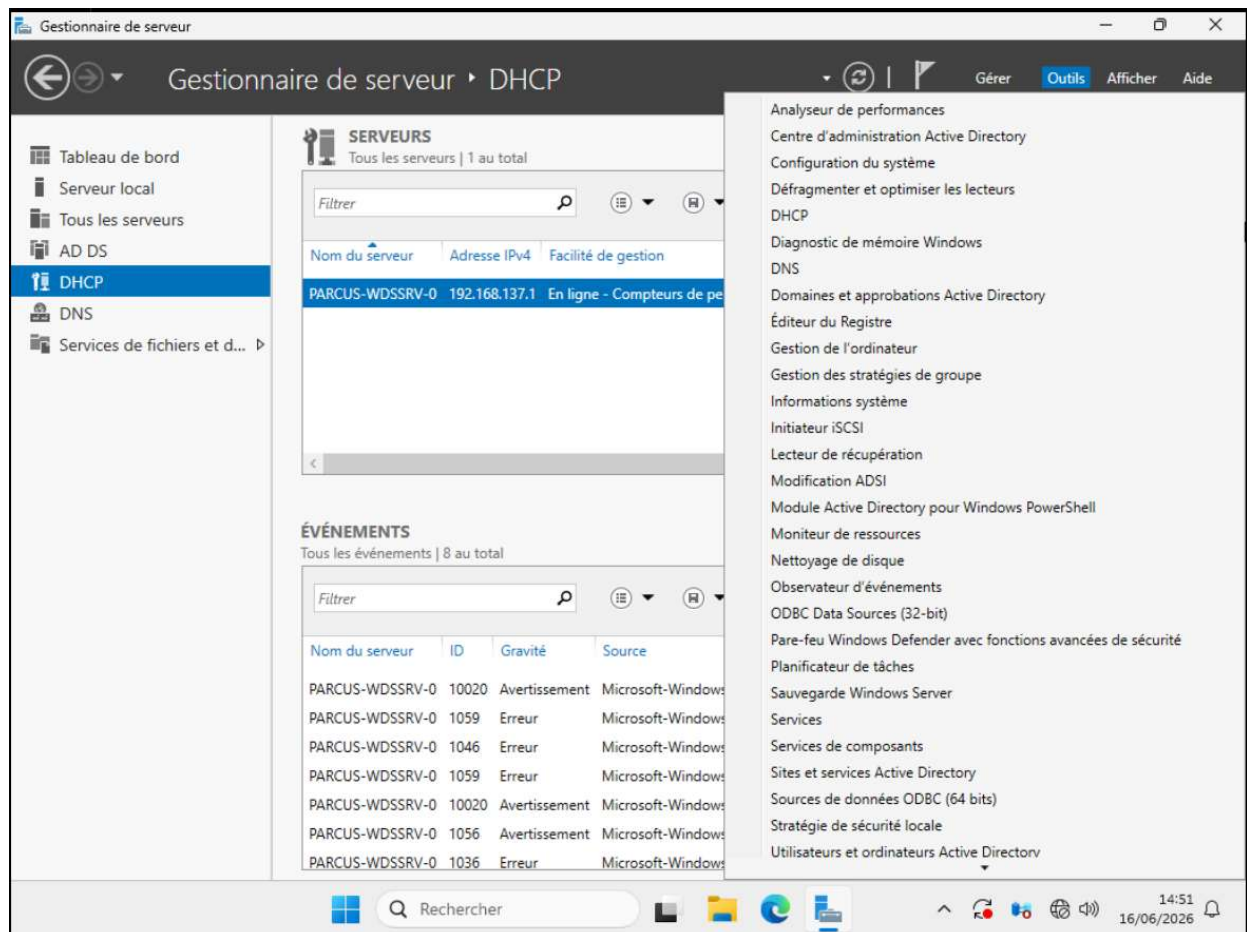
Dans un domaine Active Directory, un serveur DHCP doit être autorisé dans l'annuaire pour pouvoir distribuer des adresses : c'est une protection contre les serveurs DHCP pirates. On utilise les informations d'identification PARCUSAdministrateur puis on valide.

The screenshot shows a Windows-style window titled 'Assistant Configuration post-installation DHCP'. On the left is a sidebar with three items: 'Description', 'Autorisation' (highlighted in blue), and 'Résumé'. The main area is titled 'Autorisation' and contains the following text: 'Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.' Below this are three radio button options: 1. 'Utiliser les informations d'identification de l'utilisateur suivant' (selected), with a text box 'Nom d'utilisateur : PARCUS\Administrateur'. 2. 'Utiliser d'autres informations d'identification', with a text box 'Nom d'utilisateur : ' and a 'Spécifier...' button. 3. 'Ignorer l'autorisation AD'. At the bottom right are four buttons: '< Précédent', 'Suivant >', 'Valider', and 'Annuler'.

Autorisation du serveur DHCP dans l'AD avec le compte PARCUS\Administrateur

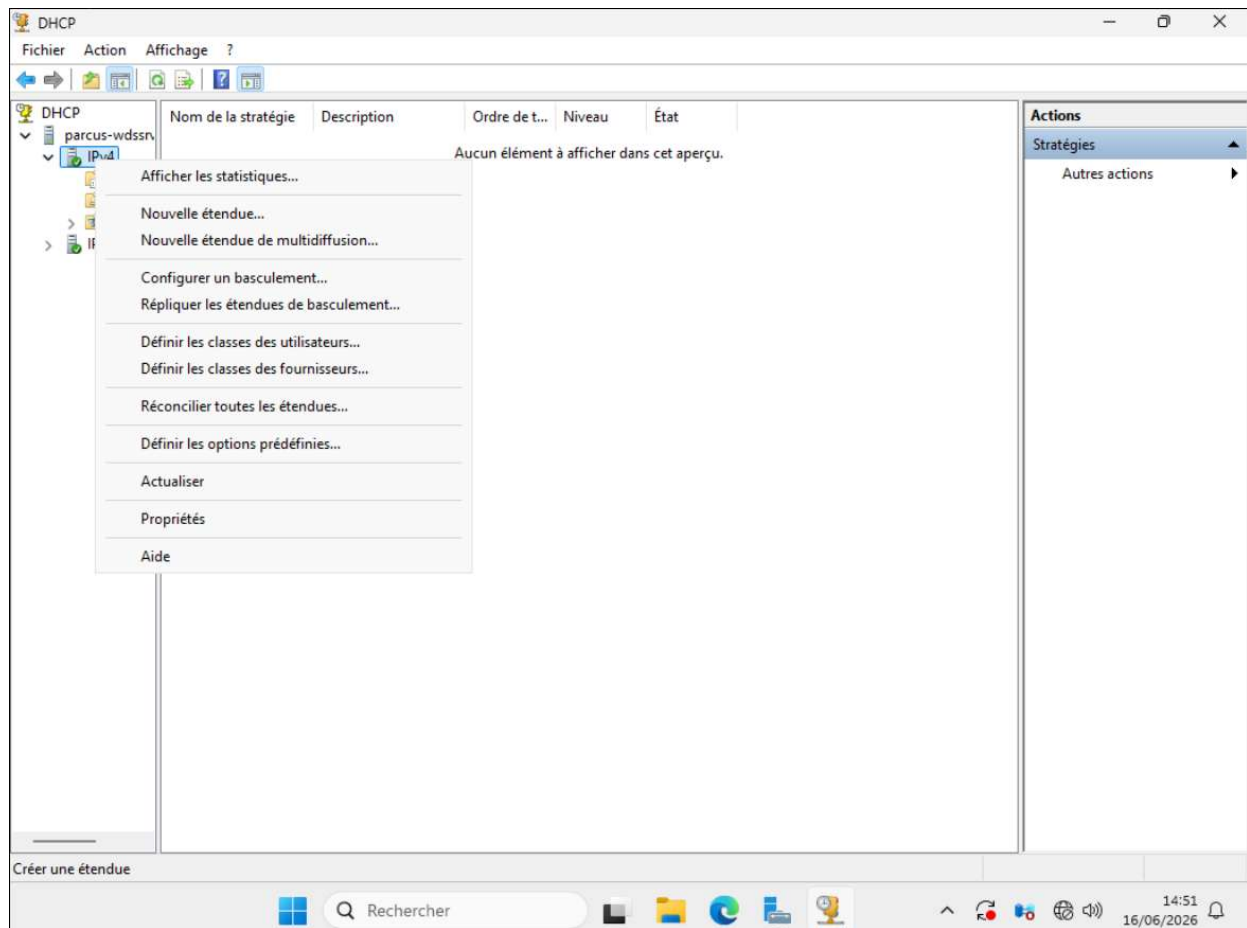
3.1.6. Création de l'étendue DHCP « UtilisateursParcus »

La console DHCP s'ouvre depuis le menu Outils du Gestionnaire de serveur.

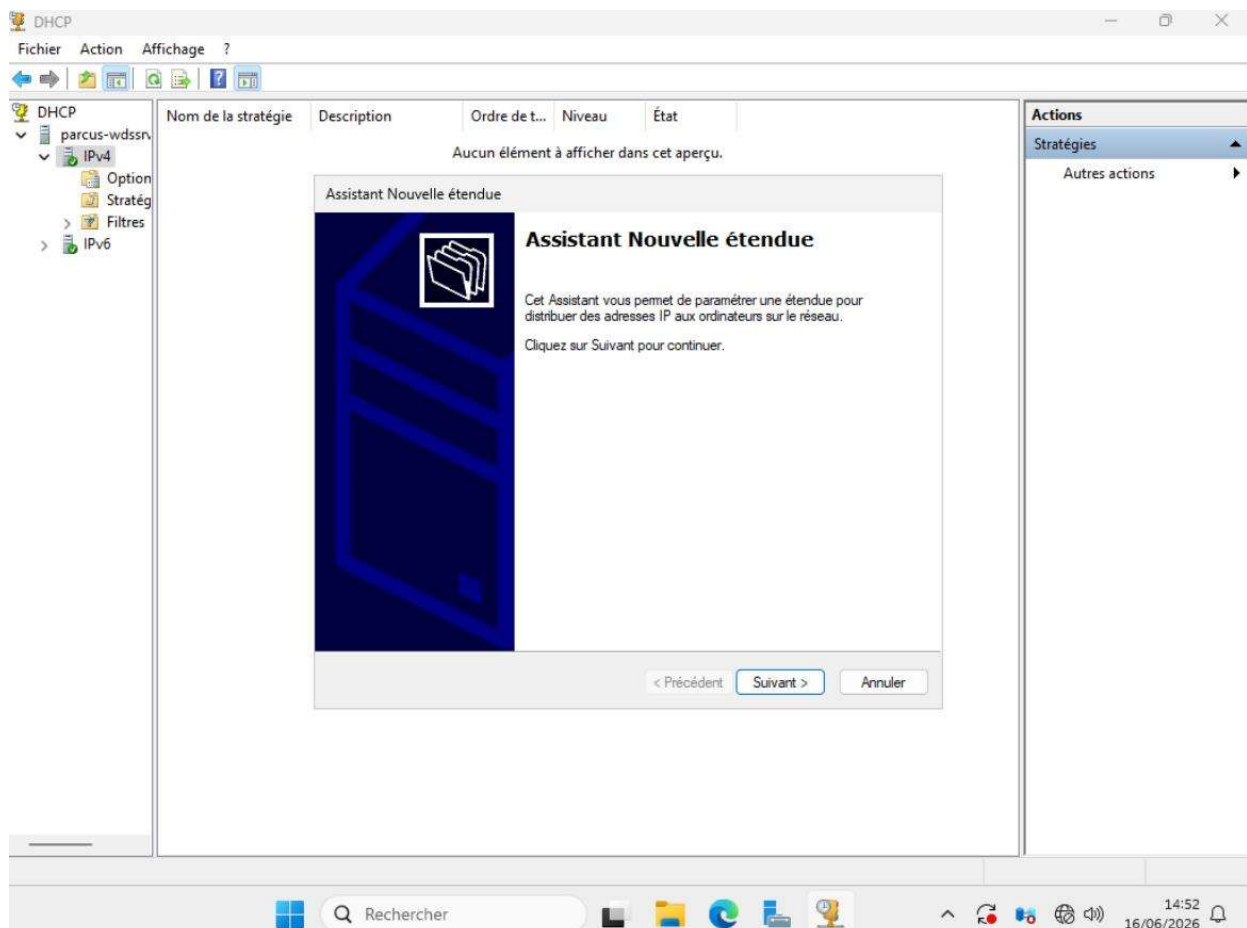


Menu Outils : ouverture de la console DHCP

Un clic droit sur IPv4 permet de créer une Nouvelle étendue..., c'est-à-dire la plage d'adresses que le serveur va distribuer aux postes.

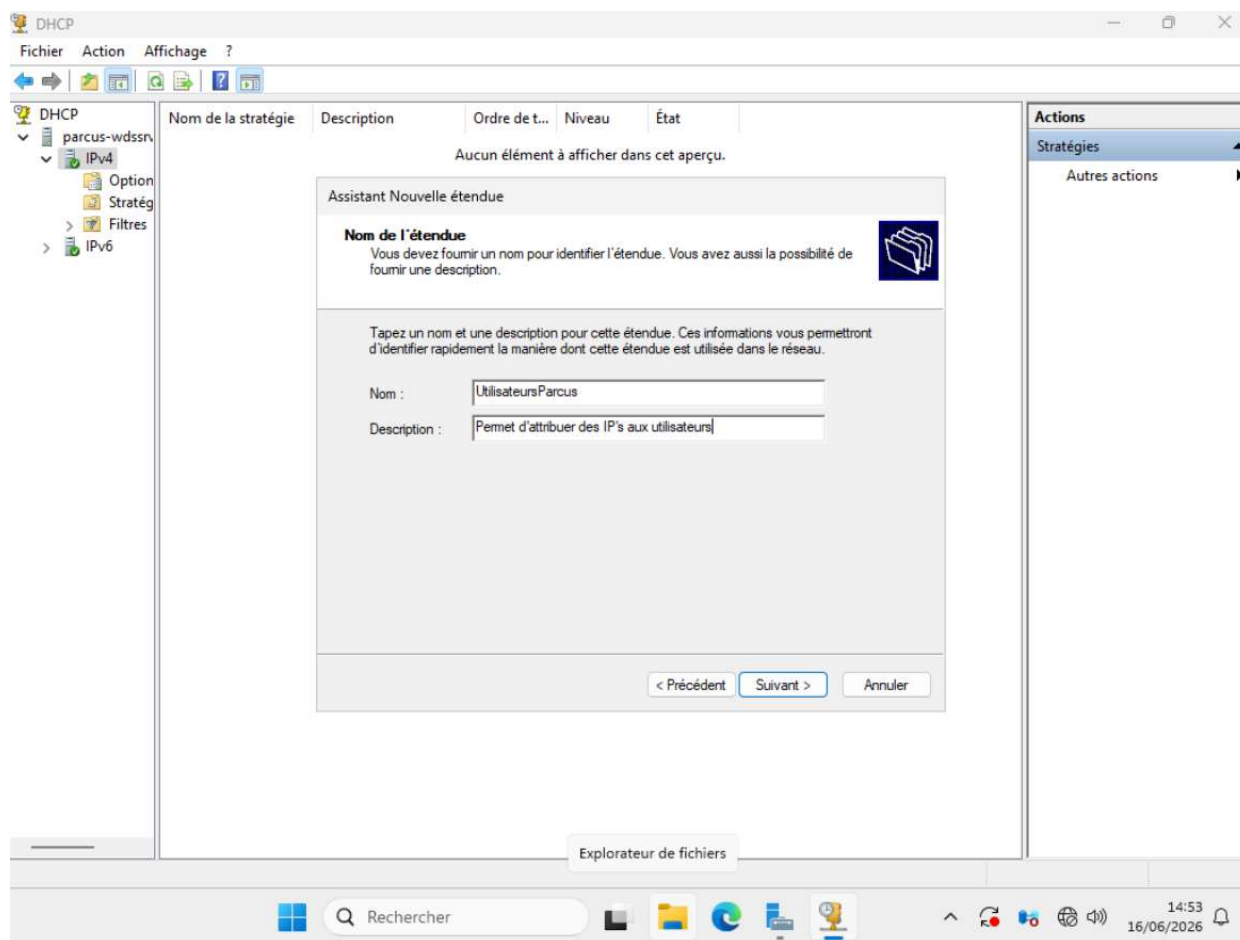


Clic droit sur IPv4 : Nouvelle étendue...



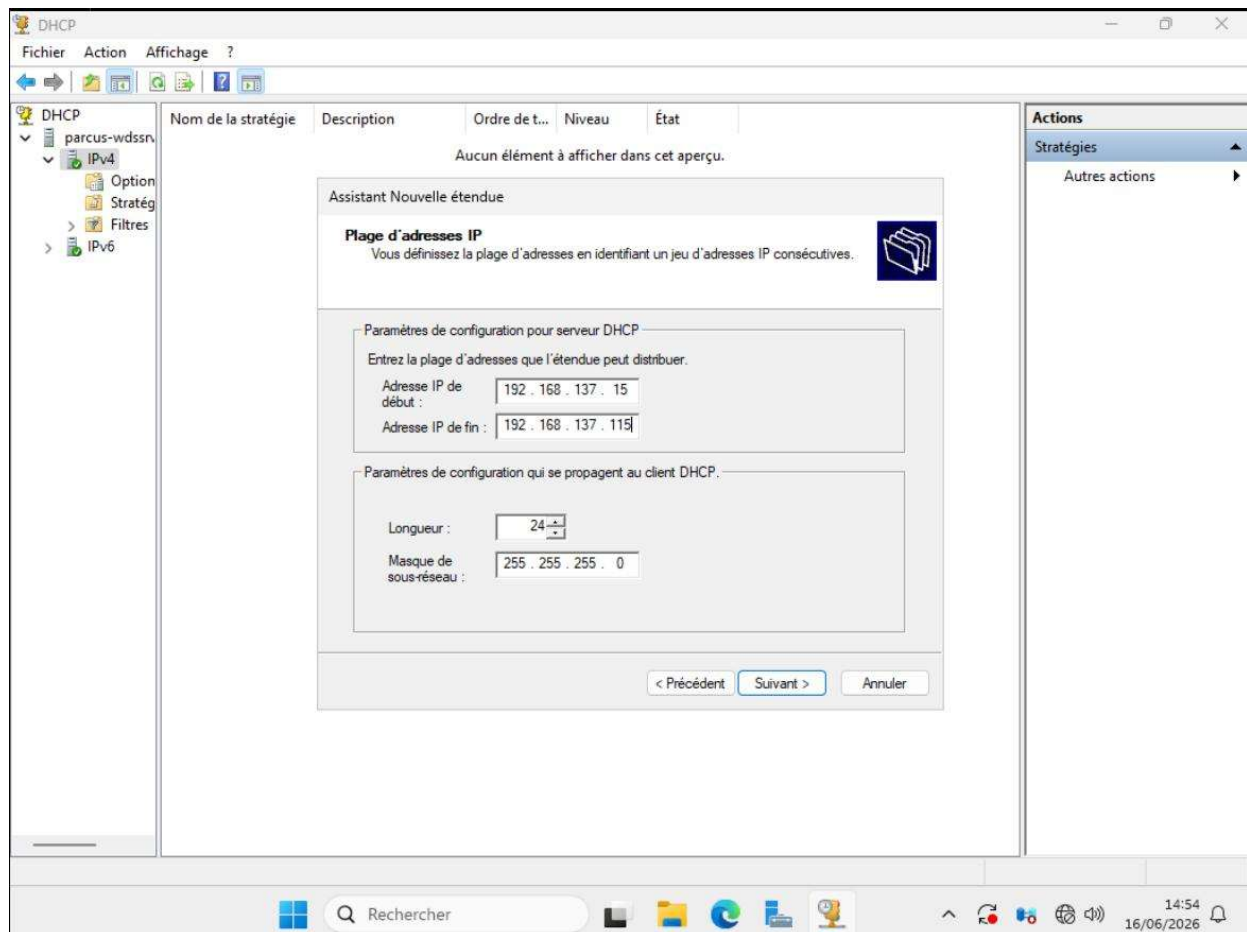
Assistant Nouvelle étendue : écran d'accueil

On nomme l'étendue UtilisateursParcus avec une description claire : elle servira aux postes des utilisateurs du domaine.



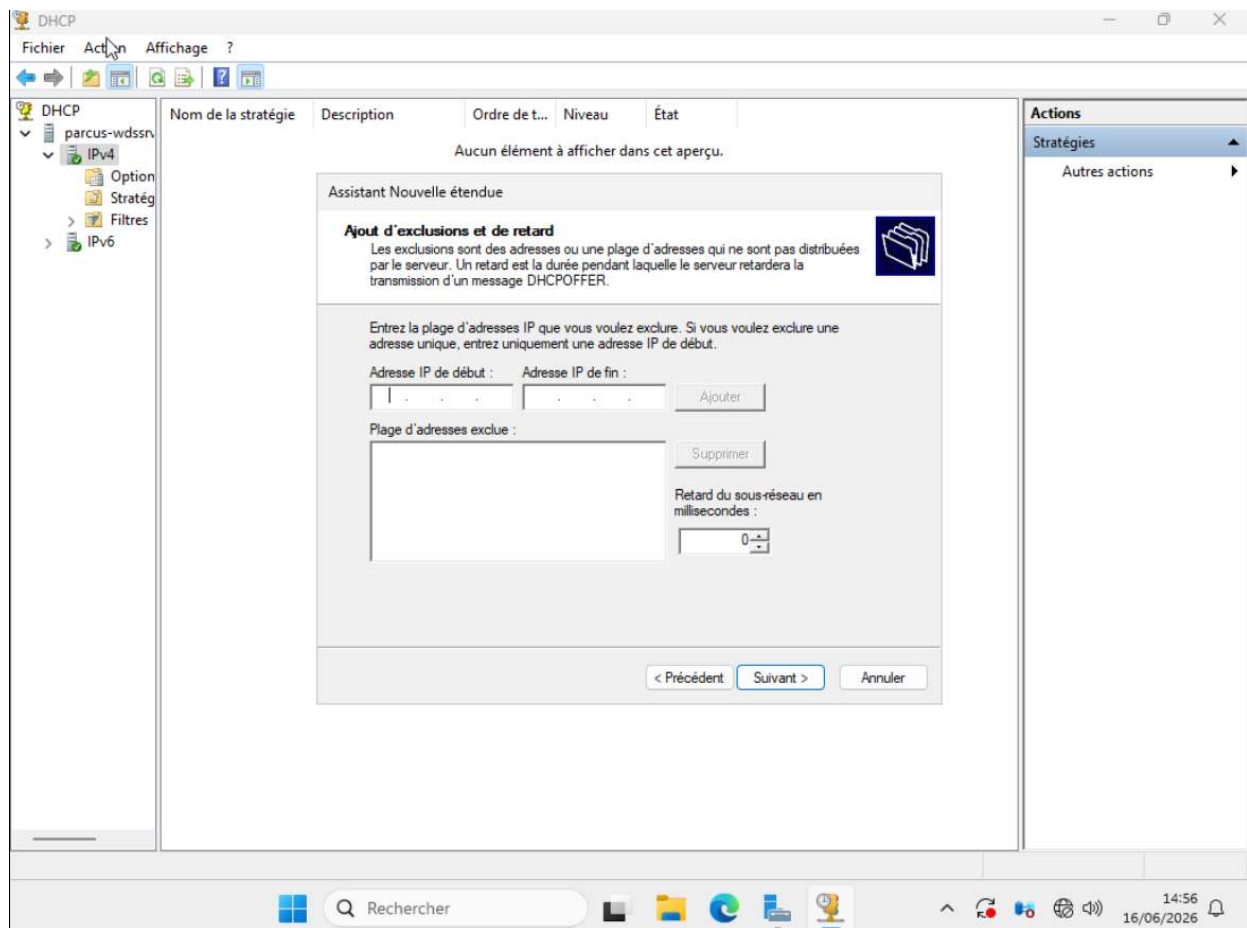
Nom et description de l'étendue

La plage distribuée va de 192.168.137.15 à 192.168.137.115, en /24 (masque 255.255.255.0). Les adresses basses (.1 à .14) restent réservées aux serveurs et équipements fixes, hors DHCP : aucun risque de conflit.

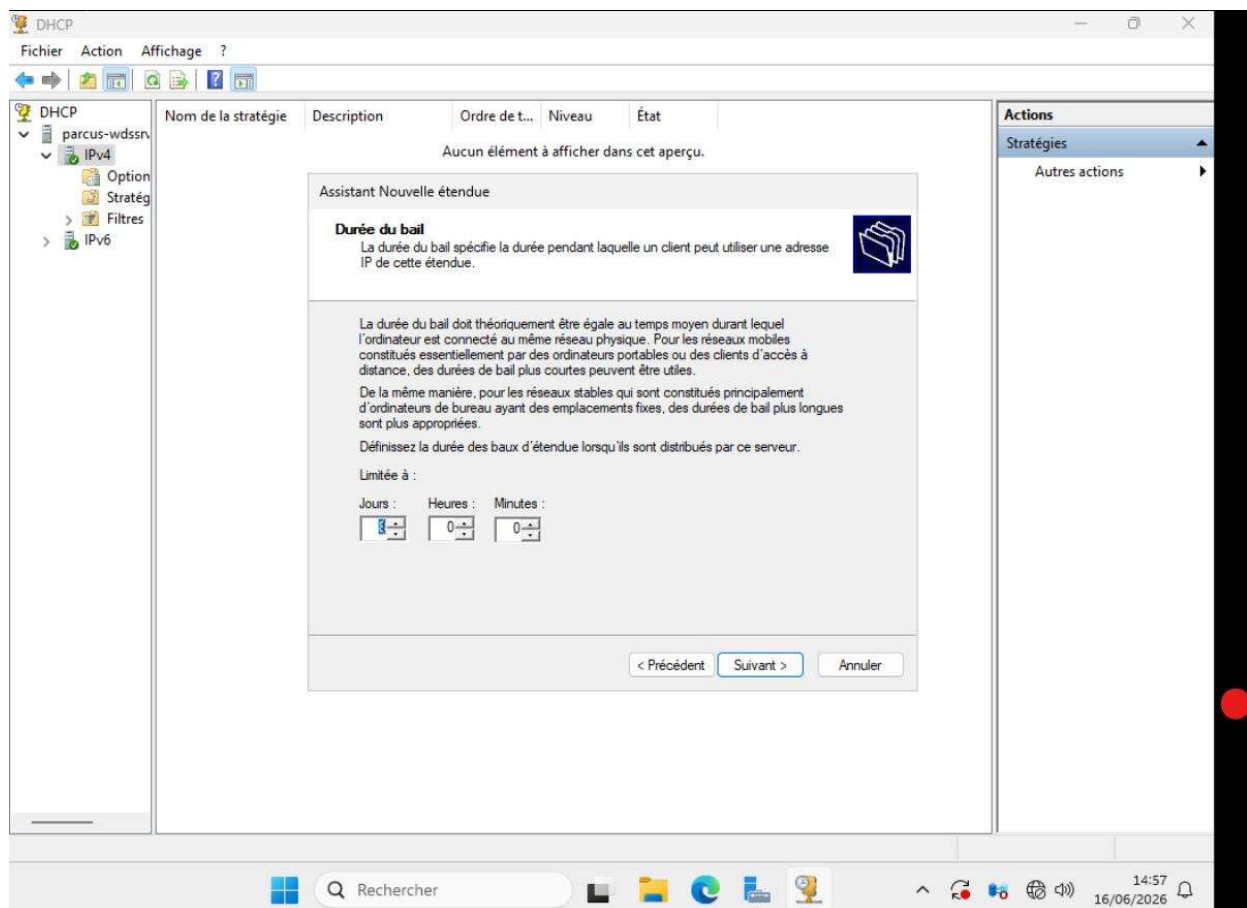


Plage d'adresses : 192.168.137.15 à 192.168.137.115, masque 255.255.255.0

On ne définit aucune exclusion (la plage a déjà été taillée pour éviter les serveurs) et on garde la durée de bail par défaut de 8 jours, adaptée à des postes fixes.

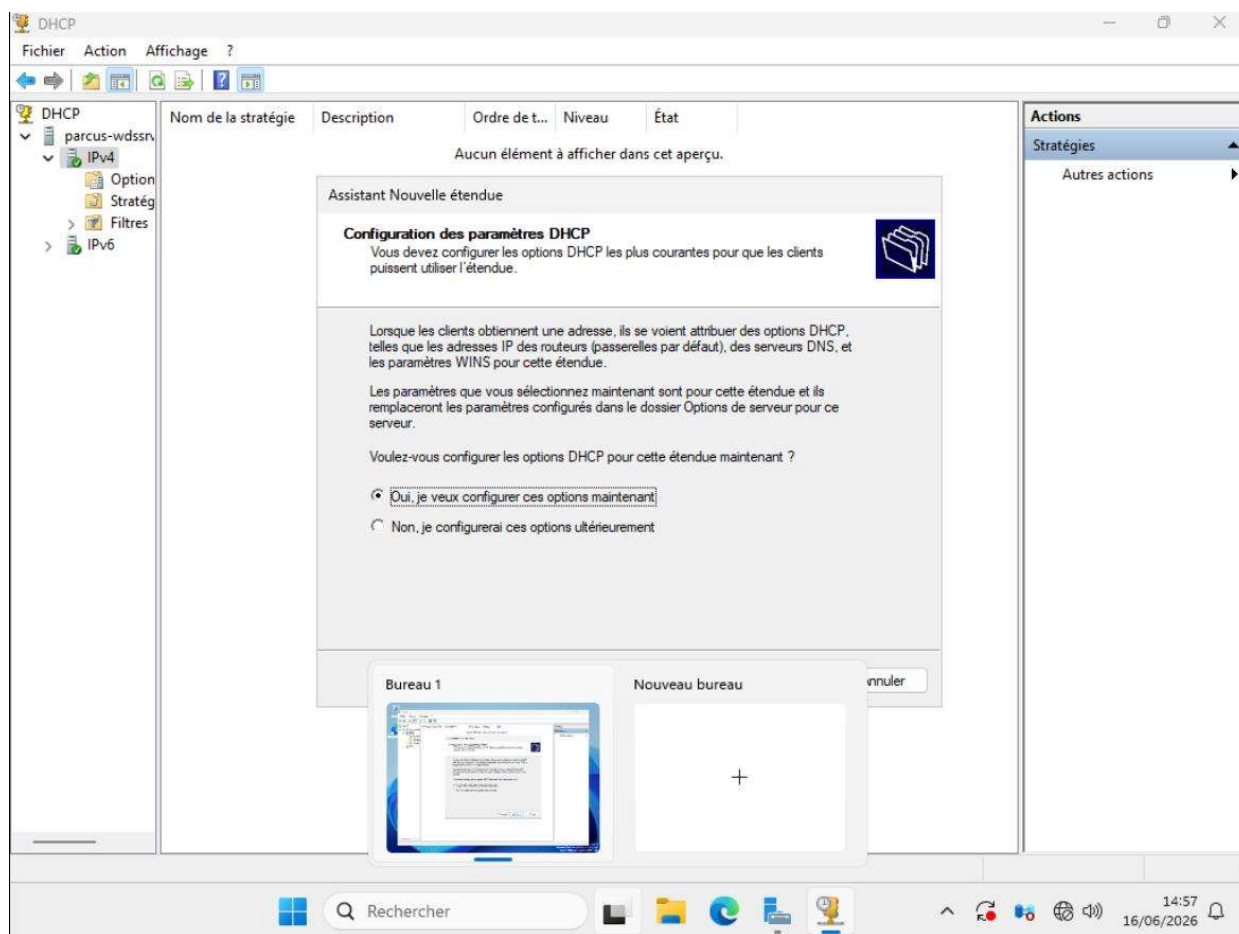


Ajout d'exclusions et de retard : laissé vide



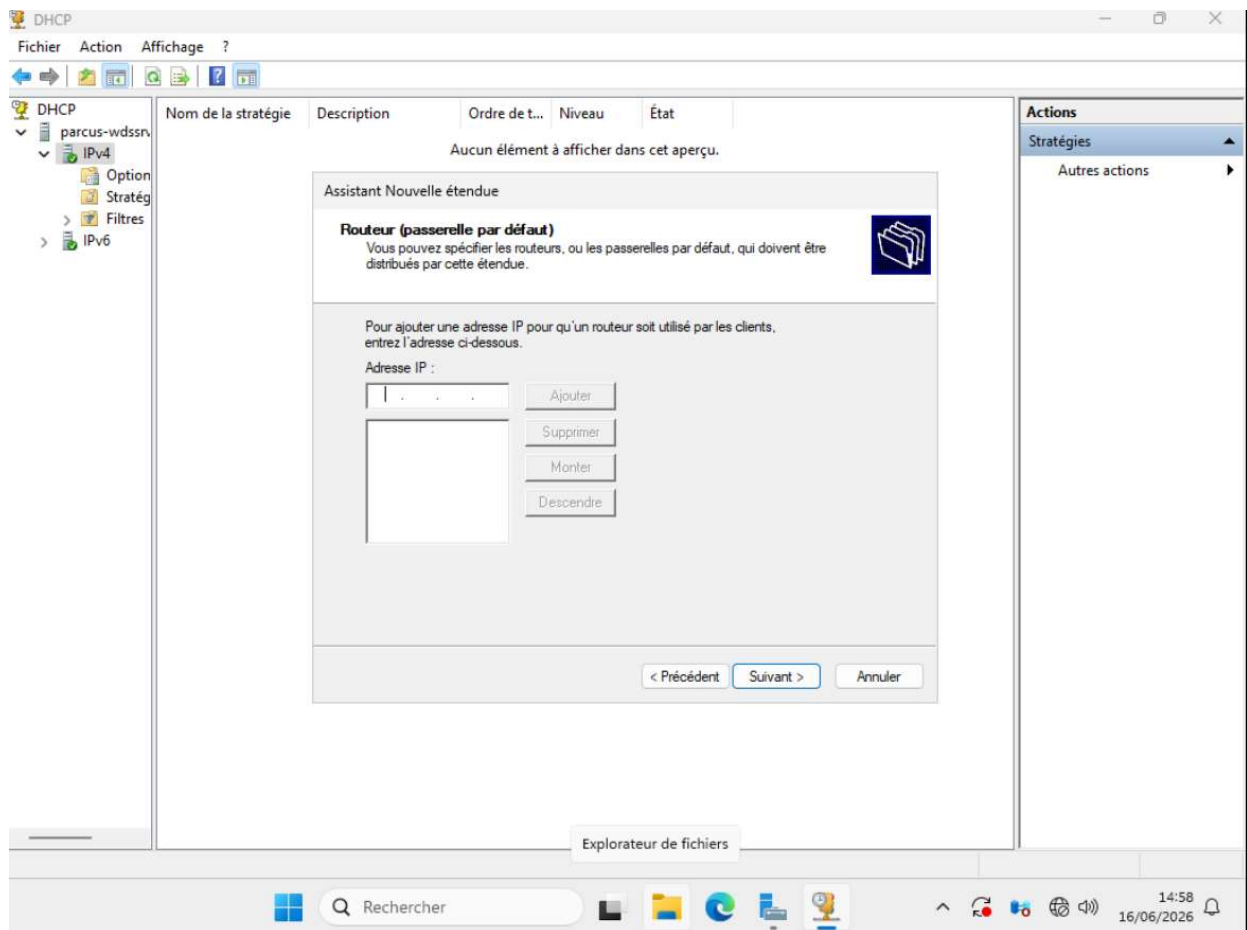
Durée du bail : 8 jours (valeur par défaut)

On choisit ensuite de configurer immédiatement les options DHCP transmises aux clients.

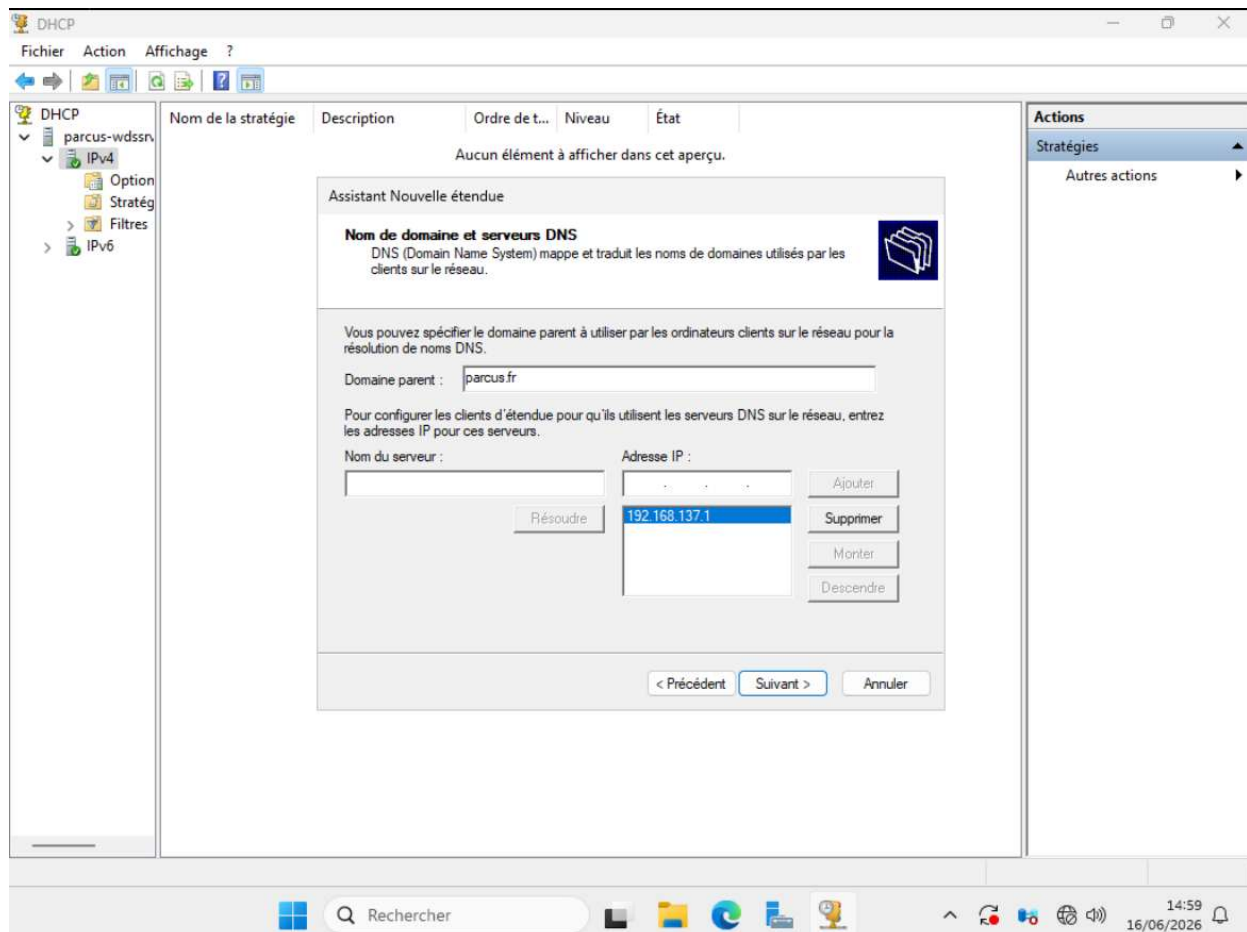


Configuration des paramètres DHCP : « Oui, je veux configurer ces options maintenant »

La page Routeur reste vide, puisque notre réseau de test n'a pas de passerelle vers l'extérieur. En revanche on renseigne le domaine parent parcus.fr et le serveur DNS 192.168.137.1 : c'est ce qui permettra aux postes de résoudre les noms du domaine et donc de le rejoindre.

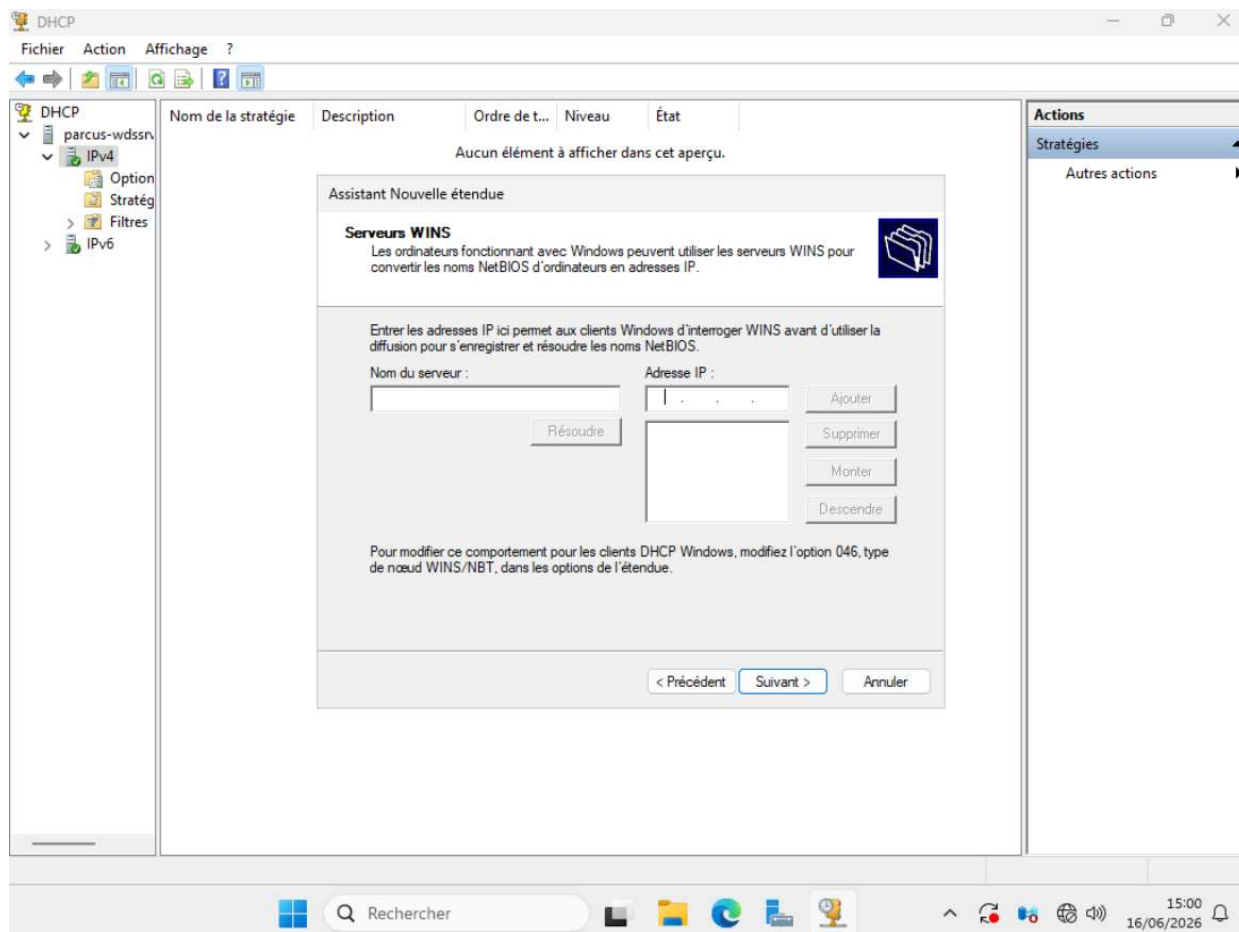


Option Routeur (passerelle par défaut) : laissée vide sur ce réseau local

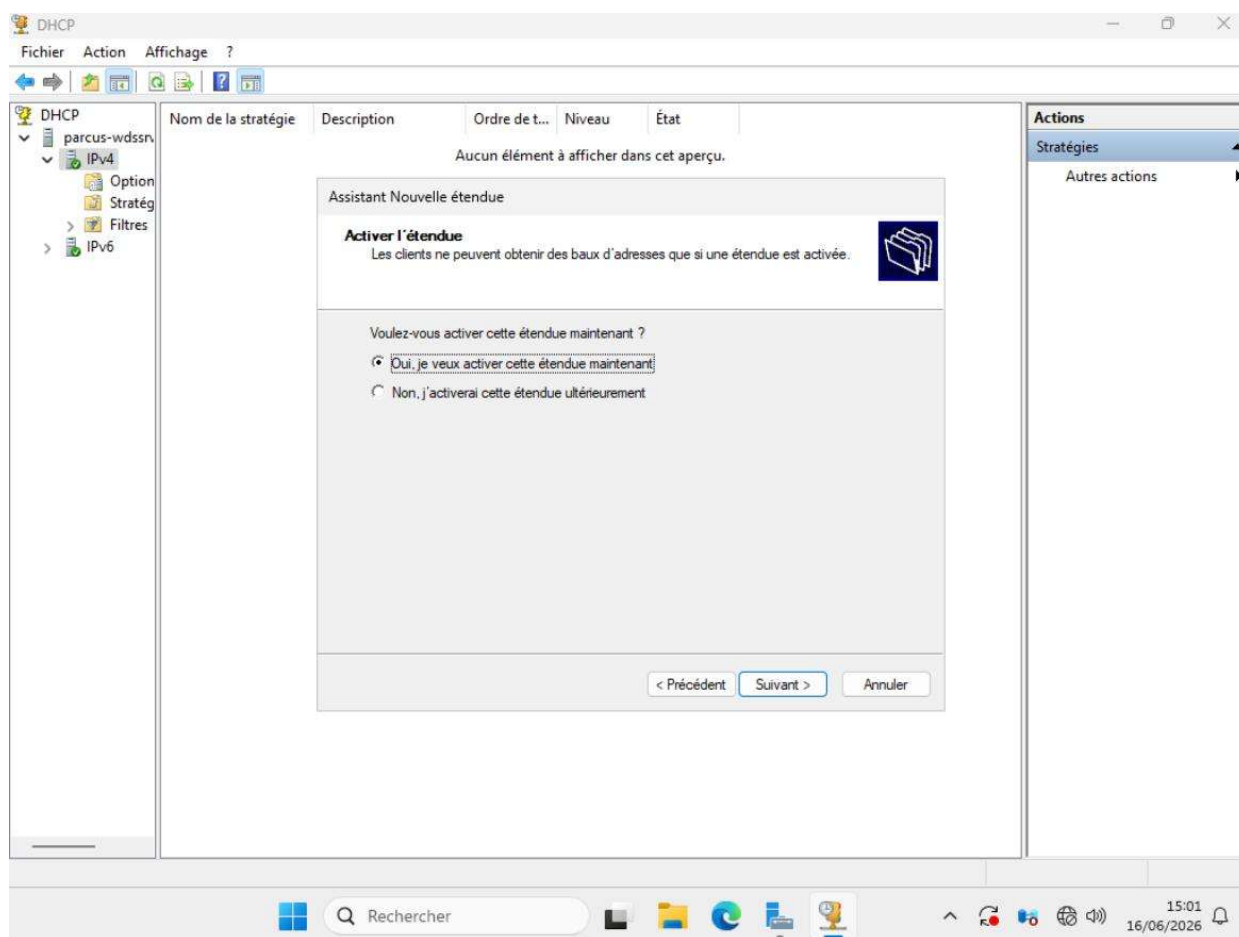


Options DNS distribuées : domaine parent parcus.fr, serveur 192.168.137.1

Les serveurs WINS ne sont plus utilisés aujourd'hui, on laisse la page vide, puis on active l'étendue immédiatement.



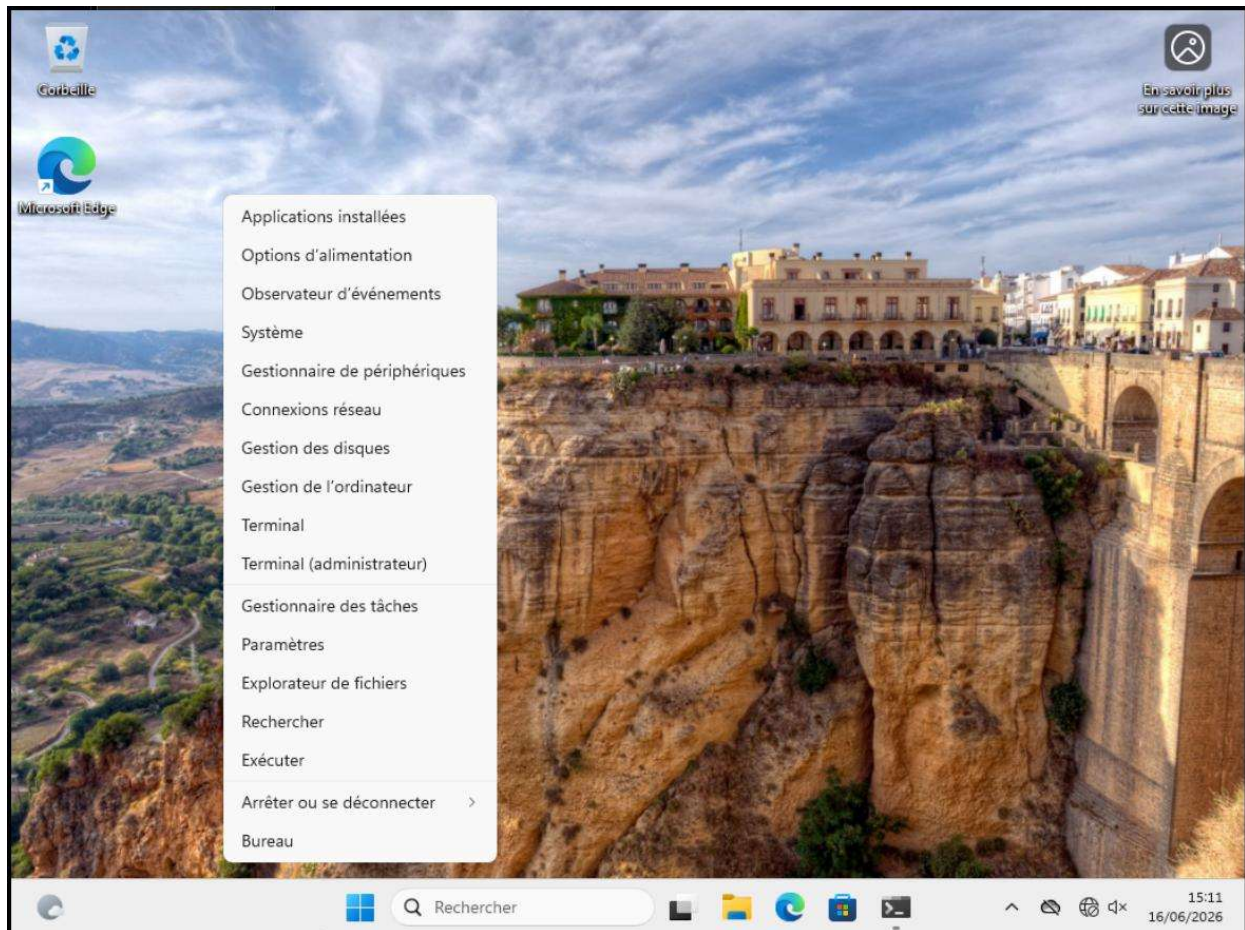
Serveurs WINS : non utilisés, page laissée vide



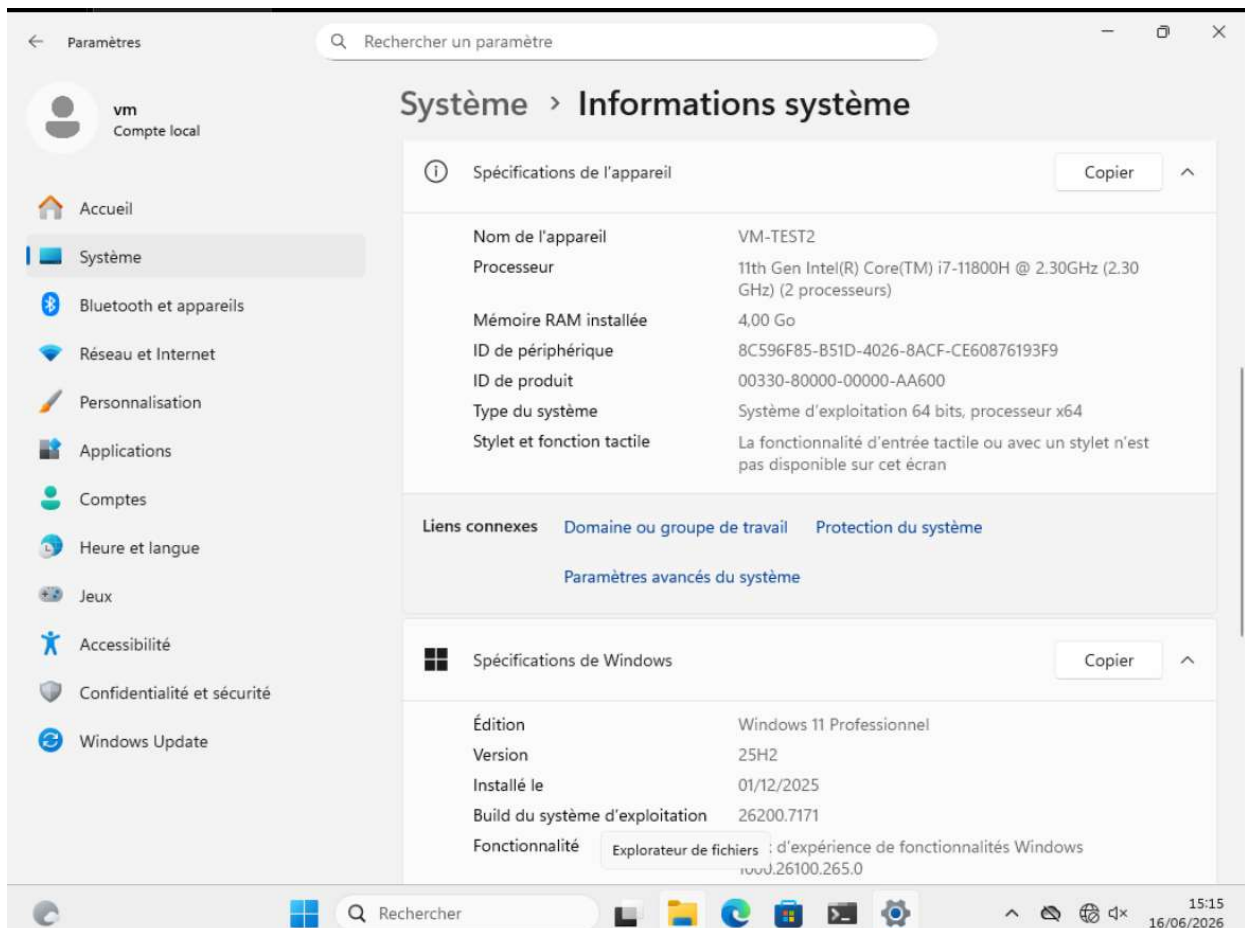
Activation immédiate de l'étendue

3.1.7. Jonction d'un poste Windows 11 au domaine

Pour valider l'ensemble (DHCP + DNS + annuaire), on joint un poste client au domaine. Le poste de test VM-TEST2 tourne sous Windows 11 Professionnel 25H2 — l'édition Famille ne sait pas rejoindre un domaine.

