PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : FOUCHER

Prénom : Alexandre

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), Foucher , Alexandre , certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Bouguenais
Date 26/03/2026

Signature

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : FOUCHER Alexandre	**N° candidat : 02542581672**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 28/05/2026

Organisation support de la réalisation professionnelle
Entreprise fictive **Oasis** et prestataire **NTxSystem**

Intitulé de la réalisation professionnelle
Mise en place d'ADDS avec AD; DNS; DHCP; DFS; DFSR; LAPS; TIERING; REPLICATION

Période de réalisation : 2024 - 2026 *Lieu :* CFA Fab'Academy Bouguenais (UIMM)
Modalité : ☐ *Seul(e)* ☒ *En équipe*

Compétences travaillées
- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)
Dans le cadre de la mission concernant la mise en place de l'infrastructure système, une solution d'annuaire Active Directory multi-sites a été déployée afin de répondre aux exigences de centralisation des identités, de gestion de fichiers, de haute disponibilité et de sécurité, tout en appliquant un modèle de cloisonnement par tiering

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Différentes ressources ont été utilisées pour la mise en place de l'infrastructure Active Directory, tout d'abord pour les ressources documentaires, les ressources principales utilisées ont été la documentation officielle Microsoft ainsi que les guides de l'ANSSI relatifs à l'administration sécurisée des systèmes d'information reposant sur Active Directory, pour les ressources matérielles, des serveurs HP en tant qu'hyperviseurs ont été utilisés, pour les ressources logicielles, VMware ESXi, Windows Server 2022, Windows Server 2022 Core et le Firewall OPNsense ont été utilisés.

Modalités d'accès aux productions[3] et à leur documentation[4]
L'ensemble des documents liés à l'infrastructure est disponible sur le partage réseau accessible depuis le réseau BTS SIO.
Cet emplacement est dédié au stockage des informations relatives à la section. Il contient notamment des documentations sur l'environnement virtuel déployé, l'ensemble de la configuration de l'infrastructure mise en place, les différentes solutions étudiées, le plan d'adressage ainsi que les différents schémas réalisés de l'infrastructure.
L'ensemble des mots de passe de l'infrastructure sont conservés dans notre gestionnaire de mot de passe Bitwarden.
Partage Réseau Documentation NTxSystem : \\partage.btssio.nte\fichiers\BAIES-PEDA\NTXSYSTEM
Identifiant Bitwarden : ntxsystem@proton.me
Mot de passe Bitwarden : NTxbitwarden44.
Lien Bitwarden : https://vault.bitwarden.com

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.
[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.
[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

À travers cette réalisation professionnelle portant sur le déploiement d'une infrastructure Active Directory multi-sites, la sécurisation de l'annuaire et la mise en place d'un partage de fichiers distribué, différents services ont été mis en place au sein de l'infrastructure, tout l'environnement est virtualisé sur des serveurs HP utilisant VMware ESXi et il y a différentes machines virtuelles dédiées à différents services.
Cette infrastructure a été construite sur cinq sites, le premier correspondant au site principal commun au groupe NTxSystem, le site de Paris, et les suivants correspondant aux sites secondaires de Marseille, Grenoble, Lille et Nantes.

L'objectif principal de cette réalisation était de mettre en place une infrastructure permettant de centraliser la gestion des identités, des ressources et des fichiers de manière sécurisée et hautement disponible. Pour répondre à ce besoin, est déployé un domaine Active Directory avec réplication inter-sites, cette solution s'appuie sur des contrôleurs de domaine Windows Server 2022 pour la gestion centralisée des utilisateurs et des machines, sur un espace de noms DFS avec réplication DFSR entre les sites pour la distribution et la haute disponibilité des partages de fichiers, et sur un modèle de tiering T0/T1/T2 pour le cloisonnement des droits d'administration.
Cette solution permet donc de simplifier l'administration de l'infrastructure, de garantir la disponibilité des fichiers sur l'ensemble des sites en cas de défaillance d'un serveur, et de réduire les risques de mouvements latéraux en cas de compromission d'un compte.