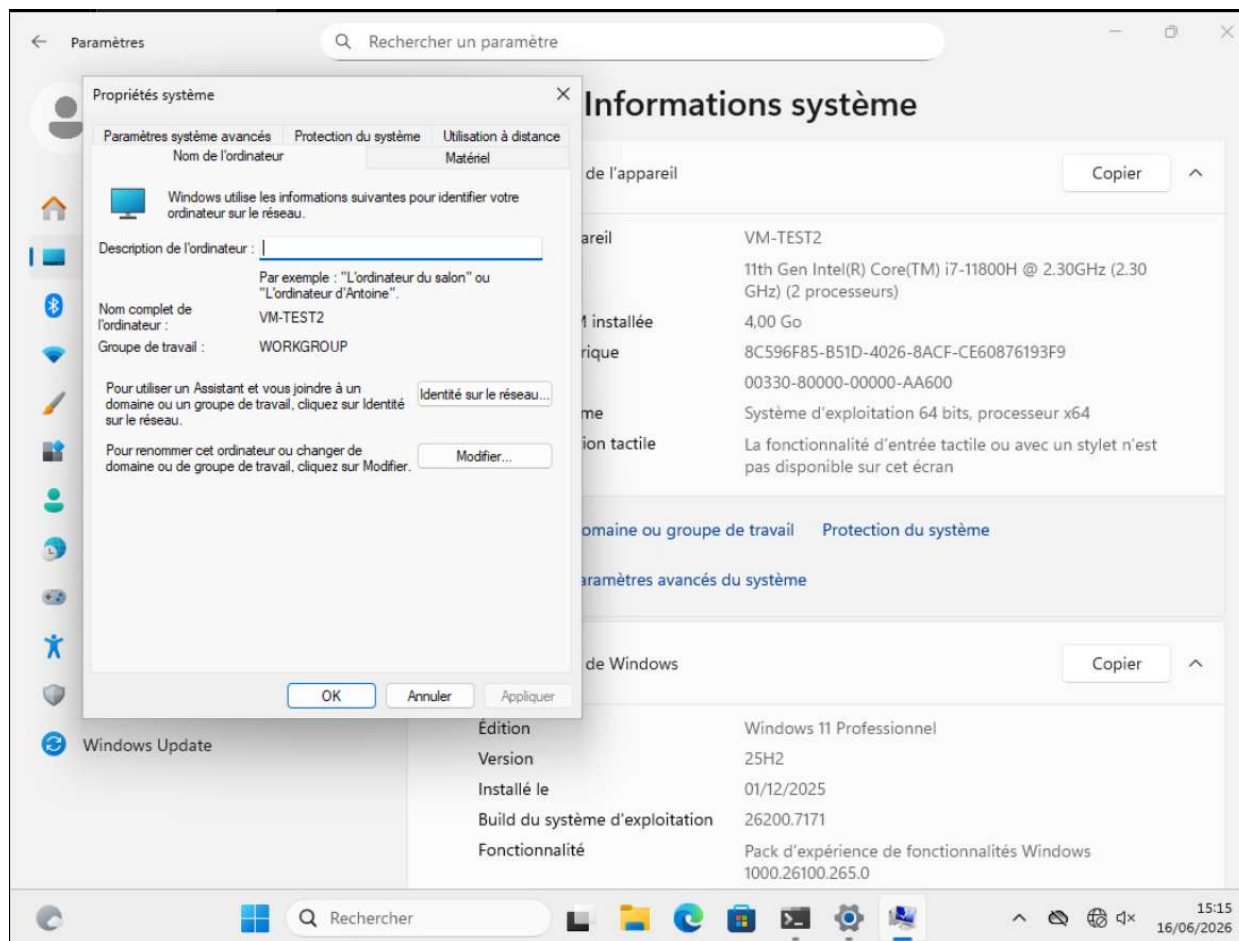


Poste client Windows 11 : le menu contextuel du bouton Démarrer donne accès au Système

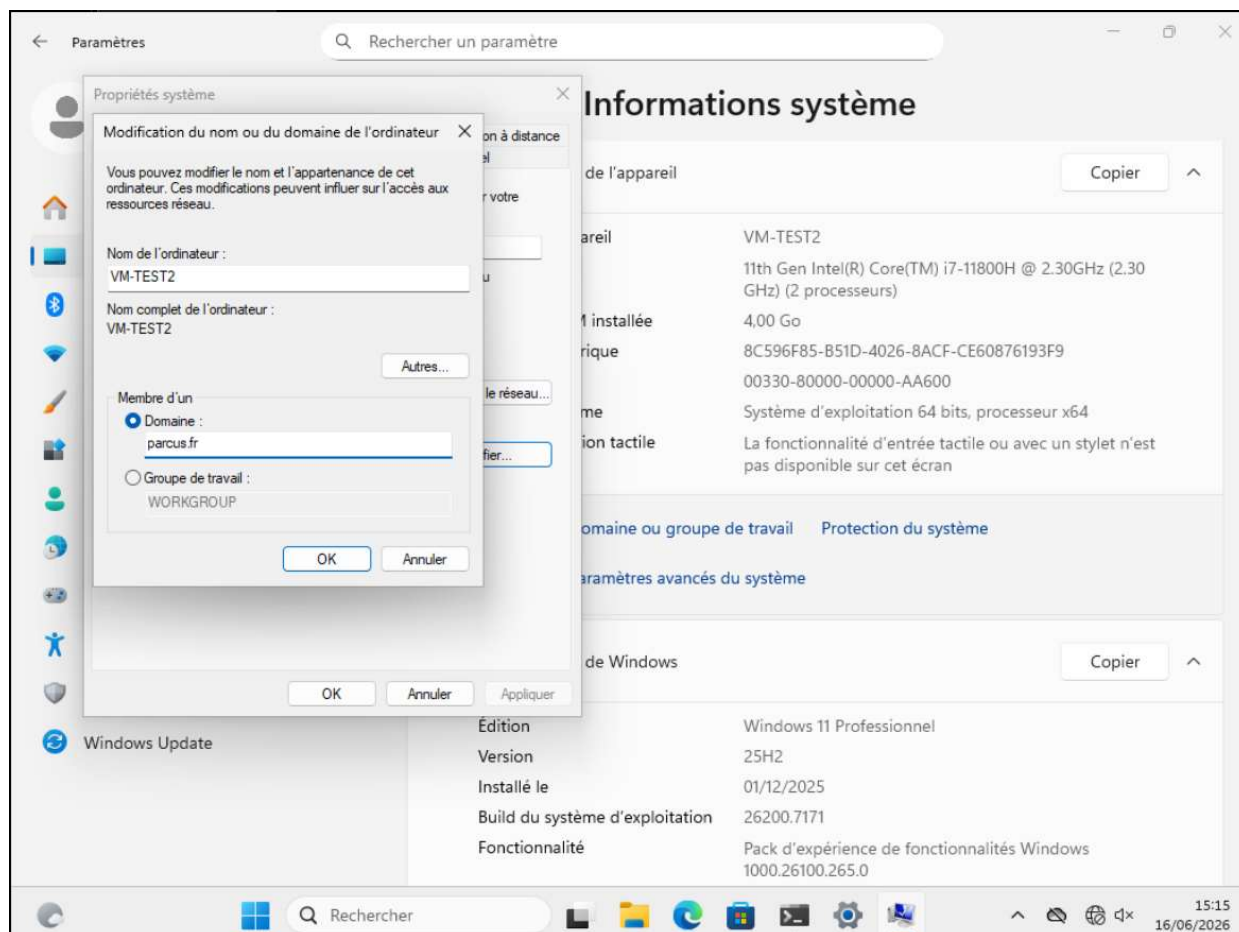


Informations système du poste VM-TEST2 : Windows 11 Professionnel 25H2, en groupe de travail

Depuis les Propriétés système du poste, on clique sur Modifier..., on coche Domaine et on saisit parcus.fr.

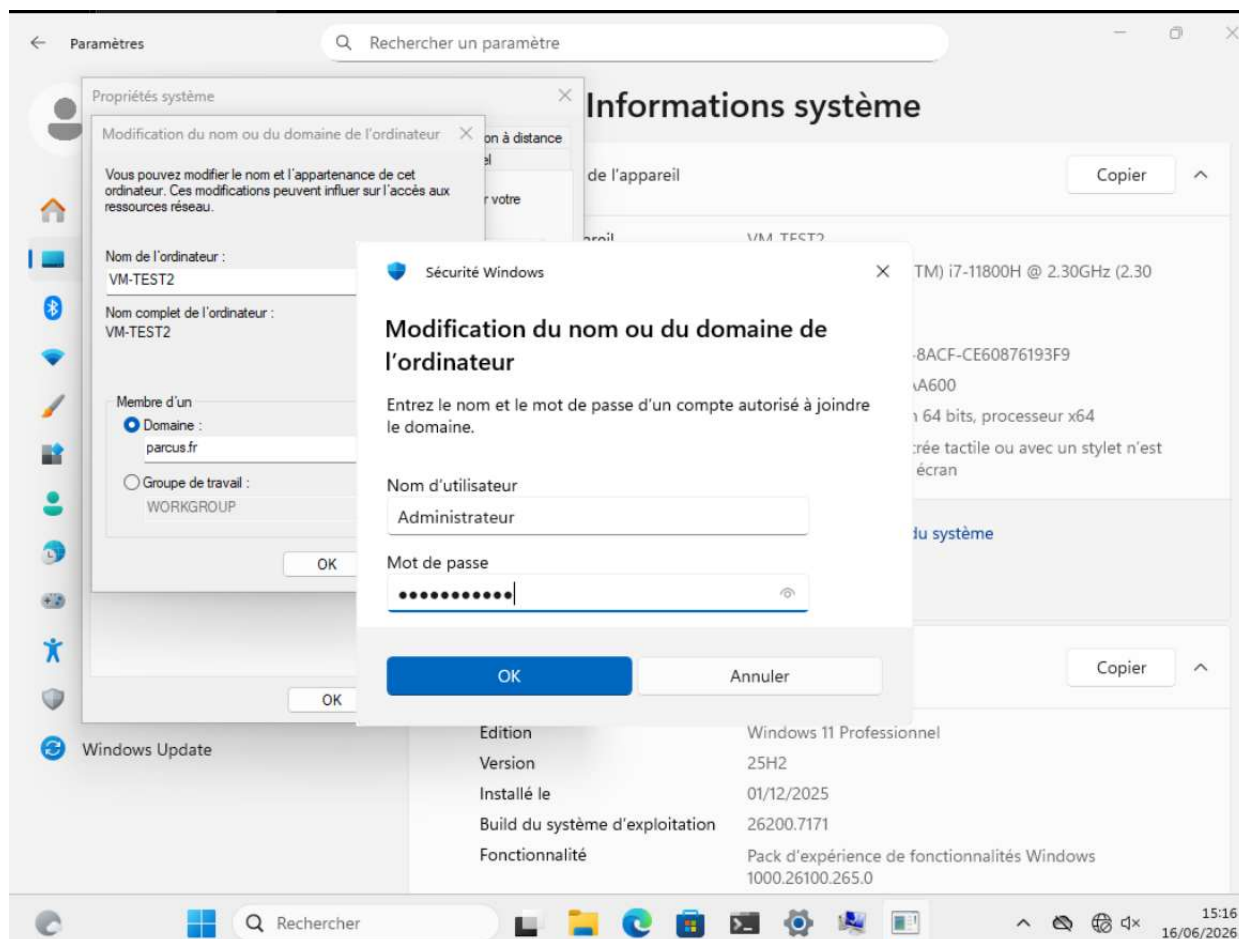


Propriétés système du poste : bouton Modifier... pour changer l'appartenance



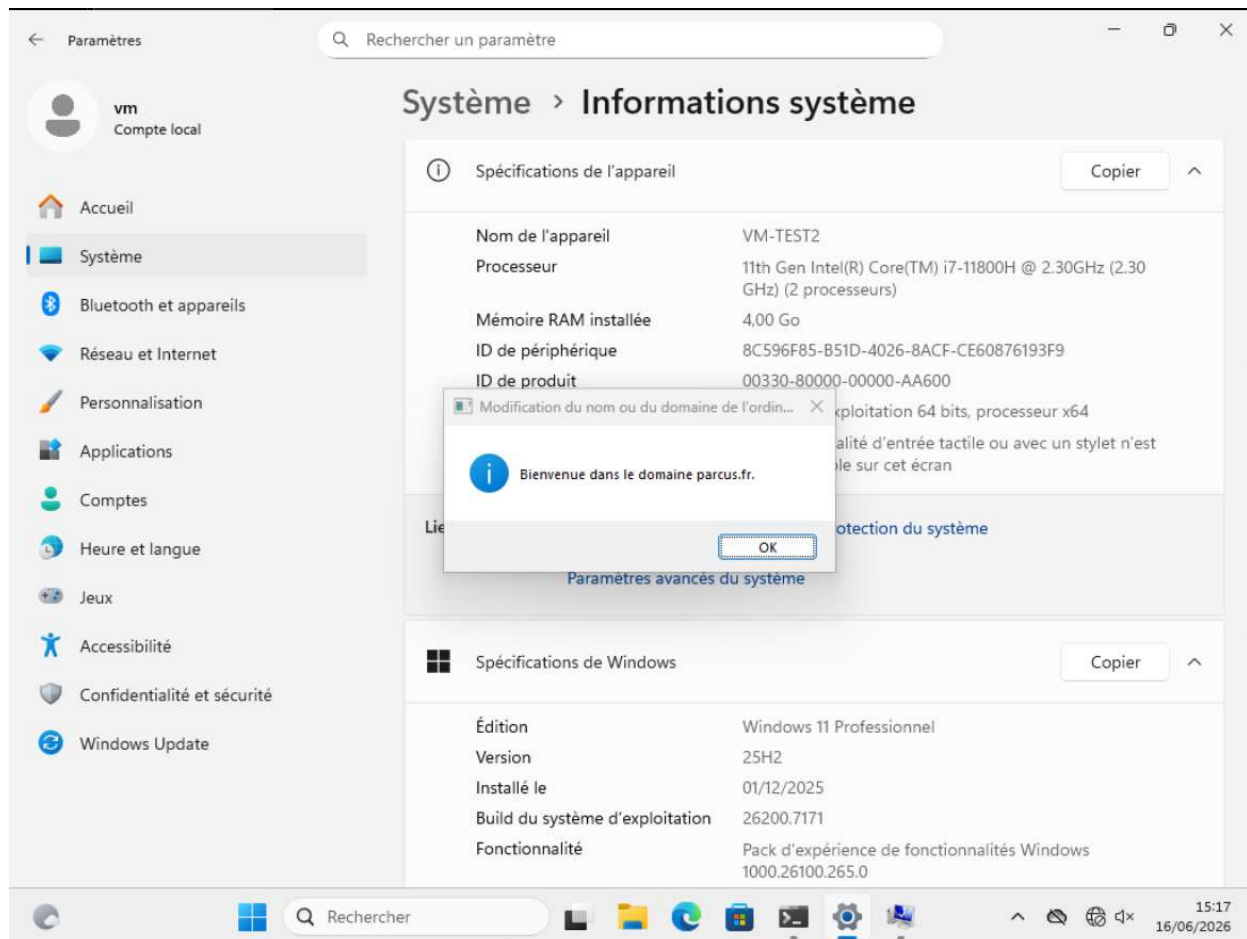
Le poste passe du groupe de travail WORKGROUP au domaine parcus.fr

Windows demande alors un compte autorisé à joindre des machines au domaine : on saisit les identifiants de l'administrateur du domaine.

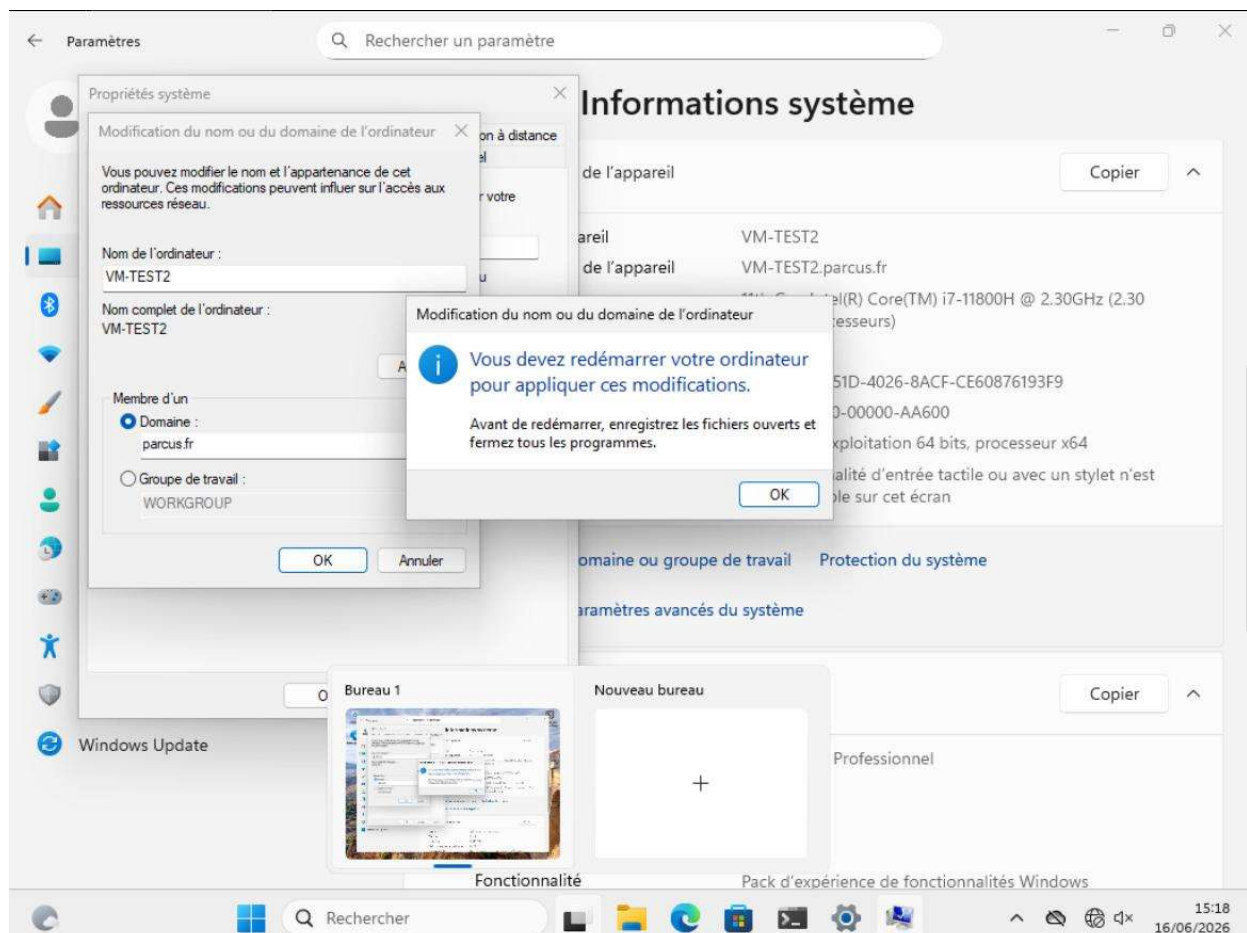


Saisie des identifiants d'un compte autorisé à joindre le domaine

Si la résolution DNS et l'annuaire fonctionnent, le message « Bienvenue dans le domaine parcus.fr » s'affiche, puis Windows demande un redémarrage.



Message de confirmation : « Bienvenue dans le domaine parcus.fr »



Redémarrage nécessaire pour appliquer la jonction au domaine

Vérification du bail DHCP. Un `ipconfig /all` sur le poste confirme toute la chaîne : adresse 192.168.137.15 (la première de l'étendue) délivrée par le serveur DHCP 192.168.137.1, suffixe DNS `parcus.fr` et serveur DNS 192.168.137.1.

```
C:\Users\vm>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : VM-TEST2
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: parcus.fr

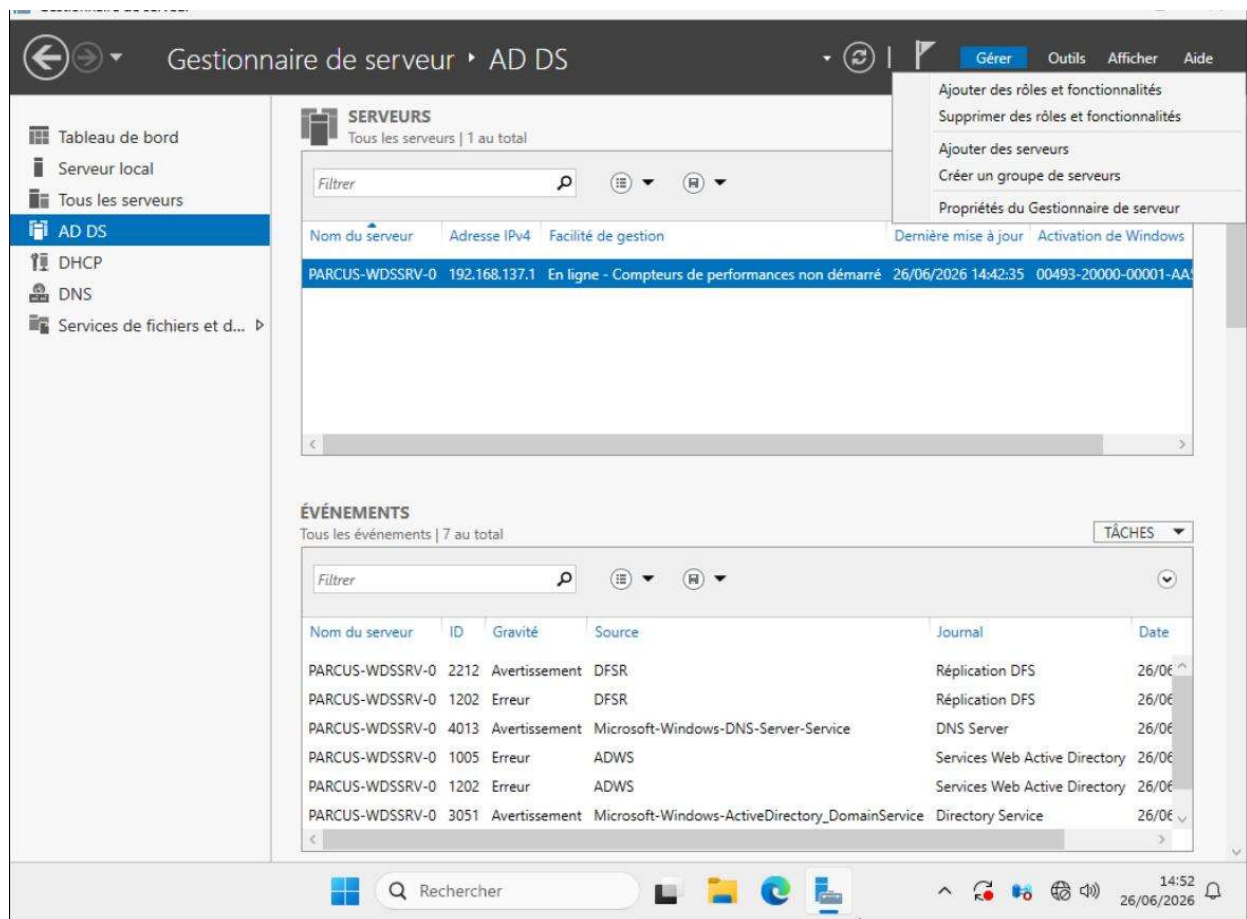
Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : parcus.fr
    Description. . . . . : Intel(R) 82574L Gigabit Network Connection
    Adresse physique . . . . . : 00-0C-29-6F-5B-5C
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::b963:bd10:ff69:d39a%9(préfééré)
    Adresse IPv4. . . . . : 192.168.137.15(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : mardi 16 juin 2026 15:08:35
    Bail expirant. . . . . : mercredi 24 juin 2026 15:08:35
    Passerelle par défaut. . . . . :
    Serveur DHCP . . . . . : 192.168.137.1
    IAID DHCPv6 . . . . . : 150998057
    DUID de client DHCPv6. . . . . : 00-01-01-00-31-BA-C0-6A-00-0C-29-6F-5B-5C
    Serveurs DNS. . . . . : 192.168.137.1
    NetBIOS sur Tcpi. . . . . : Activé
```

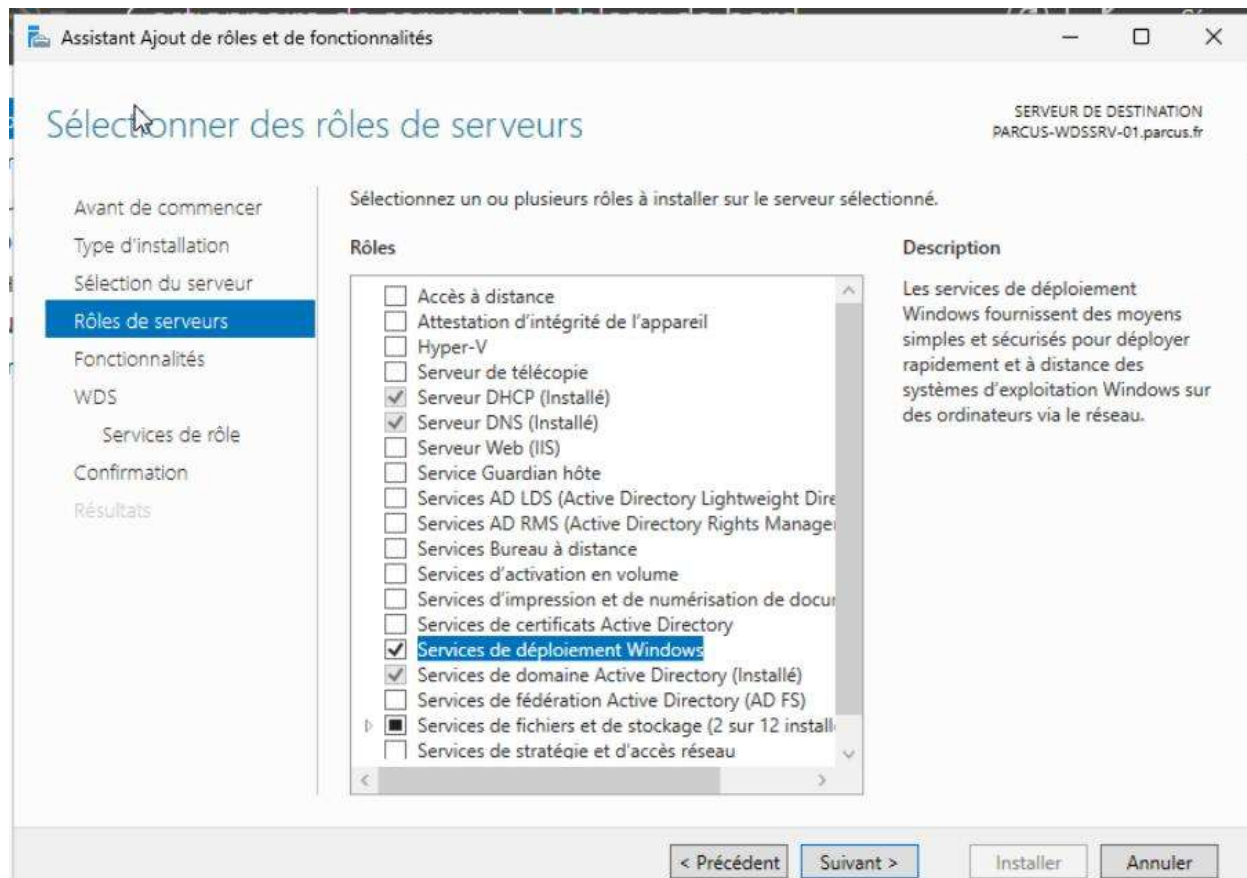
ipconfig /all sur VM-TEST2 : bail DHCP obtenu auprès de 192.168.137.1, suffixe `parcus.fr`

3.1.8. Installation du rôle WDS

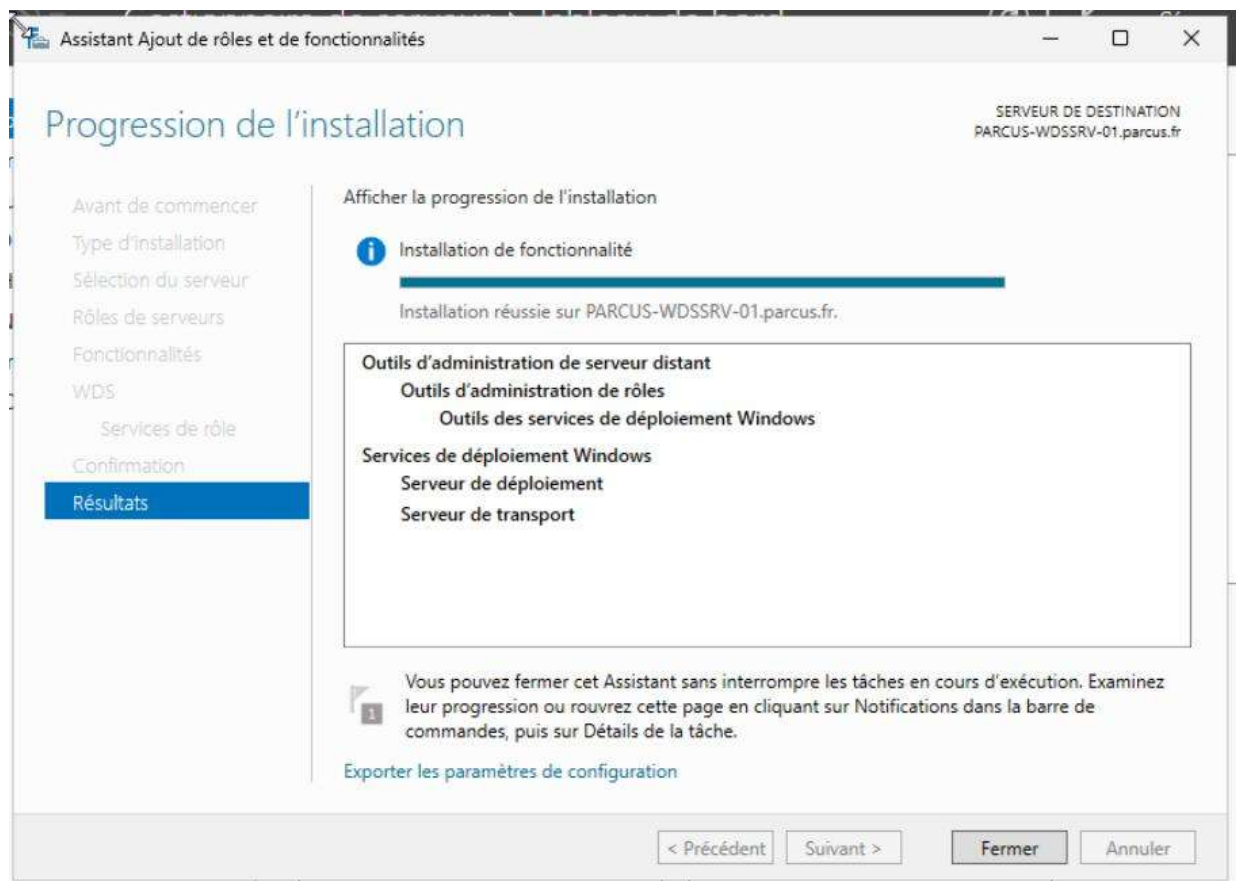
Les Services de déploiement Windows (WDS) permettent d'installer Windows sur les postes par le réseau, sans clé USB : le poste démarre en PXE, contacte le serveur et récupère son image. On ajoute le rôle comme les précédents, via le menu Gérer.



Menu Gérer depuis la vue AD DS : Ajouter des rôles et fonctionnalités

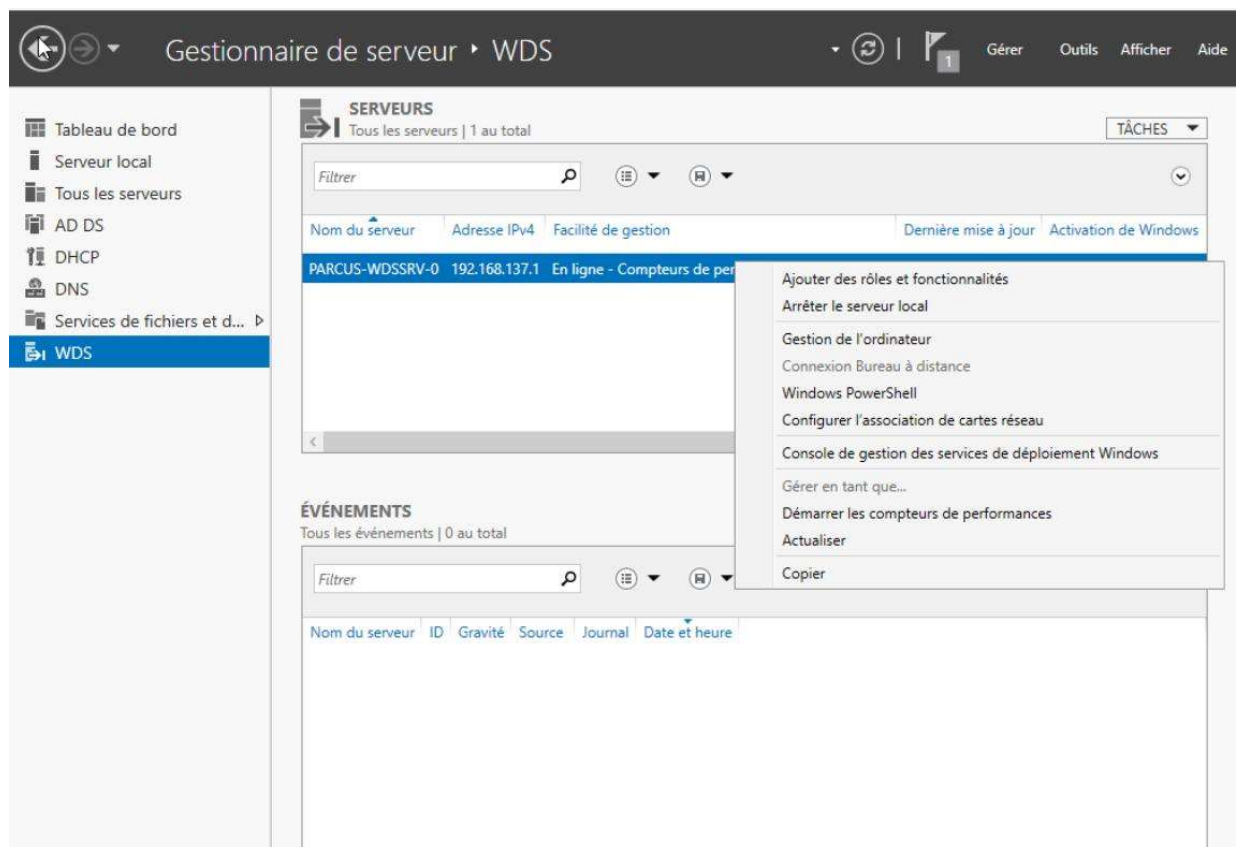


Sélection du rôle Services de déploiement Windows (DHCP, DNS et AD DS déjà installés)



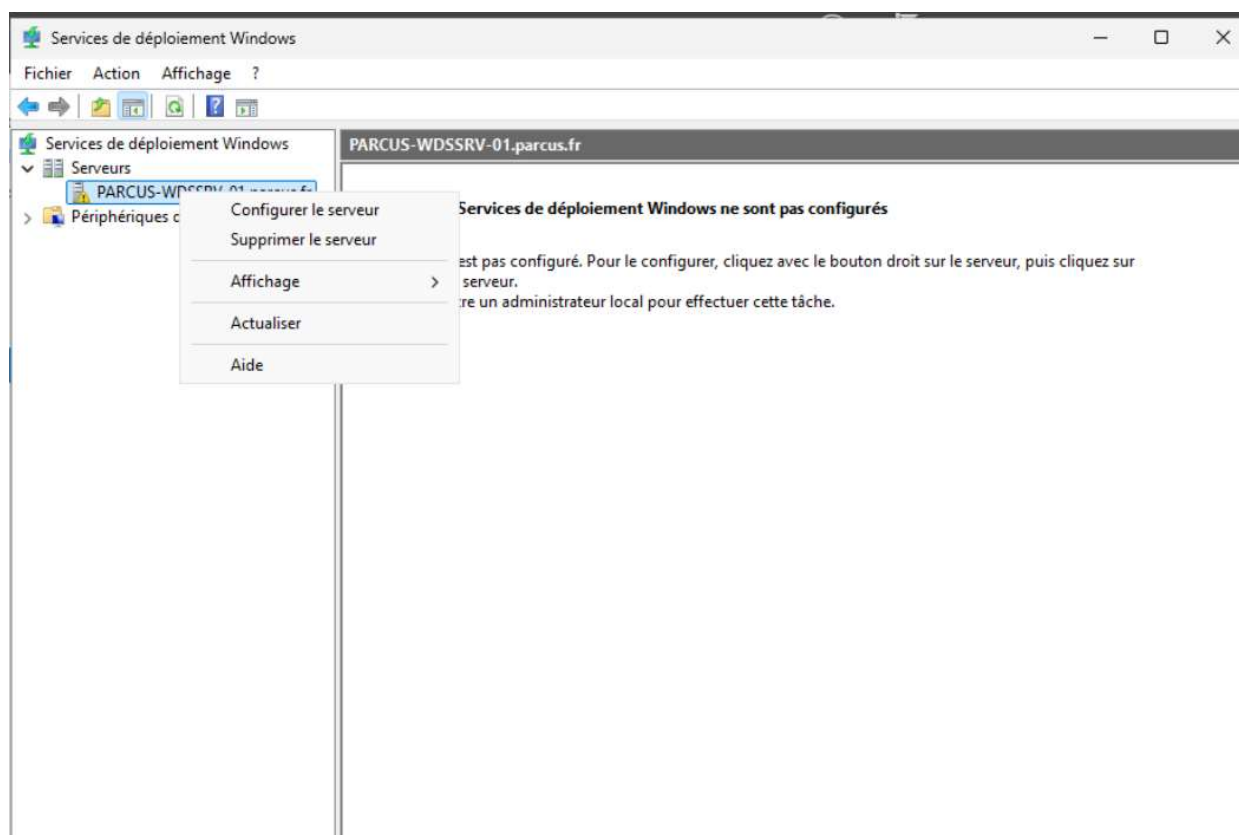
Installation du rôle WDS : serveur de déploiement et serveur de transport

La console de gestion WDS s'ouvre par un clic droit sur le serveur dans la vue WDS du Gestionnaire de serveur.



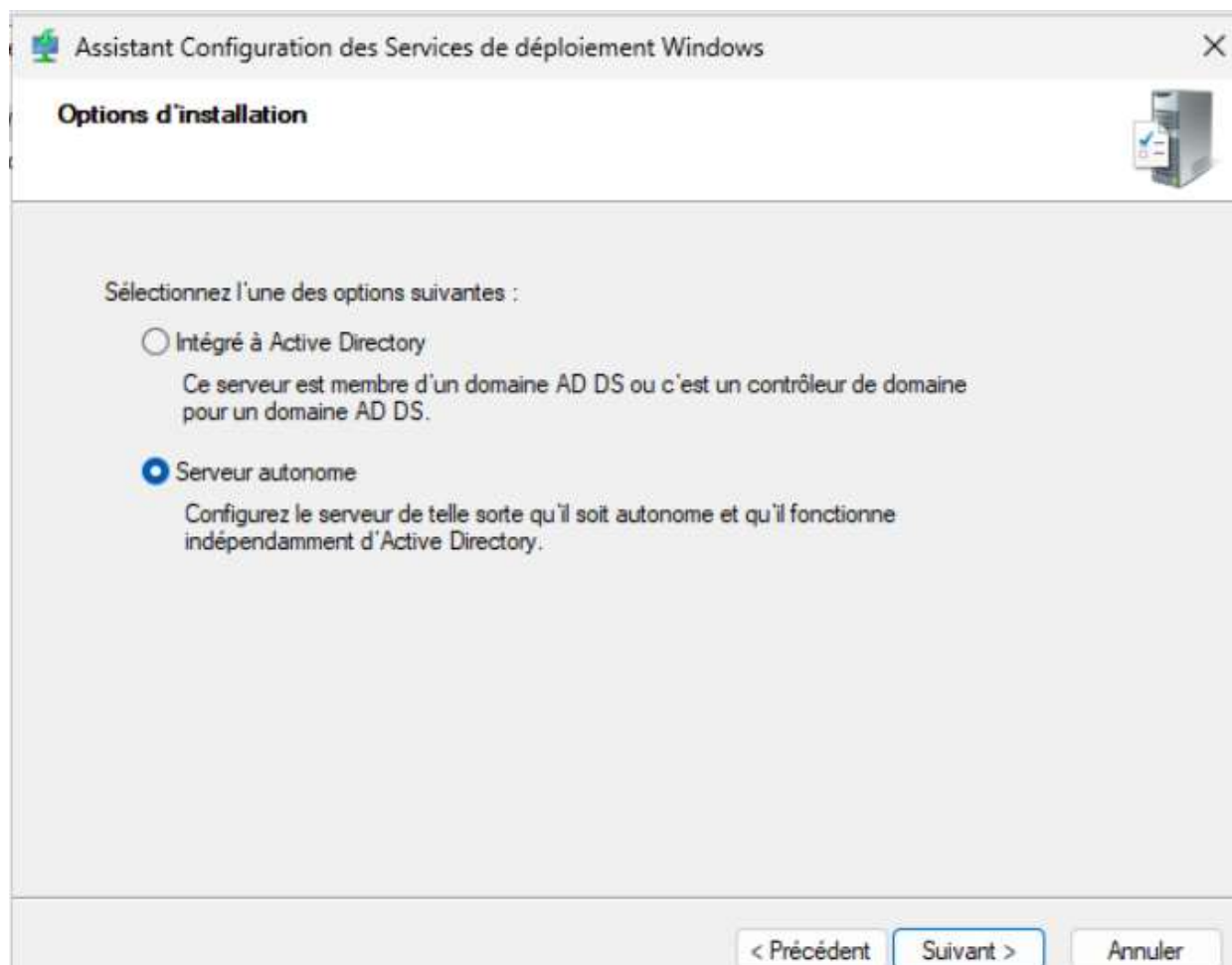
Ouverture de la Console de gestion des services de déploiement Windows

Le serveur apparaît avec un avertissement : il n'est pas encore configuré. Clic droit, puis Configurer le serveur.



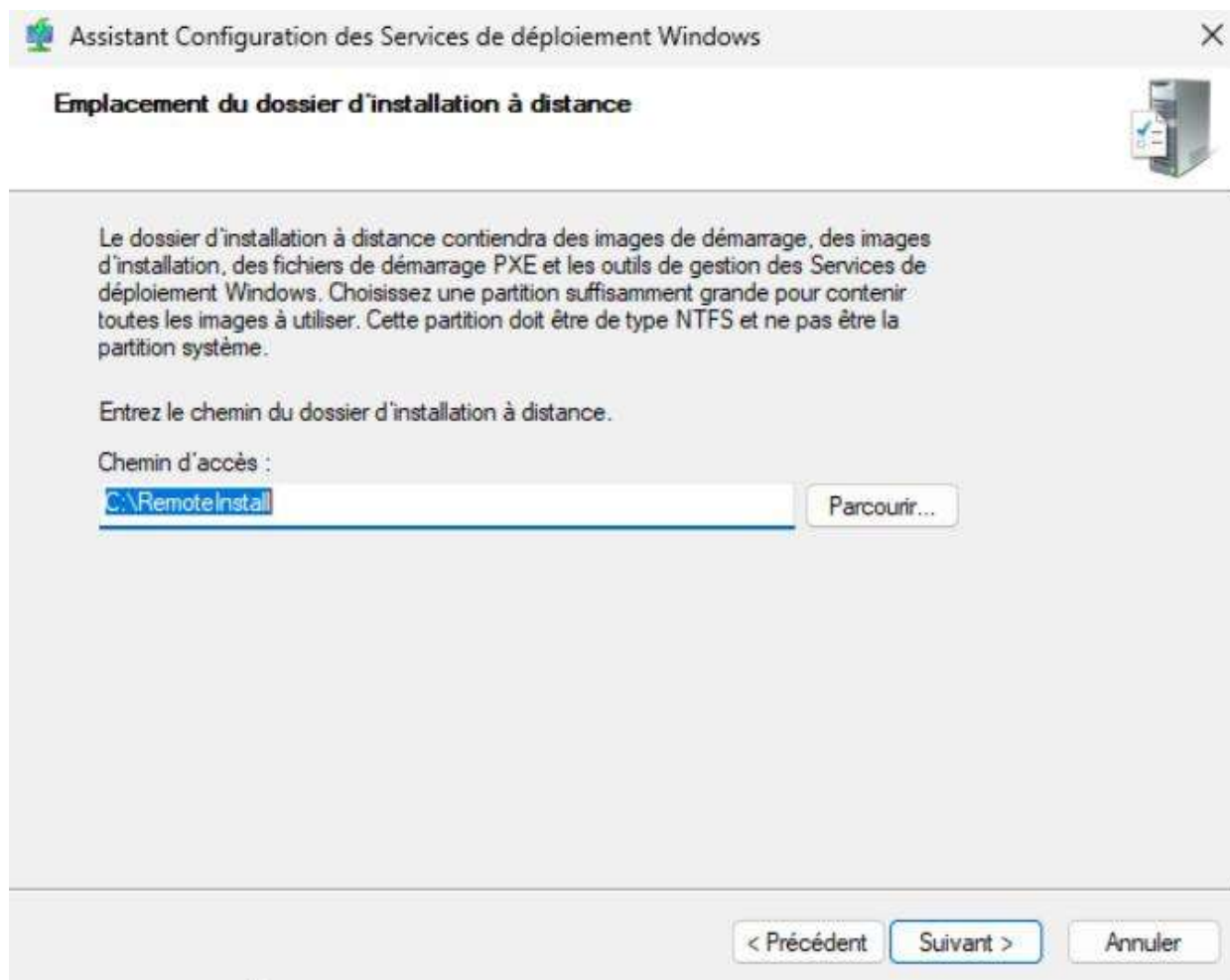
Le serveur WDS n'est pas configuré : clic droit > Configurer le serveur

L'assistant propose deux modes. Nous avons retenu le mode Serveur autonome, qui fonctionne indépendamment de l'annuaire : la gestion des autorisations se fait alors directement sur le serveur WDS, ce qui suffit pour notre déploiement en réseau local.



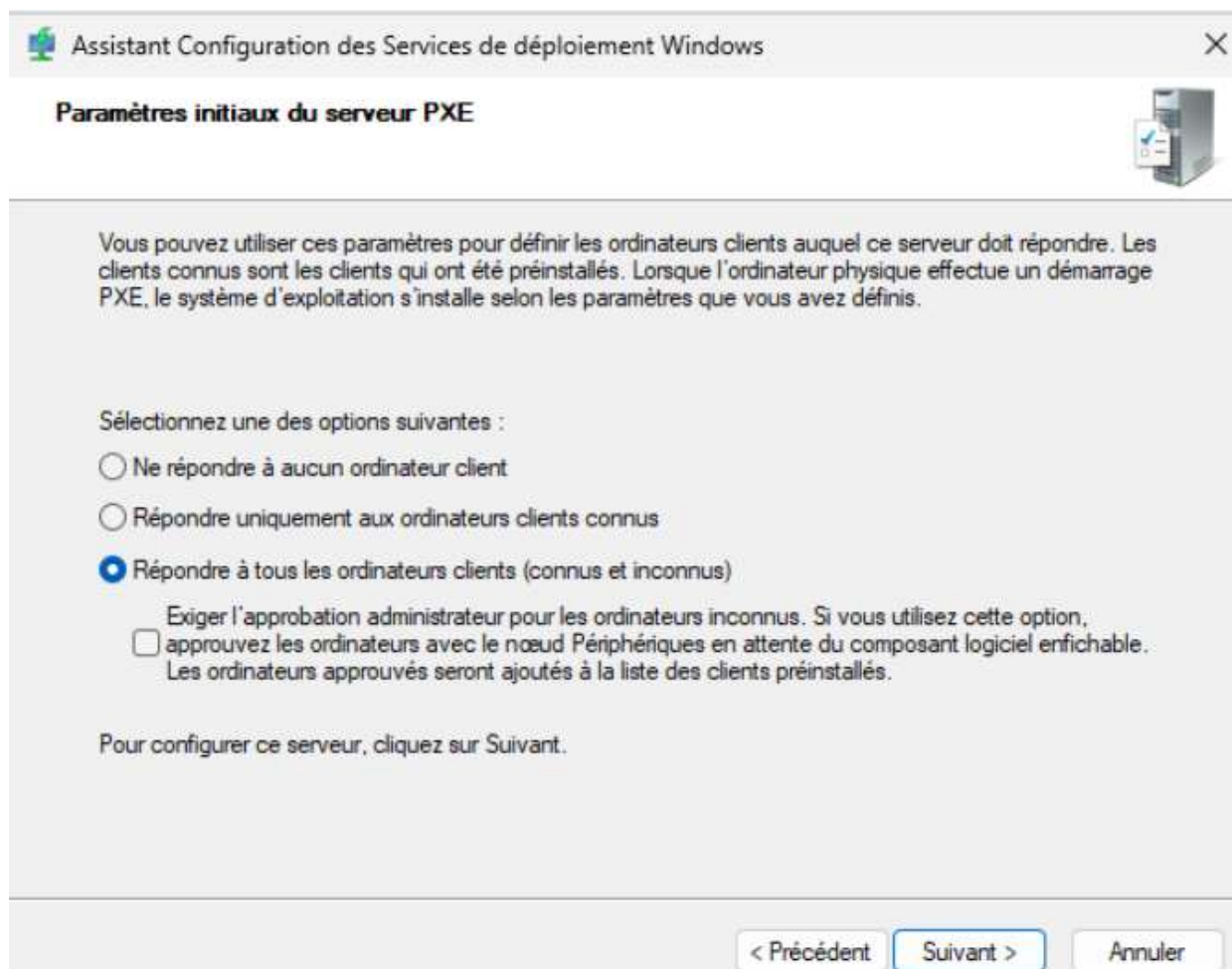
Options d'installation WDS : mode Serveur autonome

On indique ensuite le dossier d'installation à distance, qui contiendra les images de démarrage et d'installation. Il doit être sur une partition NTFS et, idéalement, pas sur la partition système : nous avons prévu un disque dédié (E:), le chemin par défaut C:\RemoteInstall n'étant utilisé que pour la capture d'écran de l'assistant.