Ci-dessous les schémas logique et physique ainsi que le plan d'adressage de l'infrastructure.

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

	Plage	Passerelle	DNS1	DNS2	Description
DHCP	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

	Plage	Passerelle	DNS1	DNS2	Description
DHCP	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

	Plage	Passerelle	DNS1	DNS2	Description
DHCP	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

Marseille

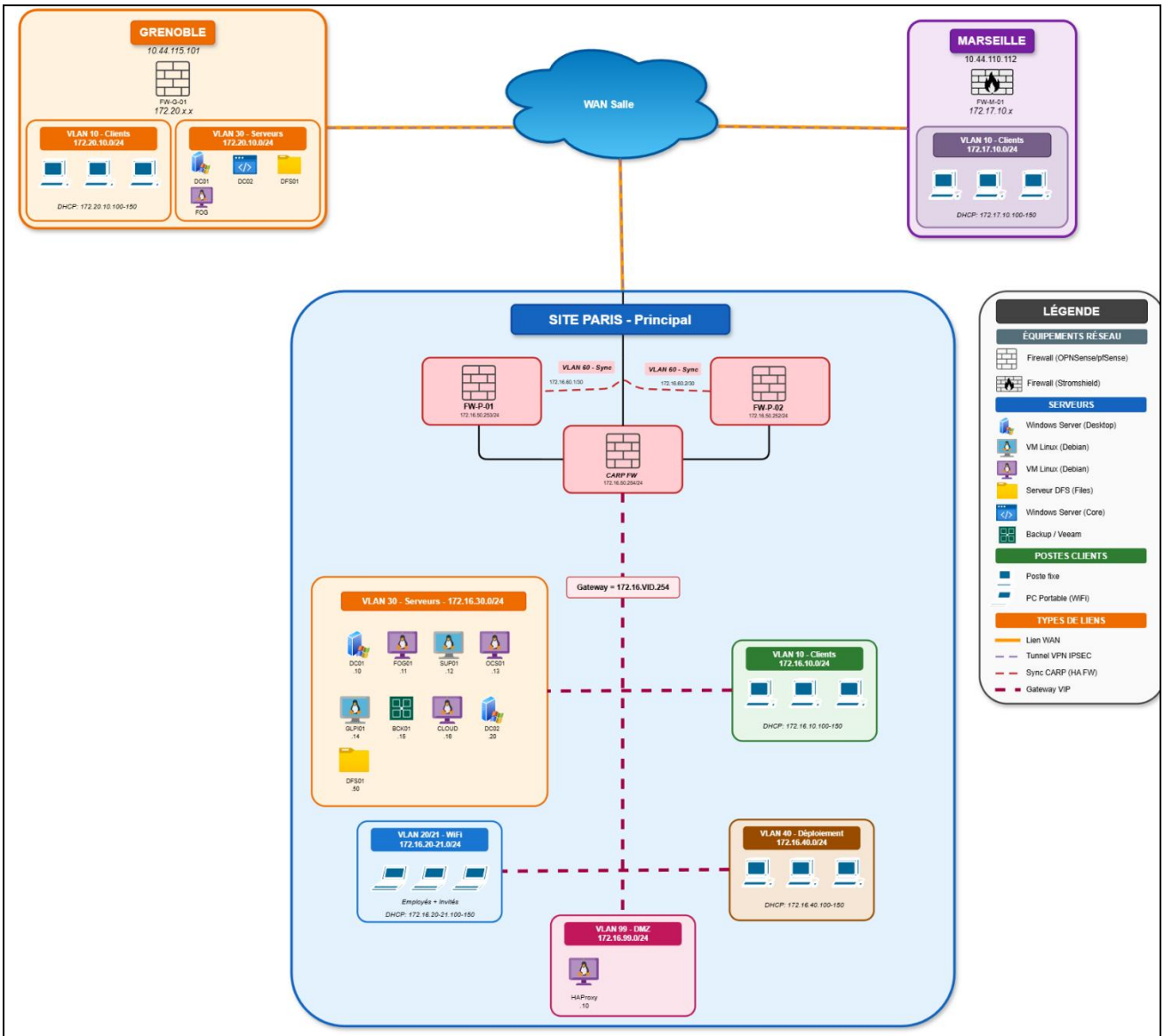
Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

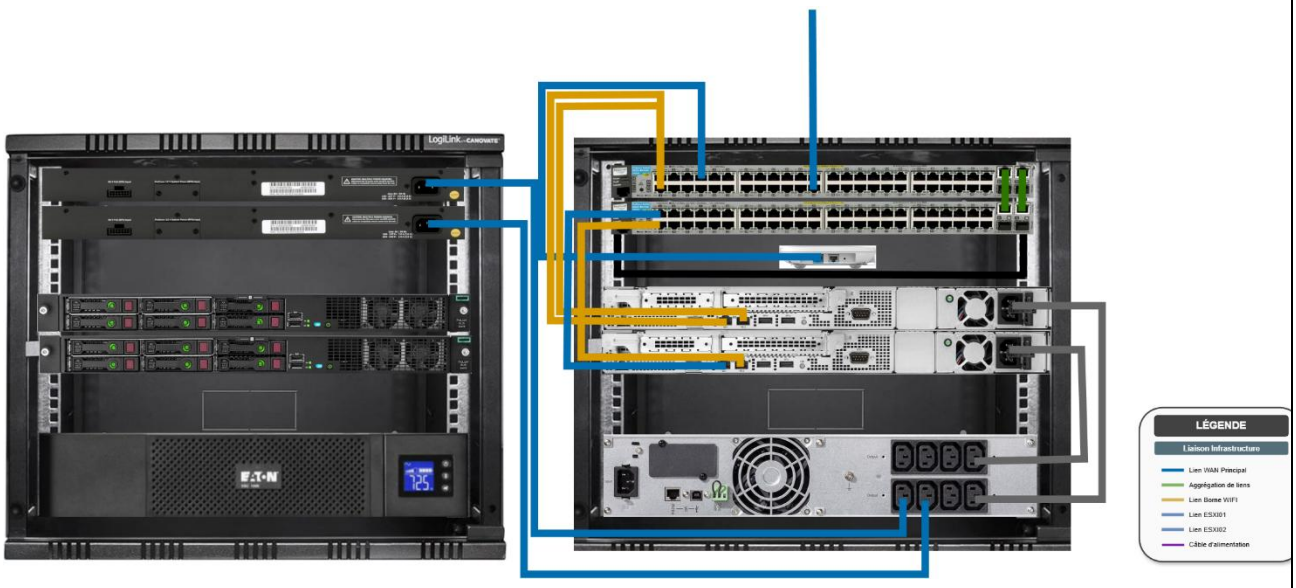
DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

Proxmox Grenoble

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-G-DC01	172.20.30.10	255.255.255.0	172.20.30.0	172.20.30.254	DC1 Grenoble
SRV-G-DC02	172.20.30.20	255.255.255.0	172.20.30.0	172.20.30.254	DC2 Core Grenoble
SRV-G-DFS01	172.20.30.50	255.255.255.0	172.20.30.0	172.20.30.254	DFS01 Grenoble
SRV-G-FOG01	172.20.30.30	255.255.255.0	172.20.30.0	172.20.30.254	FOG Grenoble
FW-G-01	172.20.10.254	255.255.255.0	172.20.10.0	172.20.10.254	IP FW-G-01 LAN Grenoble
FW-G-01	172.20.30.254	255.255.255.0	172.20.30.0	172.20.30.254	IP FW-G-01 SRV Grenoble
FW-G-01	172.20.99.254	255.255.255.0	172.20.99.0	172.20.99.254	IP FW-G-01 DMZ Grenoble
FW-G-01	10.44.115.101	255.255.255.0	10.44.115.0	10.44.115.254	IP WAN Grenoble