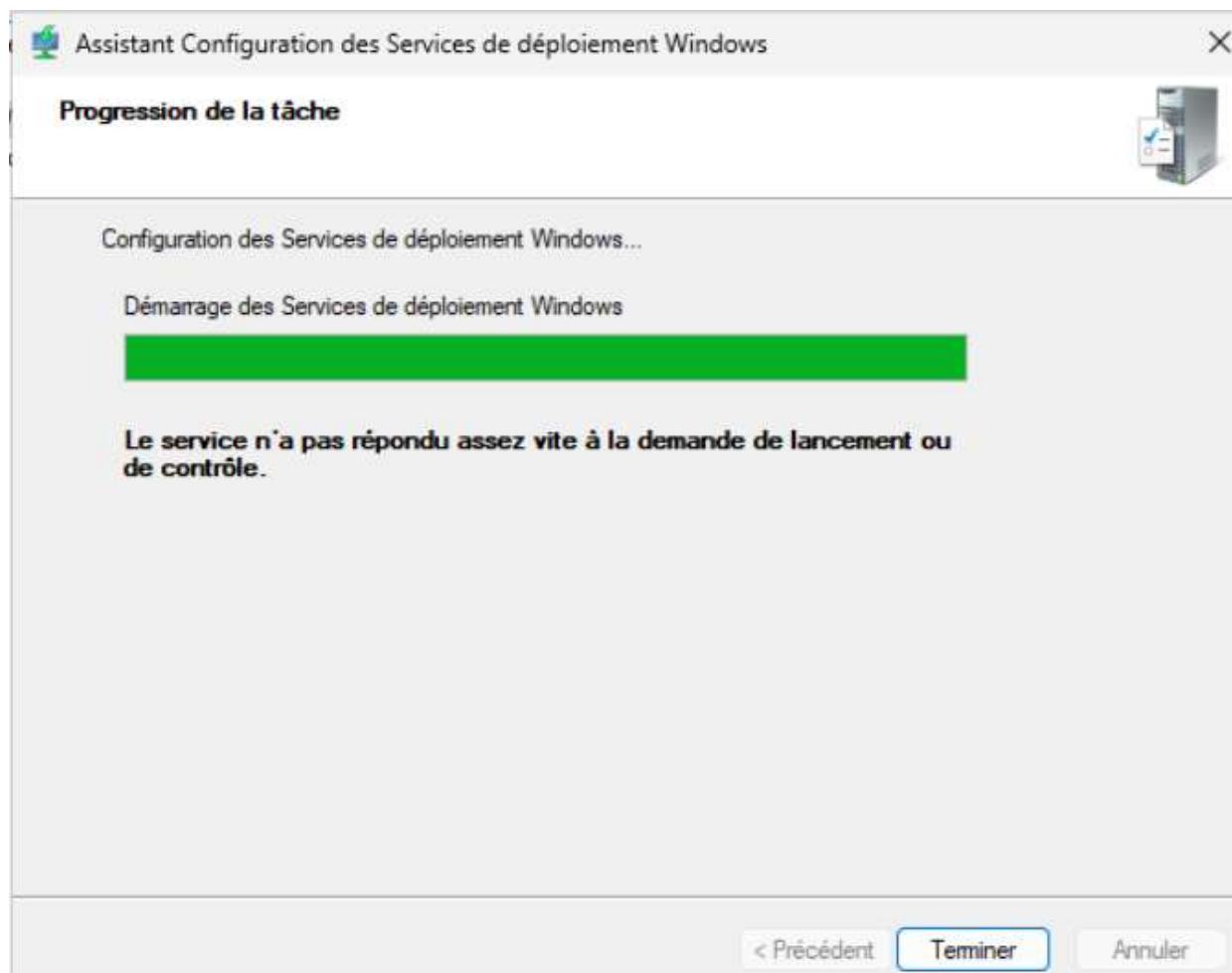
Emplacement du dossier d'installation à distance (partition NTFS)

Pour les paramètres initiaux du serveur PXE, on choisit de répondre à tous les ordinateurs clients, connus et inconnus : en maquette, cela évite d'avoir à pré-approuver chaque machine.



Paramètres PXE : le serveur répond à tous les ordinateurs clients

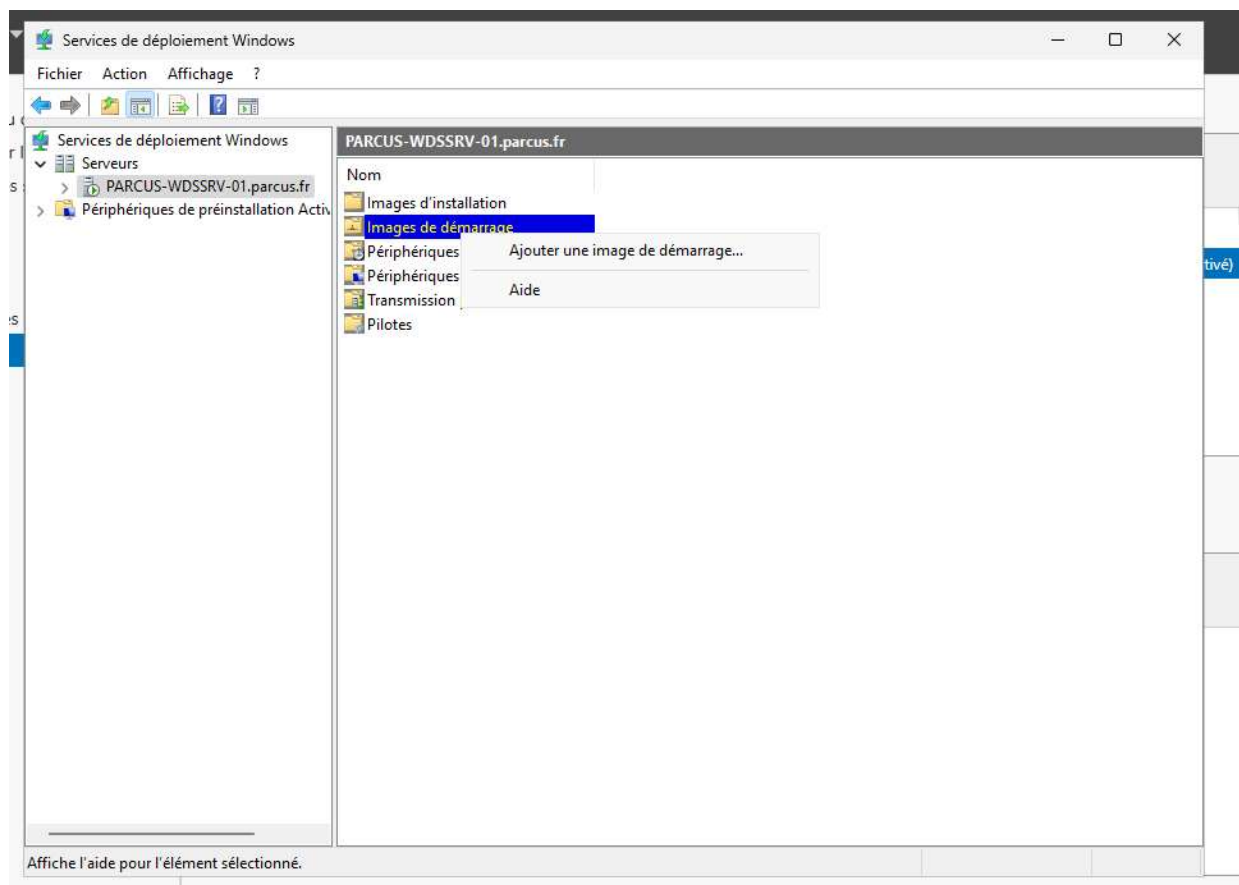
Au premier démarrage du service, l'assistant peut afficher « Le service n'a pas répondu assez vite... » : le service WDS met parfois plus de temps à démarrer que le délai d'attente de l'assistant. Ce n'est pas bloquant, le service finit de démarrer tout seul (on verra en 3.3.3 comment le vérifier en PowerShell).



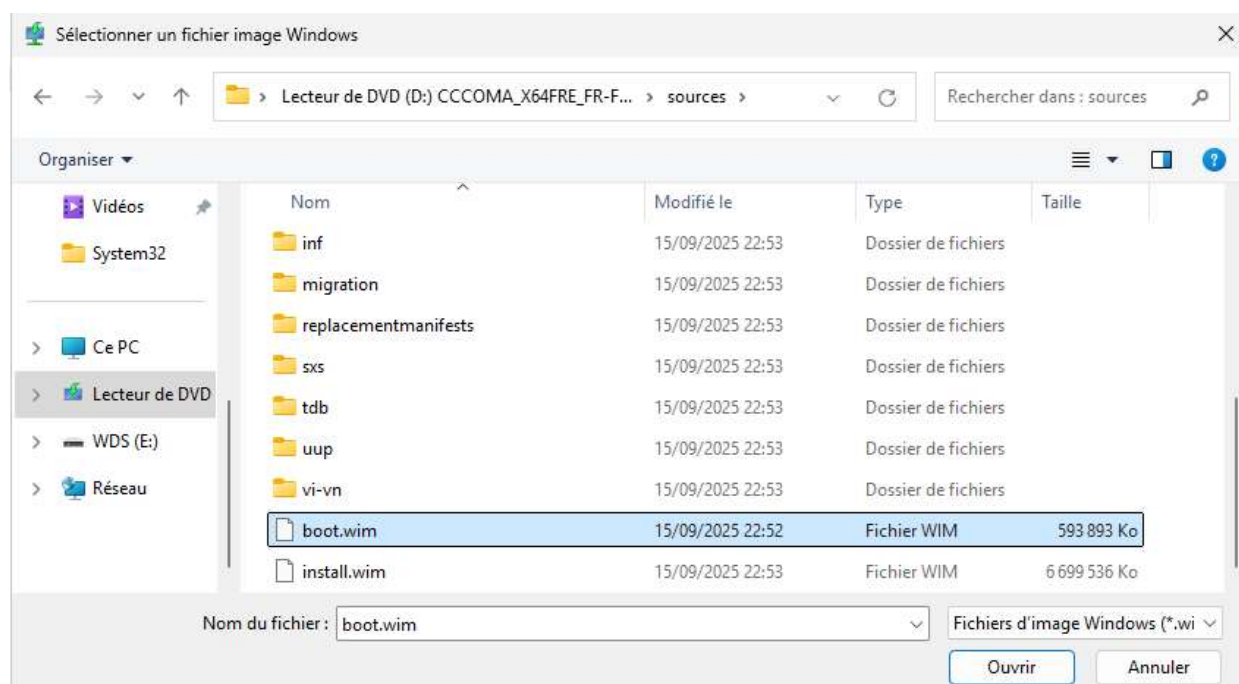
Message possible au premier démarrage : le service WDS a simplement mis du temps à répondre

3.1.9. Ajout des images de démarrage et d'installation

Image de démarrage. C'est le mini-Windows (WinPE) chargé par le poste en PXE. On la récupère directement sur l'ISO de Windows 11 : clic droit sur Images de démarrage > Ajouter une image de démarrage..., puis on pointe le fichier boot.wim du dossier sources du DVD.

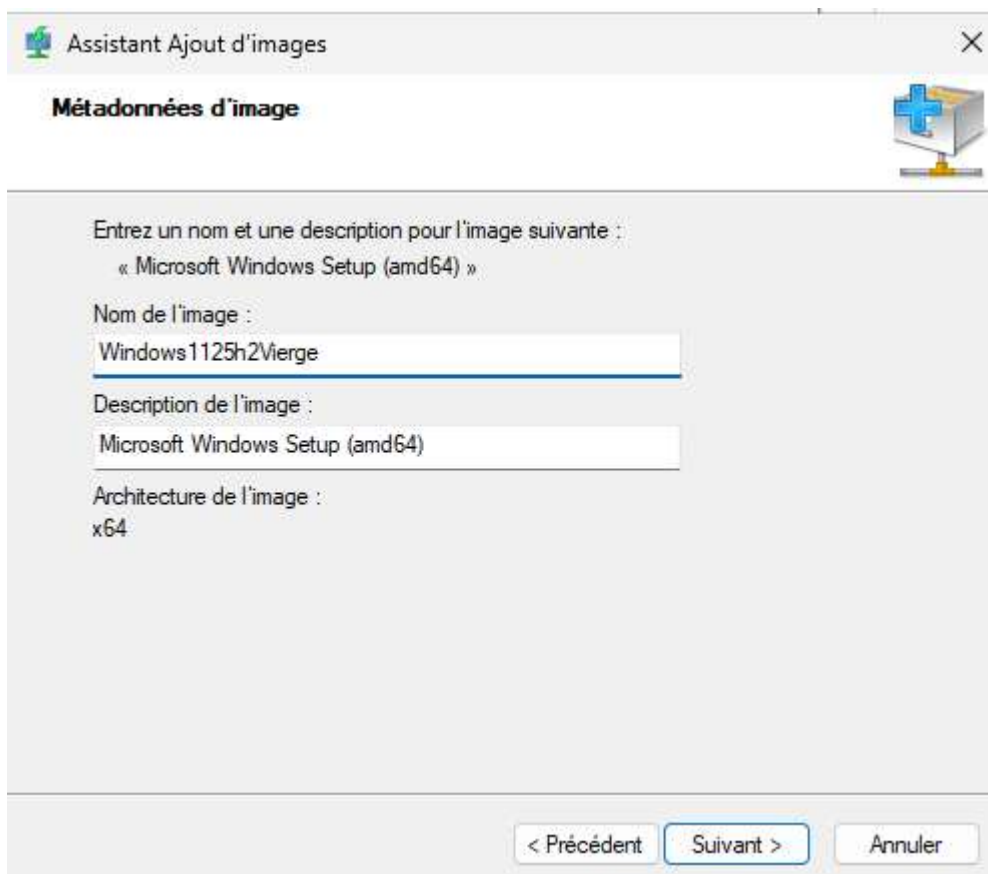


Console WDS : Ajouter une image de démarrage...



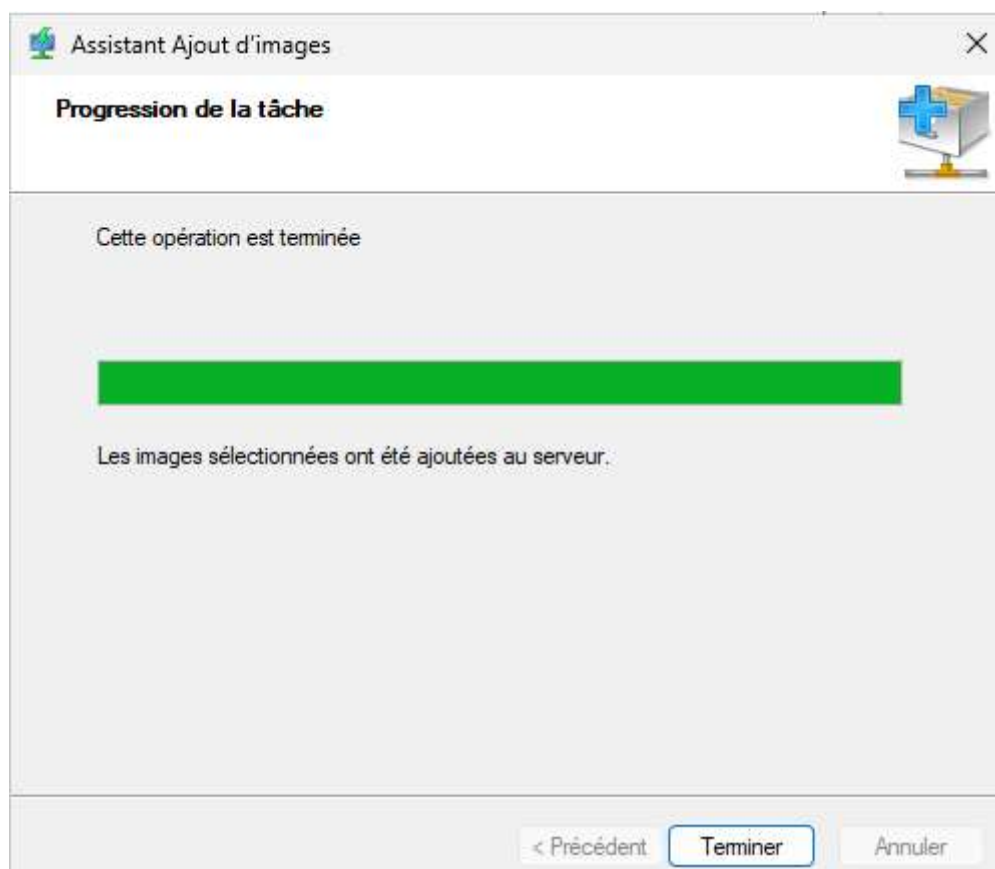
Sélection du fichier boot.wim dans le dossier sources de l'ISO Windows 11

On nomme l'image de façon parlante — ici Windows1125h2Vierge — pour la retrouver facilement quand plusieurs images cohabiteront.



The screenshot shows a Windows-style dialog box titled 'Assistant Ajout d'images'. The main heading is 'Métadonnées d'image'. Below it, the text reads: 'Entrez un nom et une description pour l'image suivante : « Microsoft Windows Setup (amd64) »'. There are three input fields: 'Nom de l'image :' with the value 'Windows1125h2Vierge', 'Description de l'image :' with the value 'Microsoft Windows Setup (amd64)', and 'Architecture de l'image :' with the value 'x64'. At the bottom right, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.

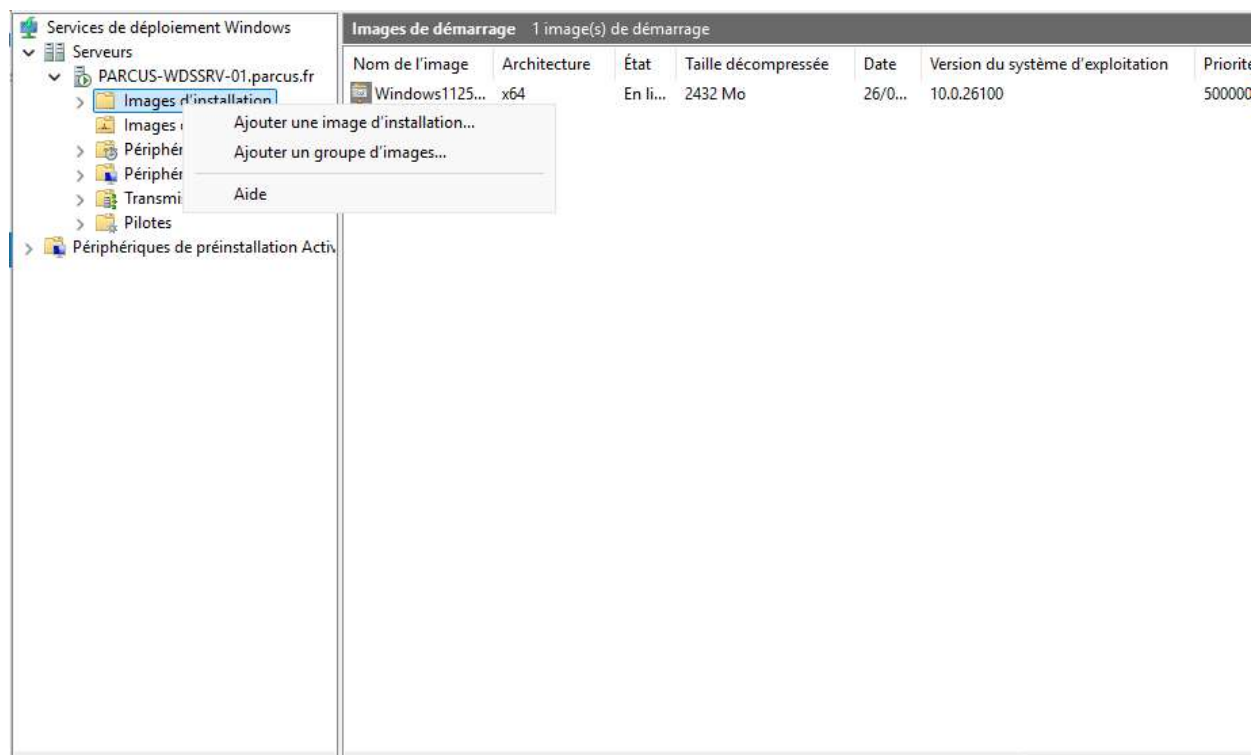
Métadonnées de l'image de démarrage : nom Windows1125h2Vierge, architecture x64



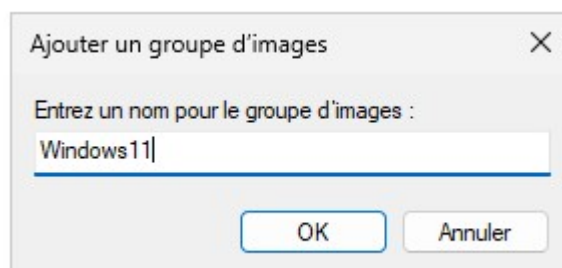
The screenshot shows the same dialog box, now at the 'Progression de la tâche' step. The text reads: 'Cette opération est terminée'. Below this is a solid green progress bar. Further down, it says: 'Les images sélectionnées ont été ajoutées au serveur.' At the bottom right, the buttons are '< Précédent', 'Terminer', and 'Annuler'.

L'image de démarrage est ajoutée au serveur

Image d'installation. C'est le Windows complet qui sera déployé. On crée d'abord un groupe d'images (clic droit sur Images d'installation > Ajouter un groupe d'images) nommé Windows11, pour classer les images par système.

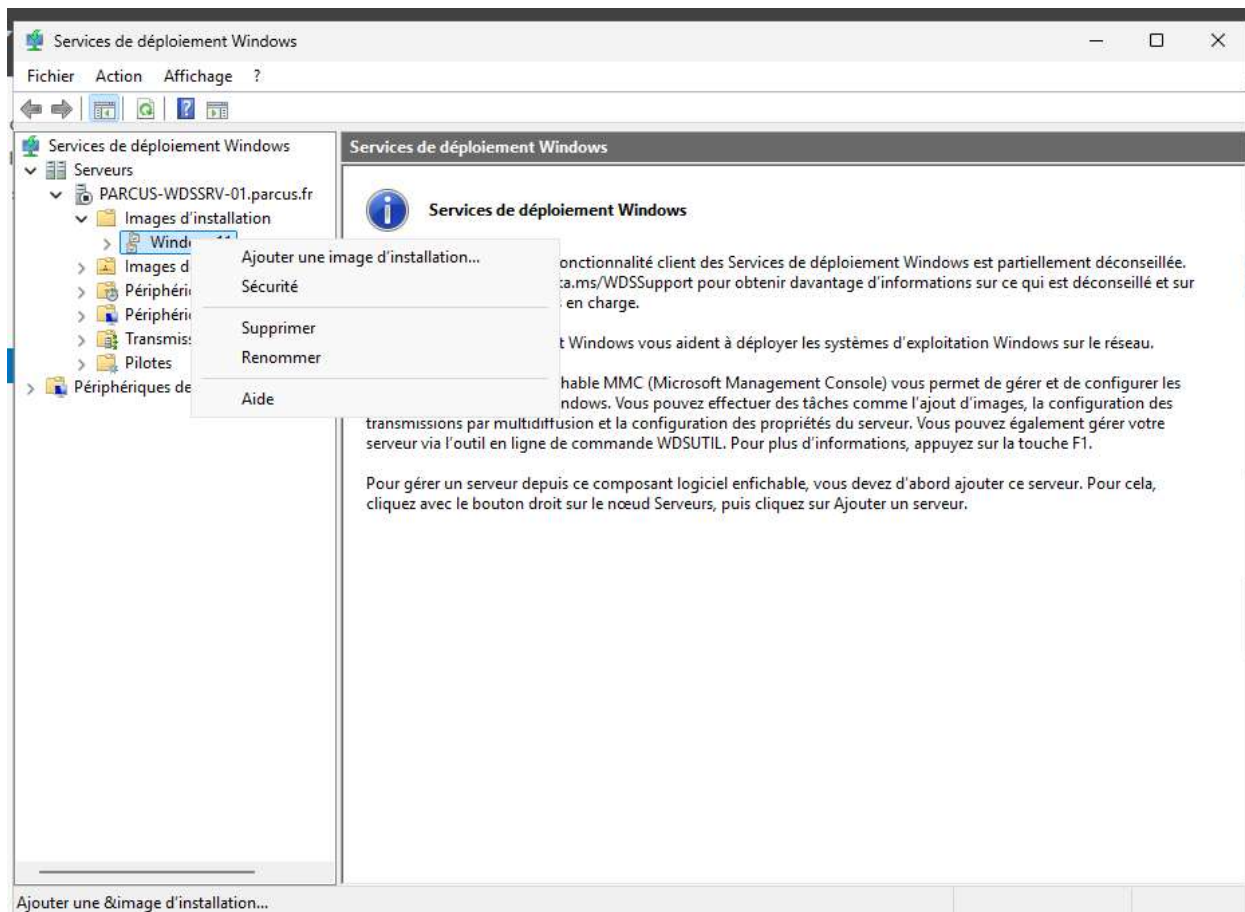


Clic droit sur Images d'installation : ajout d'un groupe d'images

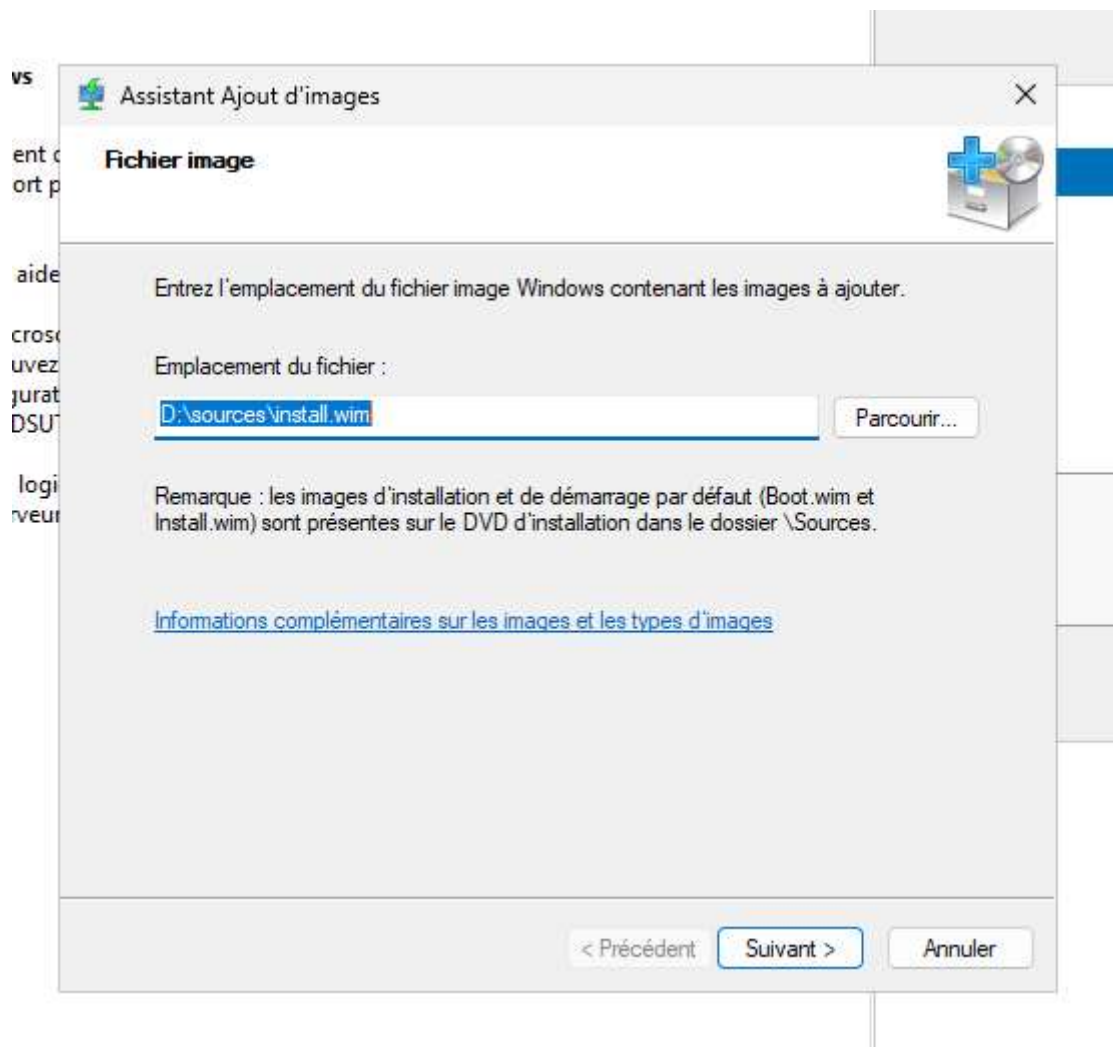


Création du groupe d'images « Windows11 »

On ajoute ensuite l'image d'installation en pointant le fichier install.wim du même ISO.

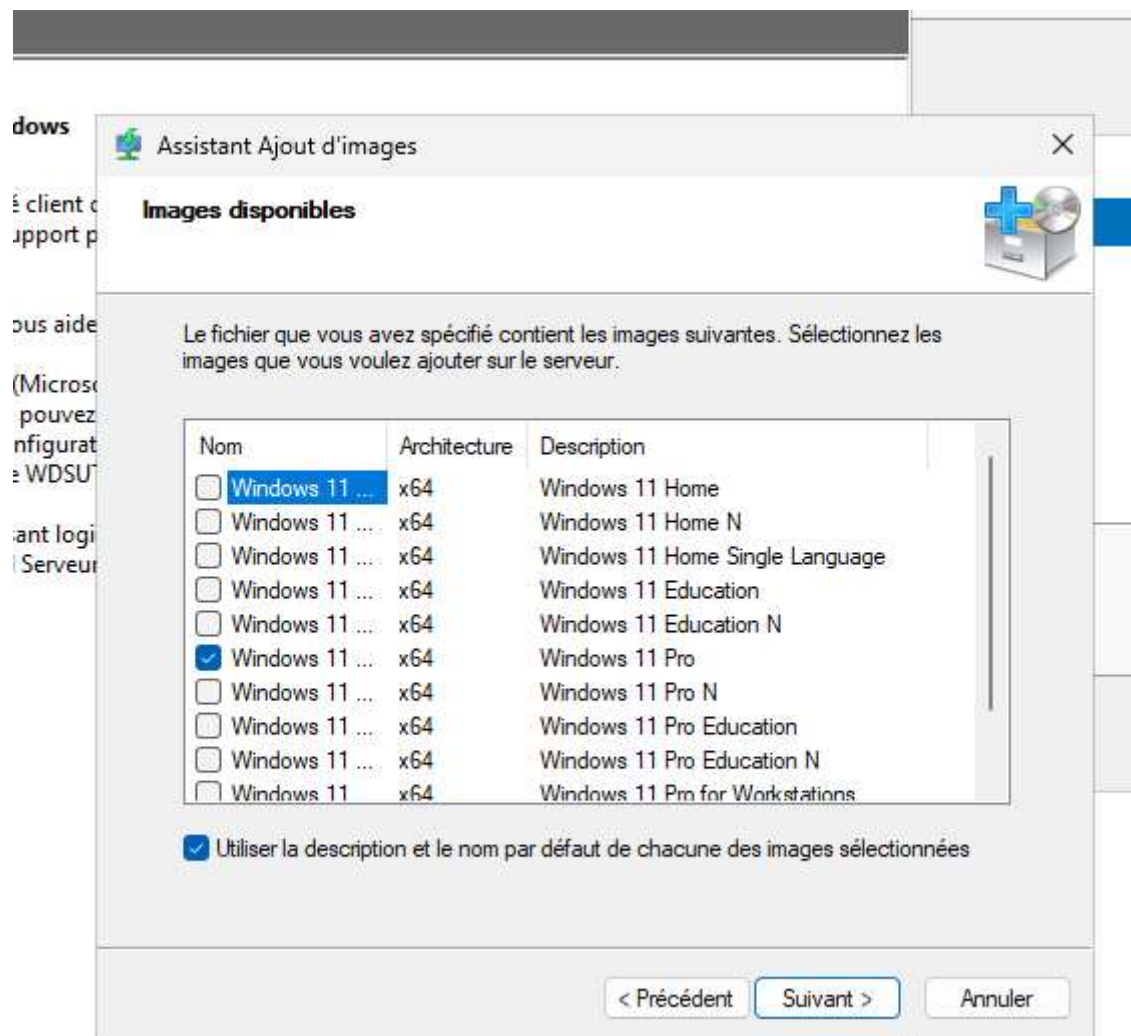


Ajout d'une image d'installation dans le groupe

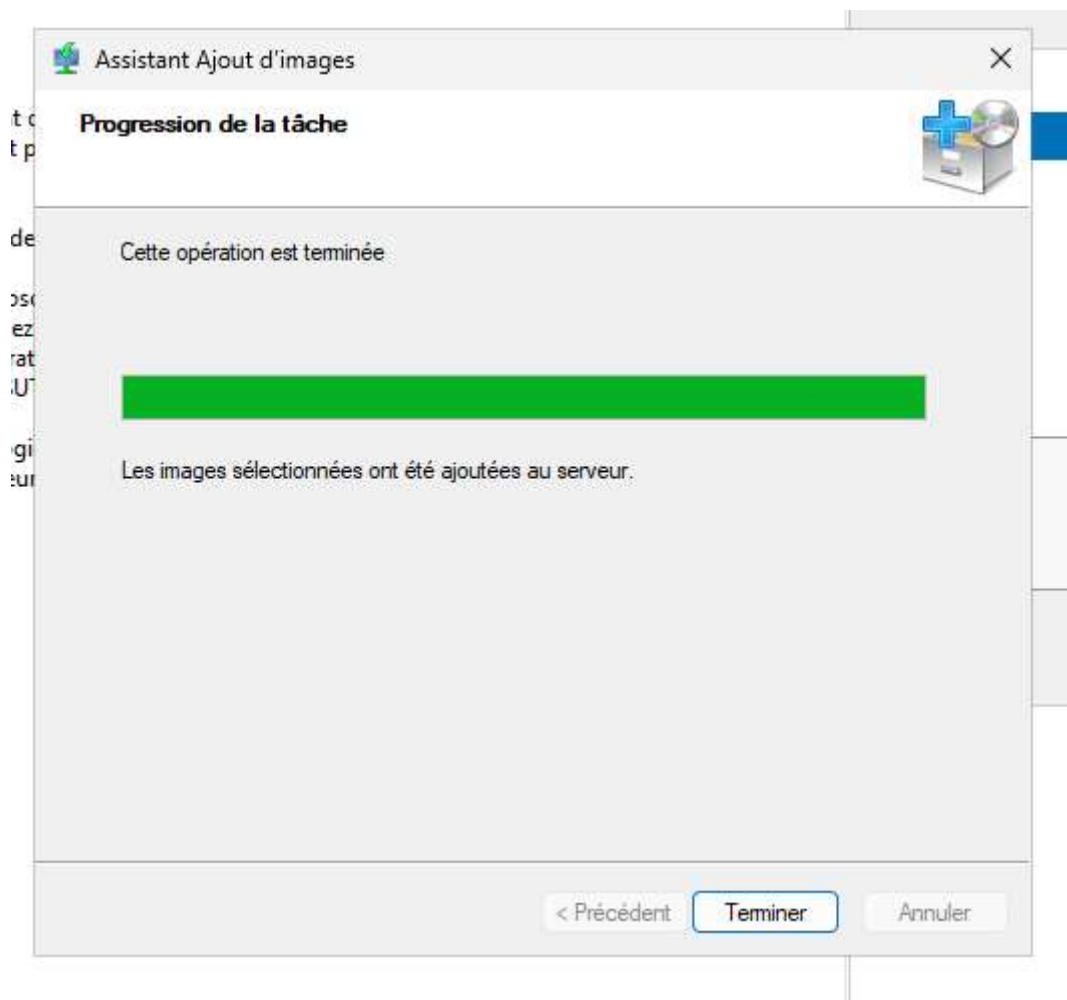


Emplacement du fichier : D:\sources\install.wim

Le fichier install.wim contient toutes les éditions de Windows 11 : on ne coche que Windows 11 Pro, la seule utilisée sur le parc (il faut une édition Pro pour joindre le domaine).



Sélection de l'édition Windows 11 Pro dans le fichier install.wim



L'image d'installation est ajoutée au serveur : le WDS est prêt à déployer

Le serveur est maintenant capable de déployer un Windows 11 Pro vierge sur n'importe quel poste qui démarre en PXE. La création d'une image personnalisée (postes déjà configurés) est traitée côté exploitation, en 3.3.2.

3.1.10. Mise en place du second serveur (PARCUS-WDSSRV-02)

Pour ne pas dépendre d'une seule machine, un second serveur Windows Server 2025 est installé puis joint au domaine : PARCUS-WDSSRV-02, en 192.168.137.2. Il recevra trois rôles : DNS (zone secondaire), DHCP (basculément) et AD CS (autorité de certification). La préparation est identique à celle du premier serveur : nom fixé, adresse statique.

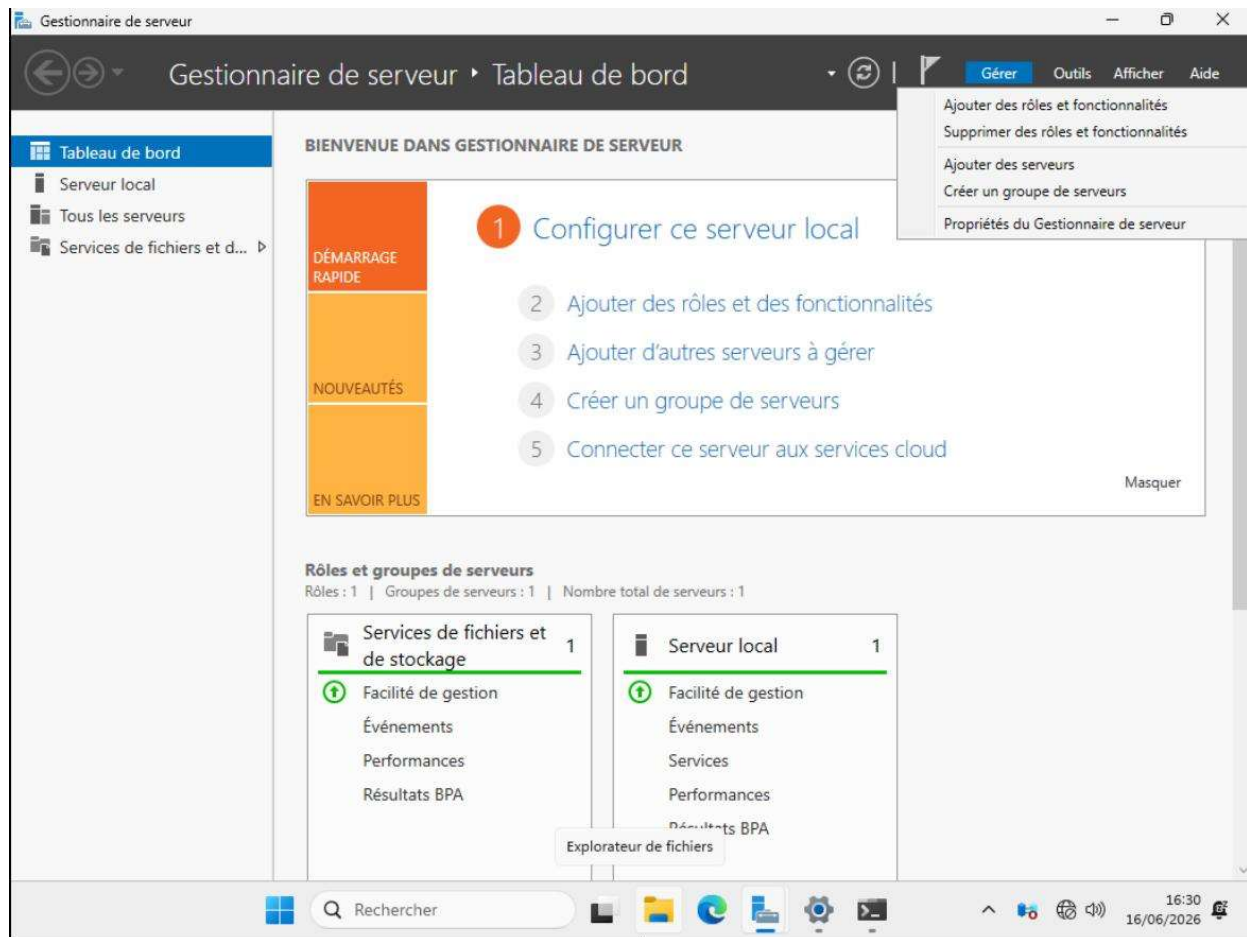
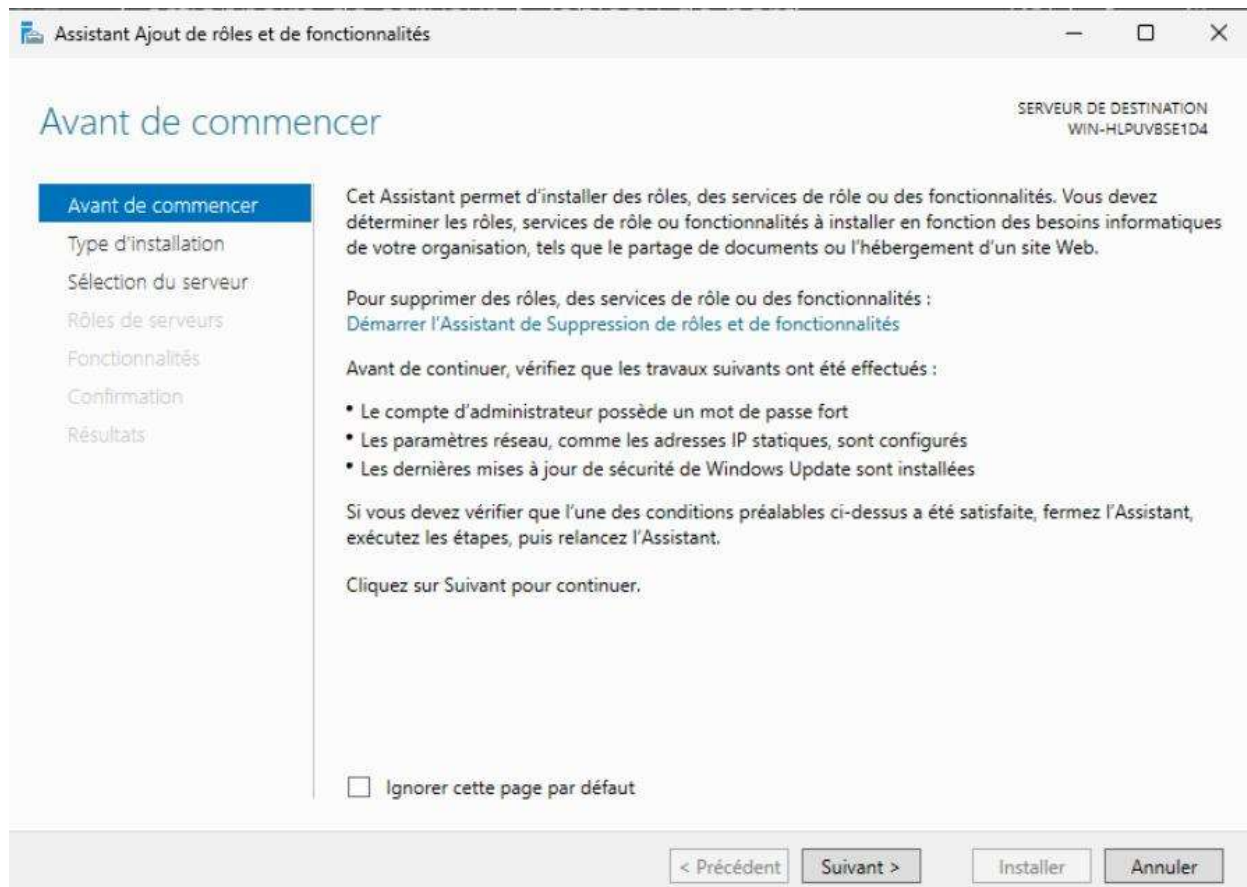
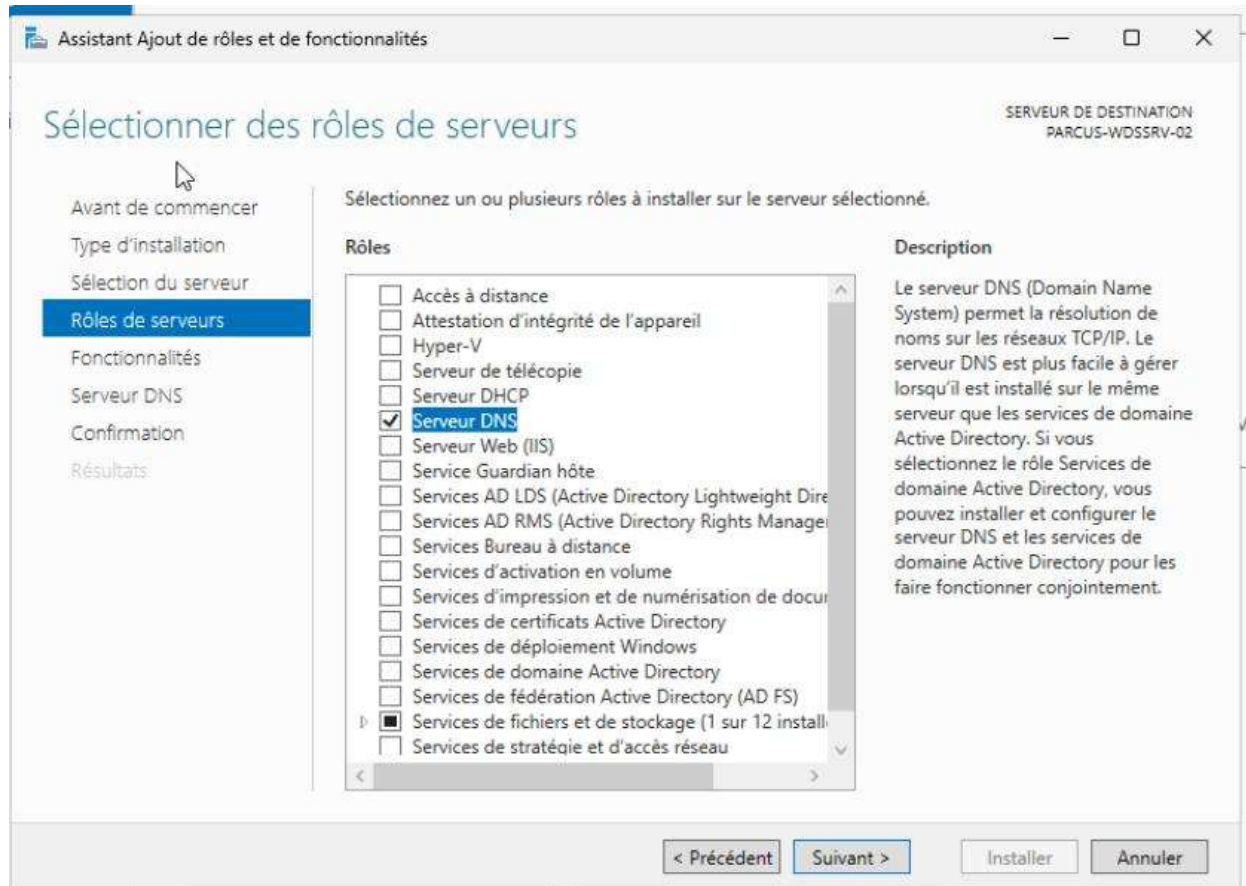


Tableau de bord du second serveur : menu Gérer > Ajouter des rôles et fonctionnalités

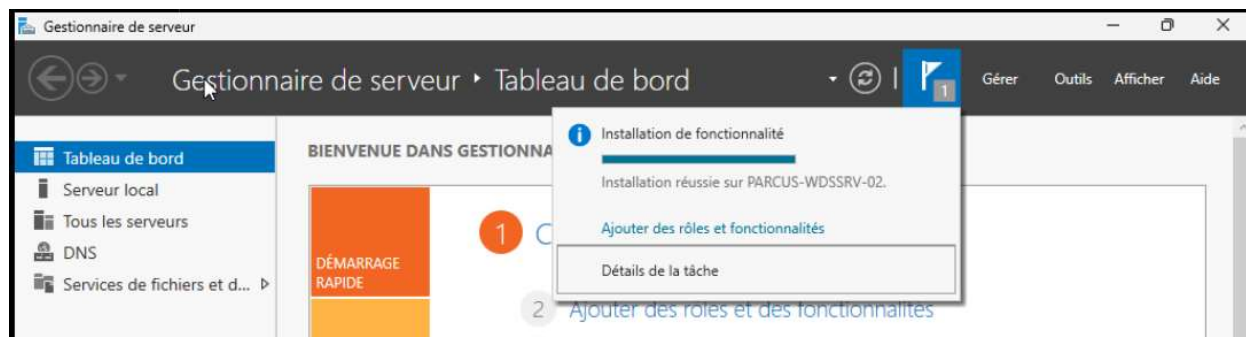


Assistant d'ajout de rôles sur le second serveur (encore sous son nom d'origine)

On installe d'abord le rôle Serveur DNS seul :

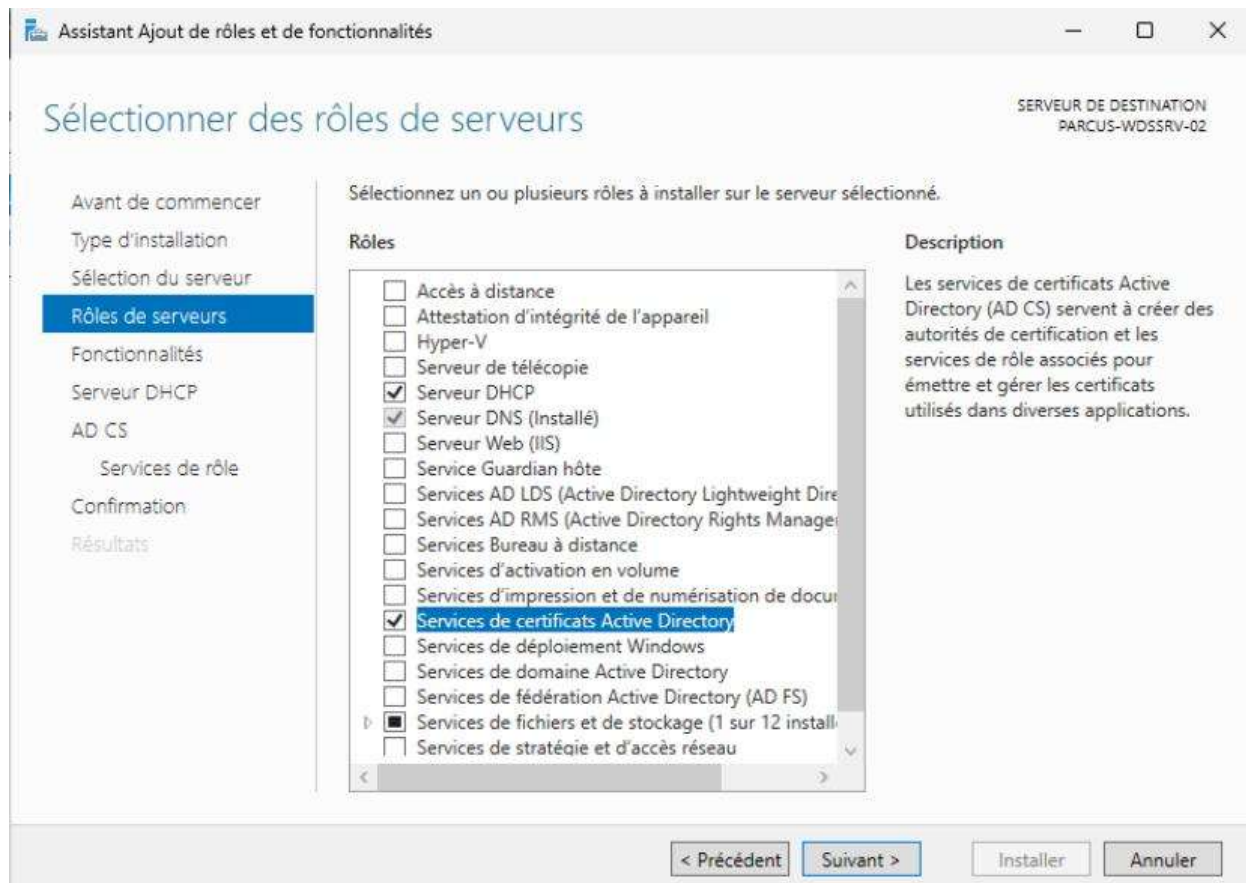


Sélection du rôle Serveur DNS sur PARCUS-WDSSRV-02

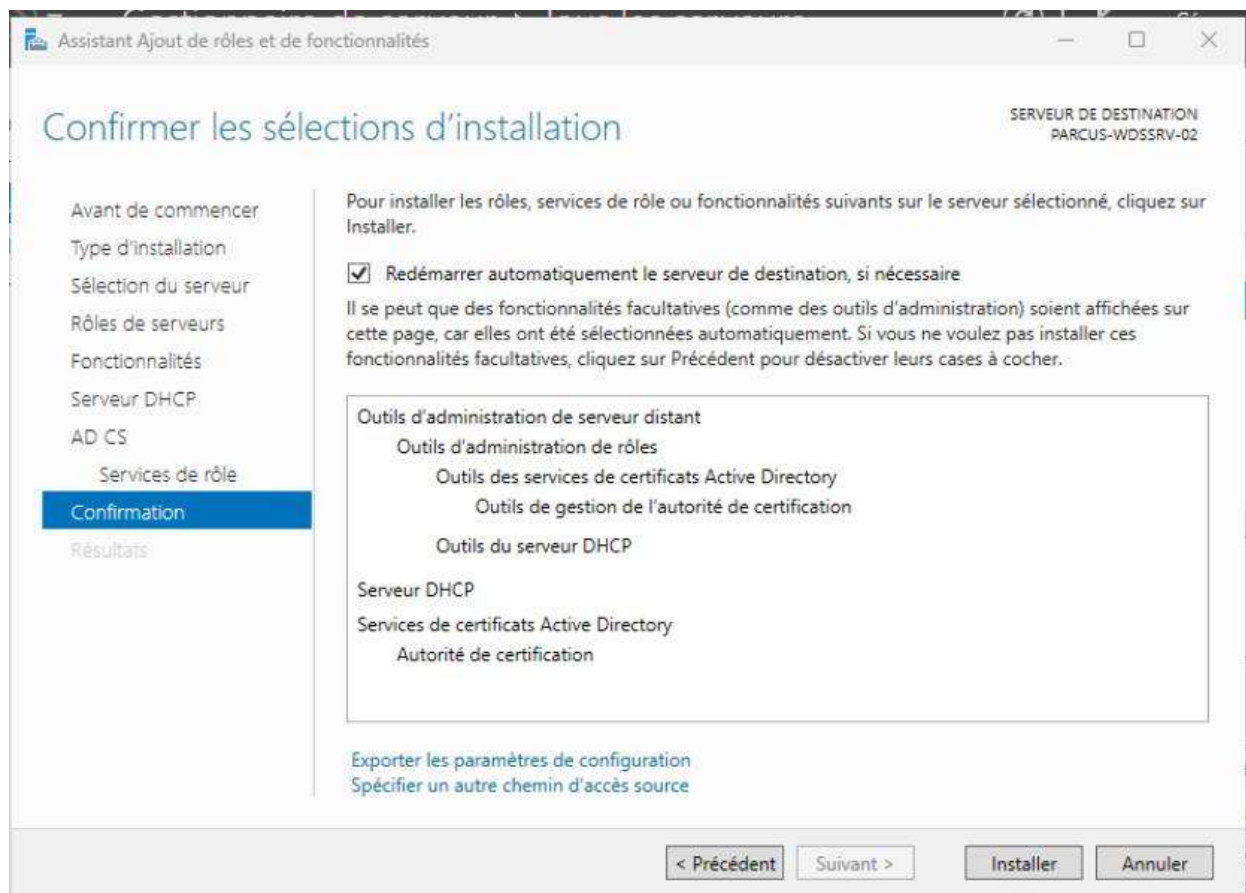


Installation du rôle DNS réussie sur PARCUS-WDSSRV-02

Puis, dans un second passage, les rôles Serveur DHCP et Services de certificats Active Directory (AD CS) avec le service de rôle Autorité de certification :



Sélection des rôles Serveur DHCP et Services de certificats Active Directory



Confirmation : DHCP, AD CS (autorité de certification) et leurs outils d'administration

DNS croisés. Chaque serveur utilise l'autre comme DNS principal et lui-même (127.0.0.1) en auxiliaire : si l'un des deux tombe, l'autre continue de résoudre parcus.fr. C'est la configuration recommandée entre contrôleurs/serveurs DNS d'un même domaine.



PARCUS-WDSSRV-02 (192.168.137.2) : DNS préféré 192.168.137.1, auxiliaire 127.0.0.1



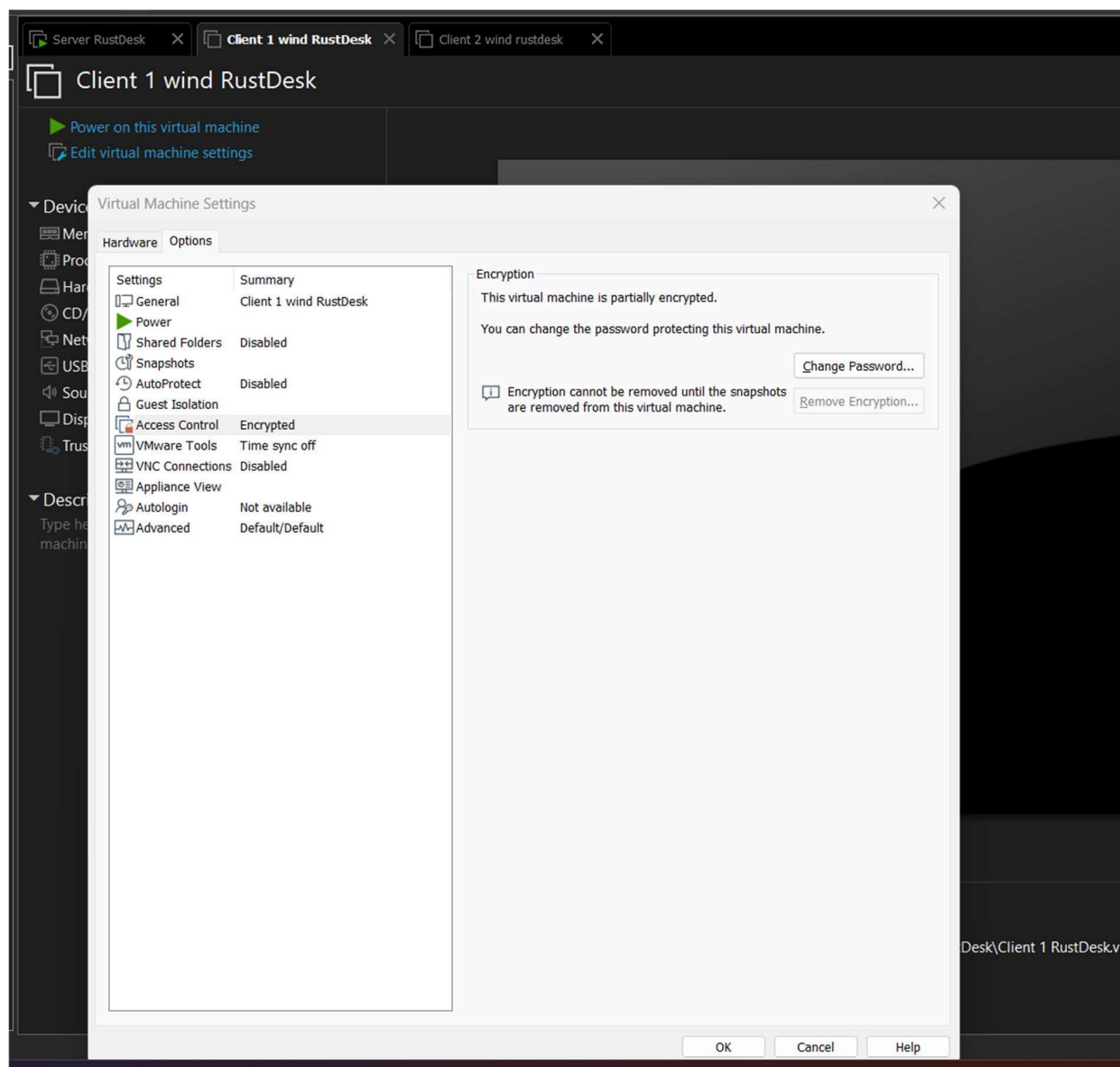
PARCUS-WDSSRV-01 (192.168.137.1) : DNS préféré 192.168.137.2, auxiliaire 127.0.0.1

La configuration proprement dite de la zone secondaire, du basculement DHCP et de l'autorité de certification est détaillée dans la documentation d'exploitation (3.3.4 à 3.3.6).

3.1.11. Préparation des postes pour BitLocker (TPM)

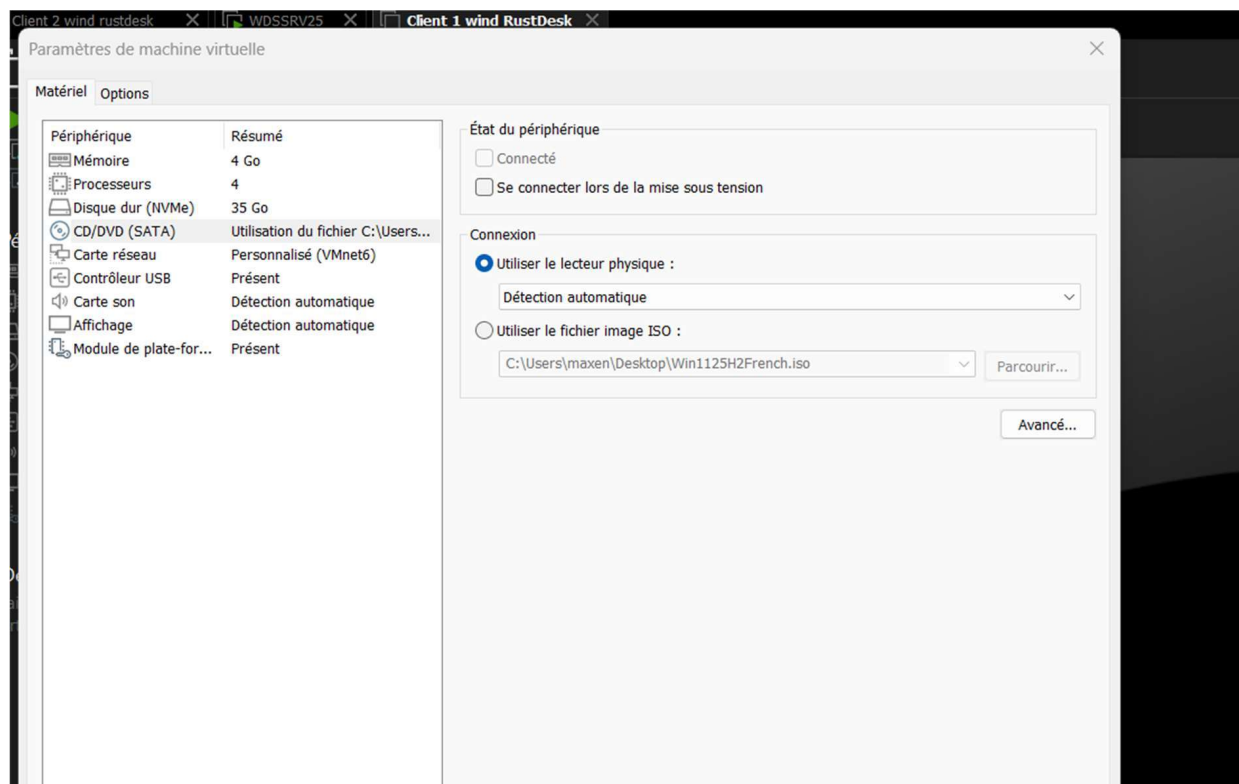
BitLocker chiffre l'intégralité du disque : en cas de vol du poste, les données sont illisibles sans la clé. Pour déverrouiller le disque au démarrage sans rien demander à l'utilisateur, BitLocker s'appuie sur la puce TPM (version 2.0) de la machine. Nos postes de test sont les deux clients Windows 11 du LOT 1 (DESKTOP-204Q3GM et DESKTOP-RIV61FL) : ce sont des VM VMware, il faut donc leur ajouter un TPM virtuel.

Chiffrer la VM. VMware n'accepte d'ajouter un module TPM virtuel que si la VM est elle-même chiffrée. Dans les paramètres de la machine, onglet Options > Access Control, on chiffre la VM (un chiffrement partiel, limité aux fichiers de configuration, suffit pour le TPM). À noter : ce chiffrement ne peut plus être retiré tant que des snapshots existent sur la VM.



Paramètres VMware du client 1 : la VM est chiffrée (Access Control : Encrypted), condition pour ajouter un TPM virtuel

Une fois la VM chiffrée, on ajoute le périphérique « Module de plateforme sécurisée » dans le matériel de la machine :

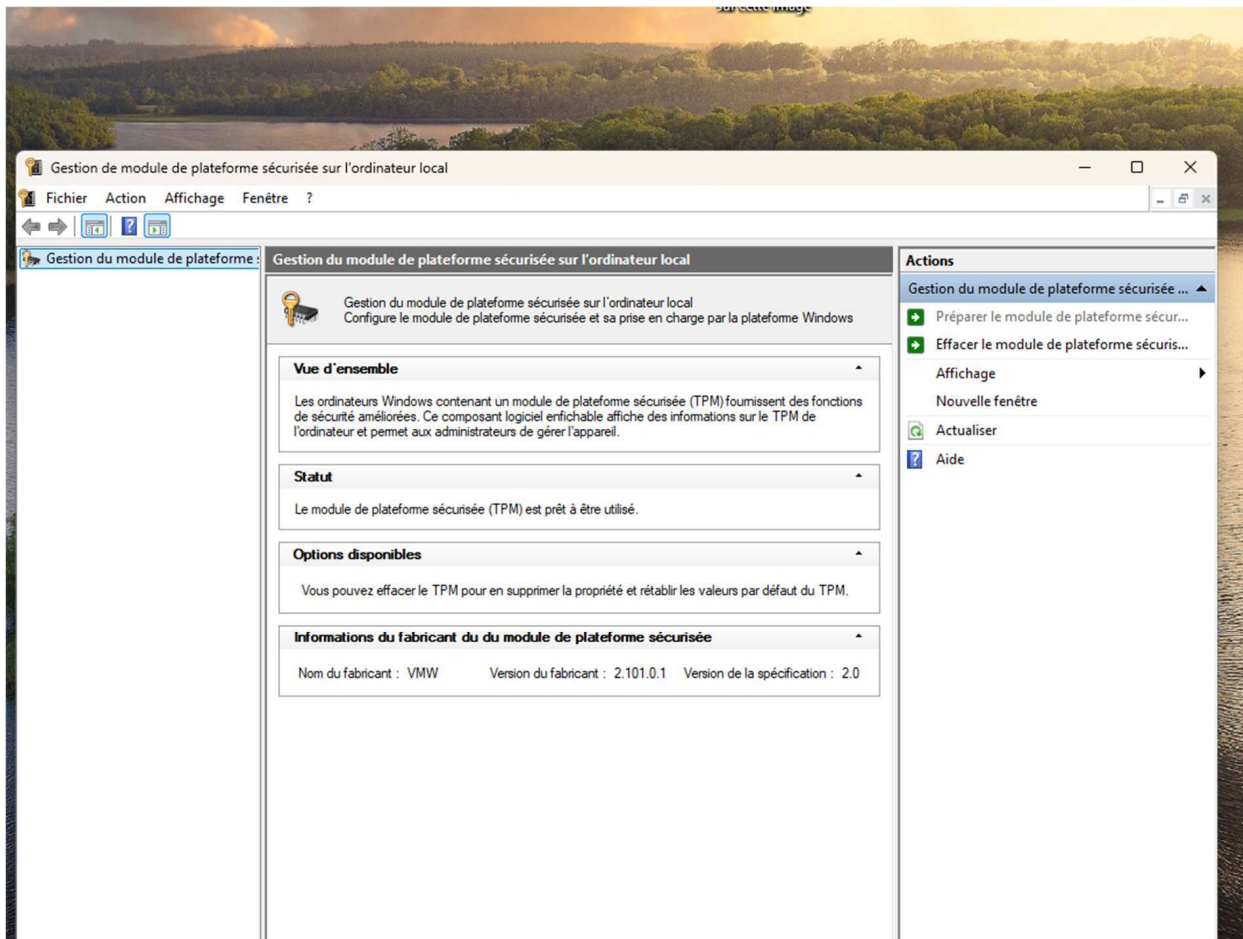


Matériel de la VM : le module de plateforme sécurisée (TPM virtuel) est « Présent »

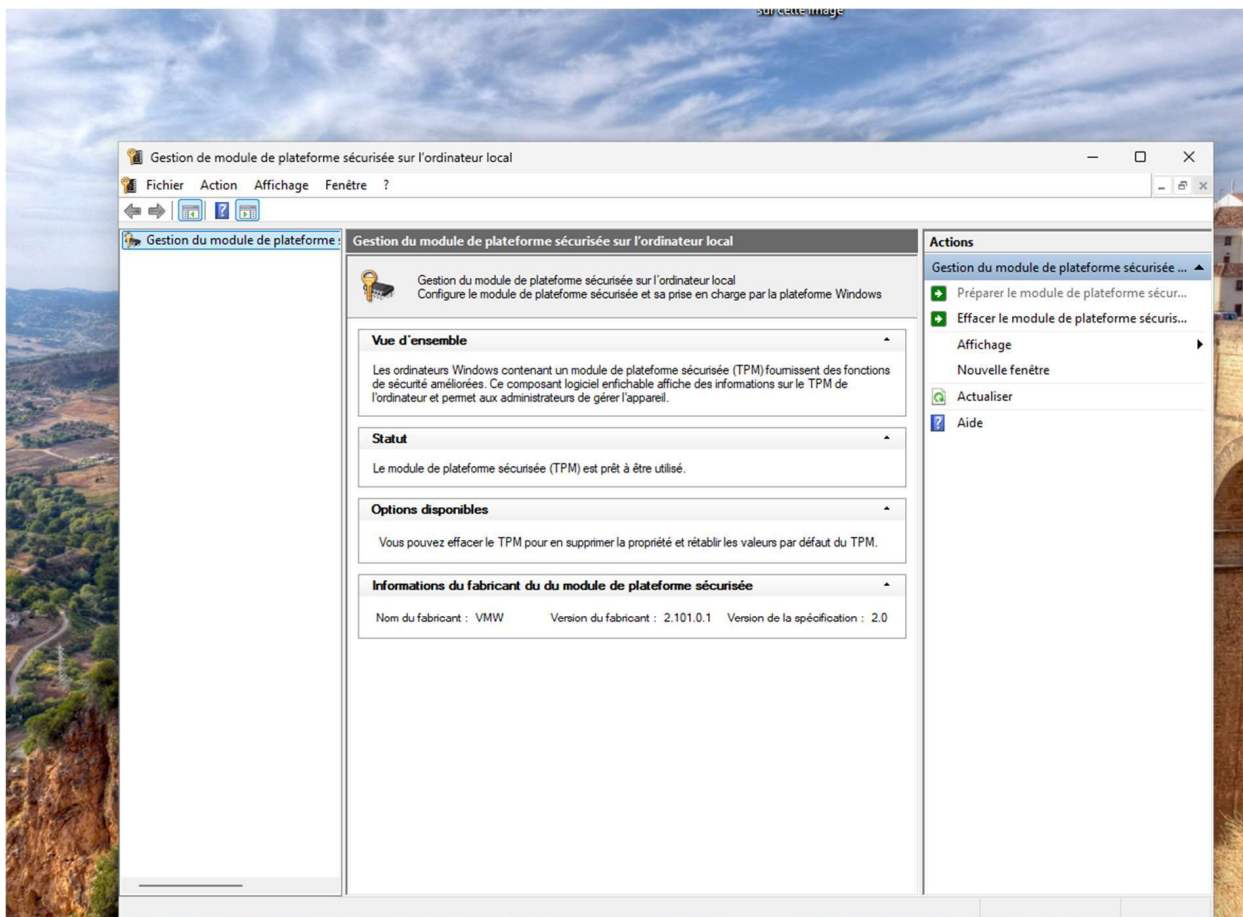
Vérifier le TPM côté Windows. Sur chaque client, la console de gestion du TPM s'ouvre avec :

```
tpm.msc
```

Le statut doit indiquer « Le module de plateforme sécurisée (TPM) est prêt à être utilisé », avec la spécification 2.0 (fabricant VMW puisqu'il s'agit du TPM virtuel de VMware). On fait la vérification sur les deux clients.



Client 1 : le TPM est prêt à être utilisé (fabricant VMW, spécification 2.0)

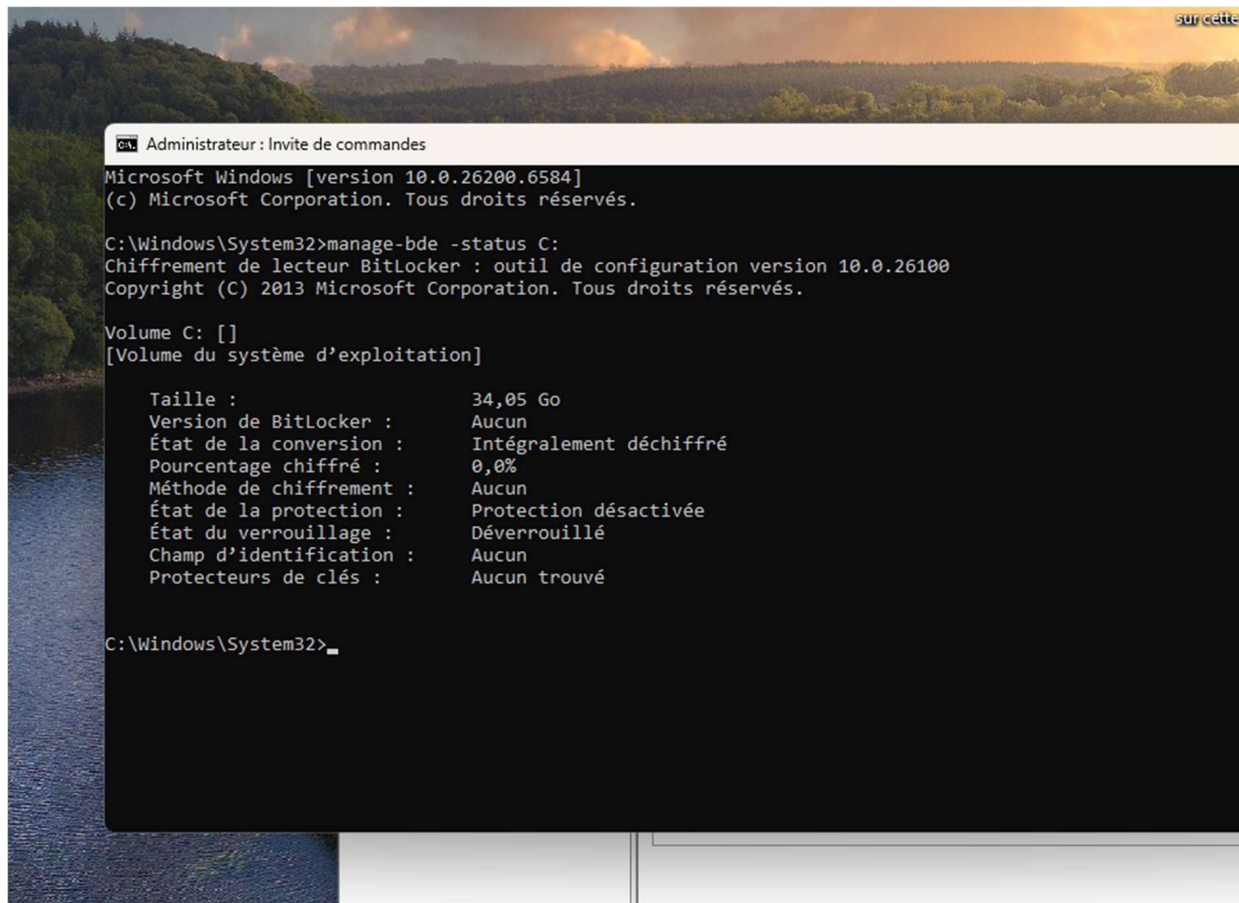


Client 2 : même vérification, le TPM virtuel est prêt

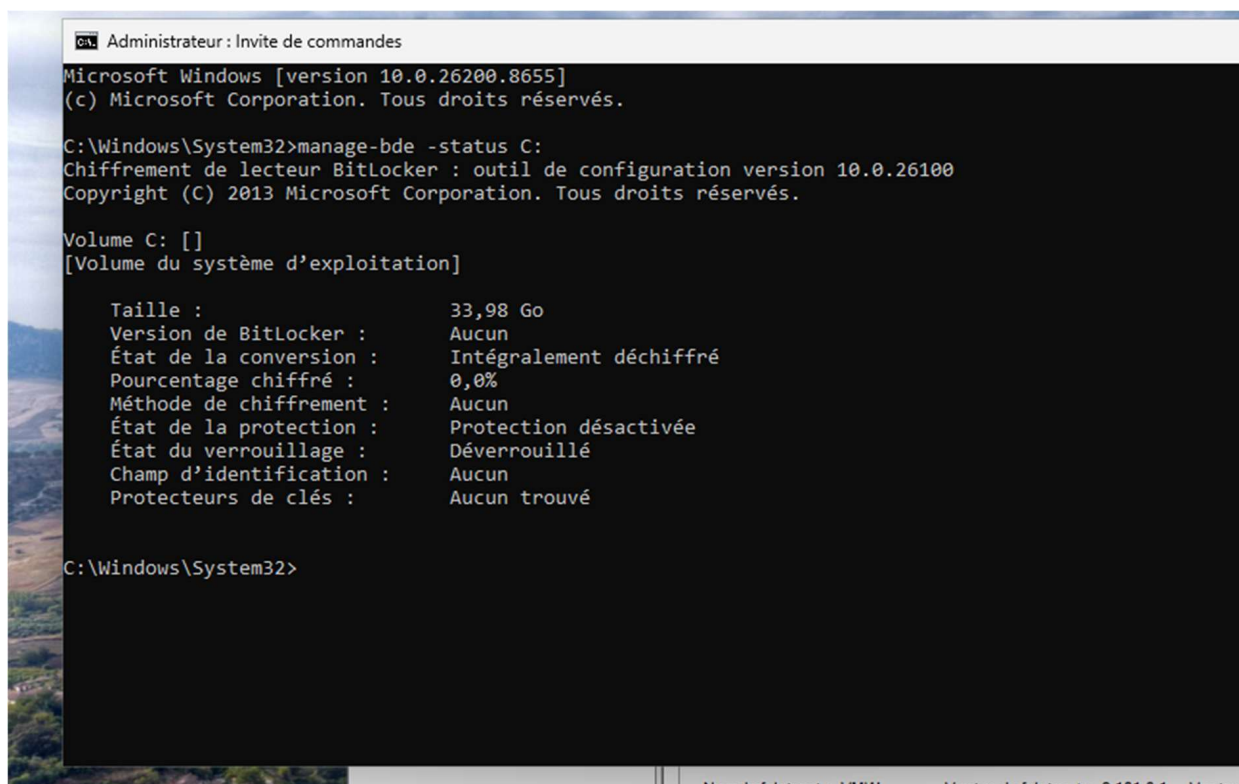
État initial de BitLocker. Avant toute configuration, on photographie l'état du lecteur système avec l'outil en ligne de commande de BitLocker :

```
manage-bde -status C:
```

Sur les deux postes, le constat est le même : aucune version de BitLocker, lecteur intégralement déchiffré (0,0 %), protection désactivée et aucun protecteur de clés. C'est notre point de départ.



Client 1 : lecteur C: intégralement déchiffré, aucun protecteur de clés



```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.26200.8655]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>manage-bde -status C:
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

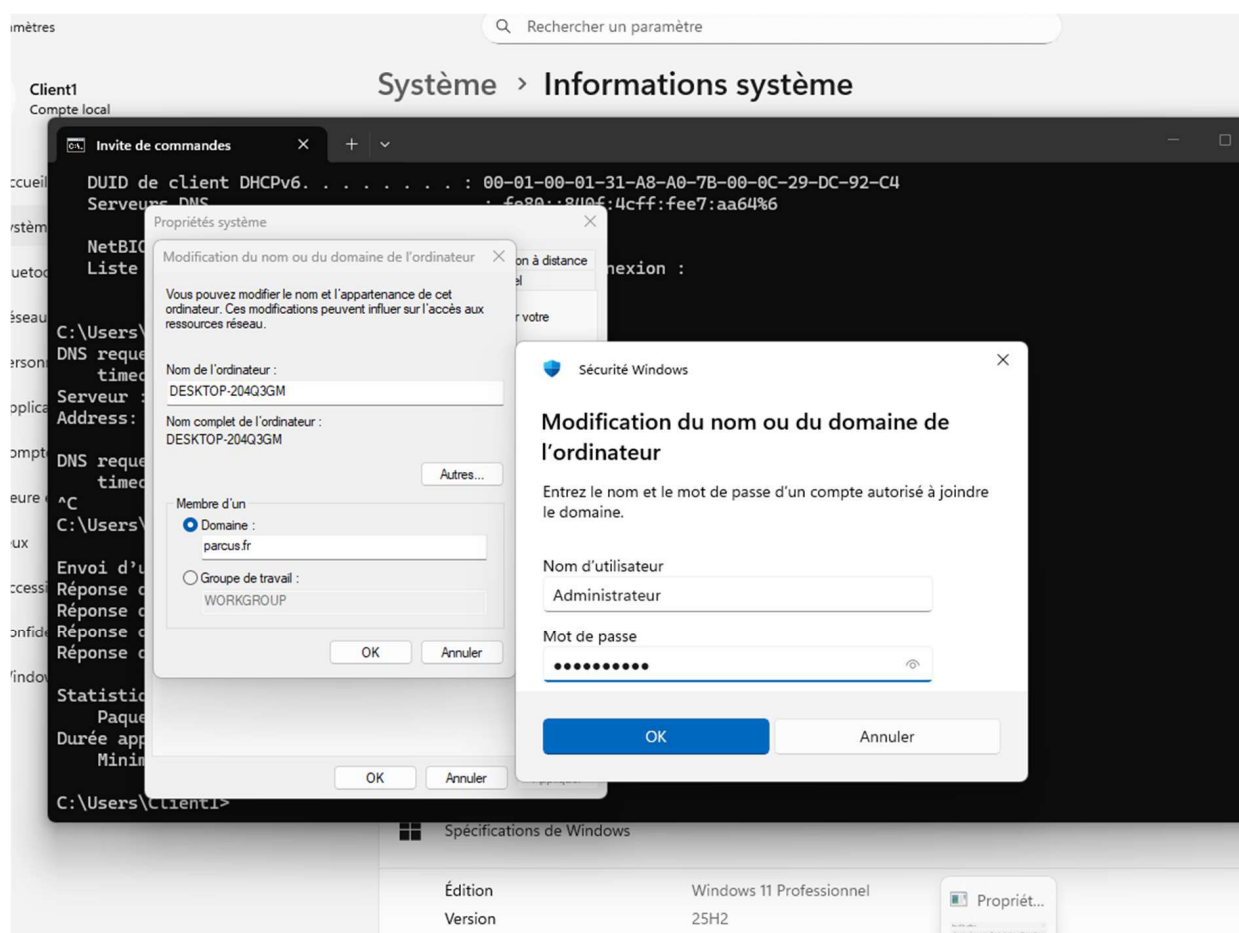
Volume C: [ ]
[Volume du système d'exploitation]

Taille : 33,98 Go
Version de BitLocker : Aucun
État de la conversion : Intégralement déchiffré
Pourcentage chiffré : 0,0%
Méthode de chiffrement : Aucun
État de la protection : Protection désactivée
État du verrouillage : Déverrouillé
Champ d'identification : Aucun
Protecteurs de clés : Aucun trouvé

C:\Windows\System32>
```

Client 2 : même état initial, BitLocker n'est pas encore utilisé

Jonction au domaine. Le chiffrement sera piloté par une GPO du domaine : les deux clients doivent donc être membres de parcus.fr. La procédure est identique à celle du poste VM-TEST2 (voir 3.1.7) : Propriétés système > Modifier, domaine parcus.fr, puis identifiants d'un compte autorisé et redémarrage.



Jonction du client 1 (DESKTOP-204Q3GM) au domaine parcus.fr, avec le compte Administrateur

3.2. Documentation utilisateur — ouvrir une session sur le domaine

Cette partie s'adresse aux salariés dont le poste a été intégré au domaine parcus.fr. Au quotidien, presque rien ne change : seules l'ouverture de session et quelques règles d'entreprise diffèrent d'un poste personnel.

- **Ouvrir sa session** : sur l'écran de connexion, saisissez l'identifiant fourni par le service informatique (par exemple PARCUS\prenom.nom ou prenom.nom@parcus.fr) et votre mot de passe. La première connexion peut prendre un peu plus de temps, le temps que Windows prépare votre profil.
- **Changer son mot de passe** : une fois connecté, appuyez sur Ctrl + Alt + Suppr puis choisissez « Modifier un mot de passe ». Le nouveau mot de passe doit respecter les règles de complexité du domaine.
- **Se connecter sur un autre poste** : votre compte fonctionne sur n'importe quel poste du domaine, avec les mêmes identifiants. En cas d'oubli du mot de passe, contactez le support (voir la documentation GLPI du LOT 2 pour créer un ticket) : un technicien le réinitialisera.
- **Fond d'écran d'entreprise** : le fond d'écran du Bureau est défini par l'entreprise et appliqué automatiquement à l'ouverture de session. Il n'est pas modifiable depuis les paramètres de personnalisation : c'est un comportement normal, pas une panne.
- **Poste chiffré (BitLocker)** : le disque de votre poste est chiffré automatiquement par l'entreprise. Au quotidien, c'est invisible : le poste démarre et s'utilise normalement. Si un écran bleu BitLocker vous demande un jour une « clé de récupération » au démarrage (après un changement de matériel par exemple), ne cherchez pas à la deviner : contactez le support, qui la retrouvera dans l'annuaire de l'entreprise.

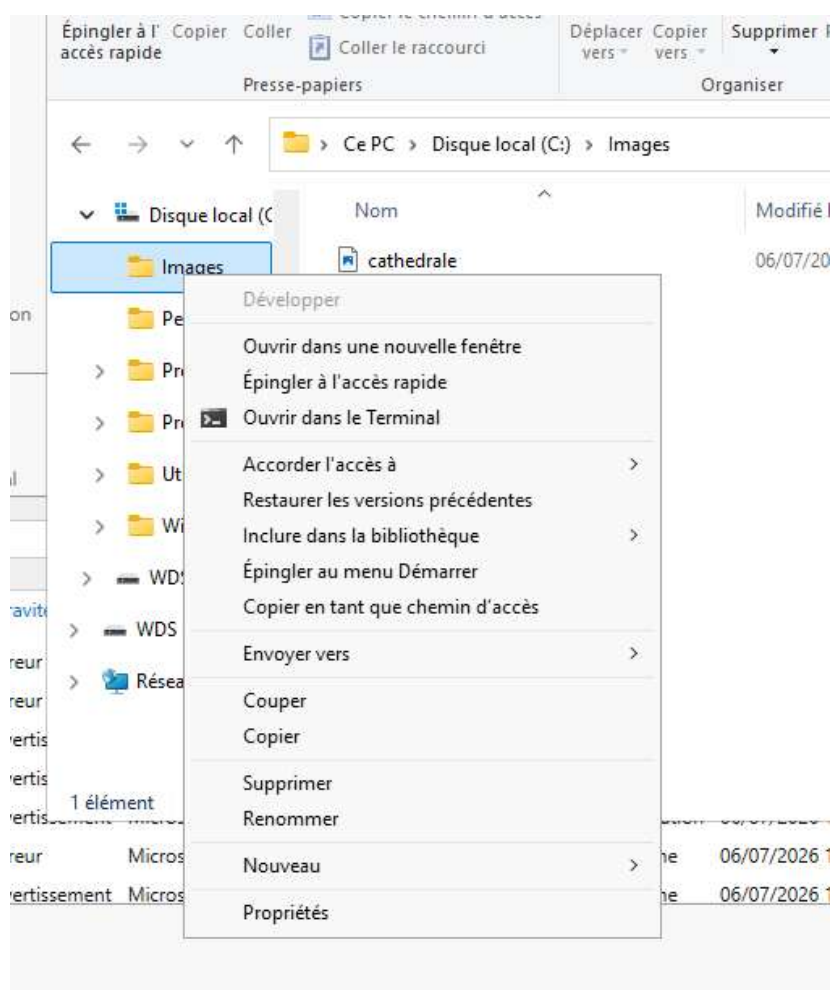
- **Poste hors réseau** : si le poste affiche « Aucun serveur de connexion disponible », il n'arrive pas à joindre le serveur (câble débranché, réseau en panne). Vérifiez le branchement réseau puis réessayez ; si le problème persiste, prévenez le support.

3.3. Documentation d'exploitation (technicien) — GPO, images WDS, BitLocker et redondance

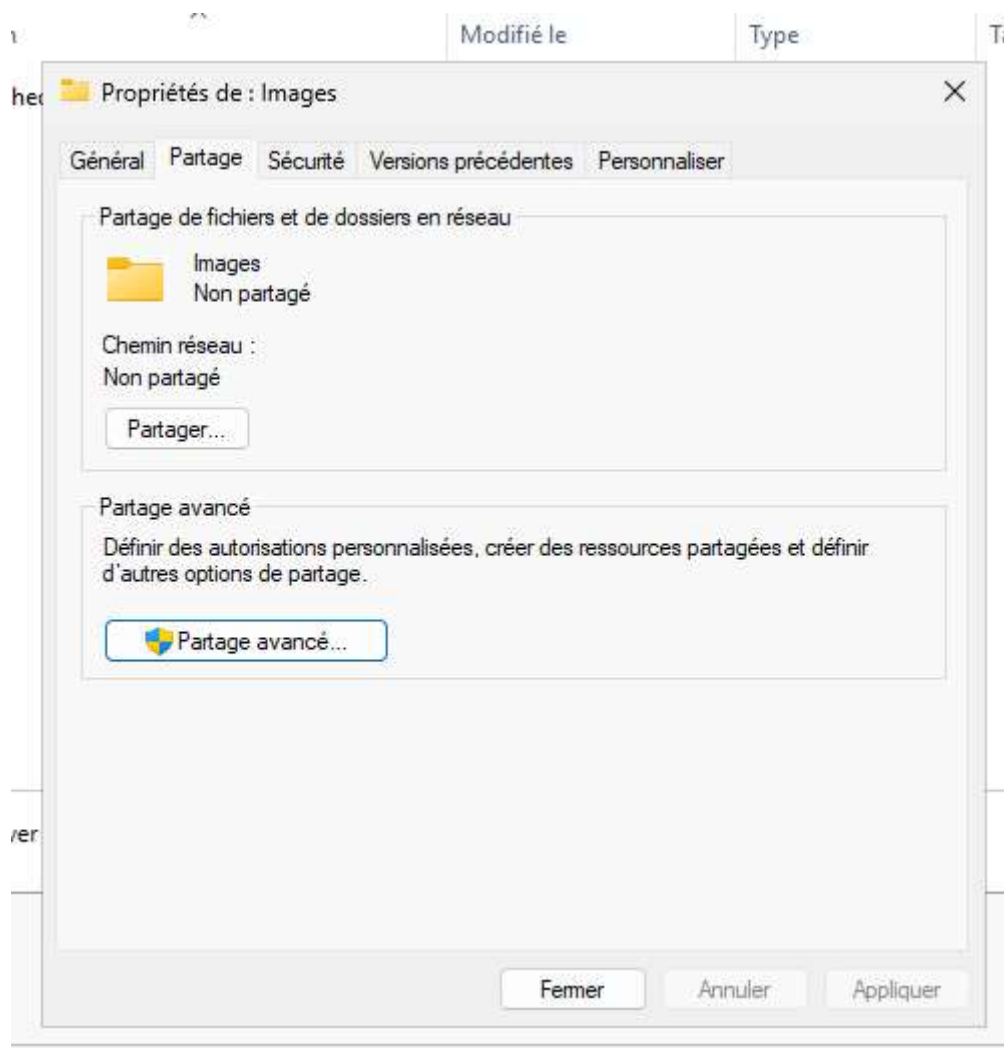
3.3.1. Déployer un fond d'écran par GPO

Objectif : imposer le même fond d'écran de Bureau à tous les utilisateurs du domaine, via une stratégie de groupe (GPO). Le principe se réutilise ensuite pour n'importe quel réglage d'entreprise. Deux étapes : partager l'image sur le réseau, puis créer et lier la GPO.

Étape 1 — partager l'image. L'image doit être lisible par tous les postes : on la place dans un dossier C:\Images du serveur (ici une photo de la cathédrale) et on partage ce dossier en lecture seule.

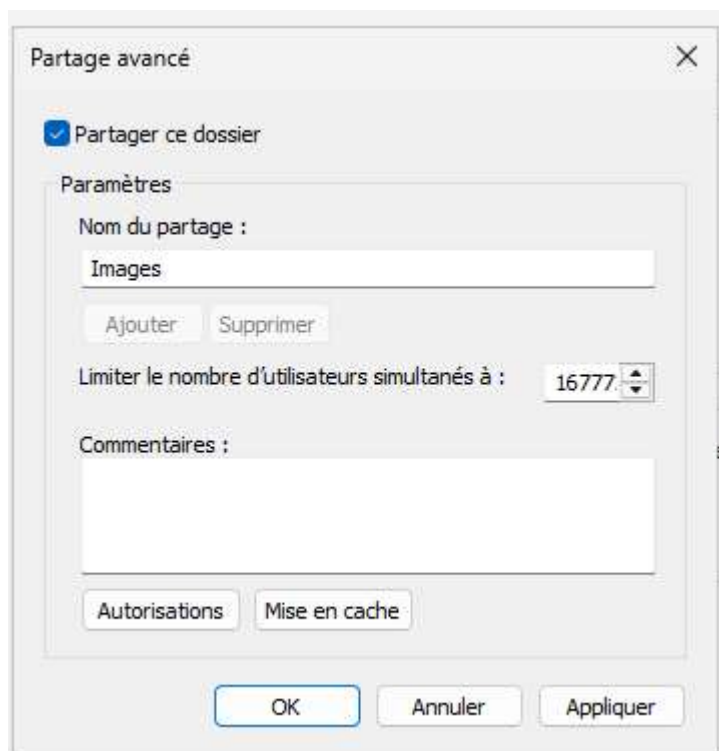


Le dossier C:\Images du serveur contient l'image du fond d'écran ; clic droit > Propriétés

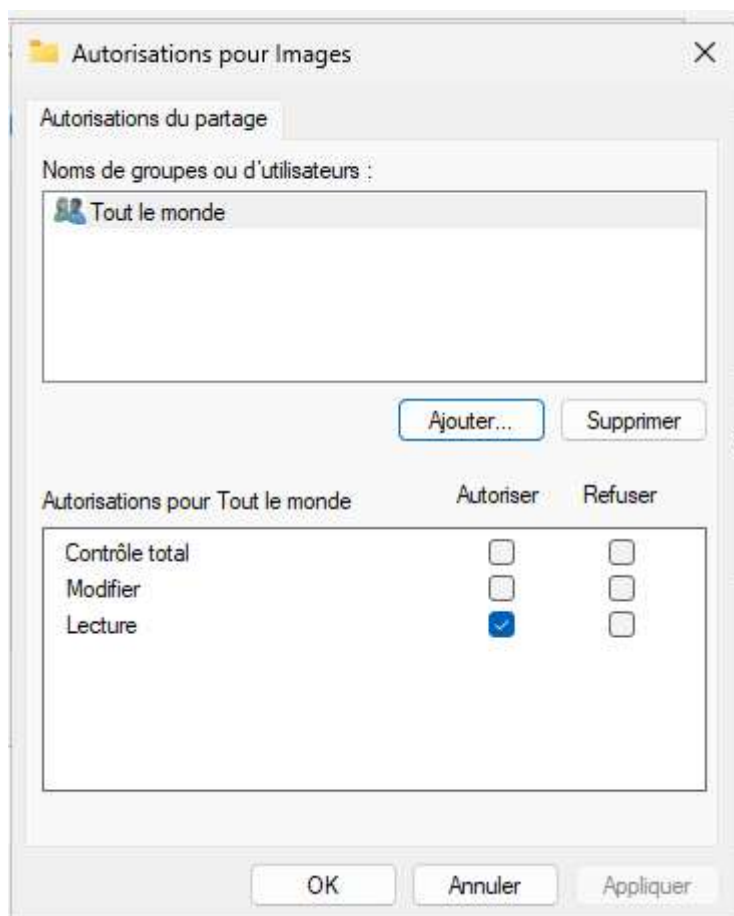


Onglet Partage des propriétés du dossier : le dossier n'est pas encore partagé

Dans Partage avancé..., on coche « Partager ce dossier » en gardant le nom de partage Images, puis dans Autorisations on laisse uniquement Lecture au groupe Tout le monde : les postes doivent pouvoir lire l'image, certainement pas la modifier.

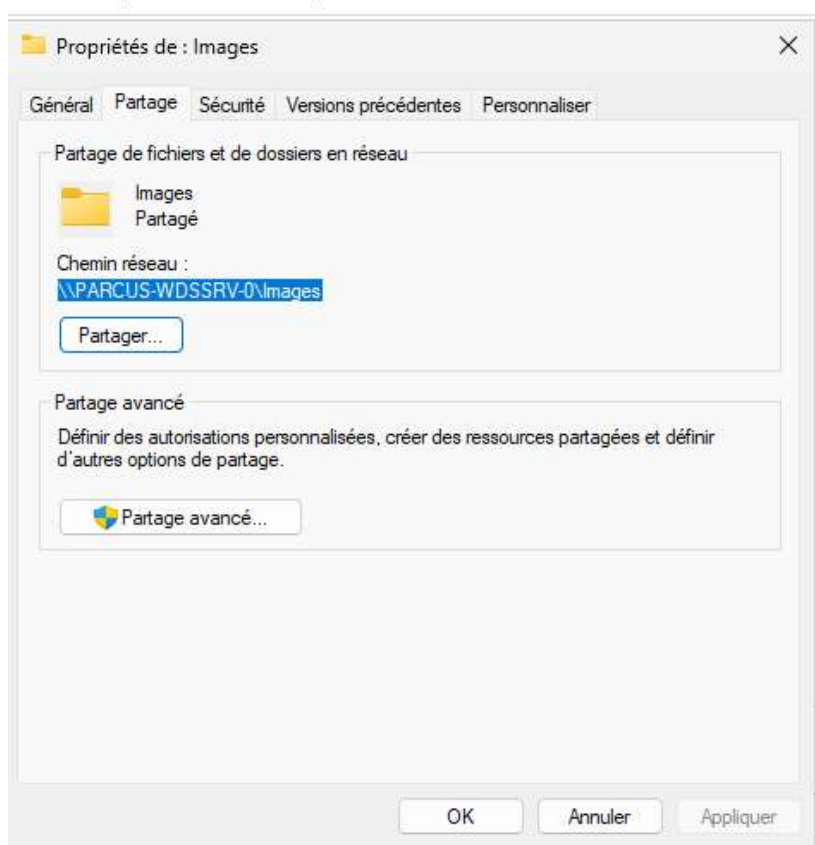


Partage avancé : partage du dossier sous le nom « Images »



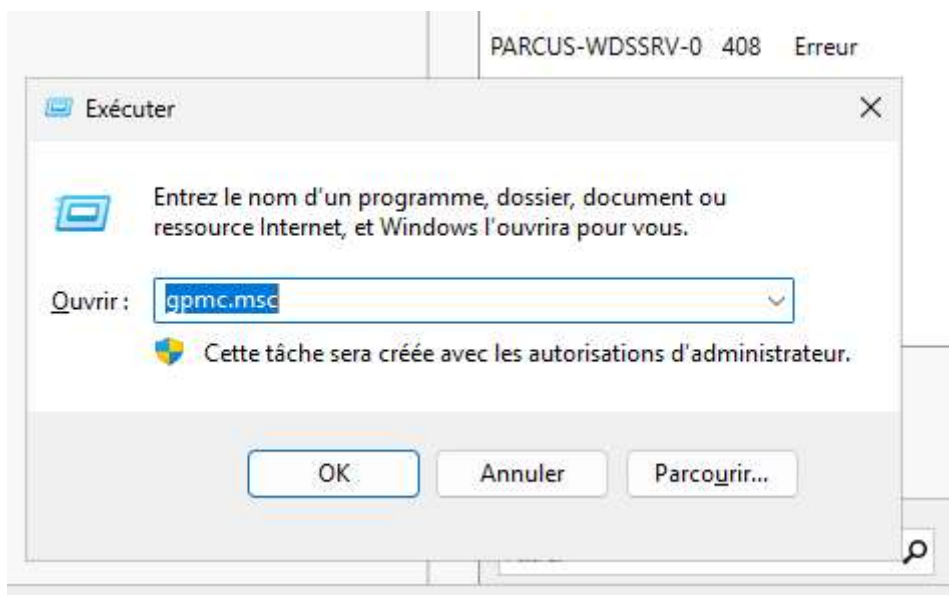
Autorisations du partage : Tout le monde en Lecture seule

Le dossier est désormais accessible par le chemin réseau \\PARCUS-WDSSRV-0\\Images ; c'est ce chemin UNC qu'on utilisera dans la stratégie.



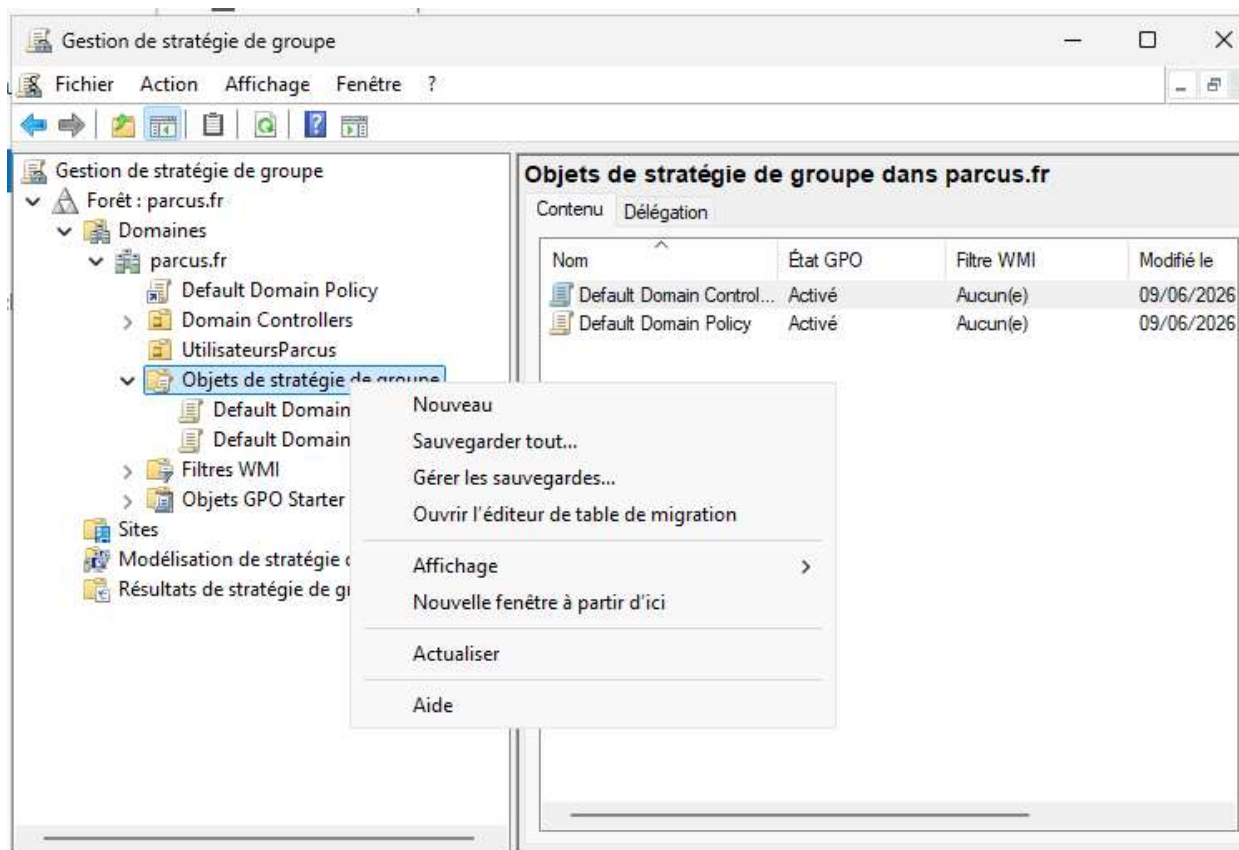
Le chemin réseau du partage : \\PARCUS-WDSSRV-0\Images

Étape 2 — créer la GPO. La console Gestion de stratégie de groupe s'ouvre avec la commande gpmmc.msc (Windows + R).

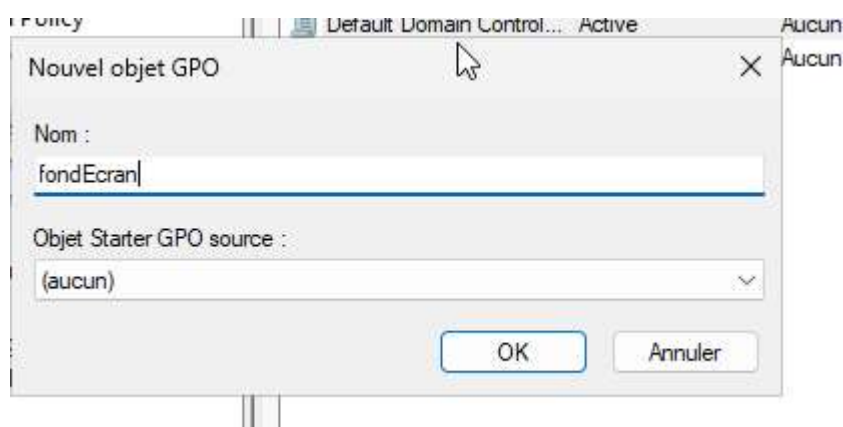


Exécuter > gpmmc.msc : ouverture de la console de gestion des stratégies de groupe

Dans l'arborescence du domaine parcus.fr, clic droit sur Objets de stratégie de groupe puis Nouveau. On nomme l'objet fondEcran, sans objet Starter.

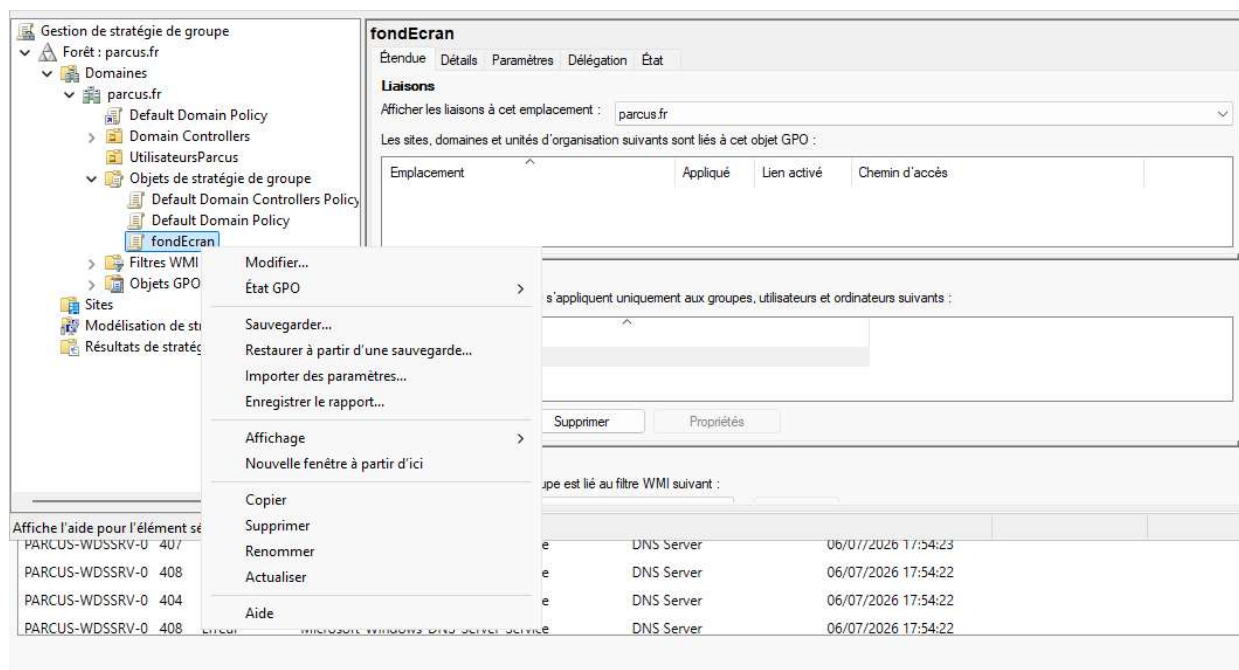


Clic droit sur « Objets de stratégie de groupe » > Nouveau



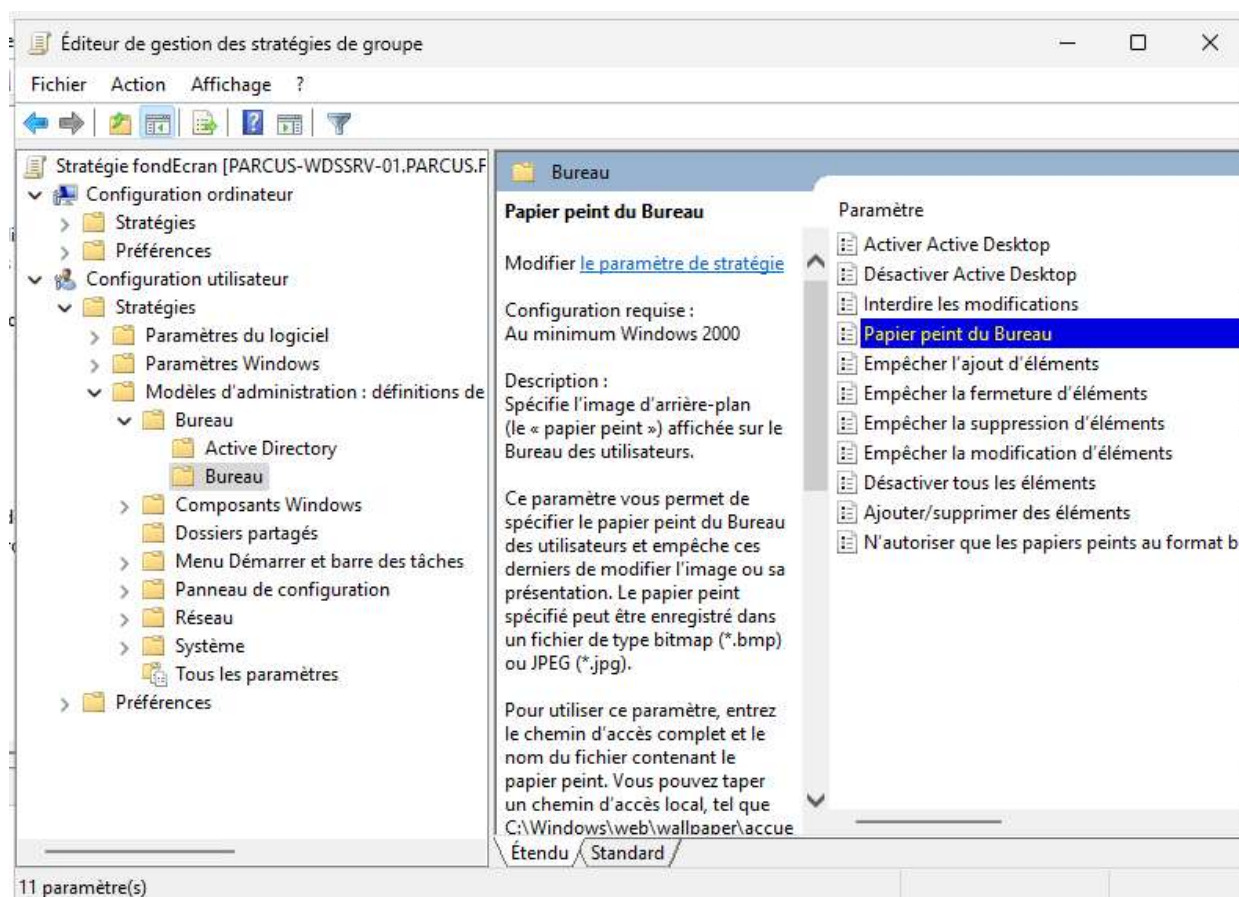
Création de l'objet GPO « fondEcran »

Clic droit sur la GPO fraîchement créée, puis Modifier... pour ouvrir l'éditeur de stratégie.



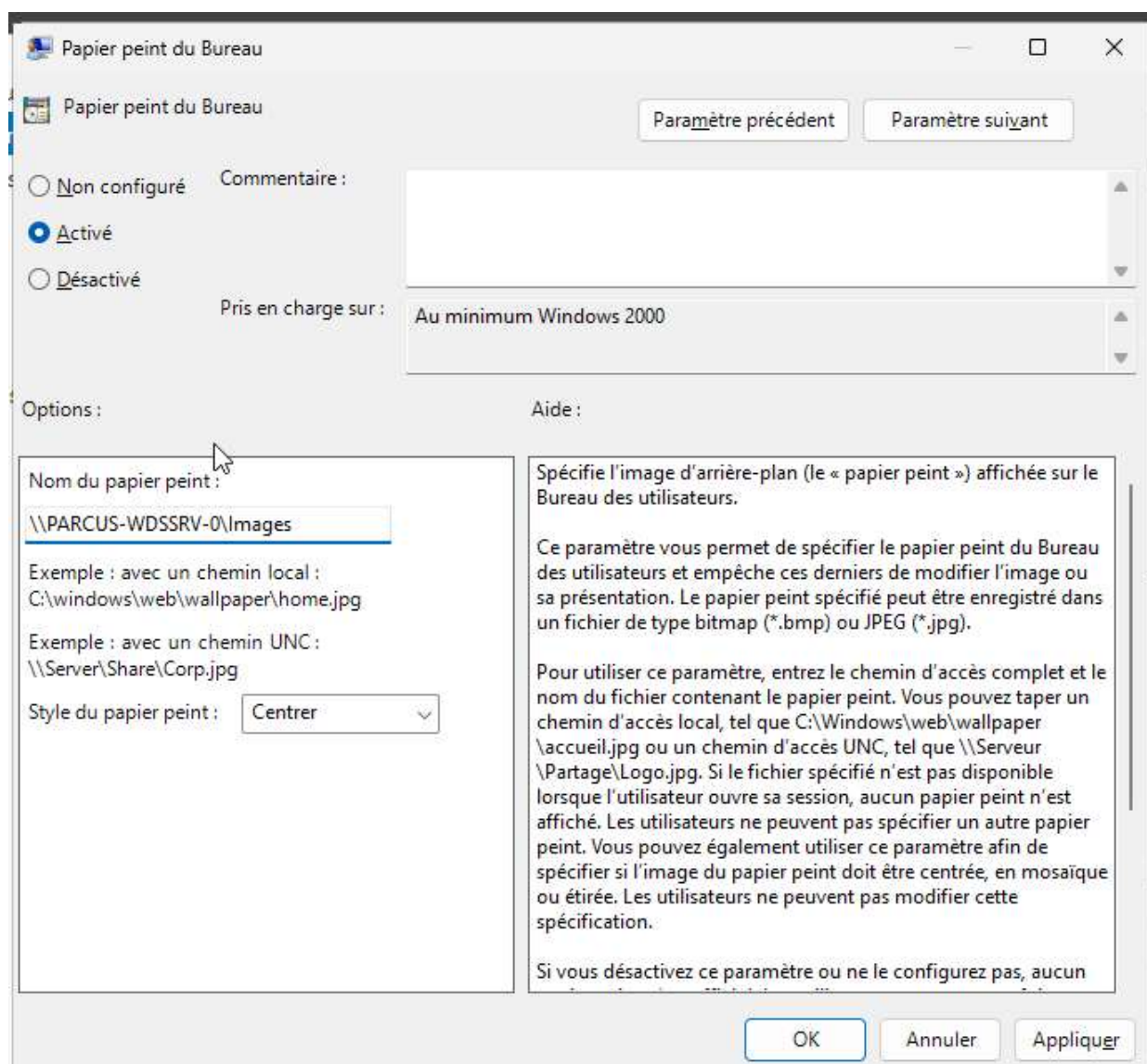
Clic droit sur la GPO fondEcran > Modifier...

Le paramètre se trouve côté utilisateur : Configuration utilisateur > Stratégies > Modèles d'administration > Bureau > Bureau > Papier peint du Bureau.



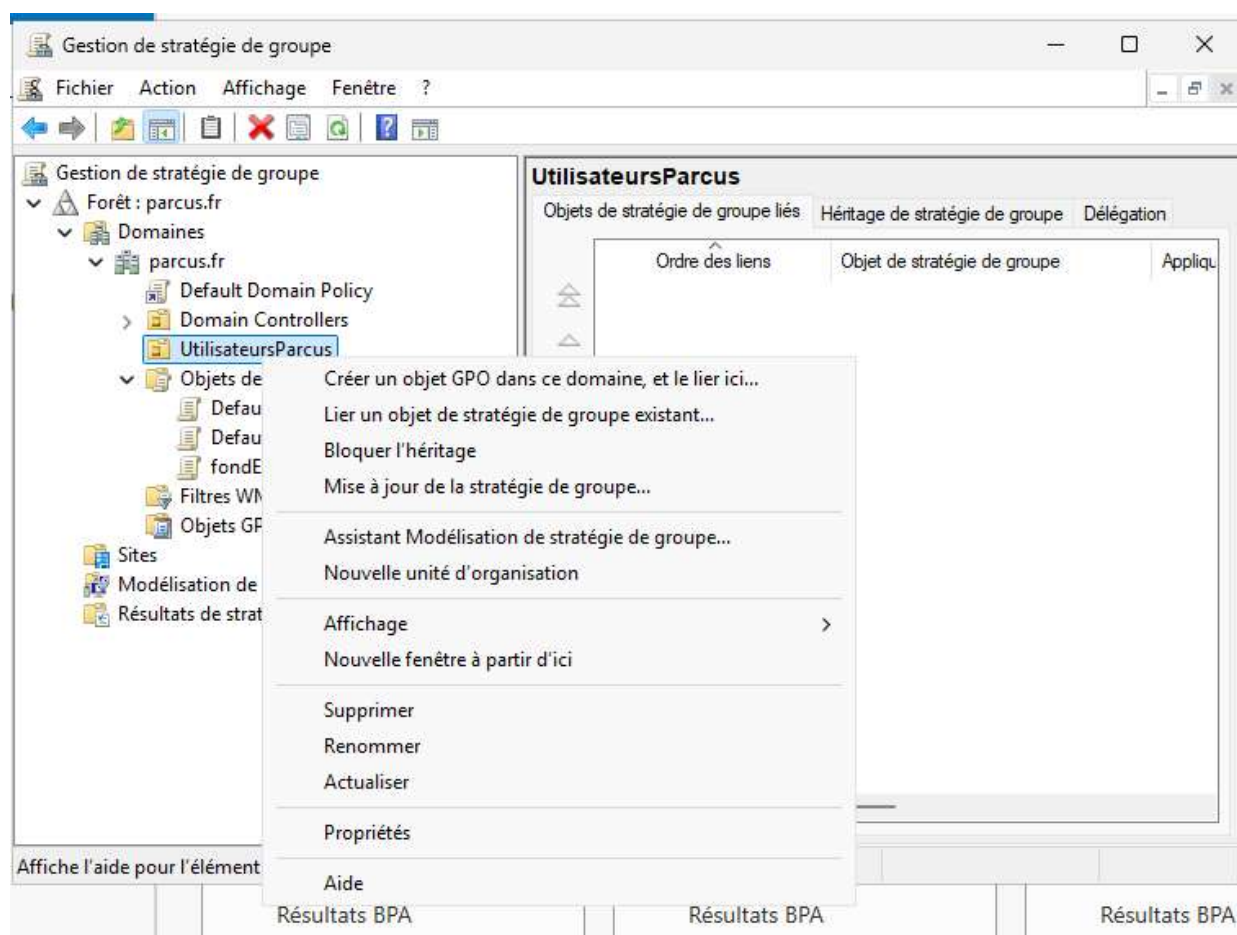
Éditeur de stratégie : le paramètre « Papier peint du Bureau » dans Configuration utilisateur

On active le paramètre et on renseigne le chemin UNC de l'image sur le partage, avec le style Centrer. Attention : le chemin doit désigner le fichier image lui-même (par exemple \\PARCUS-WDSSRV-0\Images\cathedrale.jpg) et pas seulement le dossier, sinon aucun papier peint ne s'affiche à l'ouverture de session.



Paramètre activé : chemin UNC vers le partage Images, style « Centrer »

Étape 3 — lier la GPO. Une GPO n'agit que là où elle est liée. On la lie à l'unité d'organisation UtilisateursParcus, qui regroupe les comptes des salariés : clic droit sur l'OU > « Lier un objet de stratégie de groupe existant... » et on sélectionne fondEcran.



Clic droit sur l'OU UtilisateursParcus : liaison de la GPO existante

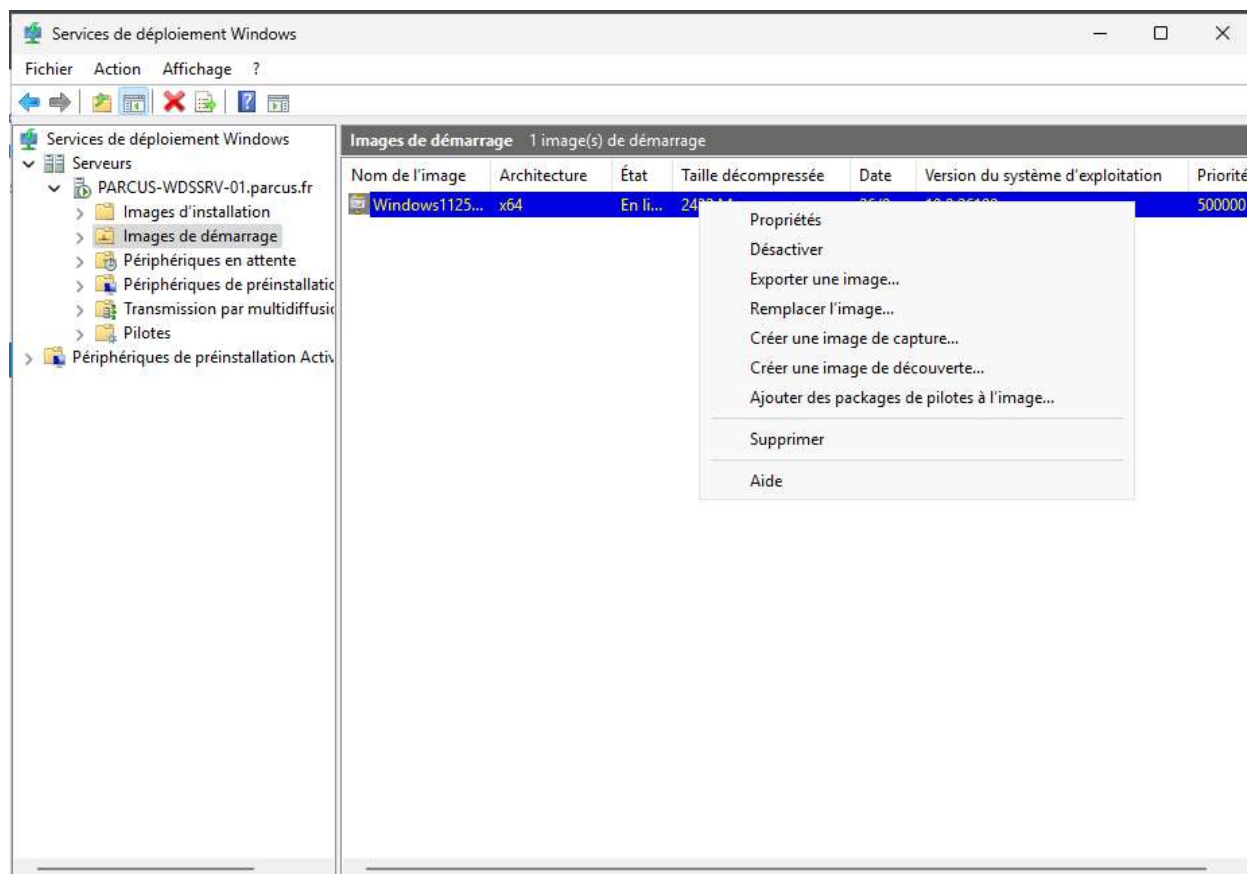
La stratégie s'applique à la prochaine ouverture de session (ou immédiatement avec `gpupdate /force` sur le poste) :

```
gpupdate /force
```

3.3.2. Préparer une image personnalisée (capture WDS et Sysprep)

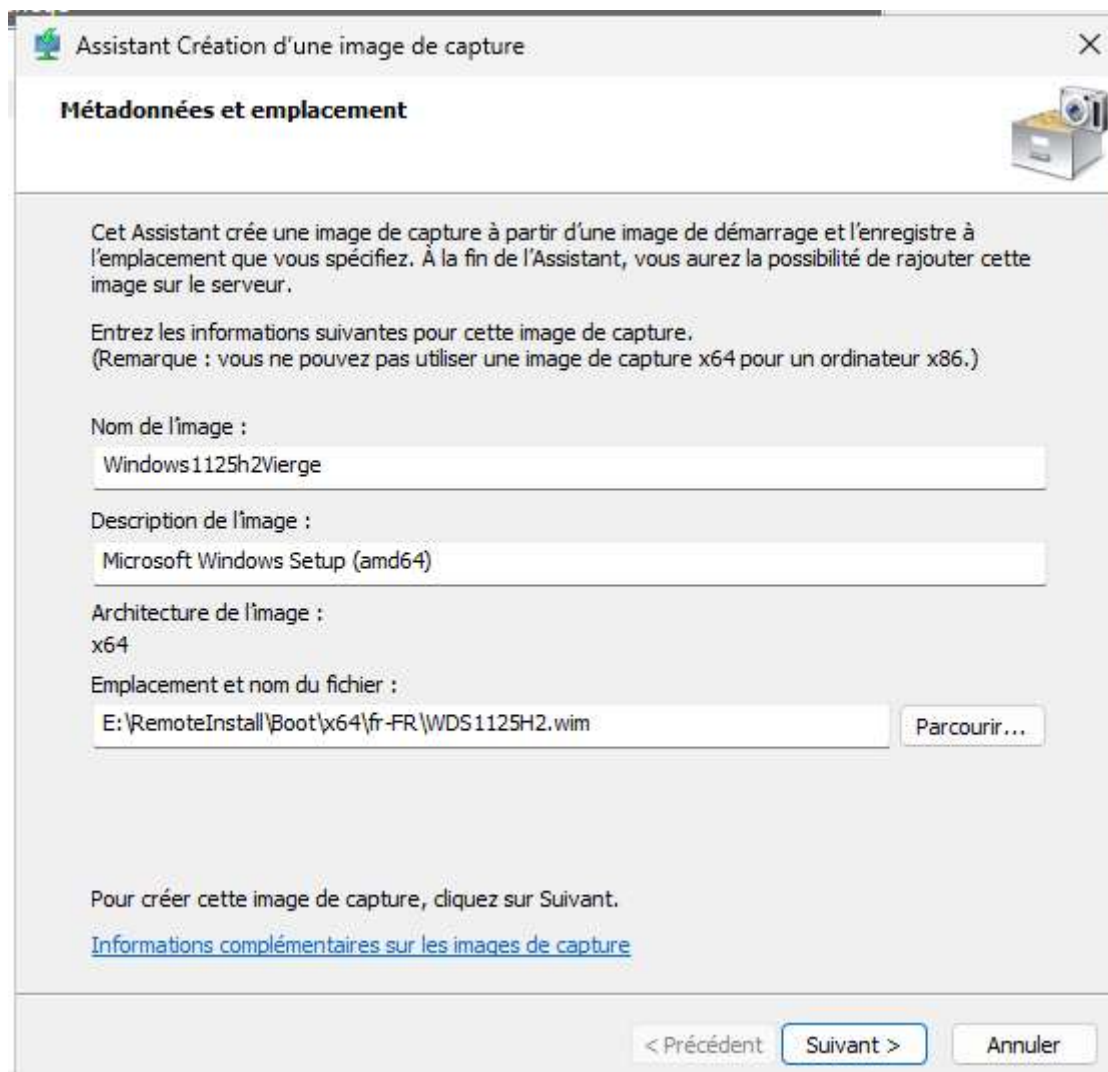
Déployer un Windows vierge, c'est bien ; déployer un Windows déjà configuré (logiciels du parc, réglages), c'est mieux. Pour cela, on prépare un poste de référence, on le généralise avec Sysprep, puis on le capture avec une image de capture WDS.

Créer l'image de capture. Dans la console WDS, clic droit sur l'image de démarrage existante > Créer une image de capture... Cette image spéciale, démarrée en PXE, sait « photographier » un poste au lieu d'installer Windows.



Clic droit sur l'image de démarrage : Créer une image de capture...

On lui donne un nom et un emplacement dans le dossier RemoteInstall du serveur ; l'assistant propose de la rajouter directement à la liste des images de démarrage à la fin.



Métadonnées de l'image de capture : fichier WDS1125H2.wim dans E:\RemoteInstall\Boot\x64\fr-FR

Généraliser le poste de référence. Sur le poste modèle, une fois tout installé et configuré, on lance Sysprep pour retirer les identifiants propres à la machine (SID, nom, pilotes spécifiques) :

```
cd c:\Windows\System32\Sysprep
Sysprep.exe /audit /reboot
```

```
C:\Users\alexis.jeanney.PARCUS>cd c:\Windows\System32\Sysprep
c:\Windows\System32\Sysprep>Sysprep.exe /audit /reboot
```

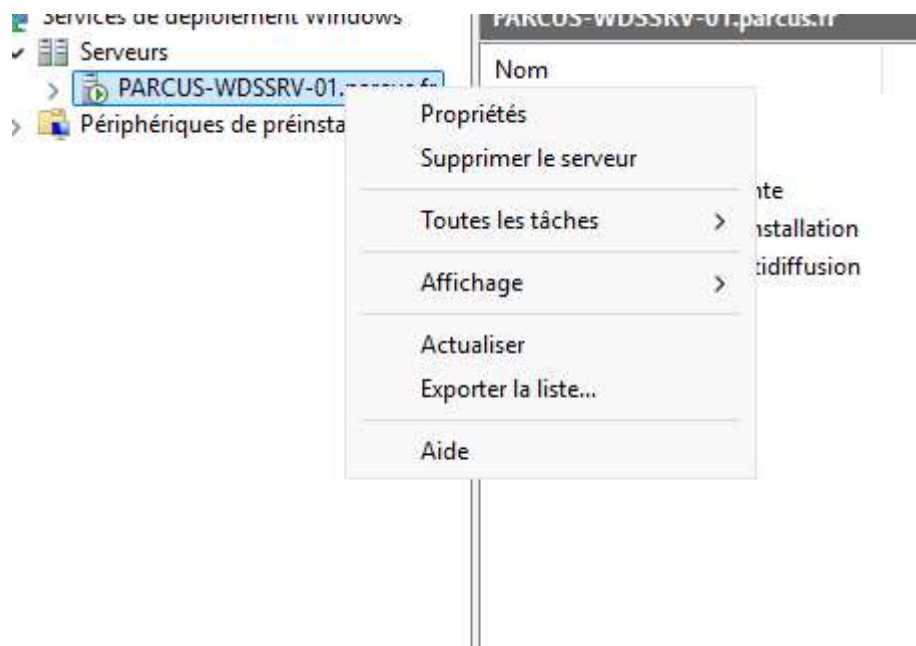
Lancement de Sysprep sur le poste de référence (mode audit)

Le poste généralisé redémarre : on le fait alors booter en PXE et on choisit l'image de capture au lieu de l'image d'installation. Le contenu du disque est enregistré en .wim sur le serveur, puis rajouté aux images d'installation, prêt à être déployé sur tout le parc.

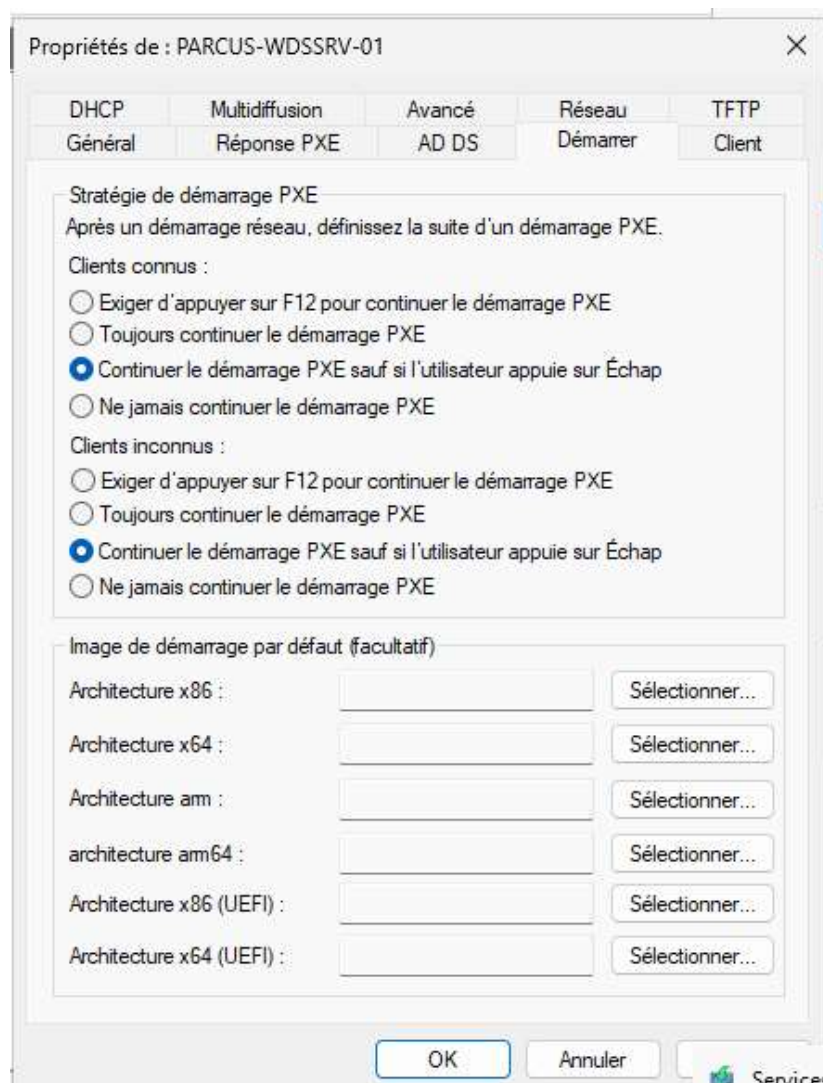
3.3.3. Déployer un poste par le réseau (démarrage PXE)

Régler la stratégie de démarrage PXE. Dans les propriétés du serveur WDS, onglet Démarrer, on définit le comportement après un démarrage réseau. Nous avons choisi « Continuer le démarrage

PXE sauf si l'utilisateur appuie sur Échap », pour les clients connus comme inconnus : un poste qui boote en PXE enchaîne tout seul, mais un utilisateur peut toujours annuler avec Échap.



Clic droit sur le serveur dans la console WDS > Propriétés



Onglet Démarrer : stratégie PXE « Continuer sauf si l'utilisateur appuie sur Échap »

Vérifier le service. Avant un déploiement, on s'assure que le service WDS Server tourne ; s'il est arrêté (cas rencontré après le premier démarrage, voir 3.1.8), on le relance en PowerShell :

```
Get-Service WDS Server
Start-Service WDS Server
```

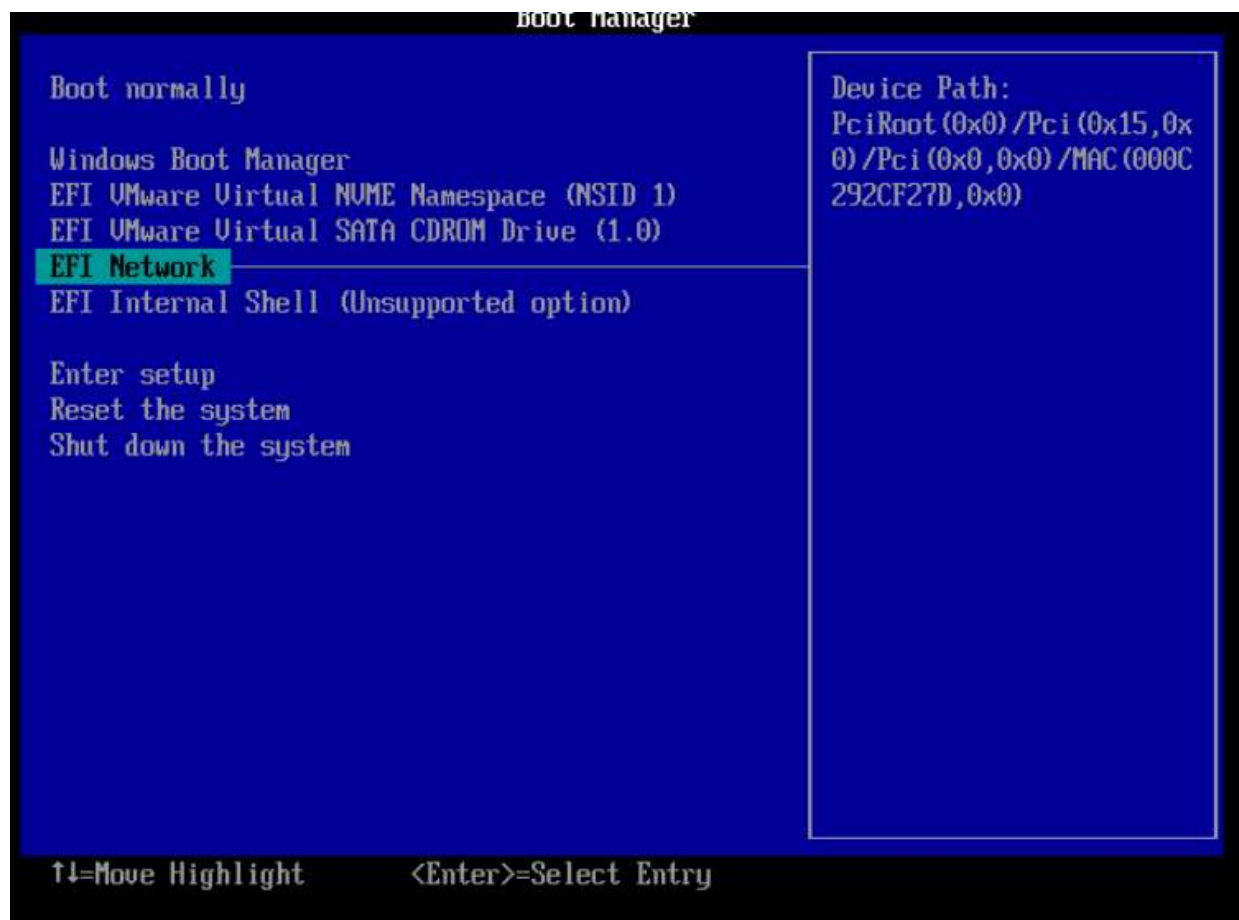
```
PS C:\Users\Administrateur> Get-Service WDS Server

Status      Name                DisplayName
-----
Stopped     WDS Server          Serveur des Services de déploiement...

PS C:\Users\Administrateur> Start-Service WDS Server
PS C:\Users\Administrateur> |
```

Le service WDS Server était arrêté : Start-Service le relance immédiatement

Démarrer le poste en PXE. Sur le poste à déployer (ici une VM en UEFI), on ouvre le Boot Manager et on choisit EFI Network : la carte réseau contacte le serveur DHCP, récupère une adresse et télécharge l'image de démarrage du WDS. Il n'y a plus qu'à suivre l'installation de Windows 11 Pro comme depuis une clé USB, l'image venant du réseau.

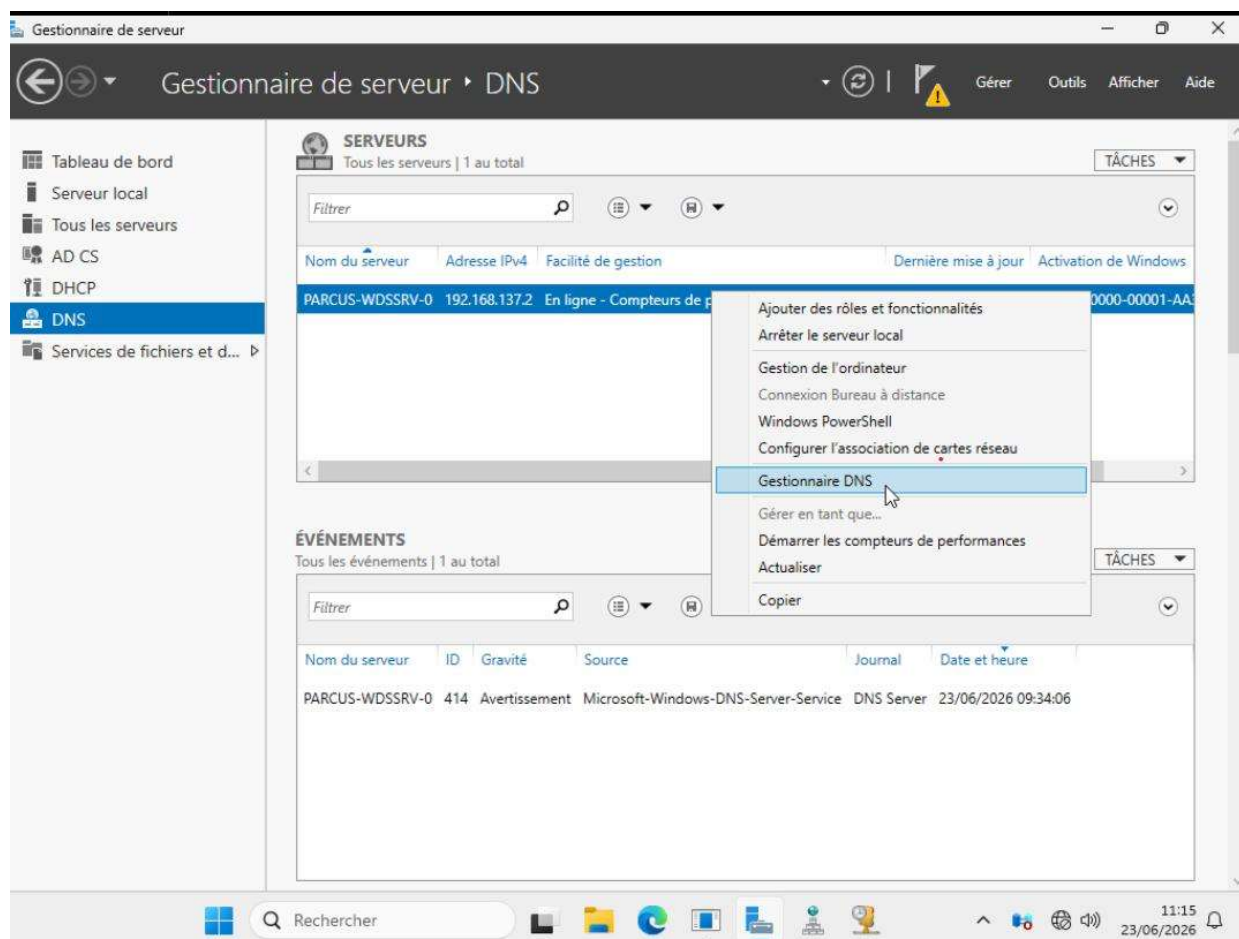


Boot Manager UEFI : démarrage sur EFI Network pour contacter le serveur WDS

3.3.4. Redondance DNS : zone secondaire sur le second serveur

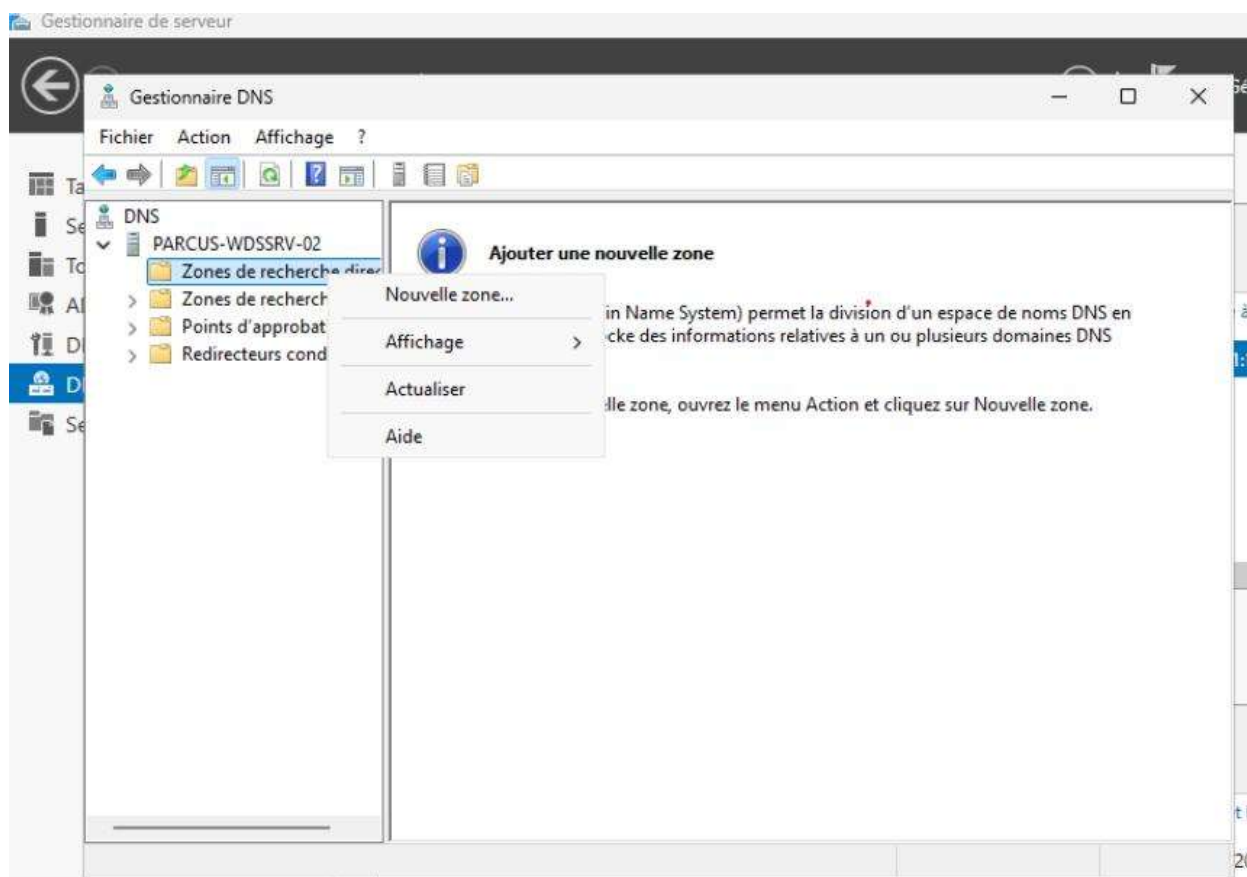
Le DNS est vital : sans lui, plus personne ne résout parcus.fr et plus rien ne s'authentifie. On crée donc sur PARCUS-WDSSRV-02 une zone secondaire, copie en lecture seule de la zone portée par le premier serveur, maintenue à jour par transfert de zone.

Sur le second serveur, on ouvre le Gestionnaire DNS (clic droit sur le serveur dans la vue DNS du Gestionnaire de serveur).

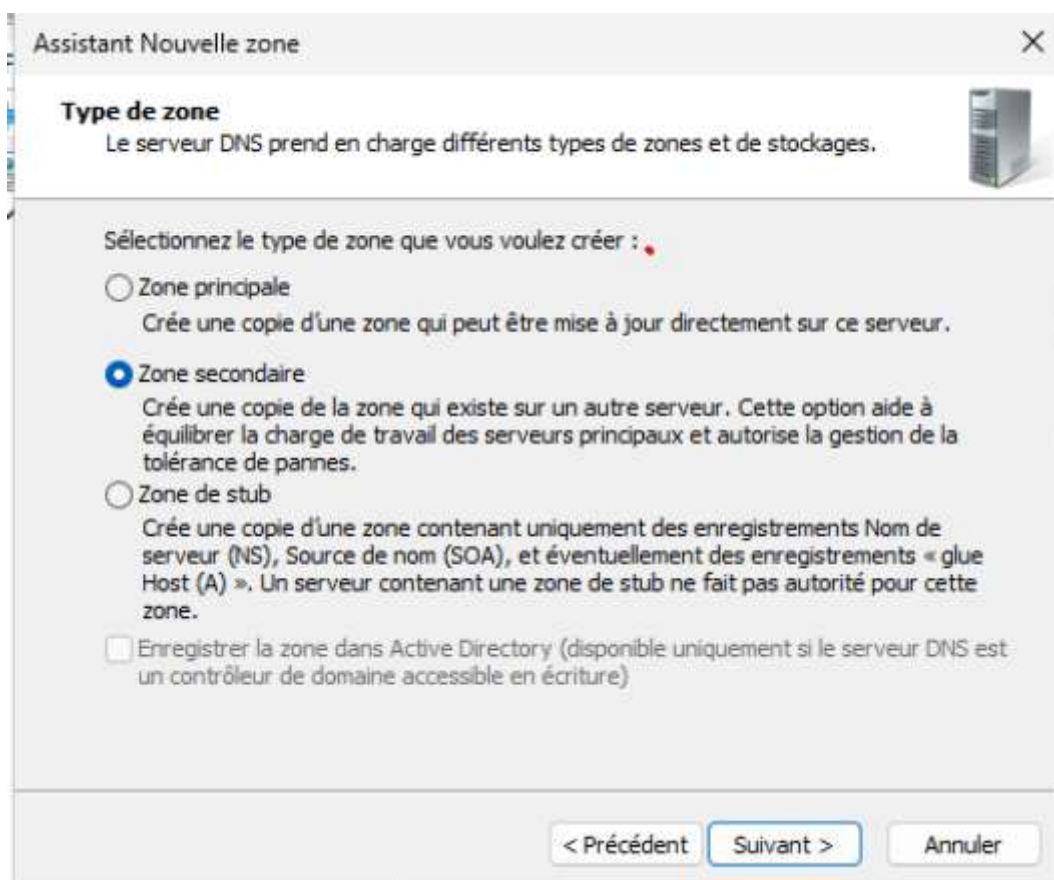


Ouverture du Gestionnaire DNS sur PARCUS-WDSSRV-02

Clic droit sur Zones de recherche directe > Nouvelle zone..., puis on choisit le type Zone secondaire.

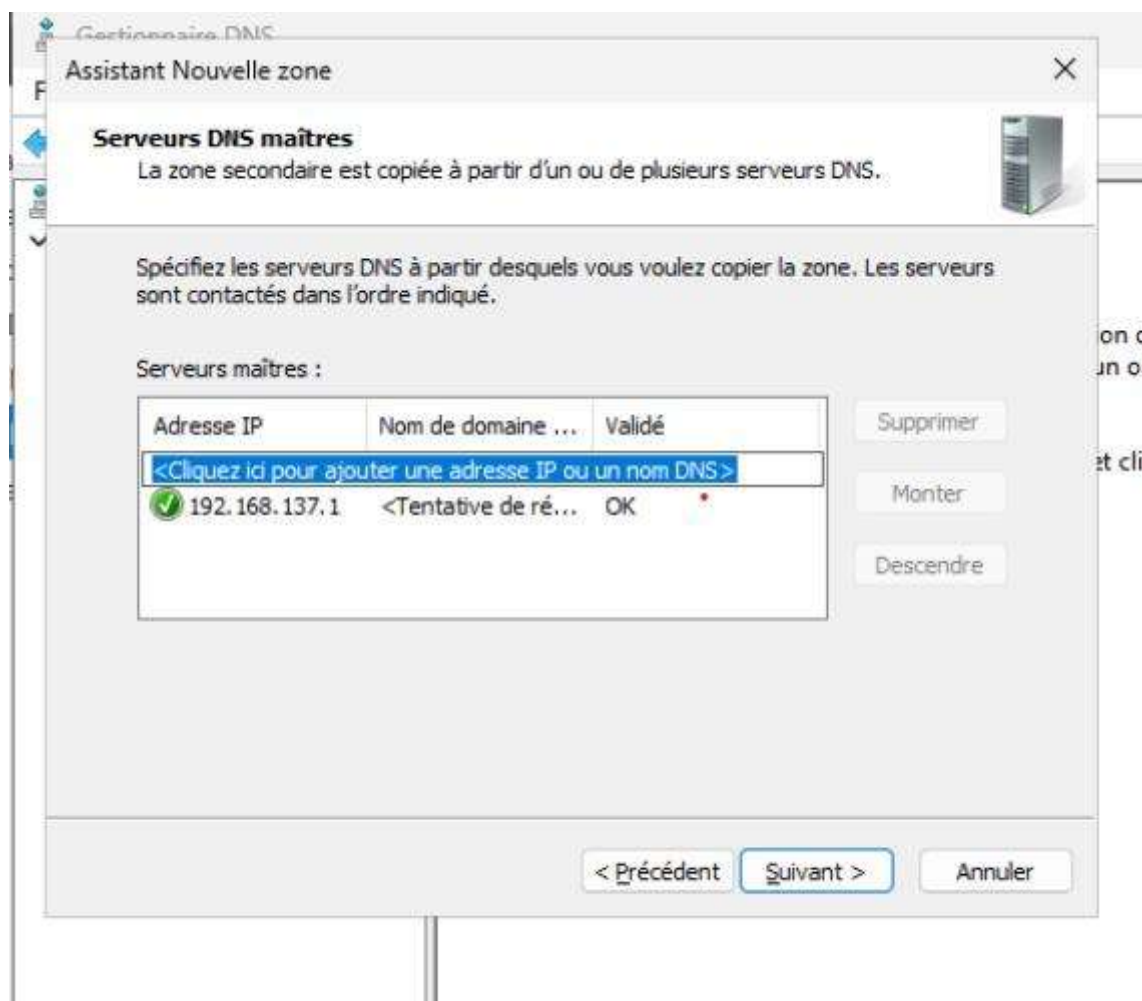


Nouvelle zone dans les zones de recherche directe du second serveur



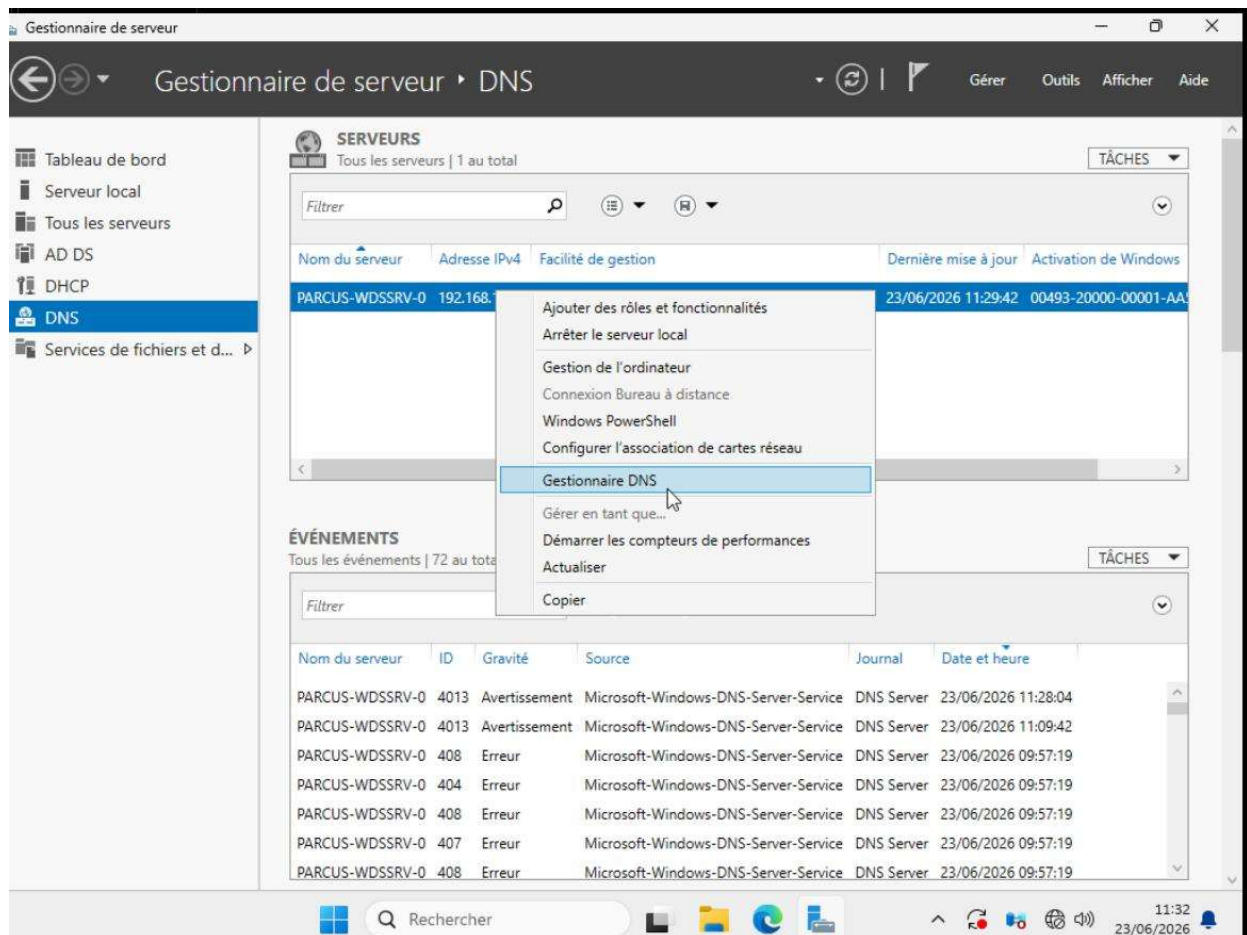
Type de zone : Zone secondaire (copie d'une zone existant sur un autre serveur)

On indique le nom de la zone (parcus.fr) puis le serveur maître à partir duquel la copier : 192.168.137.1. La validation passe au vert : le maître répond.

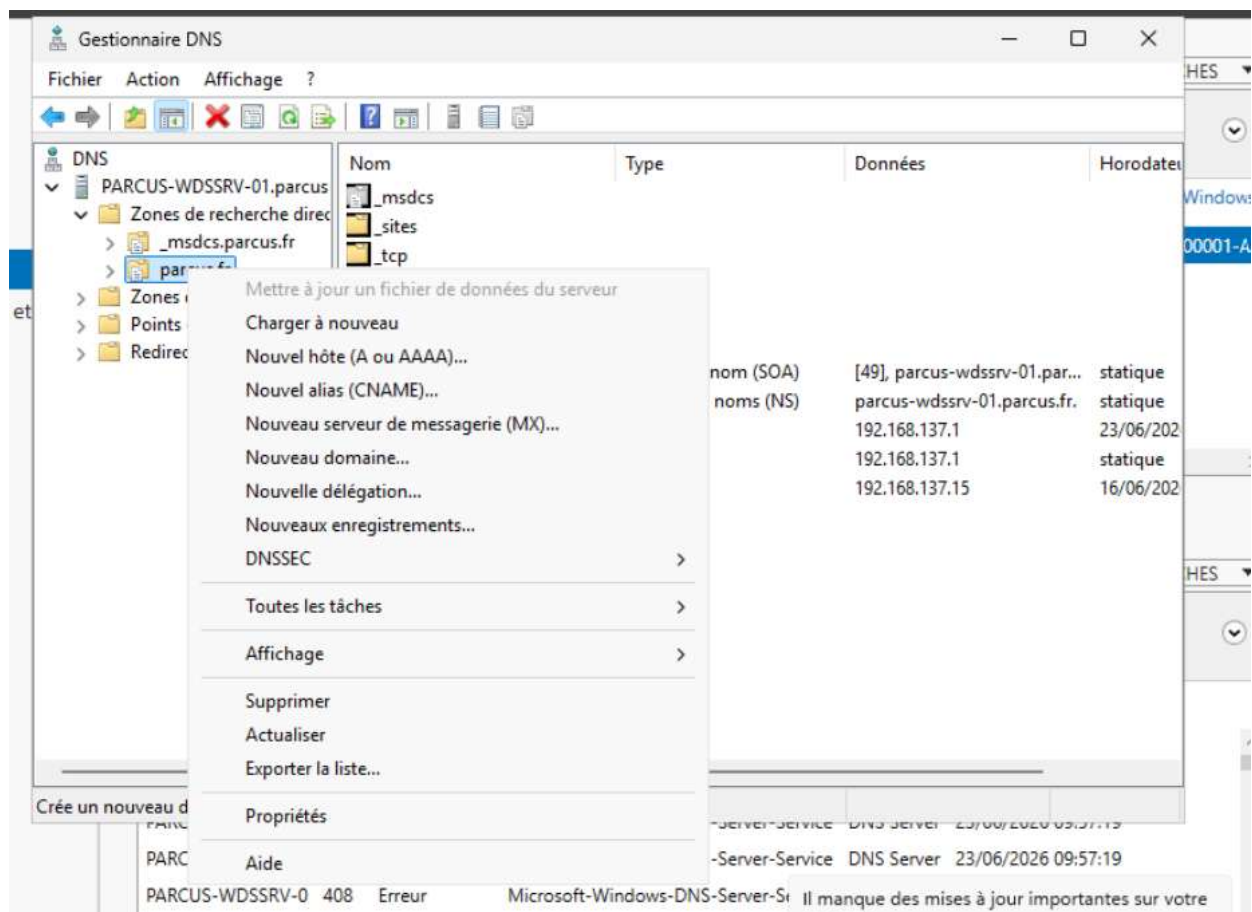


Serveur DNS maître de la zone secondaire : 192.168.137.1, validé

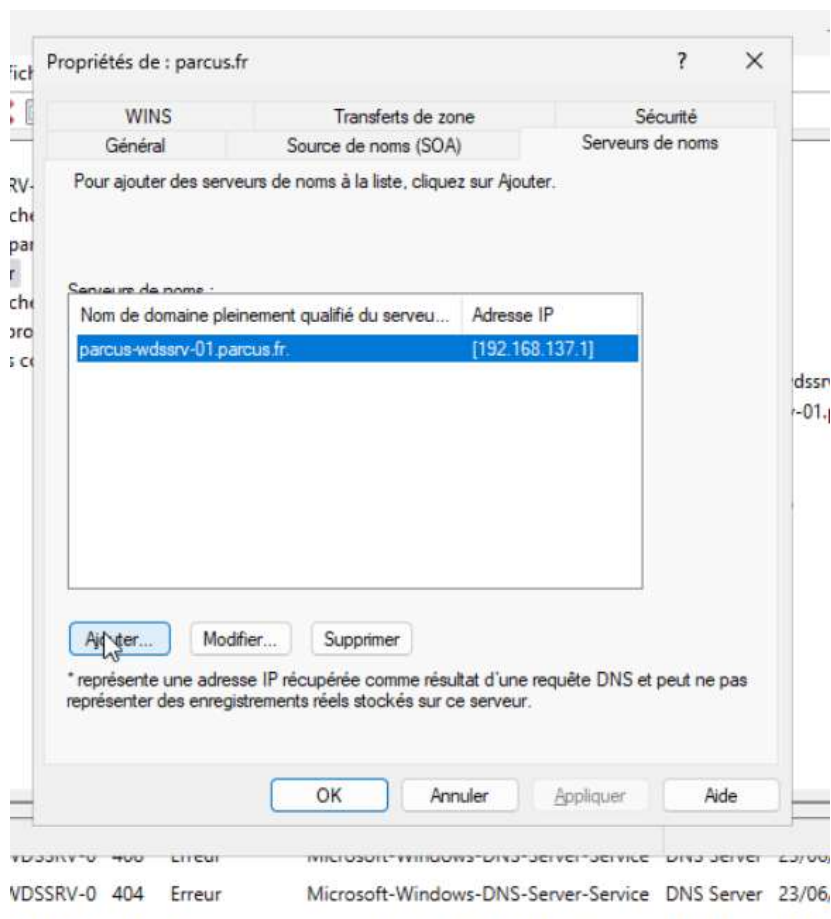
Autoriser le transfert côté maître. Par défaut, le premier serveur refuse de transférer sa zone. Sur PARCUS-WDSSRV-01, dans le Gestionnaire DNS, on ouvre les propriétés de la zone parcus.fr et, dans l'onglet Serveurs de noms, on ajoute le second serveur : il devient serveur de noms officiel de la zone et les transferts vers lui sont autorisés.



Sur le premier serveur : ouverture du Gestionnaire DNS (les erreurs 404/408 visibles correspondent aux tentatives de transfert refusées avant l'autorisation)



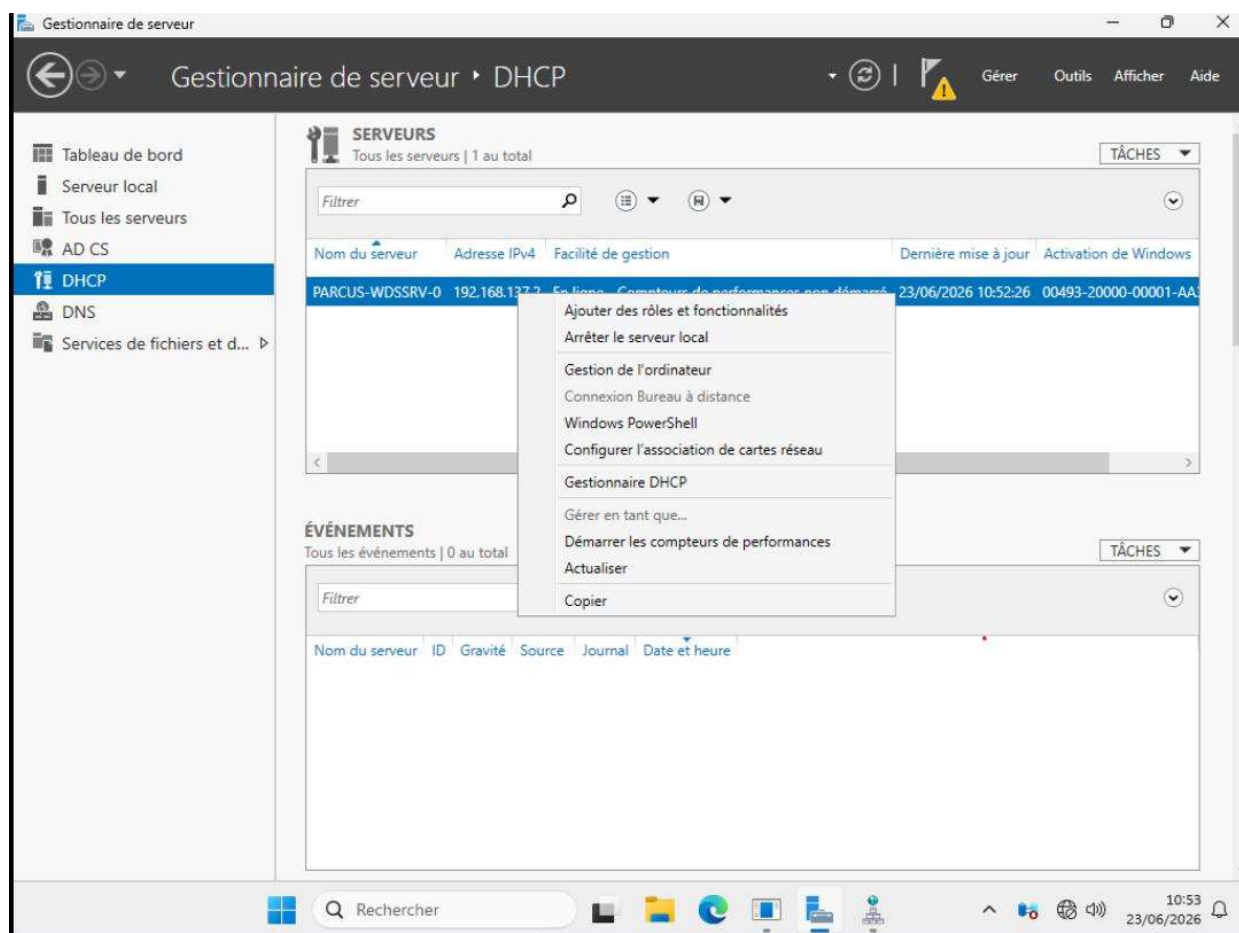
Clic droit sur la zone parcus.fr pour accéder à ses propriétés



Onglet Serveurs de noms de la zone : ajout de parcus-wdssrv-02 à la liste

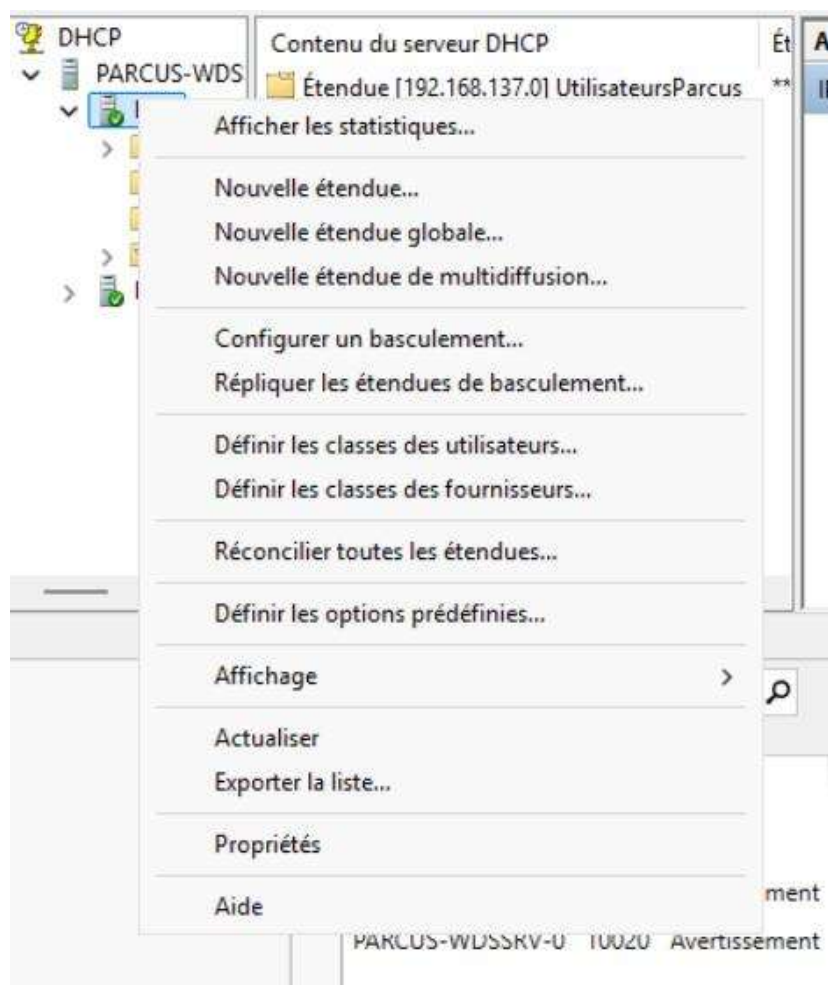
3.3.5. Haute disponibilité DHCP : le basculement

Le basculement DHCP synchronise les baux entre deux serveurs : si l'un tombe, l'autre continue de distribuer les adresses de la même étendue. Le rôle DHCP a déjà été installé sur le second serveur (3.1.10) ; la configuration se fait depuis le premier.



Ouverture du Gestionnaire DHCP

Clic droit sur IPv4 > Configurer un basculement... L'assistant liste les étendues éligibles : notre étendue 192.168.137.0 est sélectionnée.



Clic droit sur IPv4 : Configurer un basculement...



Introduction au basculement DHCP : l'étendue 192.168.137.0 est retenue

On désigne ensuite le serveur partenaire via Ajouter un serveur, en saisissant son adresse 192.168.137.2.

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent Suivant > Annuler

Choix du serveur partenaire pour le basculement

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Ajouter un serveur

Sélectionnez un serveur que vous voulez ajouter à votre console.

☒ Ce serveur :

☐ Ce serveur DHCP autorisé :

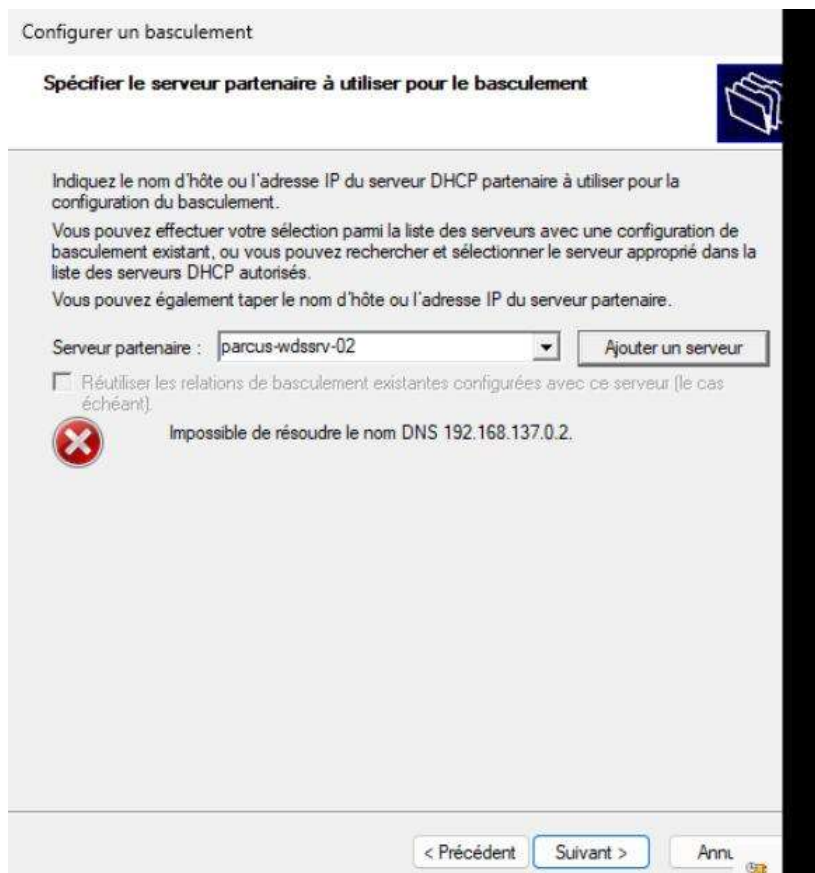
Nom	Adresse IP
parcus-wdsrv-01.parcus.fr	192.168.137.1

OK Annuler

< Précédent Suivant > Annuler

Ajout du serveur partenaire par son adresse : 192.168.137.2

Problème rencontré : lors d'un premier essai, l'assistant a affiché « Impossible de résoudre le nom DNS 192.168.137.0.2 » — l'adresse du partenaire avait été mal saisie (un .0 en trop) et l'assistant tentait de la résoudre comme un nom. En ressaisissant proprement 192.168.137.2, le partenaire parcus-wdssrv-02 est reconnu.



Erreur de résolution due à une adresse mal saisie (192.168.137.0.2 au lieu de 192.168.137.2)

On crée enfin la relation de basculement en mode Équilibrage de charge 50 % / 50 % : les deux serveurs se partagent les demandes en temps normal et se relaient en cas de panne. Le délai de transition (MCLT) reste à 1 heure et on active l'authentification des messages avec un secret partagé, pour que seuls nos deux serveurs puissent se synchroniser.

Configurer un basculement

Créer une relation de basculement 

Créer une relation de basculement avec le partenaire parcus-wdssrv-02

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

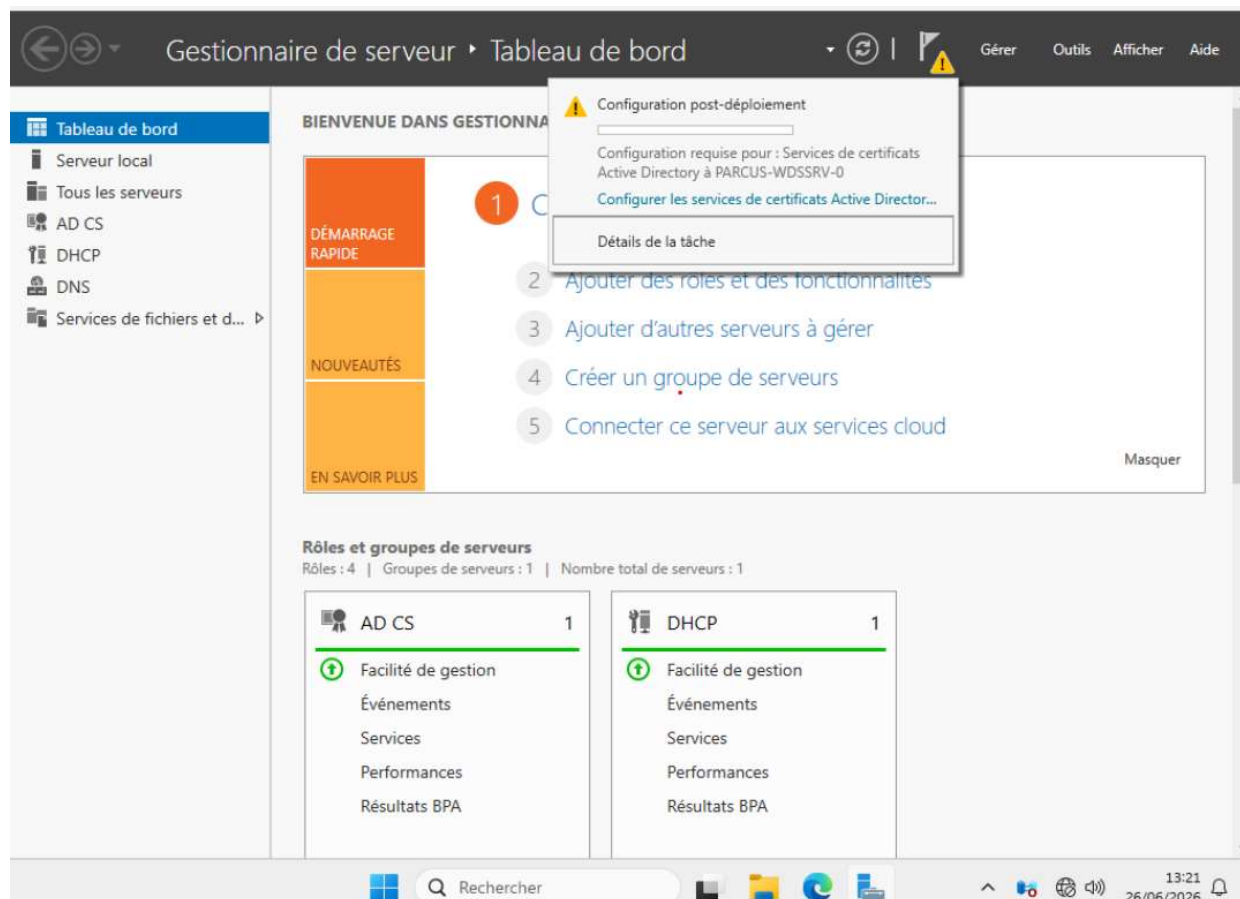
Secret partagé :

< Précédent **Suivant >**

Relation de basculement : équilibrage de charge 50/50, MCLT 1 h, secret partagé

3.3.6. Autorité de certification (AD CS)

L'autorité de certification interne émet les certificats utilisés dans le domaine — c'est elle, par exemple, qui permet le LDAPS (annuaire chiffré sur le port 636) exploité par GLPI au LOT 2. Après l'installation du rôle (3.1.10), une configuration post-déploiement est nécessaire.



Notification post-déploiement : « Configurer les services de certificats Active Directory »

L'assistant demande d'abord des informations d'identification : pour une autorité d'entreprise, le compte doit être membre des Administrateurs de l'entreprise.

Configuration des services de certificats Active Directory

Informations d'identification

SERVEUR DE DESTINATION
PARCUS-WDSSRV-02

Informations d'identification

Services de rôle

Confirmation

Progression

Résultats

Spécifier les informations d'identification pour configurer les services de rôle

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :

- Utiliser l'autorité de certification autonome
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :

- Autorité de certification d'entreprise
- Service Web Stratégie d'inscription de certificats
- Service Web Inscription de certificats
- Service d'inscription de périphériques réseau

Pour effectuer une installation à distance, vous devez entrer vos informations d'identification.

Informations d'identification :

[En savoir plus sur les rôles de serveur AD CS](#)

< Précédent Suivant > Configurer Annuler

Configuration AD CS : spécification des informations d'identification

Configuration des services de certificats Active Directory

Informations d'identification

SERVEUR DE DESTINATION
PARCUS-WDSSRV-02

Informations d'identification

Services de rôle

Confirmation

Progression

Résultats

Sécurité Windows

Tapez le nom et le mot de passe du compte d'utilisateur

Tapez le nom et le mot de passe d'un compte avec des droits d'utilisateur sur les serveurs sélectionnés.

Par exemple, xyz@example.contoso.com ou domaine\nom d'utilisateur.

Nom d'utilisateur

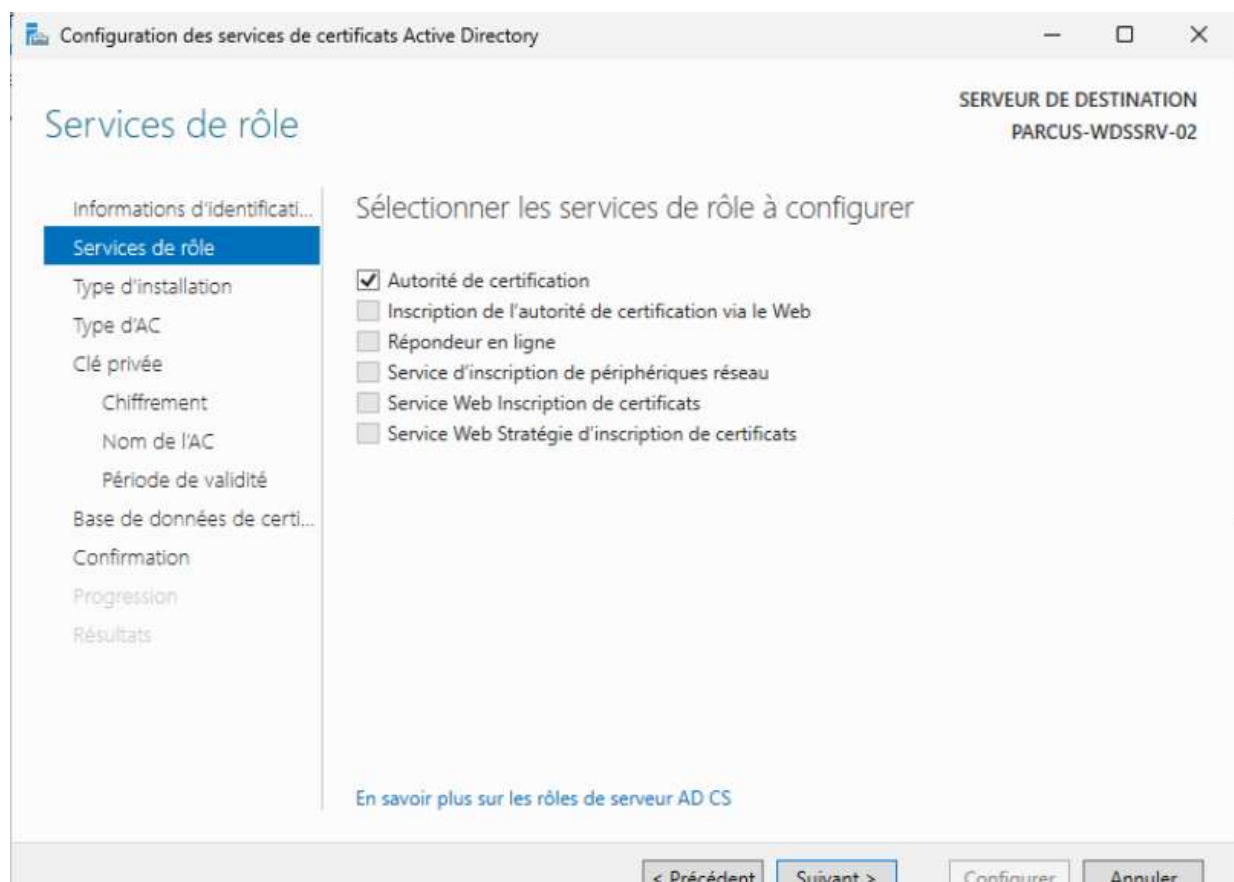
Mot de passe

[En savoir plus sur les rôles de serveur AD CS](#)

< Précédent Suivant > Configurer Annuler

Saisie du compte disposant des droits nécessaires

On sélectionne le service de rôle Autorité de certification, puis on suit l'assistant (autorité racine d'entreprise, nouvelle clé privée, valeurs par défaut). À la fin, le serveur peut émettre des certificats pour les machines du domaine — dont le certificat du contrôleur de domaine utilisé pour le LDAPS.



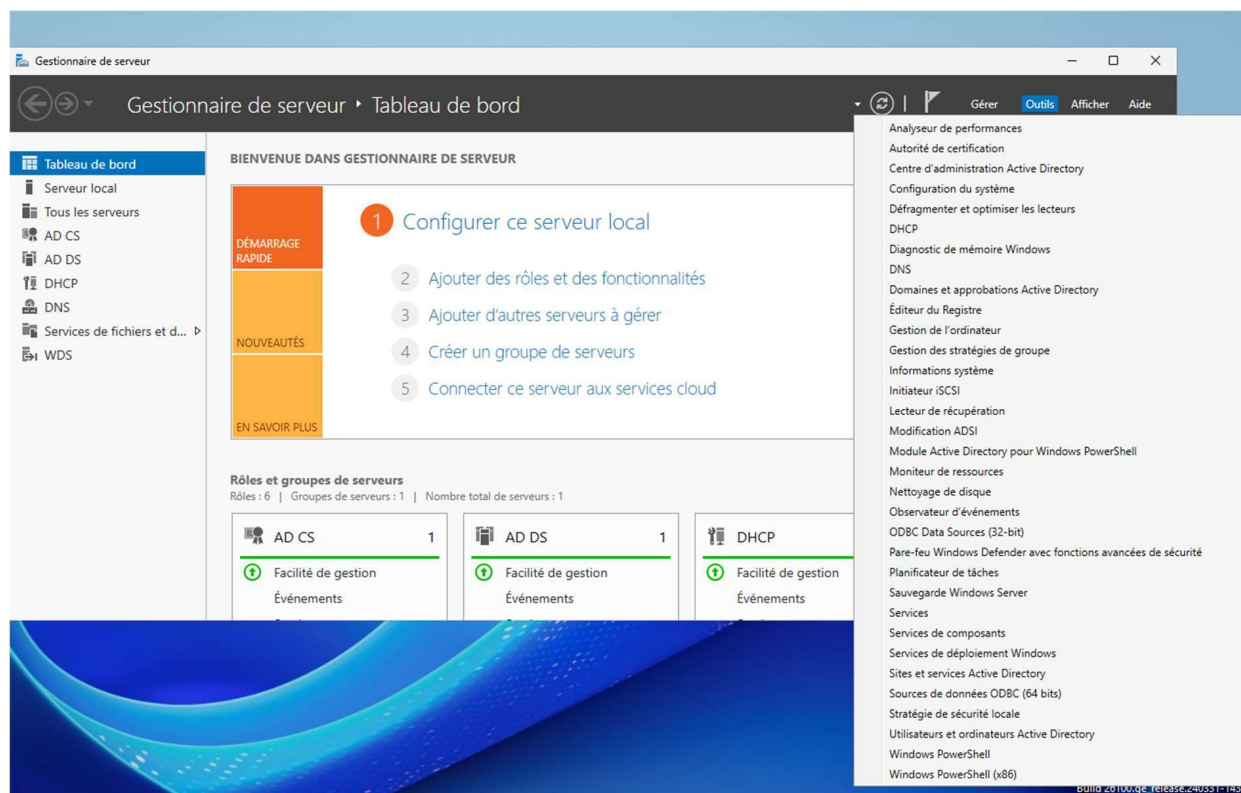
Sélection du service de rôle : Autorité de certification

Bonnes pratiques : sauvegarder la clé privée de l'autorité (sans elle, impossible de renouveler quoi que ce soit), et surveiller les dates d'expiration des certificats émis — un certificat LDAPS expiré casse l'authentification GLPI du jour au lendemain.

3.3.7. Chiffrement BitLocker piloté par GPO

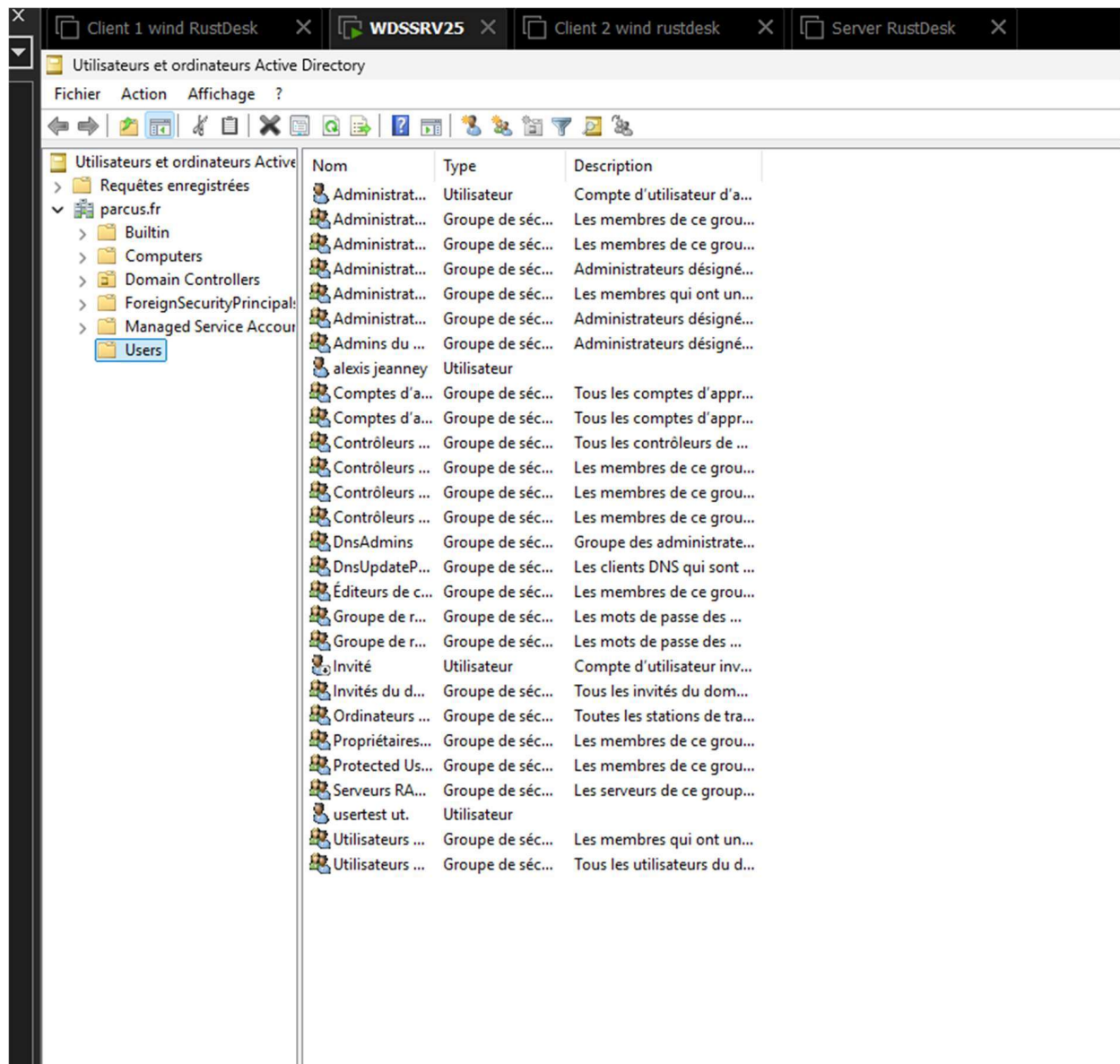
Objectif : activer BitLocker sur les postes du domaine avec des réglages imposés par GPO (méthode de chiffrement, protecteurs) et, surtout, faire sauvegarder automatiquement la clé de récupération de chaque poste dans Active Directory. En cas de problème (mot de passe TPM perdu, carte mère changée, poste verrouillé), le technicien retrouve la clé sur la fiche de l'ordinateur dans l'annuaire.

Étape 1 — organiser l'annuaire. Une GPO BitLocker est une stratégie ordinateur : elle doit être liée à une OU qui contient des comptes d'ordinateurs. On ouvre la console Utilisateurs et ordinateurs Active Directory depuis le menu Outils du Gestionnaire de serveur.



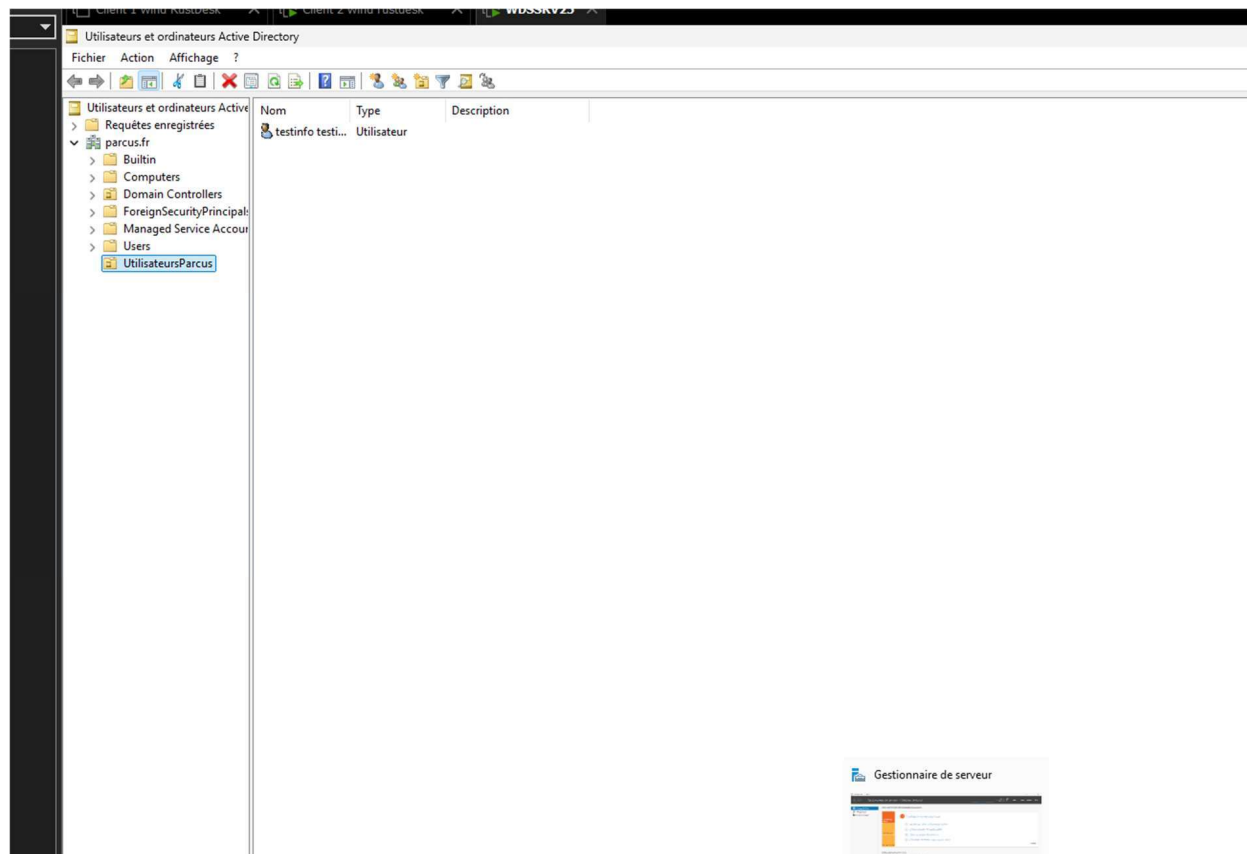
Menu Outils : ouverture de la console Utilisateurs et ordinateurs Active Directory

Par défaut, les comptes créés atterrissent dans le conteneur Users et les machines jointes dans Computers — deux conteneurs sur lesquels on ne peut pas lier de GPO. On range donc tout dans nos OU.

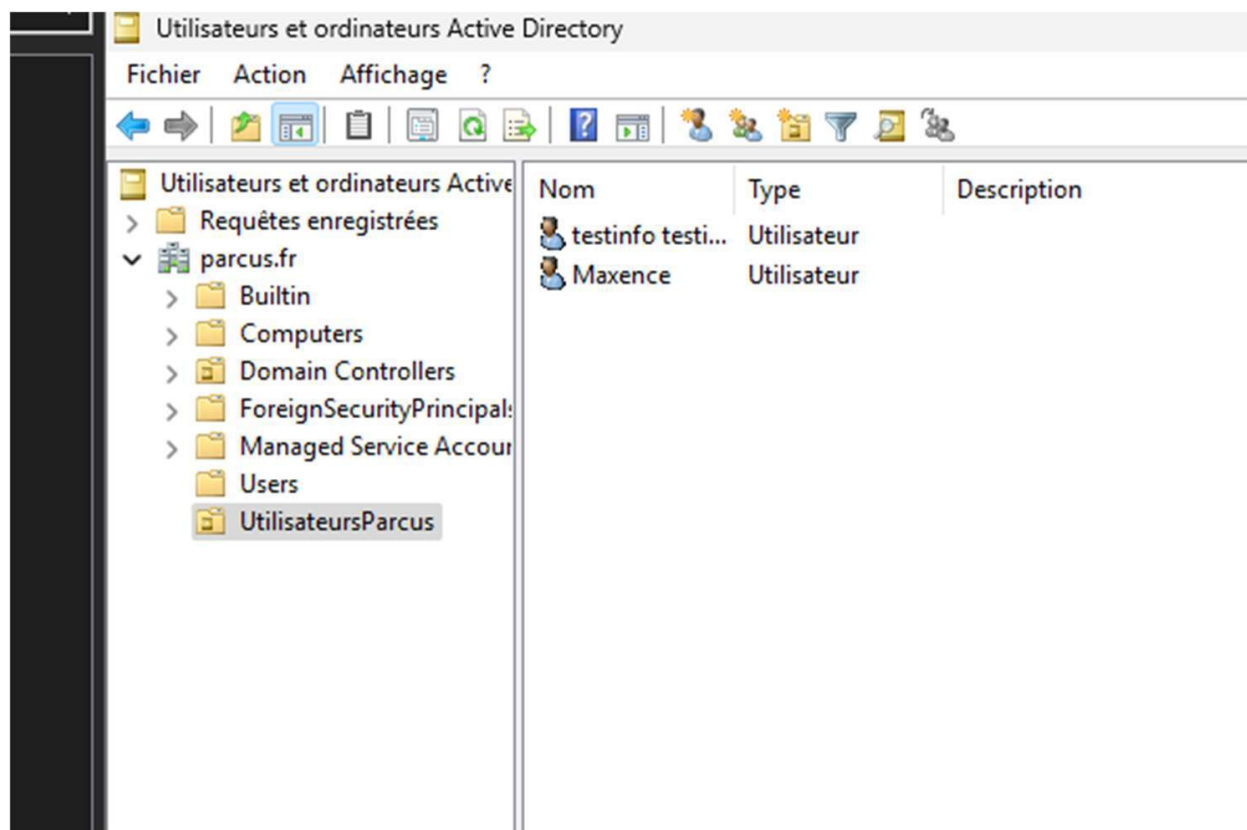


Le conteneur Users par défaut : comptes intégrés du domaine et utilisateurs créés (alexis jeanney, usertest)

Les comptes des salariés sont déplacés dans l'OU UtilisateursParcus (celle qui porte déjà la GPO fondEcran du 3.3.1) :



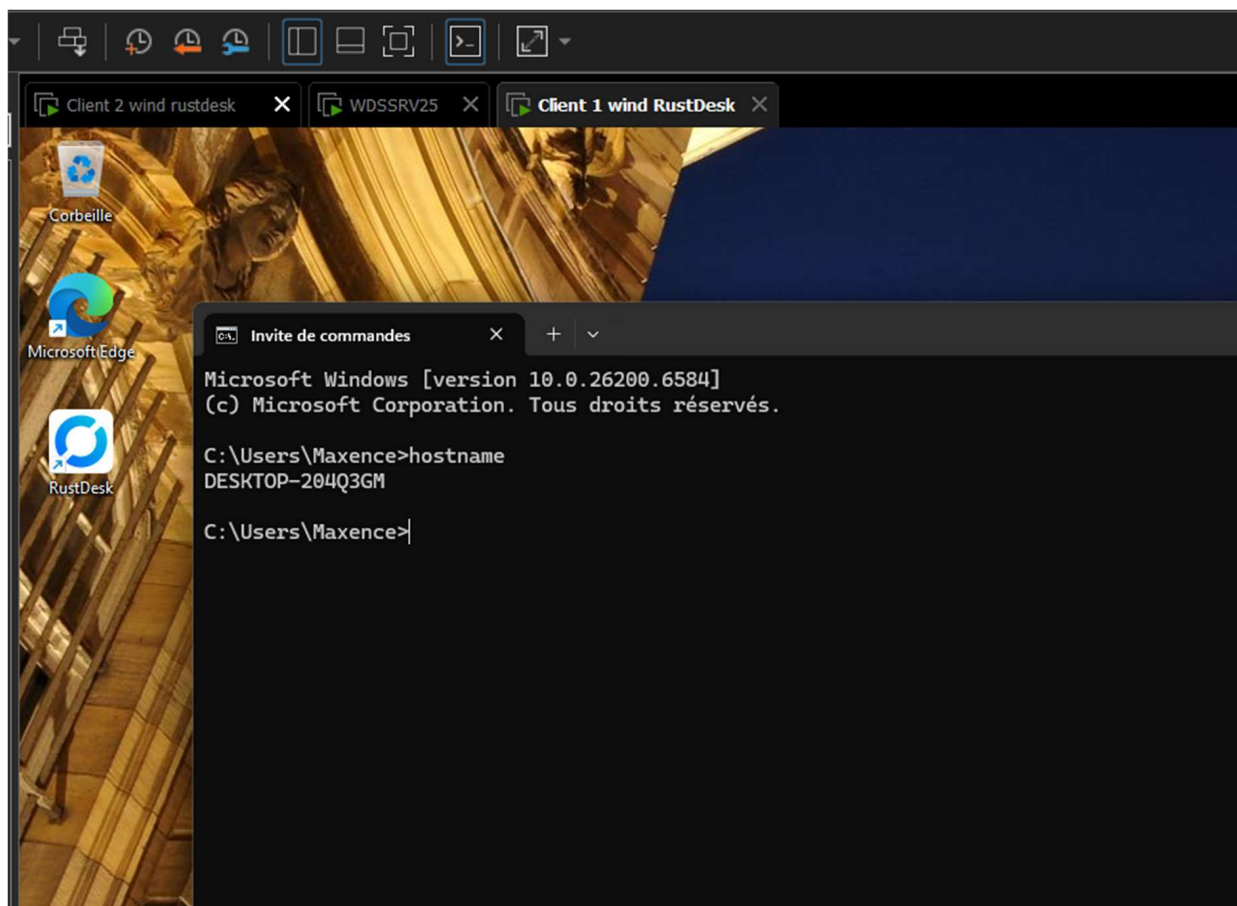
L'OU UtilisateursParcus après déplacement du compte testinfo



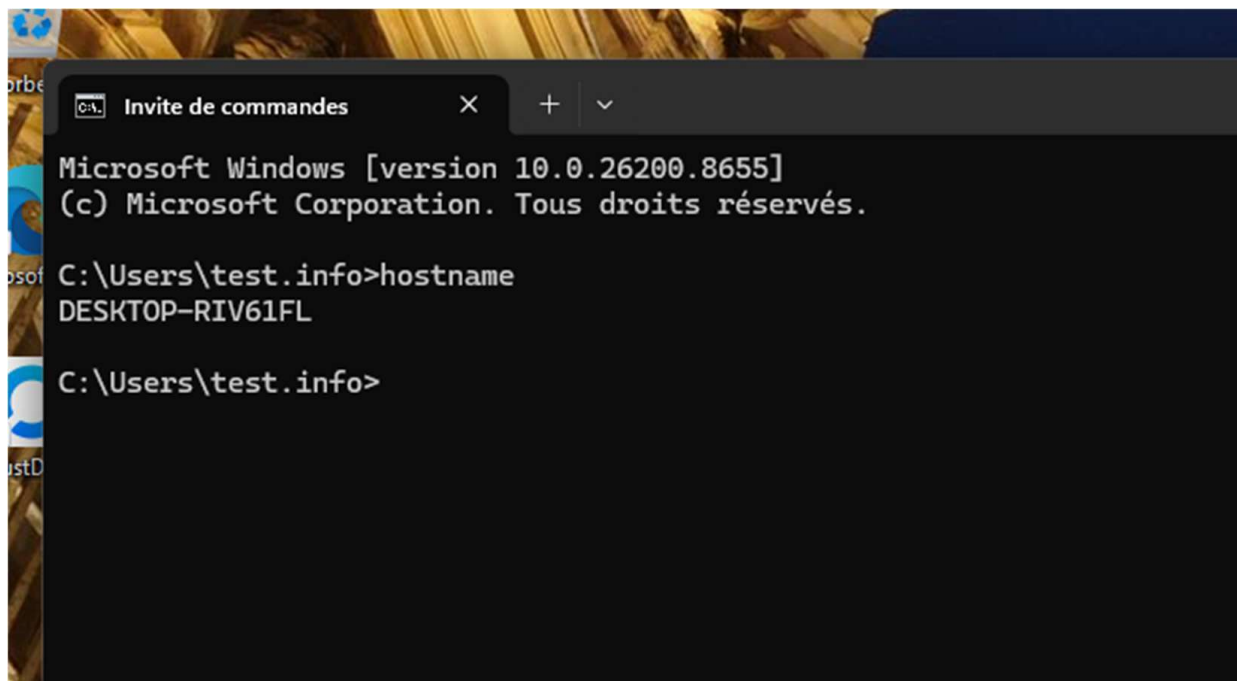
Les comptes utilisateurs testinfo et Maxence rangés dans l'OU UtilisateursParcus

Côté machines, on identifie d'abord le nom de chaque client avec la commande hostname :

```
hostname
```

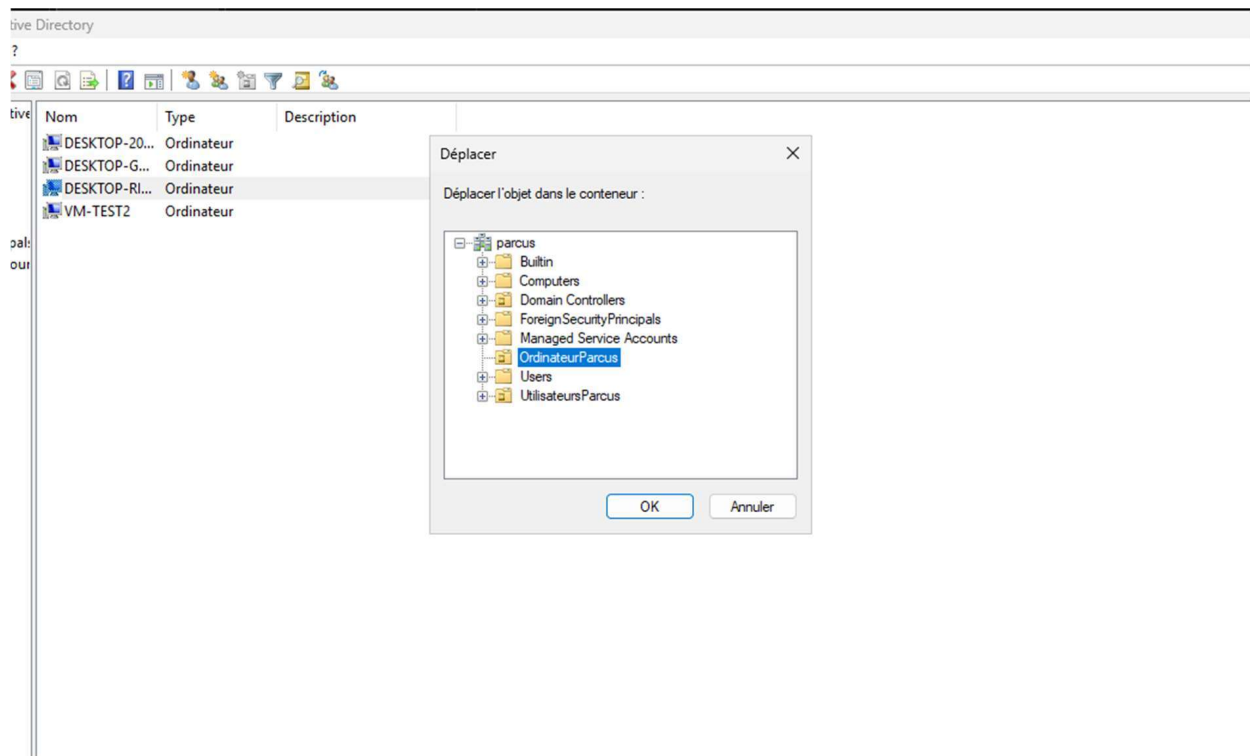


Client 1 : la session de Maxence tourne sur DESKTOP-204Q3GM

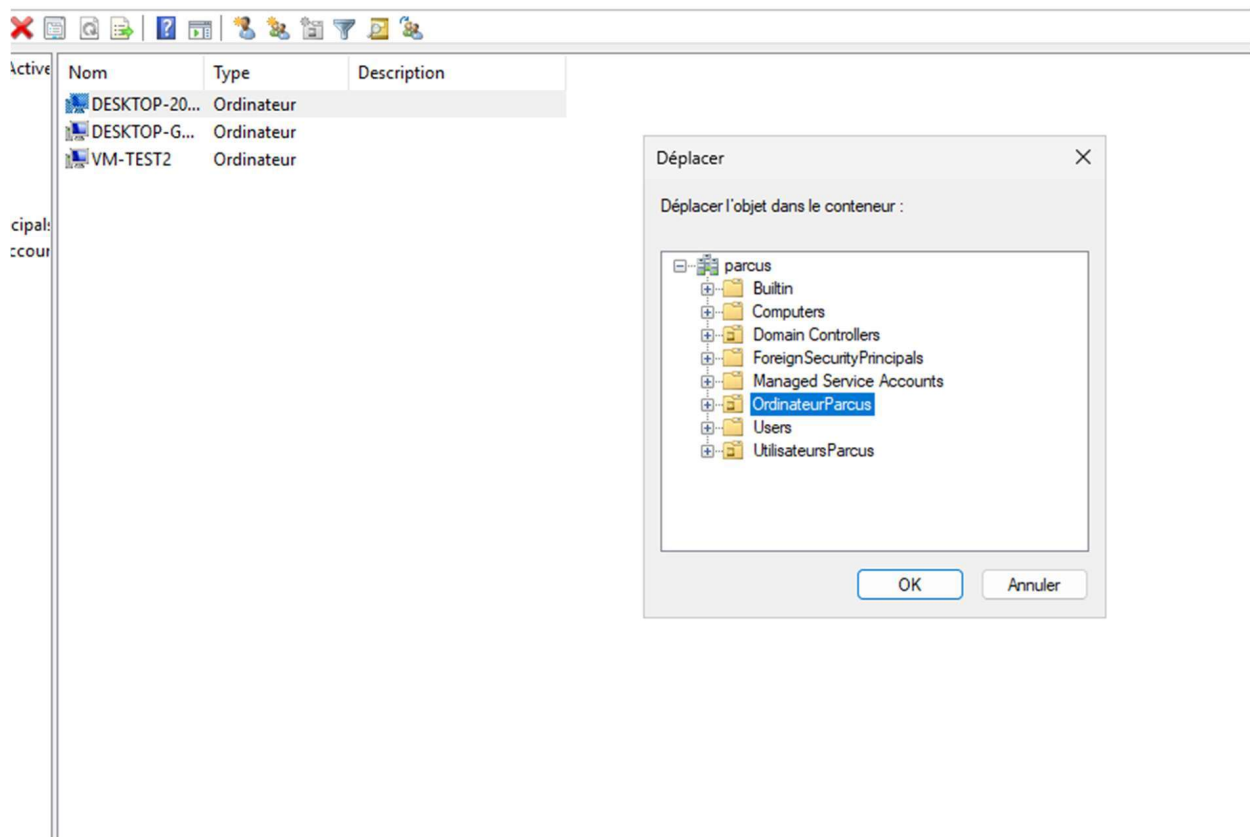


Client 2 : la session de test.info tourne sur DESKTOP-RIV61FL

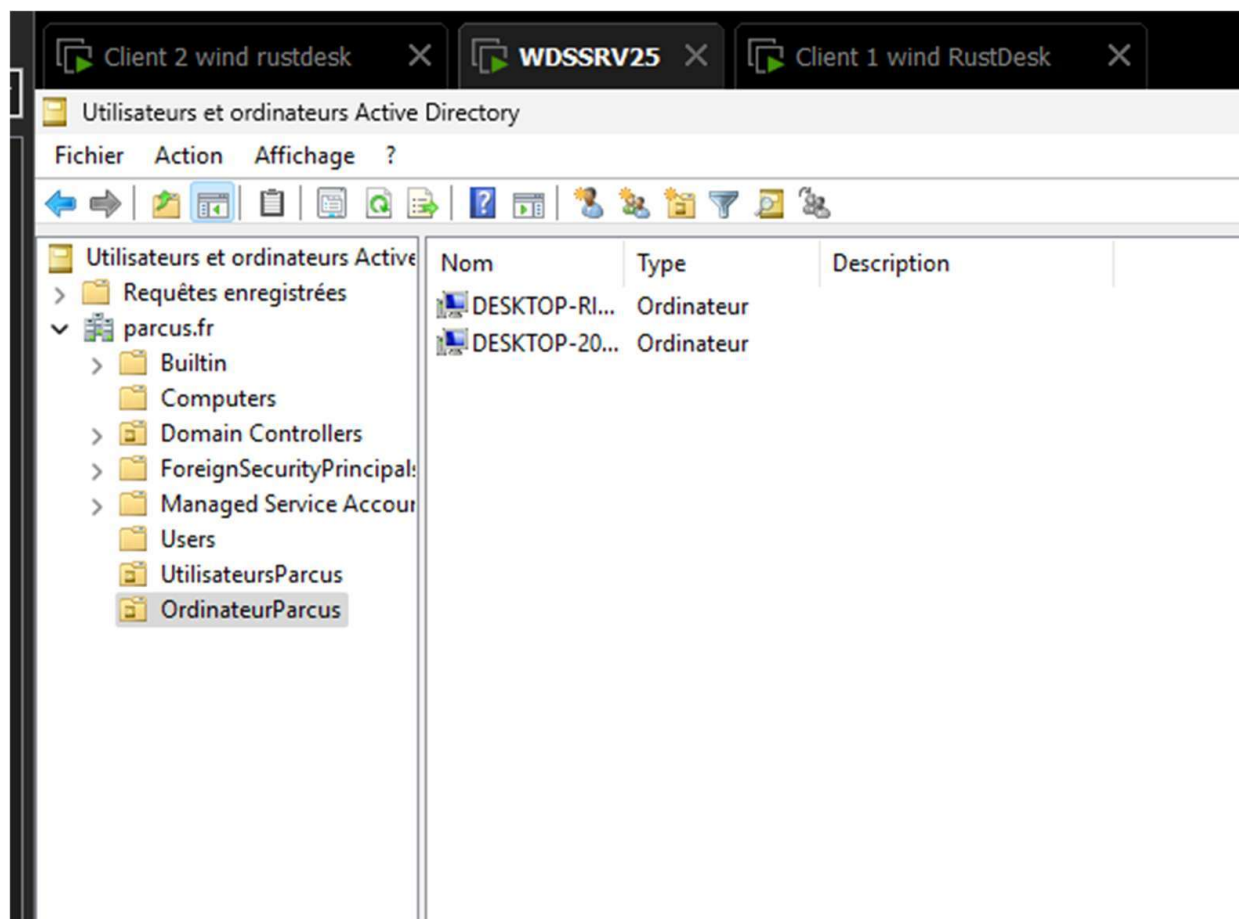
On crée une OU OrdinateurParcus, puis, dans le conteneur Computers, clic droit sur chaque poste > Déplacer... vers cette OU :



Déplacement de DESKTOP-RIV61FL du conteneur Computers vers l'OU OrdinateurParcus

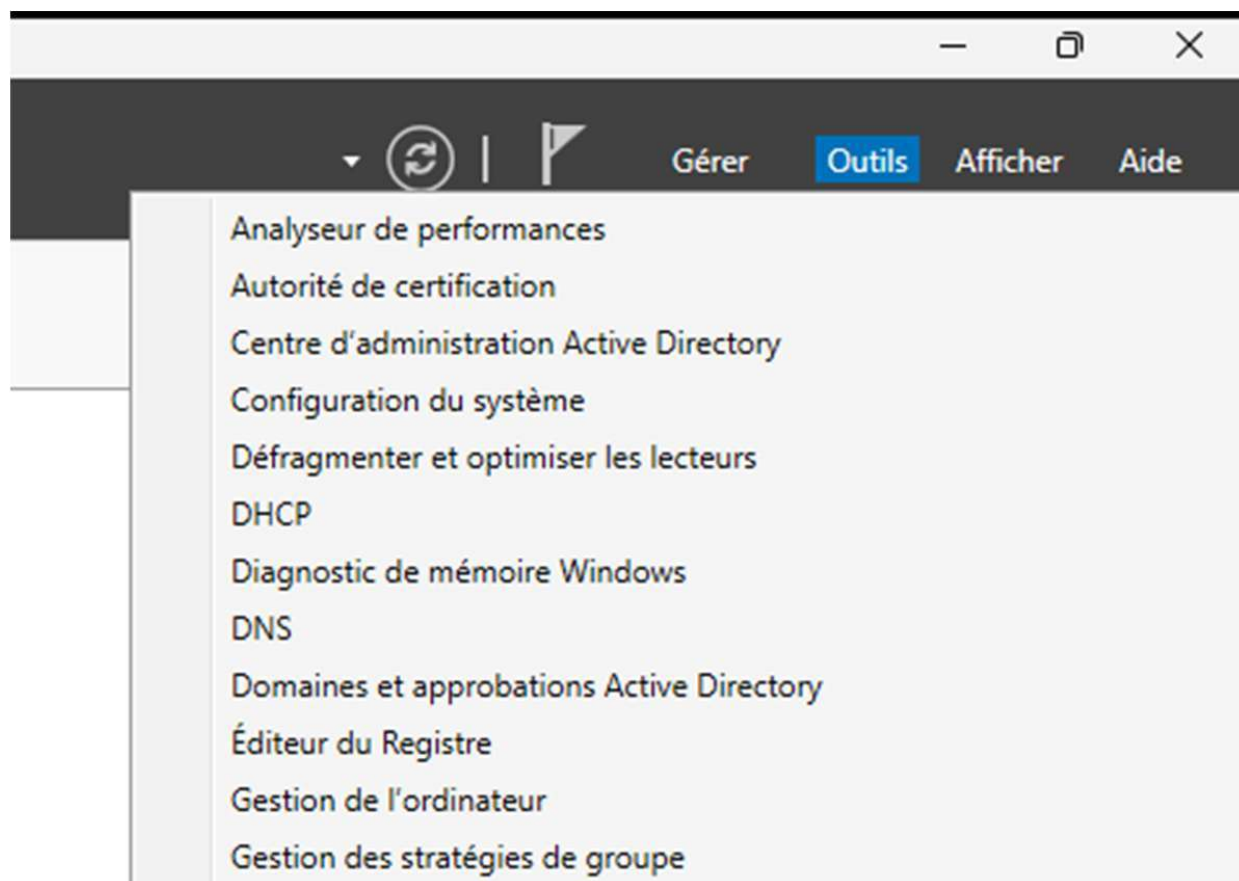


Même opération pour le second poste : destination OrdinateurParcus

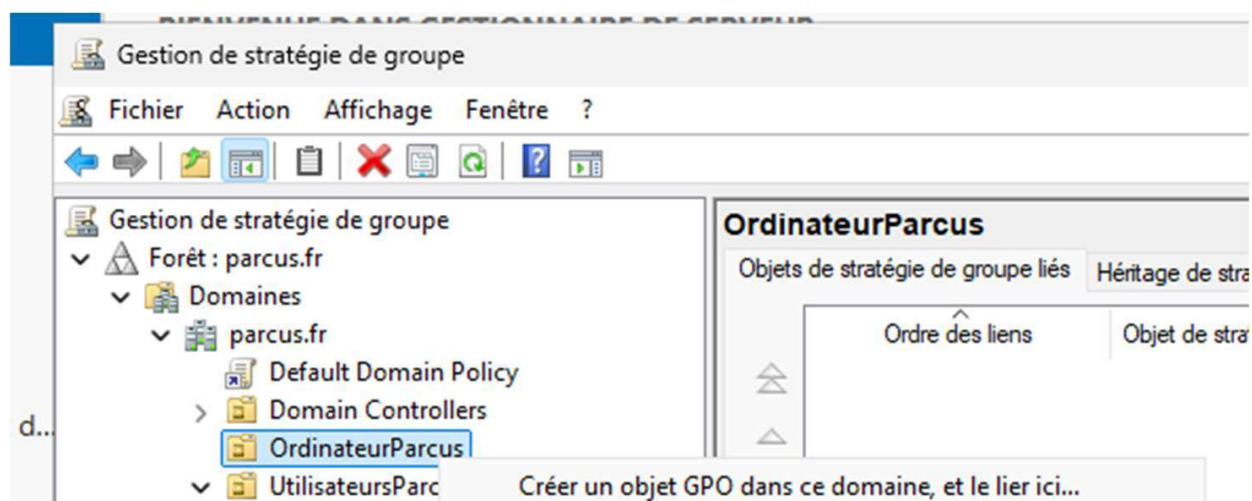


L'OU OrdinateurParcus contient désormais les deux postes clients

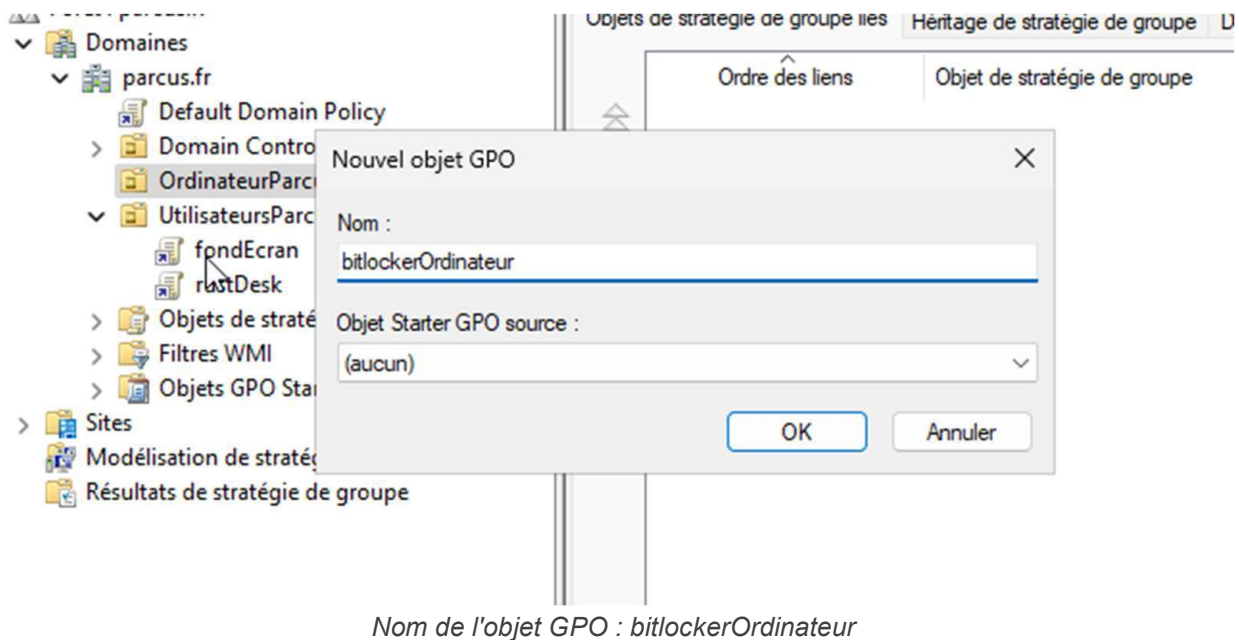
Étape 2 — créer la GPO bitlockerOrdinateur. On ouvre la Gestion des stratégies de groupe (menu Outils), puis clic droit sur l'OU OrdinateurParcus > « Créer un objet GPO dans ce domaine, et le lier ici... » : la GPO est créée et liée en une seule opération.



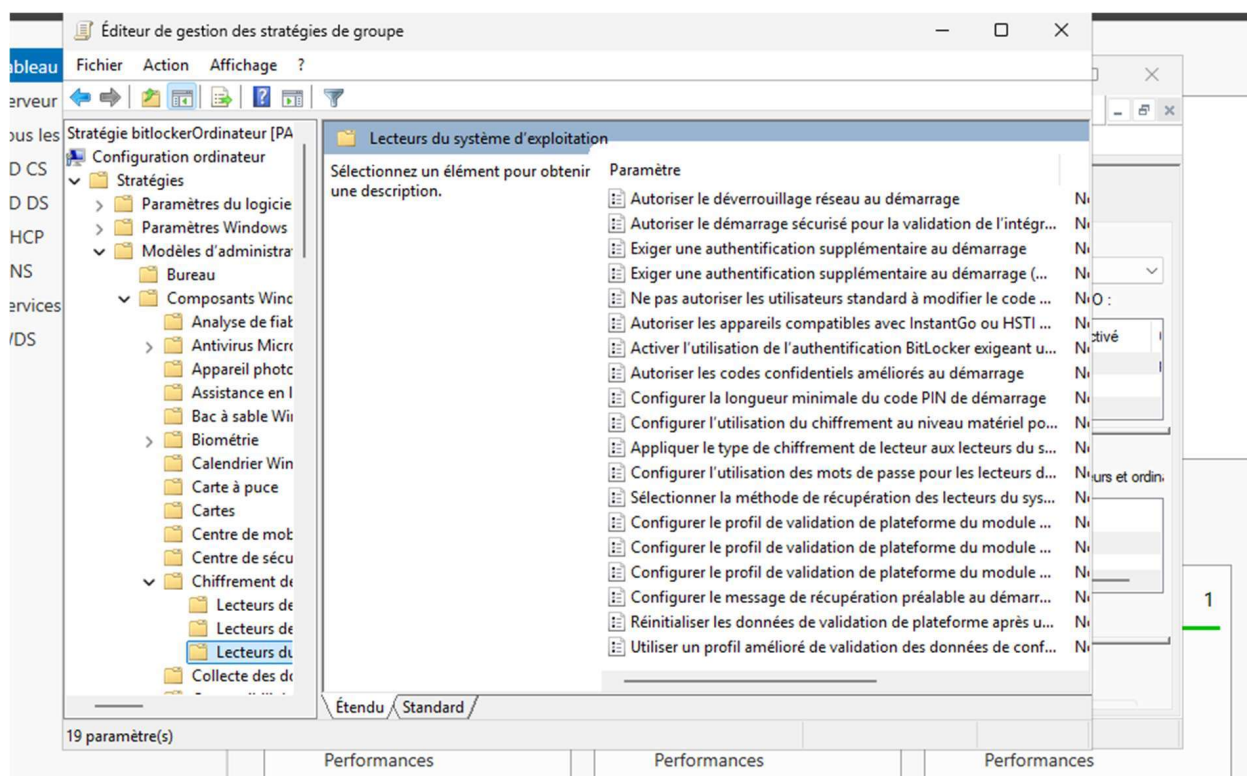
Menu Outils : Gestion des stratégies de groupe



Clic droit sur l'OU OrdinateurParcus : création et liaison de la GPO en une étape

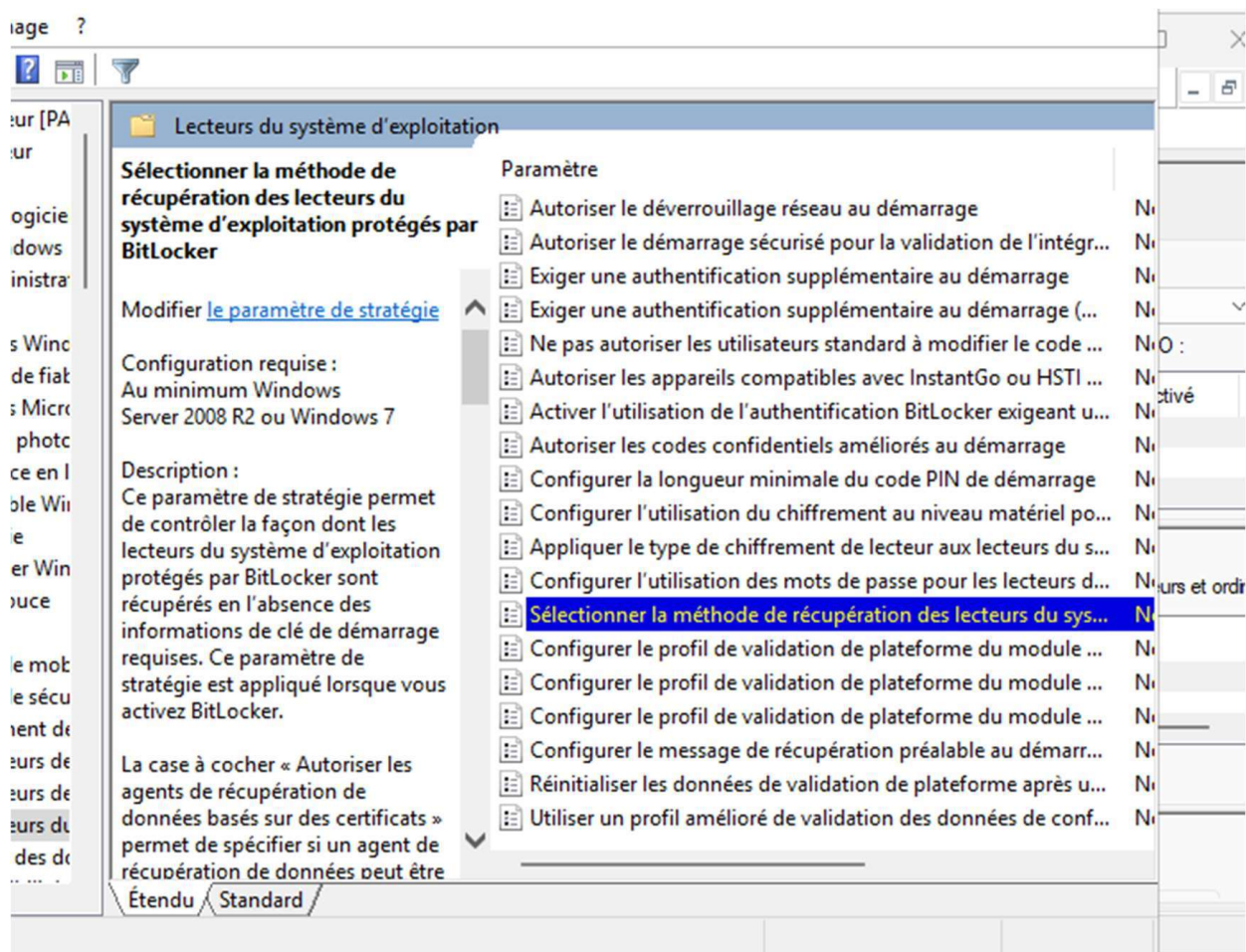


Les paramètres BitLocker se trouvent dans Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs du système d'exploitation (19 paramètres disponibles).



Éditeur de la GPO : la rubrique « Lecteurs du système d'exploitation » du chiffrement BitLocker

Paramètre 1 — Sélectionner la méthode de récupération des lecteurs du système d'exploitation protégés par BitLocker. C'est le paramètre clé du projet : activé, il contrôle la façon dont les lecteurs peuvent être récupérés et permet la sauvegarde des informations de récupération dans l'AD. Il est appliqué au moment où BitLocker est activé sur le poste.



Le paramètre « Sélectionner la méthode de récupération » dans la liste des stratégies

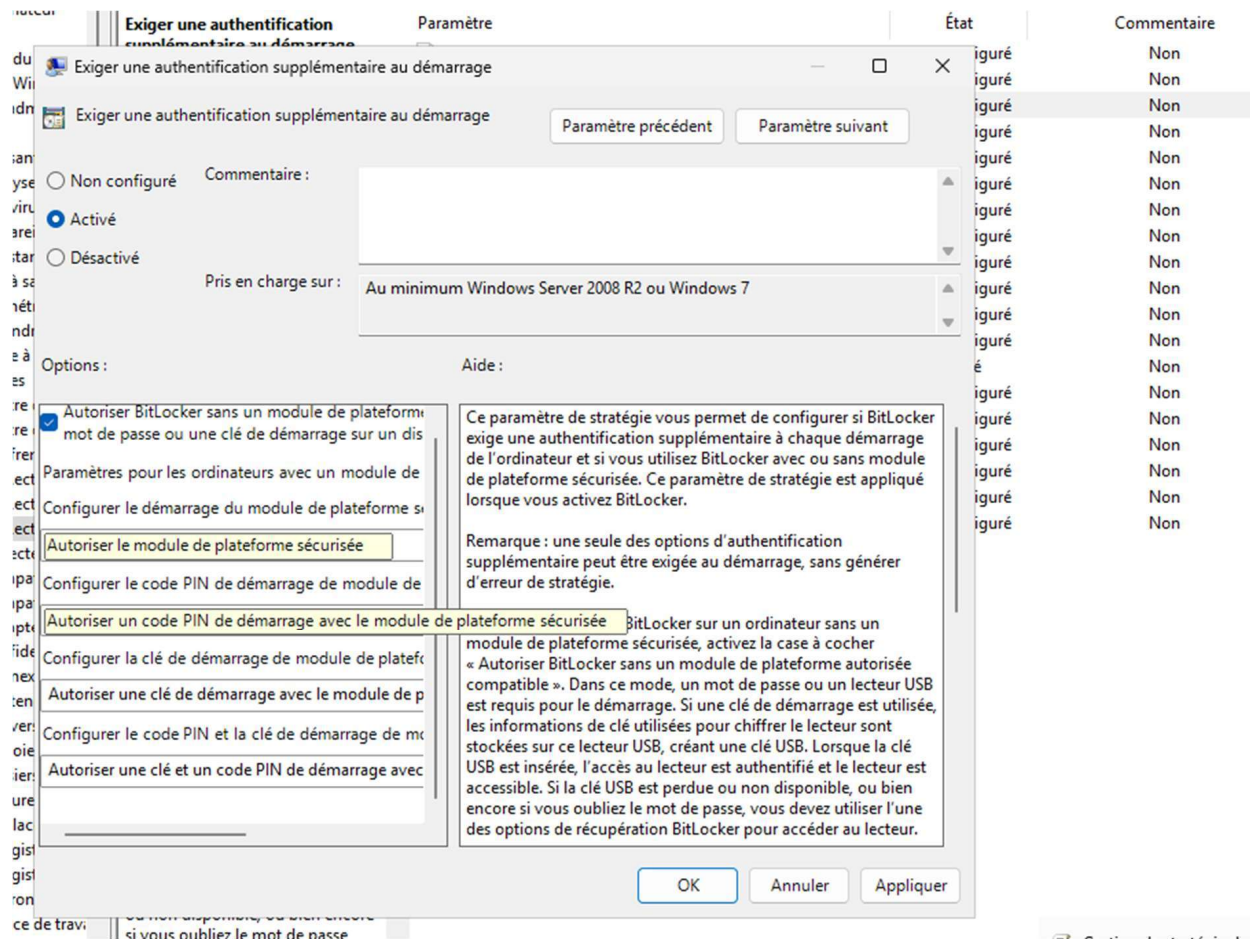
Activer l'utilisation de l'authentification BitLocker exigeant u...	Non configuré	Non
Autoriser les codes confidentiels améliorés au démarrage	Non configuré	Non
Configurer la longueur minimale du code PIN de démarrage	Non configuré	Non
Configurer l'utilisation du chiffrement au niveau matériel po...	Non configuré	Non
Appliquer le type de chiffrement de lecteur aux lecteurs du s...	Non configuré	Non
Configurer l'utilisation des mots de passe pour les lecteurs d...	Non configuré	Non
Sélectionner la méthode de récupération des lecteurs du sys...	Activé	Non
Configurer le profil de validation de plateforme du module ...	Non configuré	Non
Configurer le profil de validation de plateforme du module ...	Non configuré	Non
Configurer le profil de validation de plateforme du module ...	Non configuré	Non
Configurer le message de récupération préalable au démarr...	Non configuré	Non
Réinitialiser les données de validation de plateforme après u...	Non configuré	Non
Utiliser un profil amélioré de validation des données de conf...	Non configuré	Non

Le paramètre passe à l'état « Activé »

Paramètre 2 — Exiger une authentification supplémentaire au démarrage. Activé, il définit les protecteurs autorisés au démarrage. On garde le TPM comme protecteur principal (« Autoriser le module de plateforme sécurisée »), la case « Autoriser BitLocker sans un module de plateforme sécurisée compatible » servant de secours pour d'éventuels postes sans TPM (mot de passe ou clé USB de démarrage).

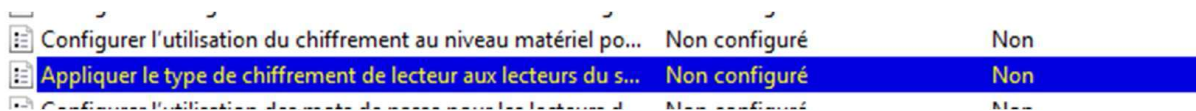
Autoriser le déverrouillage réseau au démarrage	Non configuré	Non
Autoriser le démarrage sécurisé pour la validation de l'intégr...	Non configuré	Non
Exiger une authentification supplémentaire au démarrage	Non configuré	Non
Exiger une authentification supplémentaire au démarrage (...)	Non configuré	Non

Sélection du paramètre « Exiger une authentification supplémentaire au démarrage »

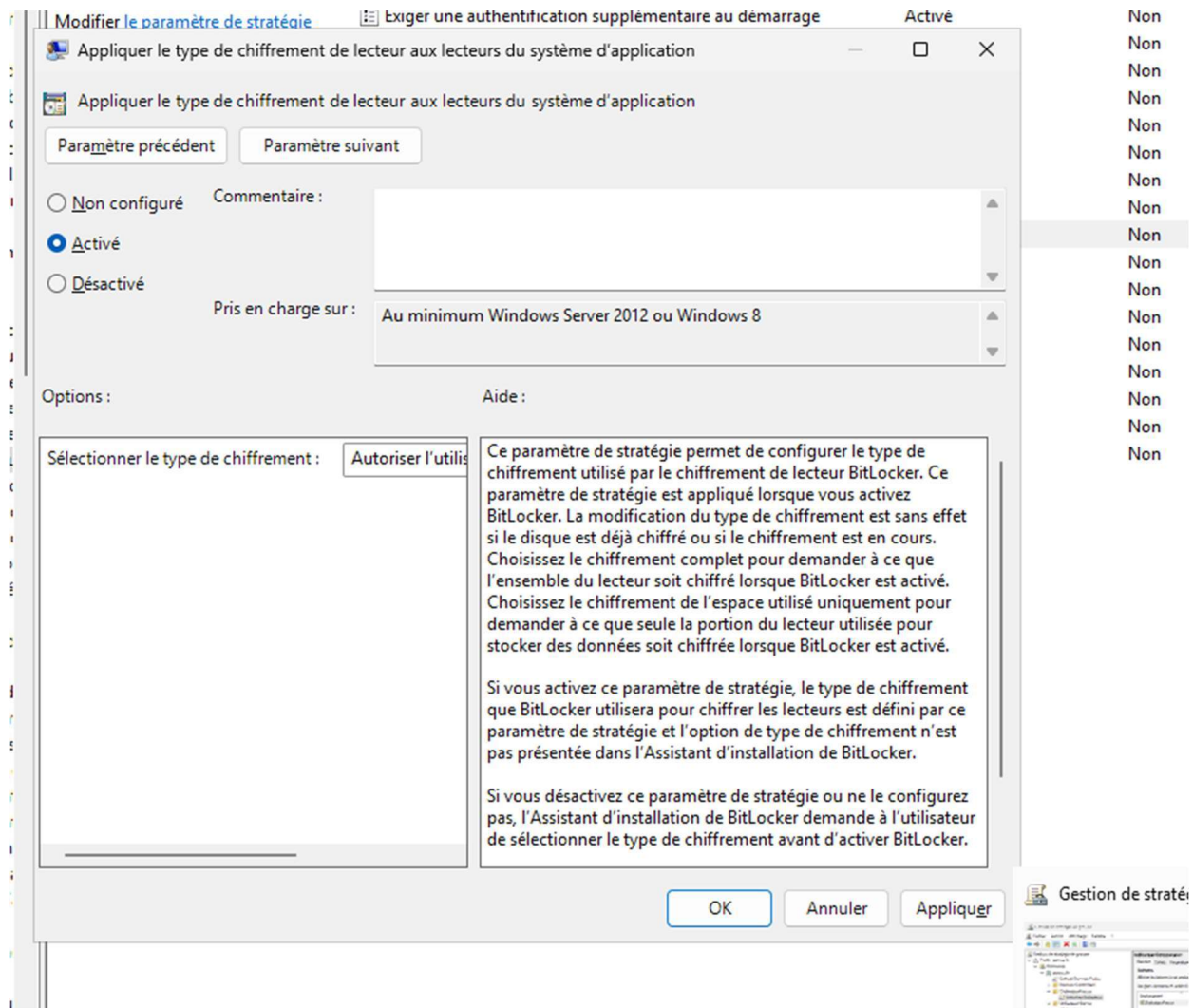


Paramètre activé : options d'authentification au démarrage, TPM autorisé

Paramètre 3 — Appliquer le type de chiffrement de lecteur. Activé, il impose le type de chiffrement (lecteur complet ou espace utilisé uniquement) au moment de l'activation : l'assistant BitLocker ne pose plus la question à l'utilisateur, tous les postes sont chiffrés de la même façon.



Sélection du paramètre « Appliquer le type de chiffrement de lecteur »



Paramètre activé : le type de chiffrement est imposé par la stratégie

Étape 3 — appliquer et vérifier la stratégie. Sur les clients, on force la mise à jour des stratégies sans attendre le cycle automatique, puis on contrôle ce qui a été appliqué :

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

```

Microsoft Windows [version 10.0.26200.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Maxence>hostname
DESKTOP-204Q3GM

C:\Users\Maxence>gpupdate /force
Mise à jour de la stratégie...

```

gpupdate /force sur DESKTOP-204Q3GM : mise à jour immédiate de la stratégie

Le rapport gpresult /r confirme les deux volets : côté utilisateur, le compte Maxence est bien dans l'OU UtilisateursParcus et reçoit ses stratégies depuis PARCUS-WDSSRV-01.parcus.fr ; côté ordinateur, le poste est dans l'OU OrdinateurParcus et la GPO bitlockerOrdinateur figure dans les objets de stratégie appliqués.

```

Microsoft Windows [version 10.0.26200.6584]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Maxence>gpresult /r

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
© Microsoft Corporation. Tous droits réservés.

Créé le 07/07/2026 à 09:44:31

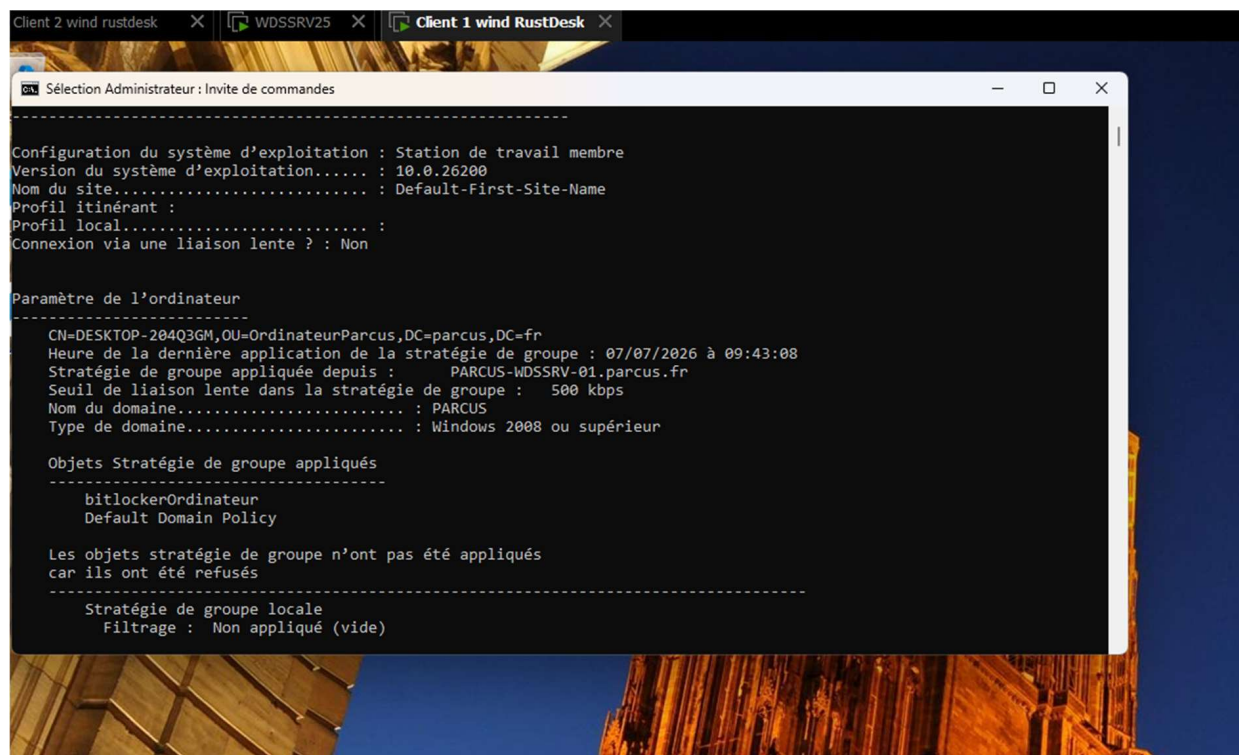
Données RSOP pour PARCUS\Maxence sur DESKTOP-204Q3GM : mode journalisation
-----

Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.26200
Nom du site..... : N/A
Profil itinérant : N/A
Profil local..... : C:\Users\Maxence
Connexion via une liaison lente ? : Non

PARAMÈTRES UTILISATEURS
-----
CN=Maxence,OU=UtilisateursParcus,DC=parcus,DC=fr
Heure de la dernière application de la stratégie de groupe : 07/07/2026 à 09:43:15
Stratégie de groupe appliquée depuis : PARCUS-WDSSRV-01.parcus.fr
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : PARCUS
Type de domaine : Windows 2008 ou supérieur

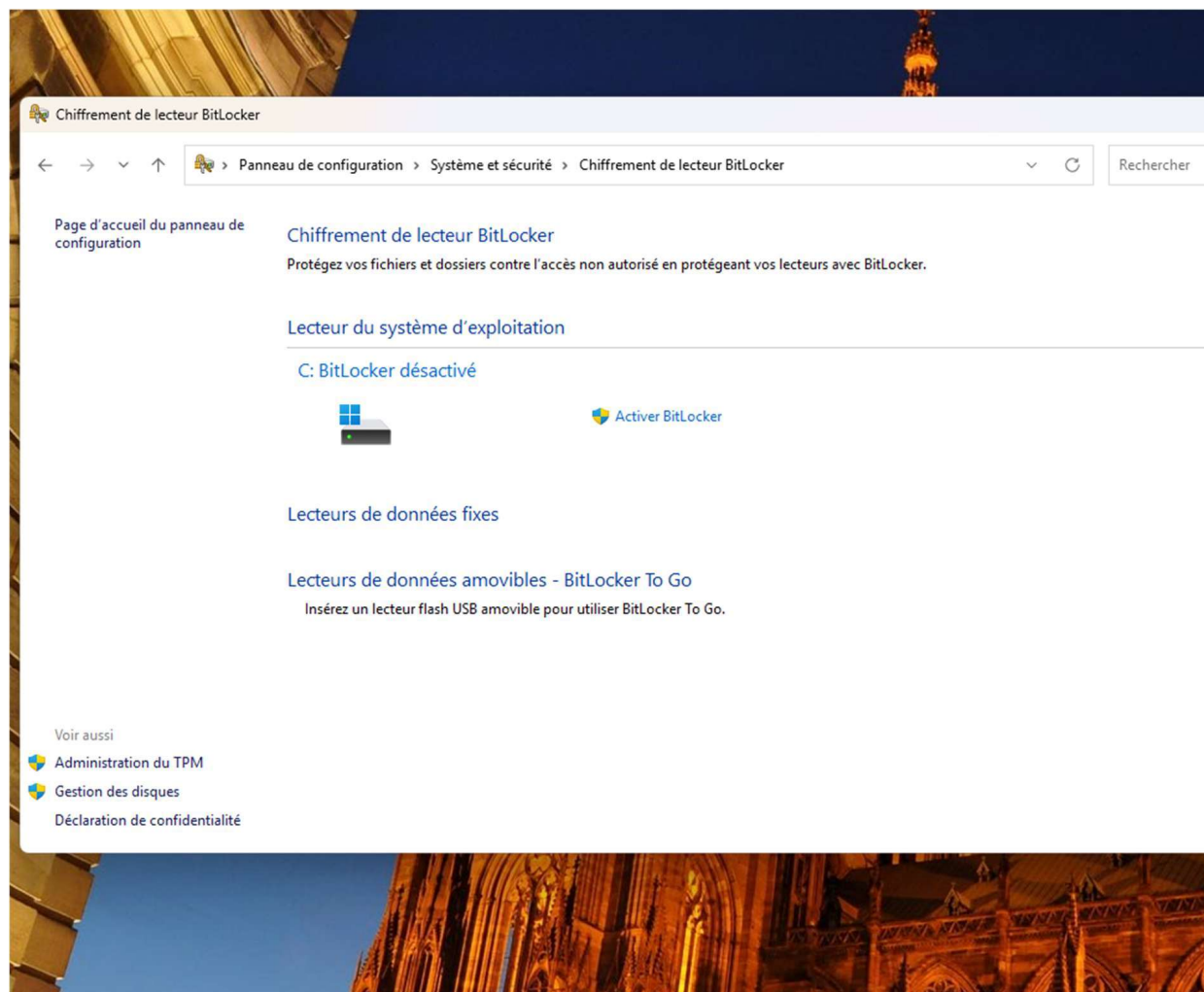
```

gpresult /r, volet utilisateur : CN=Maxence, OU=UtilisateursParcus, stratégies servies par le contrôleur de domaine



gpresult /r, volet ordinateur : la GPO bitlockerOrdinateur est appliquée au poste

Étape 4 — activer BitLocker sur le poste. L'activation se fait dans Panneau de configuration > Système et sécurité > Chiffrement de lecteur BitLocker, lien « Activer BitLocker » sur le lecteur C:.



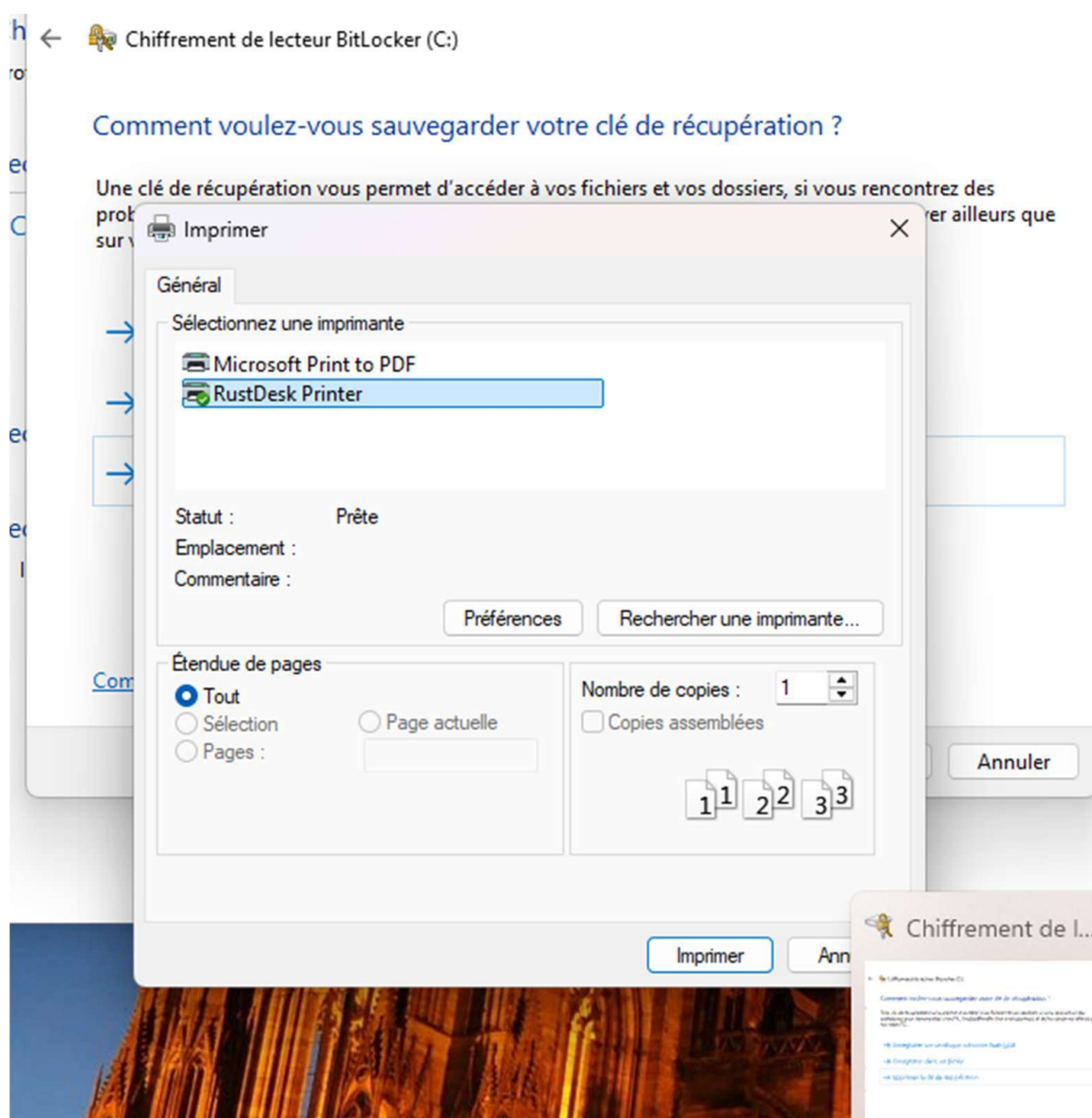
Panneau de configuration : activation de BitLocker sur le lecteur du système d'exploitation

Grâce au TPM, le déverrouillage du lecteur au démarrage sera automatique : aucun code à saisir au quotidien.

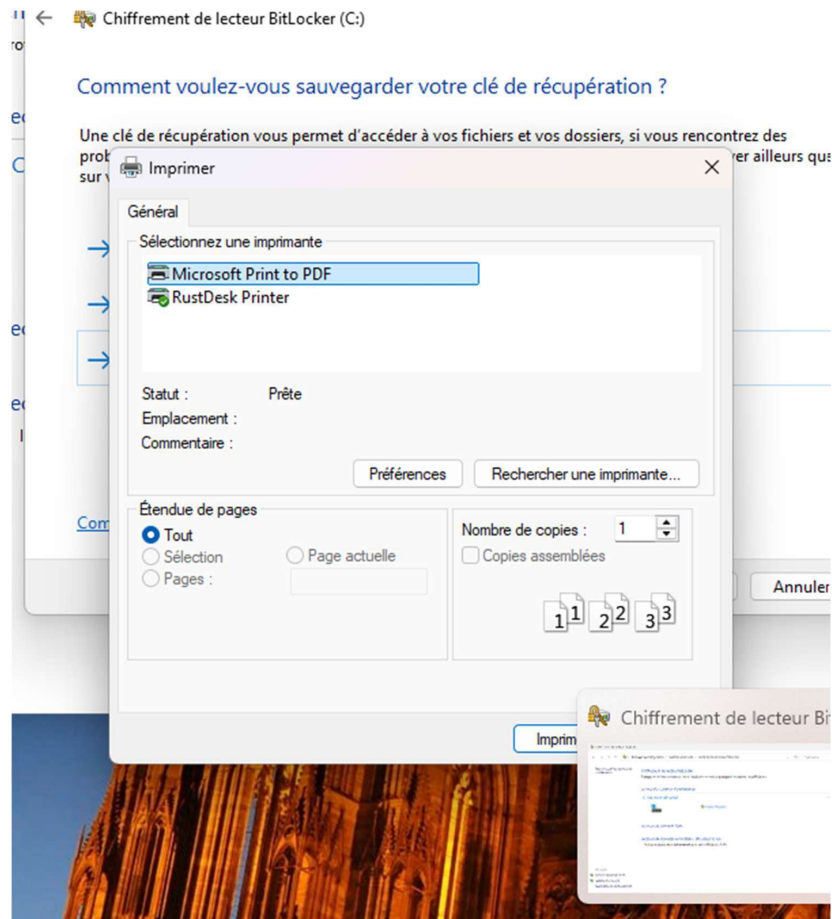
→ Laisser BitLocker déverrouiller automatiquement mon lecteur

L'assistant propose de laisser BitLocker déverrouiller automatiquement le lecteur (TPM)

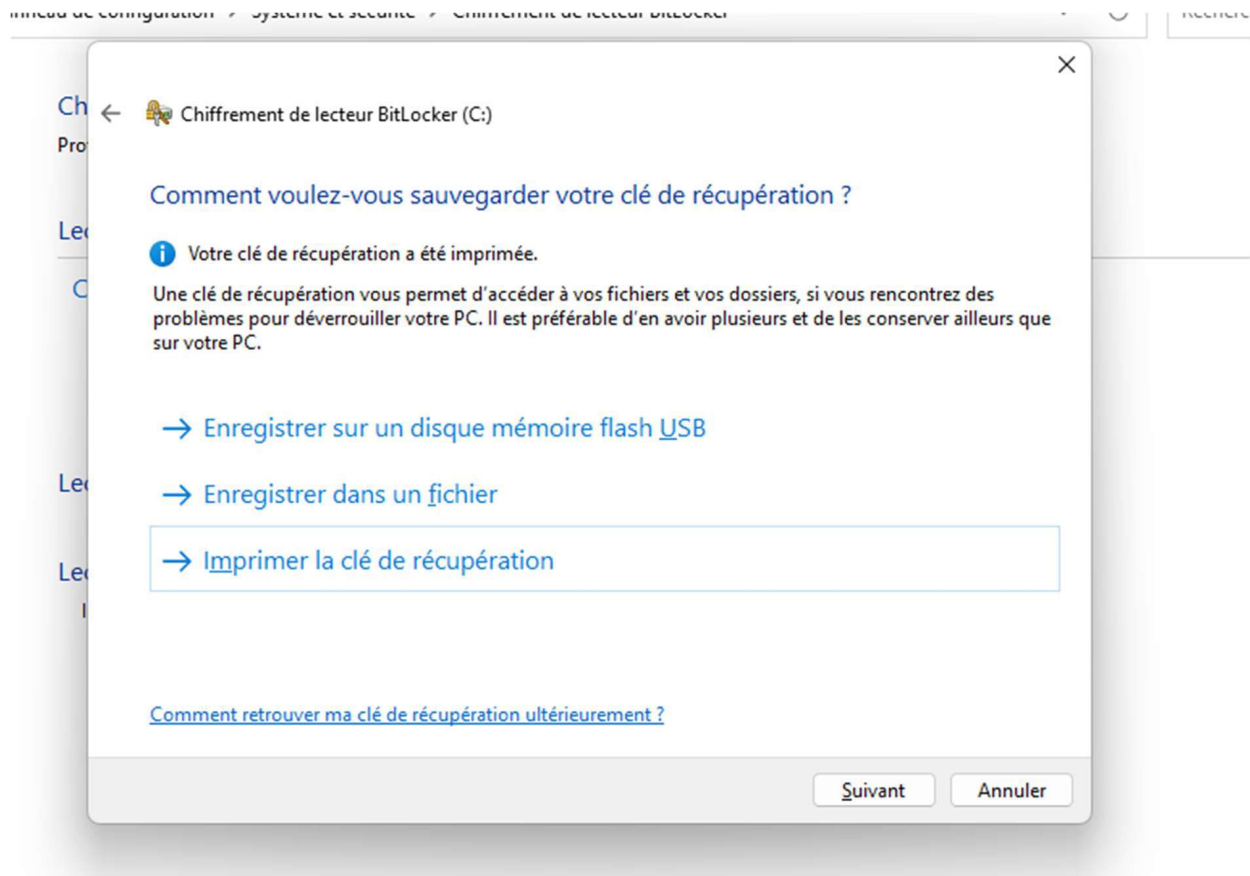
L'assistant demande ensuite comment sauvegarder la clé de récupération. En plus de la sauvegarde automatique dans l'AD imposée par la GPO, on en conserve une copie : sur le client 1, la clé est imprimée via l'imprimante virtuelle RustDesk (clin d'œil au LOT 1), sur le client 2 via Microsoft Print to PDF.



Client 1 : impression de la clé de récupération (imprimante virtuelle RustDesk)

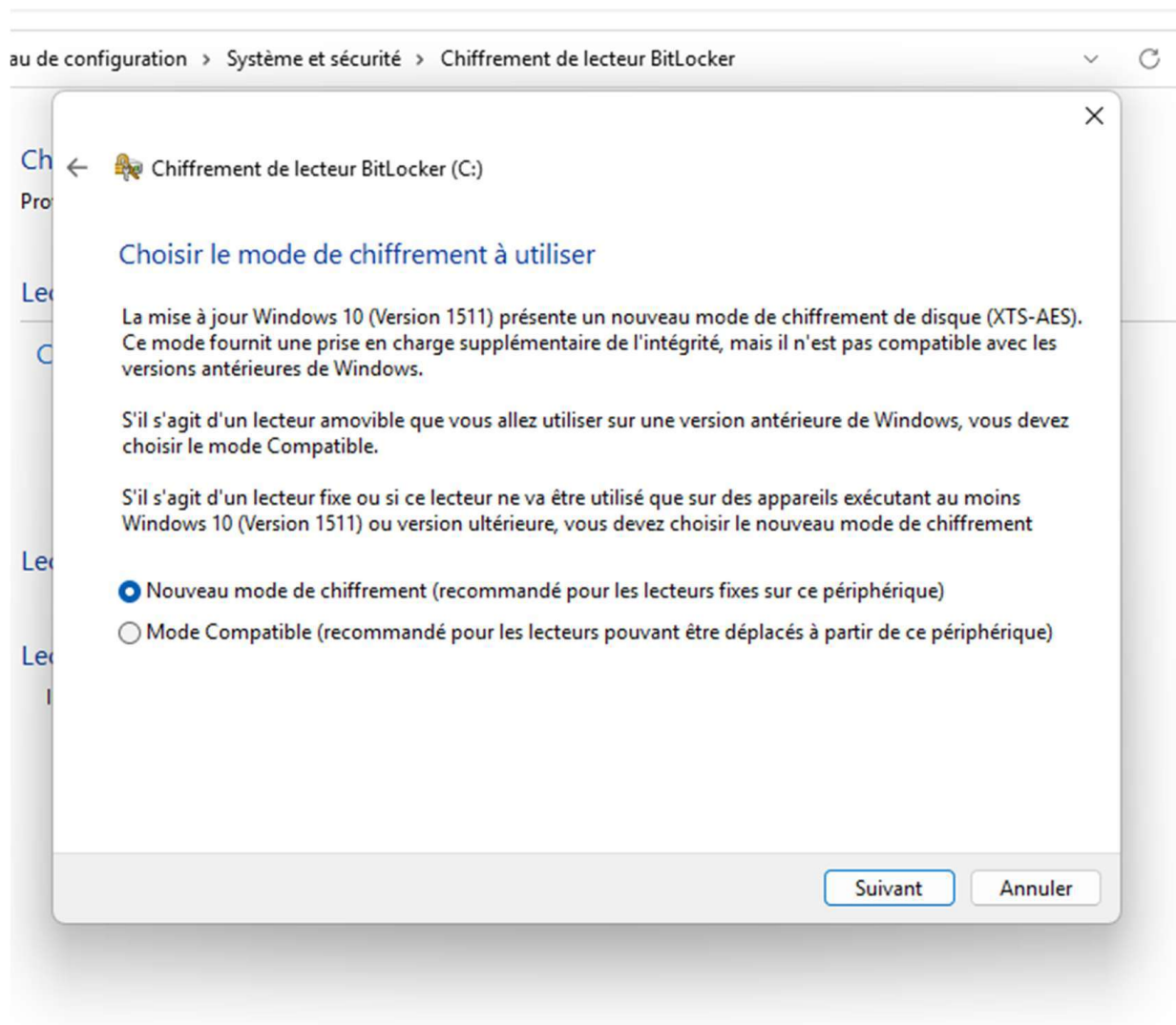


Client 2 : la clé est imprimée vers un fichier PDF (Microsoft Print to PDF)



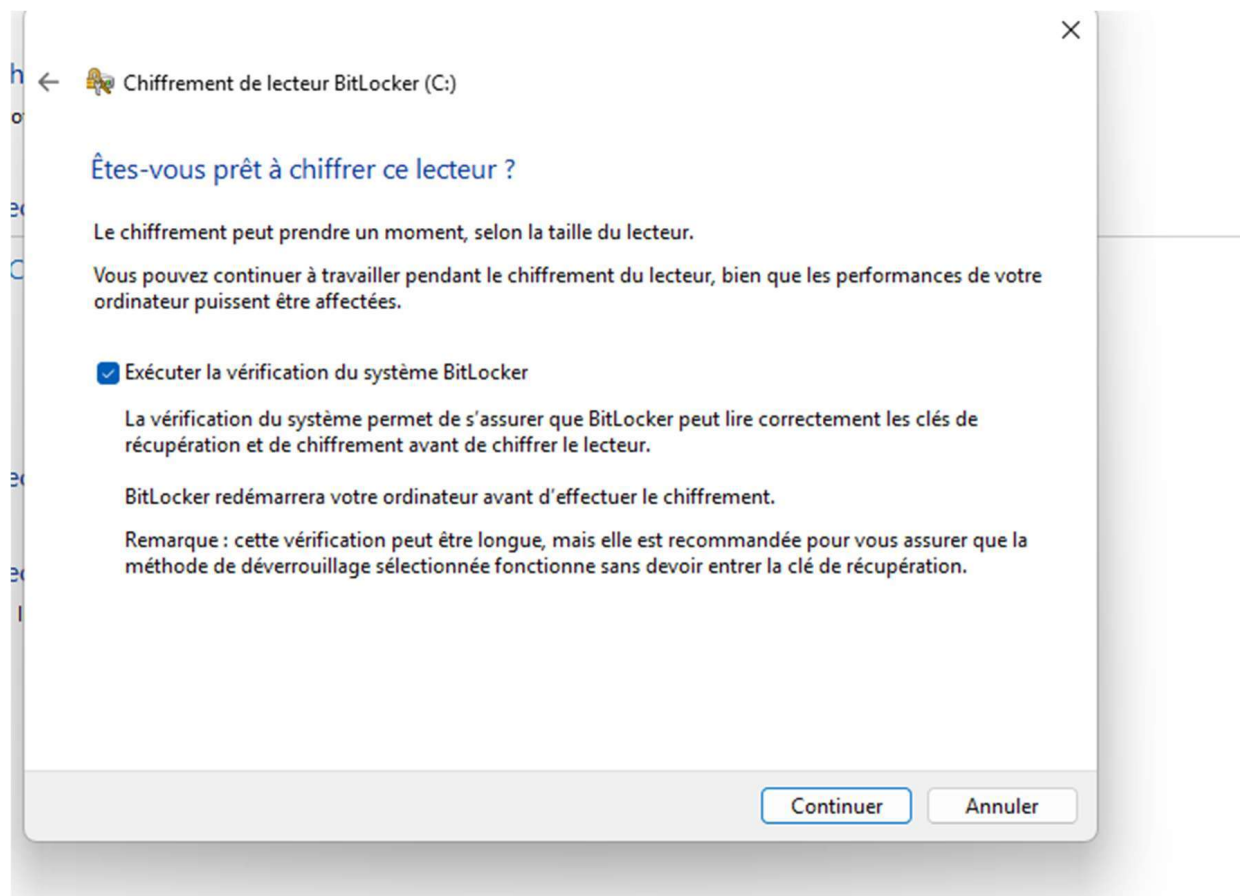
La clé de récupération a été imprimée ; l'assistant peut continuer

On choisit le nouveau mode de chiffrement XTS-AES, recommandé pour les lecteurs fixes (le mode Compatible ne sert que pour des disques amenés à être lus par d'anciennes versions de Windows).

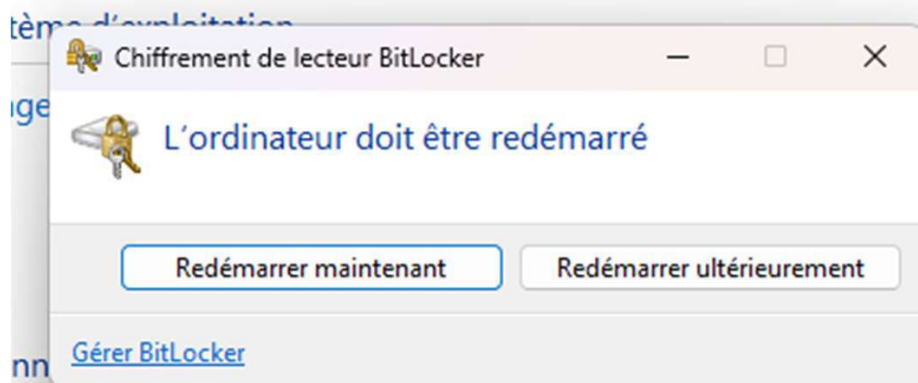


Choix du mode de chiffrement : nouveau mode XTS-AES pour le lecteur fixe

Dernière étape : on laisse cochée l'exécution de la vérification du système BitLocker — le poste redémarre une fois pour valider que le TPM sait bien déverrouiller le lecteur avant de lancer le chiffrement.

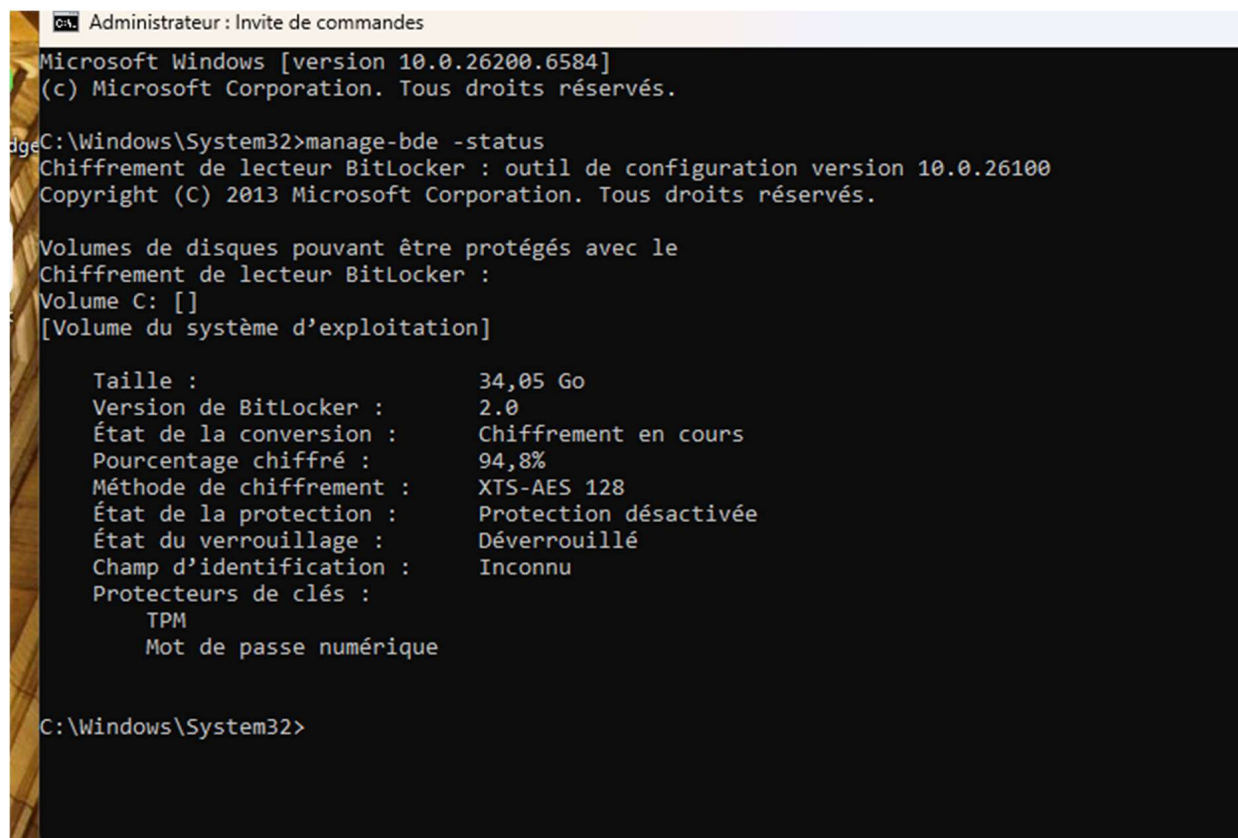


Vérification du système BitLocker avant chiffrement : recommandé, le poste va redémarrer



Redémarrage demandé pour lancer le chiffrement

Après le redémarrage, le chiffrement tourne en tâche de fond ; on peut suivre sa progression avec `manage-bde -status` :



```

Administrateur : Invite de commandes
Microsoft Windows [version 10.0.26200.6584]
(c) Microsoft Corporation. Tous droits réservés.

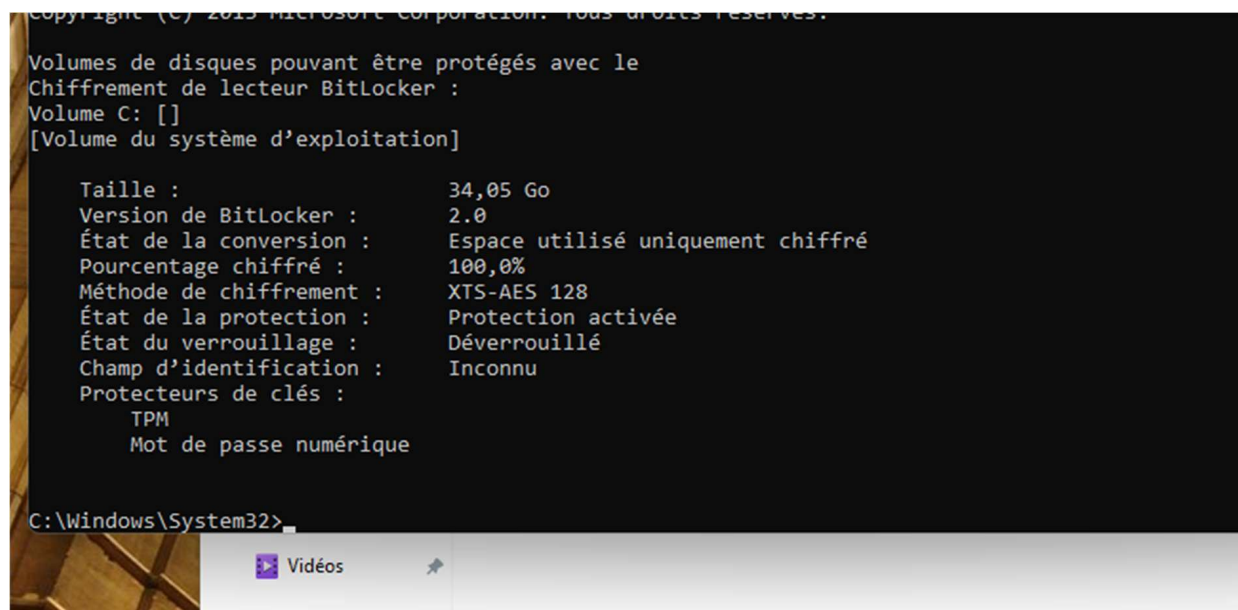
C:\Windows\System32>manage-bde -status
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volumes de disques pouvant être protégés avec le
Chiffrement de lecteur BitLocker :
Volume C: [ ]
[Volume du système d'exploitation]

Taille : 34,05 Go
Version de BitLocker : 2.0
État de la conversion : Chiffrement en cours
Pourcentage chiffré : 94,8%
Méthode de chiffrement : XTS-AES 128
État de la protection : Protection désactivée
État du verrouillage : Déverrouillé
Champ d'identification : Inconnu
Protecteurs de clés :
    TPM
    Mot de passe numérique

C:\Windows\System32>
  
```

Chiffrement en cours : 94,8 % du volume traité, méthode XTS-AES 128



```

Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volumes de disques pouvant être protégés avec le
Chiffrement de lecteur BitLocker :
Volume C: [ ]
[Volume du système d'exploitation]

Taille : 34,05 Go
Version de BitLocker : 2.0
État de la conversion : Espace utilisé uniquement chiffré
Pourcentage chiffré : 100,0%
Méthode de chiffrement : XTS-AES 128
État de la protection : Protection activée
État du verrouillage : Déverrouillé
Champ d'identification : Inconnu
Protecteurs de clés :
    TPM
    Mot de passe numérique

C:\Windows\System32>
  
```

Chiffrement terminé : 100 %, protection activée, protecteurs TPM et mot de passe numérique

Étape 5 — vérifier la clé de récupération dans l'AD. Côté client, on liste les protecteurs de clés du volume :

```
manage-bde -protectors -get C:
```

La sortie affiche le protecteur TPM et le mot de passe numérique de récupération (48 chiffres), avec la mention qui nous intéresse : type de sauvegarde « Sauvegarde de l'AD » — la GPO a bien poussé la clé dans l'annuaire au moment de l'activation.

```

C:\Windows\System32>manage-bde -protectors -get C:
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volume C: [ ]
Tous les protecteurs de clés

TPM :
  ID : {14C65455-95BA-485C-890F-E3514F965B77}
  Profil de validation PCR :
    0, 2, 4, 11

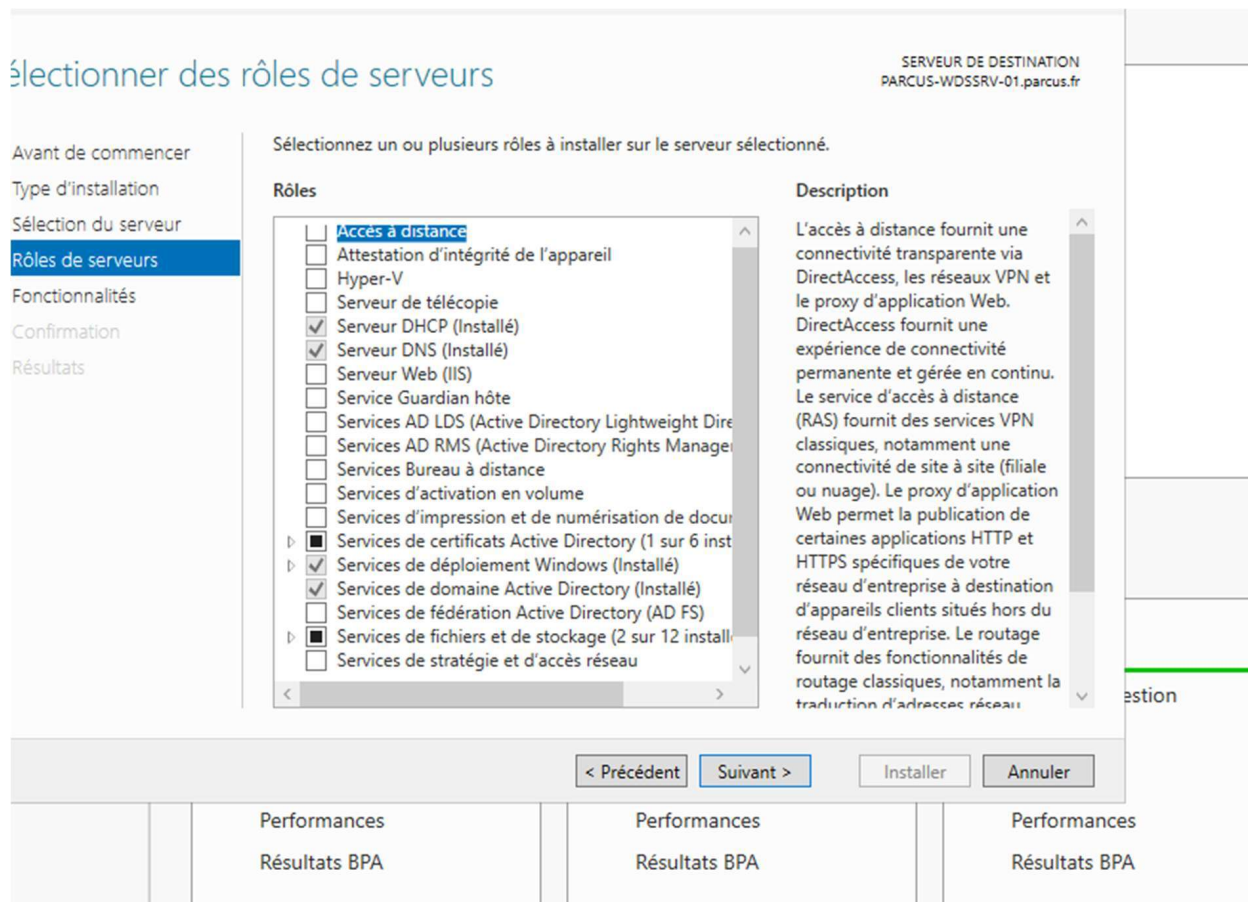
Mot de passe numérique :
  ID : {1911F82D-1A0D-412F-A49F-B08FAFB5A42B}
  Mot de passe :
    160842-236038-045661-104544-175989-568304-060302-176429
  Type de sauvegarde :
    Sauvegarde de l'AD
    Imprimé

C:\Windows\System32>

```

Protecteurs du volume C: du client 1 : mot de passe numérique avec sauvegarde dans l'AD (et copie imprimée)

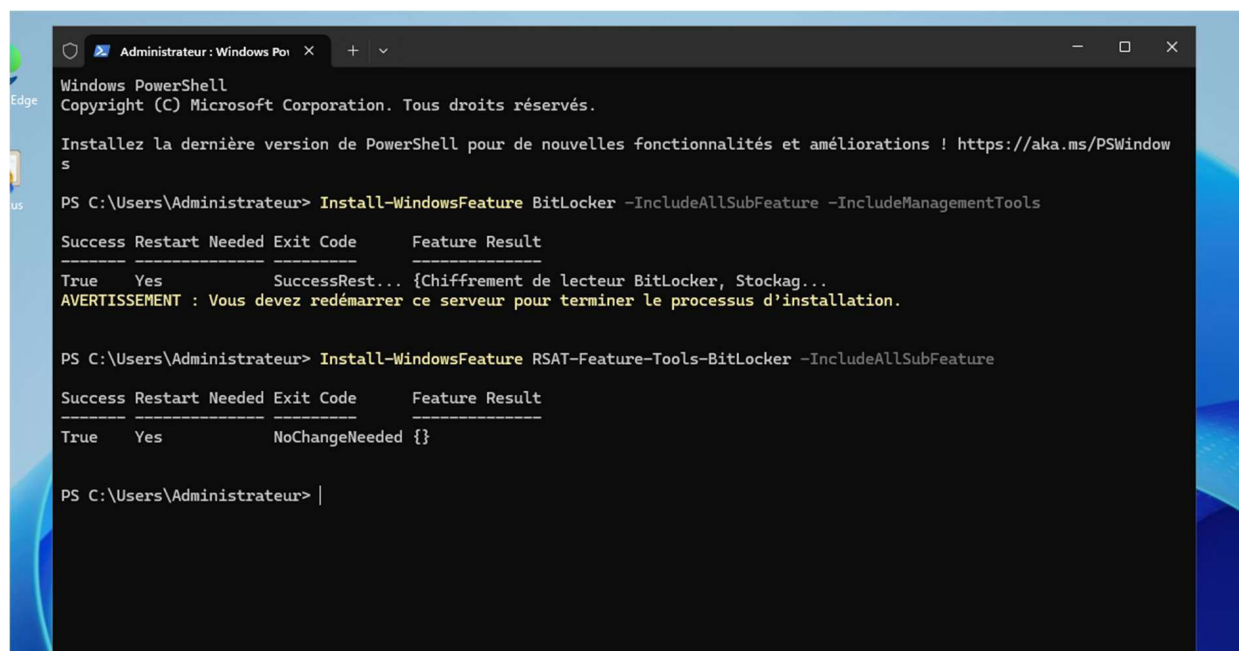
Côté serveur, l'onglet de visualisation des clés n'existe pas par défaut dans la console ADUC : il faut installer la fonctionnalité BitLocker et ses outils d'administration RSAT sur le contrôleur de domaine. Plutôt que de cocher les fonctionnalités une à une dans l'assistant graphique, on passe par PowerShell :



L'assistant de rôles du serveur : on préfère installer les outils BitLocker en PowerShell

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools
```

```
Install-WindowsFeature RSAT-Feature-Tools-BitLocker -IncludeAllSubFeature
```



Installation des fonctionnalités BitLocker et RSAT sur PARCUS-WDSSRV-01 (un redémarrage est demandé pour la première)

```
Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools
```

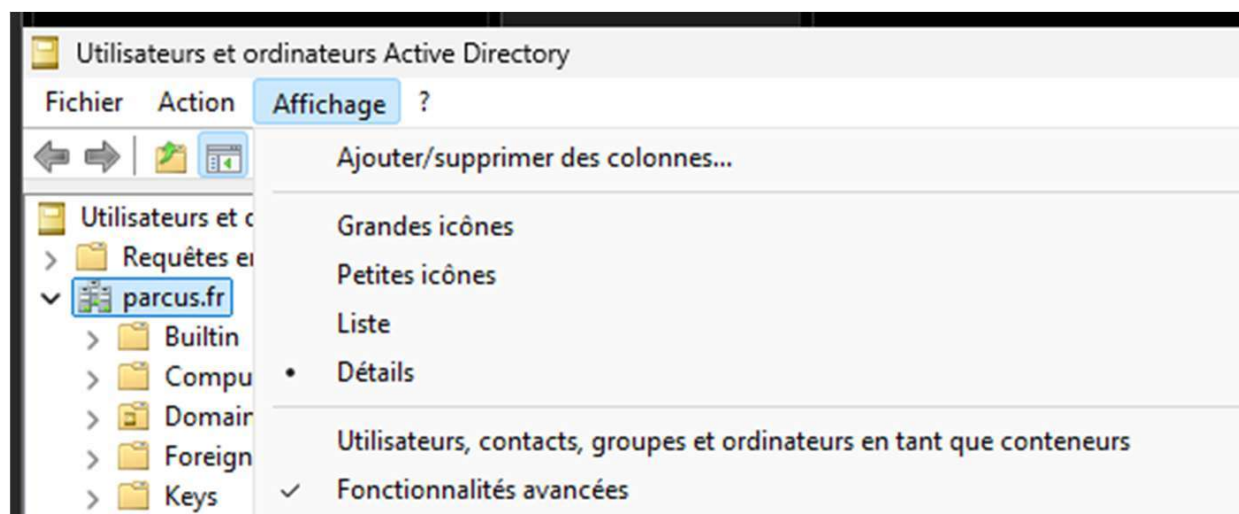
La commande d'installation de la fonctionnalité BitLocker et de ses outils de gestion

</> PowerShell

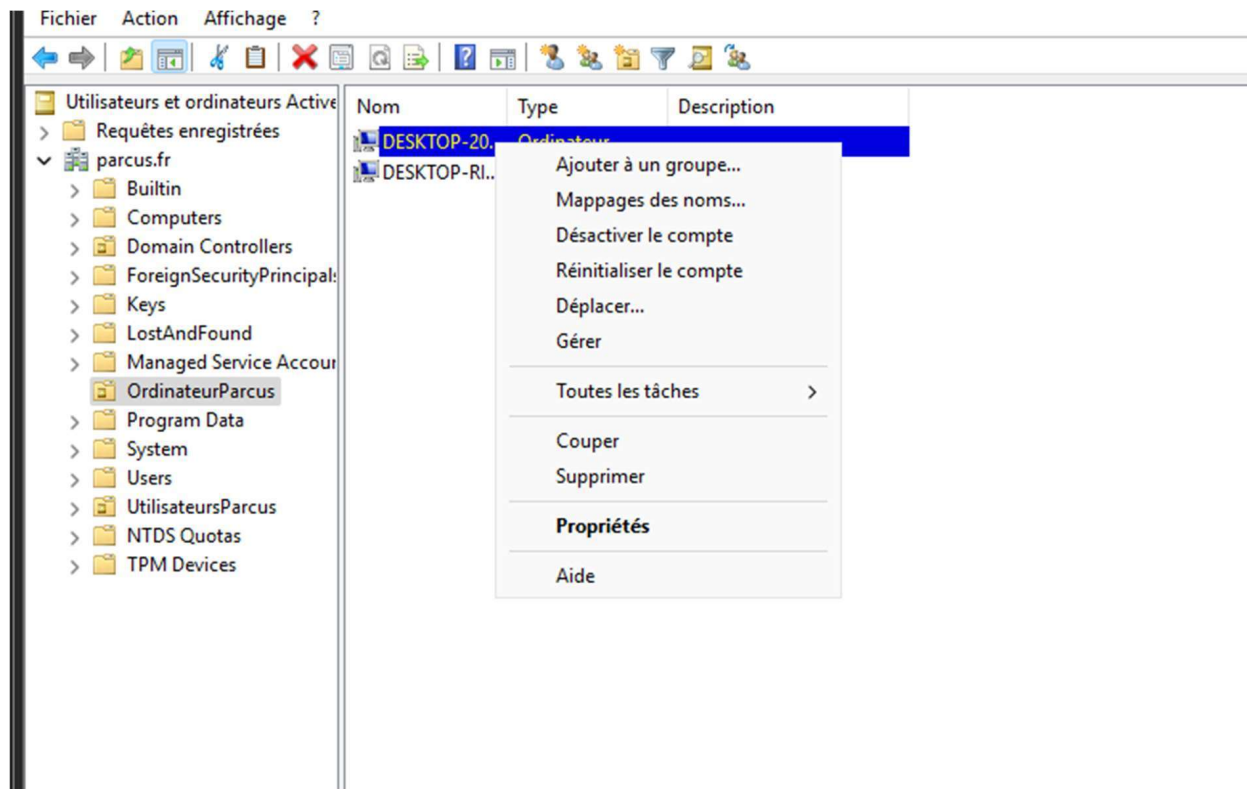
```
Install-WindowsFeature RSAT-Feature-Tools-BitLocker -IncludeAllSubFeature
```

La commande d'installation des outils RSAT de visualisation BitLocker

Dans la console ADUC, on active ensuite Affichage > Fonctionnalités avancées, puis on ouvre les Propriétés du poste dans l'OU OrdinateurParcus :

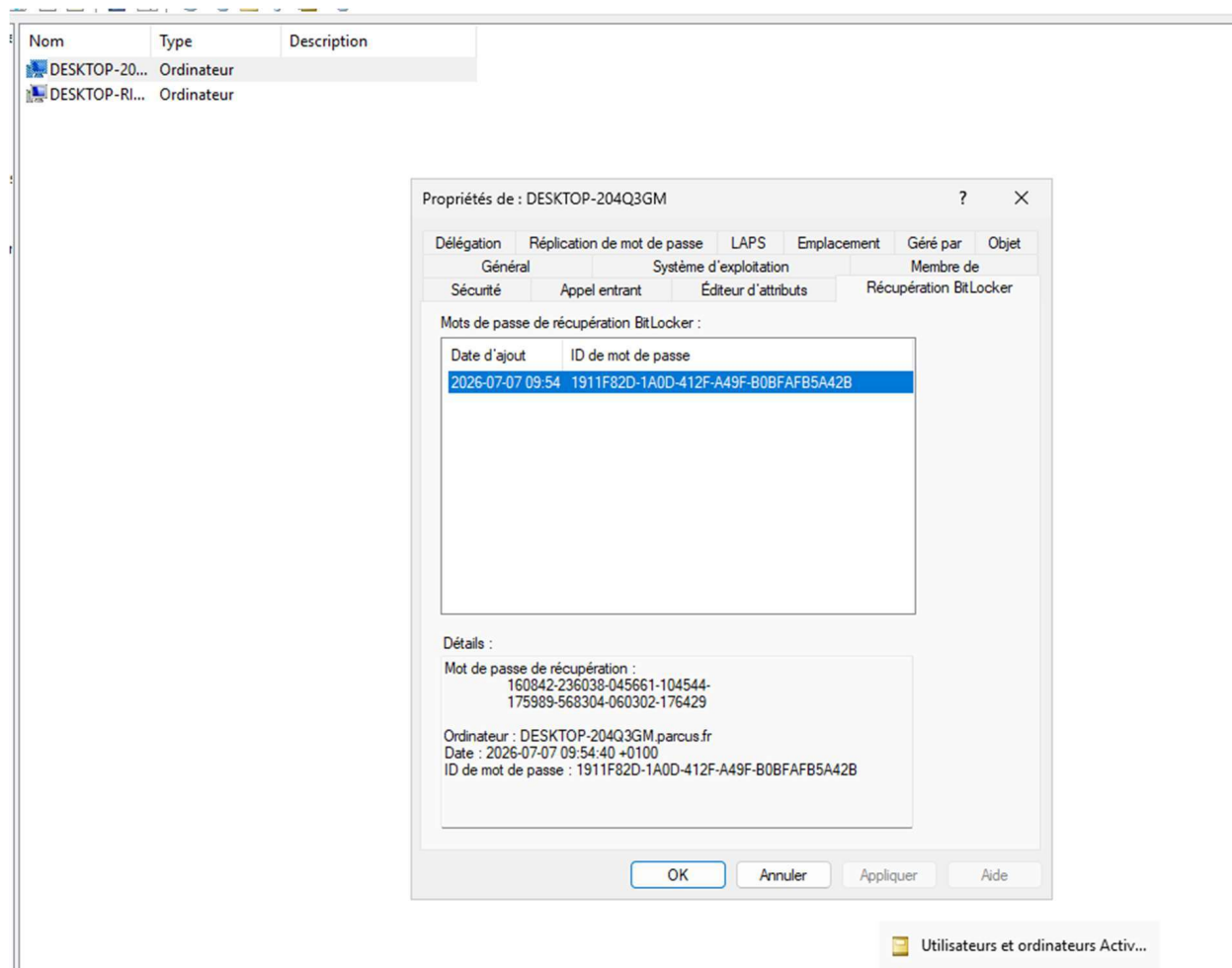


Console ADUC : activation des Fonctionnalités avancées dans le menu Affichage



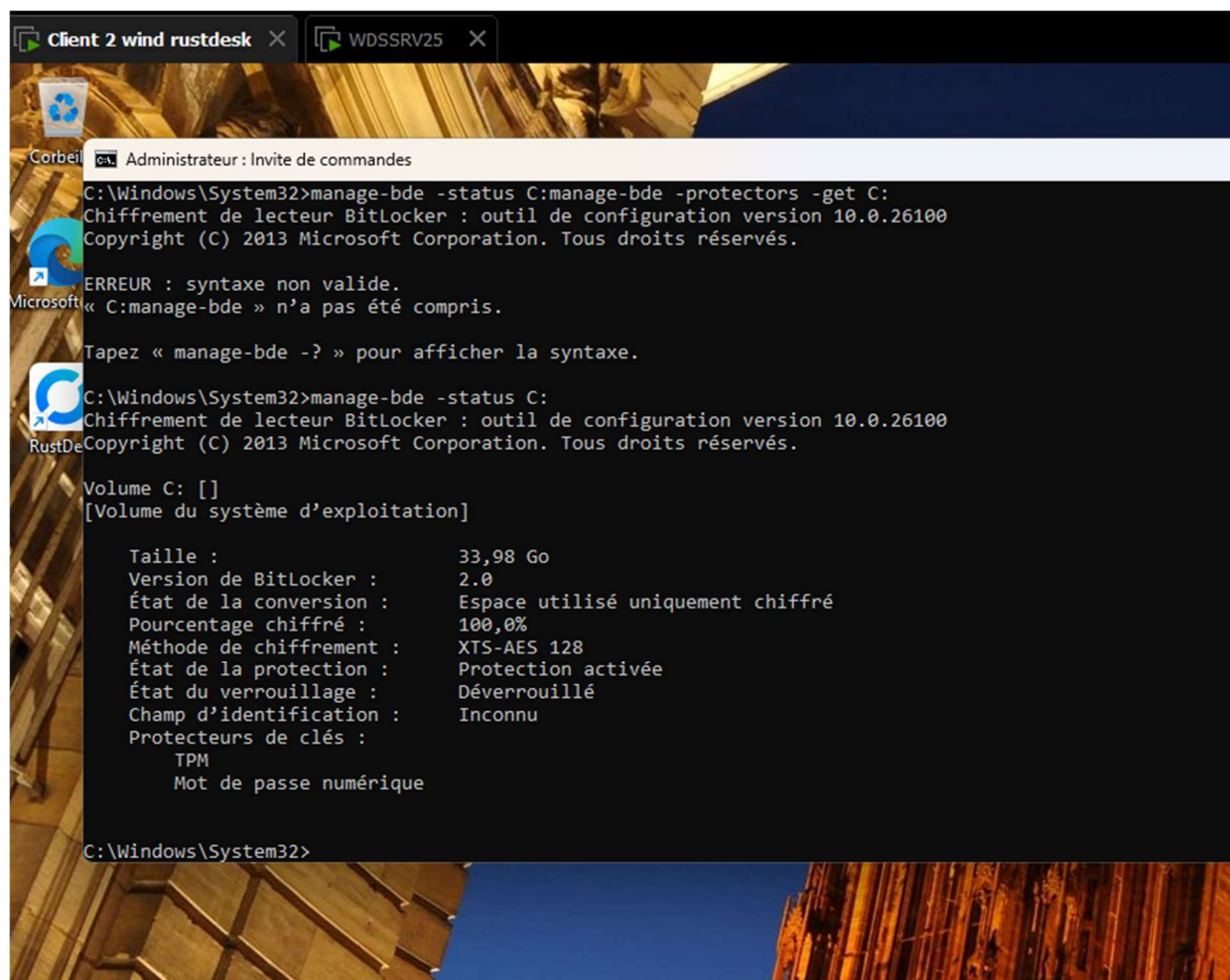
Clic droit sur le poste DESKTOP-204Q3GM : Propriétés

L'onglet Récupération BitLocker liste les mots de passe de récupération du poste : la date d'ajout, l'identifiant du mot de passe et la clé de 48 chiffres — les mêmes que dans la sortie manage-bde du client. Le technicien peut donc dépanner n'importe quel poste verrouillé sans toucher à la machine.



Onglet Récupération BitLocker de DESKTOP-204Q3GM : la clé de récupération est bien stockée dans l'annuaire

Second client. La même procédure est déroulée sur DESKTOP-RIV61FL : chiffrement à 100 % en XTS-AES 128, protection activée, protecteurs TPM et mot de passe numérique. Petit détail visible sur la capture : la première commande renvoie « syntaxe non valide » parce que les deux commandes manage-bde ont été collées sur la même ligne — ressaisies séparément, tout fonctionne.



```
Client 2 wind rustdesk x WDSSRV25 x
Corbeil Administrateur : Invite de commandes
C:\Windows\System32>manage-bde -status C:manage-bde -protectors -get C:
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

ERREUR : syntaxe non valide.
« C:manage-bde » n'a pas été compris.

Tapez « manage-bde -? » pour afficher la syntaxe.

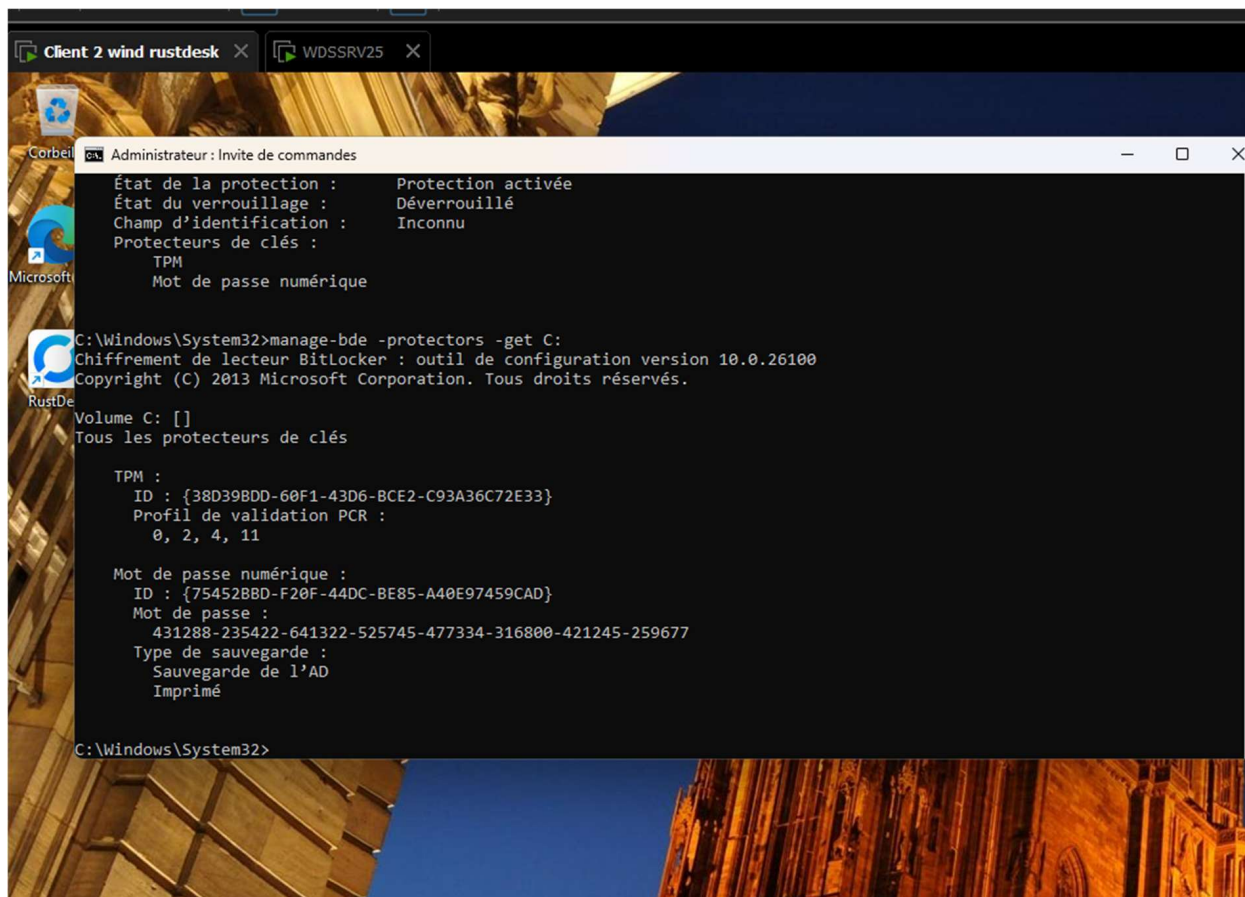
C:\Windows\System32>manage-bde -status C:
Chiffrement de lecteur BitLocker : outil de configuration version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volume C: []
[Volume du système d'exploitation]

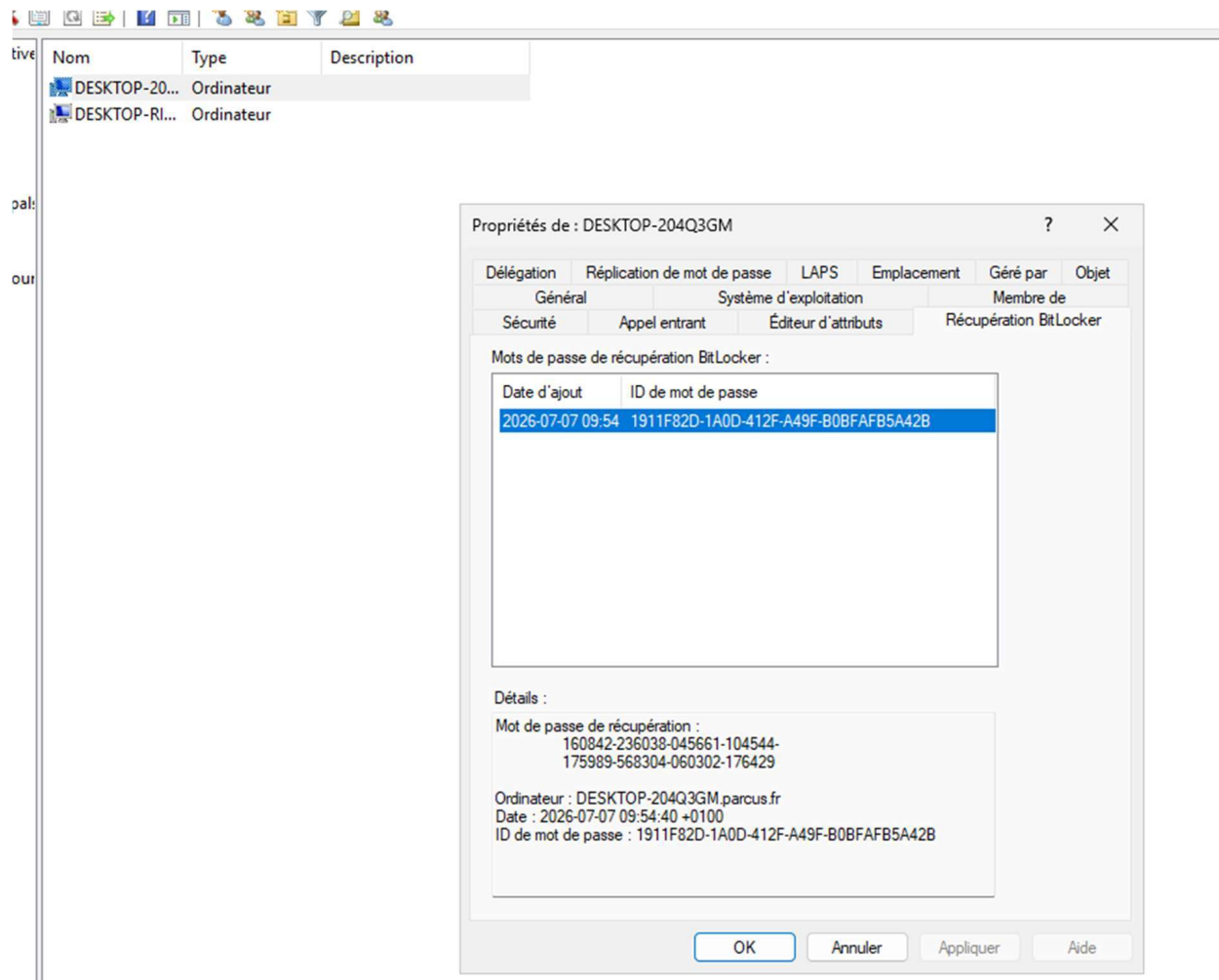
Taille : 33,98 Go
Version de BitLocker : 2.0
État de la conversion : Espace utilisé uniquement chiffré
Pourcentage chiffré : 100,0%
Méthode de chiffrement : XTS-AES 128
État de la protection : Protection activée
État du verrouillage : Déverrouillé
Champ d'identification : Inconnu
Protecteurs de clés :
    TPM
    Mot de passe numérique

C:\Windows\System32>
```

Client 2 : lecteur chiffré à 100 %, protection activée (la première ligne était une faute de frappe, deux commandes collées)



Protecteurs du client 2 : mot de passe numérique sauvegardé dans l'AD, comme sur le client 1



L'onglet Récupération BitLocker centralise ainsi les clés de tous les postes du domaine, poste par poste

Le chiffrement BitLocker de la maquette est complet : postes chiffrés en XTS-AES 128, déverrouillage transparent par TPM, et clés de récupération centralisées dans Active Directory, consultables uniquement par les administrateurs du domaine.

Plan de tests

Ce plan de tests valide le bon fonctionnement de chaque lot du projet. Chaque test précise l'objectif, la procédure suivie, le résultat attendu et le statut constaté lors de la recette. Les tests ont été rejoués après chaque modification importante de l'infrastructure.

Tests du LOT 1 — RustDesk

N°	Objectif du test	Procédure	Résultat attendu	Statut
RD-01	Adressage du serveur	Sur la VM RustDesk, exécuter <code>ip a</code> et vérifier l'adresse portée par <code>ens33</code> .	<code>ens33</code> porte l'IP fixe 192.168.137.4.	OK
RD-02	Accès Internet de la VM	Exécuter <code>ping -c 4 8.8.8.8</code> depuis la VM serveur.	Les 4 pings répondent (sortie via <code>ens37</code> en DHCP).	OK
RD-03	Service Docker actif	Exécuter <code>systemctl status docker</code> .	Statut « active (running) », service « enabled » au démarrage.	OK
RD-04	Conteneurs RustDesk démarrés	Exécuter <code>sudo docker ps</code> sur le serveur.	<code>hbbs</code> et <code>hbbr</code> apparaissent au statut « Up ».	OK
RD-05	Clé publique générée	Exécuter <code>cat ~/.rustdesk/id_ed25519.pub</code> .	Une clé se terminant par « = » est affichée.	OK
RD-06	Persistance après redémarrage	Redémarrer la VM serveur, puis refaire <code>docker ps</code> .	Les deux conteneurs redémarrent seuls (restart unless-stopped).	OK
RD-07	Joignabilité depuis un client	Depuis Client 1 (192.168.137.11), ping 192.168.137.4.	Le serveur répond au ping.	OK
RD-08	Enregistrement d'un client	Configurer Serveur ID + clé sur un poste, observer l'écran d'accueil.	Le client affiche « prêt » (pastille verte) et son ID.	OK
RD-09	Connexion par mot de passe	Depuis Client 1, saisir l'ID de Client 2 puis le mot de passe à usage unique communiqué.	La session de prise en main s'ouvre.	OK
RD-10	Connexion par acceptation	Depuis Client 1, demander la connexion ; sur Client 2, cliquer sur Accepter.	La session s'ouvre après validation de l'utilisateur.	OK
RD-11	Contrôle effectif du poste	Pendant la session, déplacer la souris et taper au clavier depuis le poste technicien.	Les actions s'exécutent sur le poste distant.	OK
RD-12	Déconnexion côté utilisateur	Pendant une session, cliquer sur Déconnecter côté poste contrôlé.	La prise en main s'arrête immédiatement.	OK
RD-13	Clé invalide refusée	Renseigner volontairement une clé erronée sur un client puis tenter une connexion.	La connexion est refusée (« Clé invalide »).	OK

Tests du LOT 2 — GLPI

N°	Objectif du test	Procédure	Résultat attendu	Statut
GL-01	Accès à l'interface web	Depuis un navigateur du LAN, ouvrir http://ADRESSE_IP/glpi .	La page de connexion GLPI s'affiche.	OK
GL-02	Authentification	Se connecter avec le compte administrateur.	Le tableau de bord GLPI s'affiche.	OK
GL-03	Sécurisation post-installation	Vérifier l'absence du dossier /install et l'alerte GLPI.	Aucune alerte de sécurité ; dossier install supprimé.	OK
GL-04	Extension php-imap présente	Exécuter <code>php -m grep imap</code> sur le serveur.	La ligne « imap » est retournée.	OK
GL-05	Inventaire activé	Aller dans Administration > Inventaire.	La case « Activer l'inventaire » est cochée.	OK
GL-06	Remontée de l'agent	Installer le GLPI Agent sur le poste Windows puis consulter Parc > Ordinateurs.	Le poste apparaît avec ses caractéristiques (CPU, RAM, disques, logiciels).	OK
GL-07	Inventaire forcé	Ouvrir http://127.0.0.1:62354 sur le poste client et lancer un inventaire.	La date du dernier inventaire est mise à jour côté serveur.	OK
GL-08	Ticket via Self-Service	Avec le compte post-only, signaler un incident depuis le portail.	Le ticket est créé au statut « Nouveau » avec un numéro.	OK
GL-09	Ticket par courriel	Envoyer un mail à la boîte de support et attendre le relevé du collecteur.	Un ticket est créé automatiquement, source « E-Mail ».	OK
GL-10	Visibilité côté technicien	Se connecter avec le compte tech et ouvrir Assistance > Tickets.	Le nouveau ticket apparaît dans la liste.	OK
GL-11	Prise en charge	S'attribuer le ticket et passer le statut à « En cours (attribué) ».	Le statut évolue et l'attribution est enregistrée.	OK
GL-12	Réponse au demandeur	Utiliser le bouton « Answer » pour ajouter un suivi.	Le suivi est visible côté utilisateur dans le détail du ticket.	OK
GL-13	Passage en attente	Passer le ticket au statut « En attente » (Pending).	L'utilisateur voit le statut « Pending » côté Self-Service.	OK
GL-14	Résolution et clôture	Passer le ticket en « Résolu » avec une solution, puis valider côté utilisateur.	Le ticket passe en « Clos ».	OK
GL-15	Pièce jointe	Joindre une capture d'écran (< 2 Mio) lors de la création d'un ticket.	La pièce jointe est acceptée et consultable dans le ticket.	OK
GL-16	Connexion IMAP du collecteur	Sur la fiche du collecteur, cliquer sur « Tester ».	La connexion à imap.gmail.com:993 (SSL) réussit.	OK
GL-17	Relevé forcé mailgate	Envoyer un mail de test puis exécuter l'action automatique mailgate.	Le mail est relevé et transformé en ticket.	OK

N°	Objectif du test	Procédure	Résultat attendu	Statut
GL-18	Confiance certificat LDAPS	Après update-ca-certificates, tester la connexion depuis la fiche annuaire GLPI.	Le test de connexion LDAPS (port 636) réussit sans erreur de certificat.	OK
GL-19	Import LDAP	Lancer l'importation de nouveaux utilisateurs depuis la liaison annuaire.	Les comptes AD sélectionnés sont créés dans GLPI avec le profil Self-Service.	OK
GL-20	Connexion avec un compte AD	Ouvrir une session GLPI avec un identifiant Windows (samaccountname) et le mot de passe AD.	La session s'ouvre sur le portail Self-Service.	OK
GL-21	Compte AD désactivé	Désactiver un compte dans l'AD puis tenter une connexion GLPI avec ce compte.	La connexion est refusée.	OK

Tests du LOT 3 — Windows Server 2025

Chaque service du LOT 3 a été validé de bout en bout : configuration du serveur, annuaire, résolution DNS, distribution DHCP, déploiement réseau, stratégie de groupe et mécanismes de redondance.

N°	Objectif du test	Procédure	Résultat attendu	Statut
WS-01	Nom et adresse du serveur	Sur PARCUS-WDSSRV-01, exécuter ipconfig /all et vérifier le nom de l'ordinateur.	Nom PARCUS-WDSSRV-01, adresse fixe 192.168.137.1 /24.	OK
WS-02	Promotion du contrôleur de domaine	Après redémarrage, ouvrir une session PARCUS\Administrateur et vérifier la présence des outils AD DS.	La session de domaine s'ouvre ; le domaine parcus.fr existe.	OK
WS-03	Résolution DNS du domaine	Depuis un poste du LAN, exécuter nslookup parcus.fr.	La réponse renvoie 192.168.137.1 (et 192.168.137.2 après mise en place de la zone secondaire).	OK
WS-04	Autorisation du serveur DHCP	Dans la console DHCP, vérifier l'état du serveur après la configuration post-installation.	Le serveur apparaît autorisé dans l'AD (pastille verte), l'étendue est active.	OK
WS-05	Attribution d'un bail DHCP	Démarrer VM-TEST2 en « Obtenir une adresse IP automatiquement » puis exécuter ipconfig /all.	Adresse dans la plage .15-.115 délivrée par 192.168.137.1, suffixe DNS parcus.fr.	OK
WS-06	Jonction d'un poste au domaine	Depuis les propriétés système de VM-TEST2, rejoindre le domaine parcus.fr avec un compte autorisé.	Message « Bienvenue dans le domaine parcus.fr », puis redémarrage.	OK
WS-07	Ouverture de session avec un compte du domaine	Sur VM-TEST2, ouvrir une session avec un compte de l'annuaire (PARCUS\utilisateur).	La session s'ouvre et le profil est créé.	OK

N°	Objectif du test	Procédure	Résultat attendu	Statut
WS-08	Service WDS opérationnel	Exécuter Get-Service WDSServer sur le serveur ; le démarrer avec Start-Service si besoin.	Le service passe (ou est) à l'état Running.	OK
WS-09	Démarrage PXE d'un client	Démarrer un poste UEFI sur EFI Network.	Le poste obtient une adresse DHCP et charge l'image de démarrage du serveur WDS.	OK
WS-10	Déploiement de Windows 11 Pro via WDS	Poursuivre l'installation proposée après le démarrage PXE avec l'image Windows1125h2Vierge.	Windows 11 Pro s'installe depuis le réseau sans support USB.	OK
WS-11	Application de la GPO fondEcran	Lier la GPO à l'OU UtilisateursParcus, exécuter gpupdate /force puis rouvrir une session utilisateur.	Le fond d'écran d'entreprise s'affiche et n'est pas modifiable par l'utilisateur.	OK
WS-12	Transfert de la zone DNS secondaire	Sur PARCUS-WDSSRV-02, ouvrir la zone secondaire parcus.fr après ajout du serveur dans l'onglet Serveurs de noms du maître.	La zone est copiée et cohérente avec le serveur maître 192.168.137.1.	OK
WS-13	Basculement DHCP	Arrêter le service DHCP de PARCUS-WDSSRV-01, puis exécuter ipconfig /release et /renew sur un client.	Le client obtient un bail servi par le partenaire 192.168.137.2.	OK
WS-14	Autorité de certification active	Après configuration d'AD CS, ouvrir la console Autorité de certification sur PARCUS-WDSSRV-02.	L'autorité est démarrée et peut émettre des certificats pour le domaine.	OK
WS-15	Module TPM présent et prêt	Chiffrer la VM, ajouter le module de plateforme sécurisée, puis ouvrir tpm.msc sur chaque client.	Le TPM (spécification 2.0) est « prêt à être utilisé » sur les deux postes.	OK
WS-16	Application de la GPO bitlockerOrdinateur	Déplacer le poste dans l'OU OrdinateurParcus, exécuter gpupdate /force puis gpresult /r.	La GPO bitlockerOrdinateur figure dans les stratégies appliquées au volet ordinateur.	OK
WS-17	Chiffrement du lecteur système	Activer BitLocker sur C:, laisser la vérification système redémarrer le poste, puis exécuter manage-bde -status C:.	Chiffrement à 100 % en XTS-AES 128, protection activée, protecteurs TPM + mot de passe numérique.	OK
WS-18	Clé de récupération sauvegardée dans l'AD	Exécuter manage-bde -protectors -get C: puis ouvrir l'onglet Récupération BitLocker des propriétés du poste dans l'ADUC.	Type de sauvegarde « Sauvegarde de l'AD » ; le mot de passe de récupération apparaît sur la fiche du poste.	OK