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.20.10.100-150	172.20.10.254	172.20.30.10	172.20.30.20	Plage DHCP Client Grenoble


GRENOBLE
10.44.115.101
FW-G-01
172.20.x.x
VLAN 10 - Clients
172.20.10.0/24
DHCP: 172.20.10.100-150
VLAN 30 - Serveurs
172.20.10.0/24
DC01
DC02
DFS01
FOG
WAN Salle
MARSEILLE
10.44.110.112
FW-M-01
172.17.10.x
VLAN 10 - Clients
172.17.10.0/24
DHCP: 172.17.10.100-150
SITE PARIS - Principal
FW-P-01
VLAN 60 - Sync
VLAN 60 - Sync
FW-P-02
CARP FW
Gateway = 172.16.VID.254
VLAN 30 - Serveurs - 172.16.30.0/24
DC01 .10
FOG01 .11
SUP01 .12
DCS01 .13
GLPI01 .14
BCK01 .15
CLOUD .16
DC02 .20
DFS01 .50
VLAN 10 - Clients
172.16.10.0/24
DHCP: 172.16.10.100-150
VLAN 20/21 - WiFi
172.16.20-21.0/24
Employés + Invités
DHCP: 172.16.20-21.100-150
VLAN 40 - Déploiement
172.16.40.0/24
DHCP: 172.16.40.100-150
VLAN 99 - DMZ
172.16.99.0/24
HAProxy .10
LÉGENDE
ÉQUIPEMENTS RÉSEAU
Firewall (OPNSense/pfSense)
Firewall (Stormshield)
SERVEURS
Windows Server (Desktop)
VM Linux (Debian)
VM Linux (Debian)
Serveur DFS (Files)
Windows Server (Core)
Backup / Veeam
POSTES CLIENTS
Poste fixe
PC Portable (WiFi)
TYPES DE LIENS
Lien WAN
Tunnel VPN IPSEC
Sync CARP (HA FW)
Gateway VIP


LÉGENDE
Liaison Infrastructure
Lien WAN Principal
Agrégation de liens
Lien Borne WiFi
Lien ESXi01
Lien ESXi02
Câble d'alimentation

BTS Services informatiques aux organisations SESSION 2026
ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate
Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE
En référence à l'annexe II.E – « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[5]	**Fab'Academy, 9 Rue de l'Halbrane, 44340 Bouguenais**	**SISR**

1. Environnement commun aux deux options
1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	**Active Directory Windows**	
Un SGBD	**MySQL / MariaDB**	
Un accès sécurisé à internet	**Firewall OPNsense, Stormshield**	
Un environnement de travail collaboratif	**Nextcloud**	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	**GLPI (Debian), Windows Server 2022**	

[5] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Veeam B&R	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Nextcloud, DFS, DFSR	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Tablette / PC Portable via connexion Wifi	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI	
Détection et prévention des intrusions	Wazuh, Stormshield	
Chiffrement	TLS, IPsec, SSH, PKI	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Segmentation VLANs via Switch	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Partage Réseau avec droits d'accès via DFS, DFSR suivant la méthode AGDLP	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Ansible, GPO	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH, RDP, HTTPS	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Centreon	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Firewall OPNsense, HaProxy, VPN	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	**Veeam B&R, Haute disponibilité OPNsense**	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	**RAID 1, redondance switch et Firewall OPNsense**	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	**DFS, DFSR, DHCP, DNS, Firewall OPNsense**	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	**VPN IPsec**	
Une solution permettant le déploiement des solutions techniques d'accès	**FOG, Ansible**	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	**Ansible, Batch GPO**	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	**Stormshield IPS, Wazuh**	

SOMMAIRE

1. Introduction

Dans le cadre de ma formation BTS SIO option SISR, j'ai eu l'opportunité d'intervenir sur un projet de mise en place d'infrastructure système pour l'entreprise Oasis.

L'objectif principal était d'accompagner Oasis dans la structuration de son annuaire Active Directory, afin de centraliser la gestion des identités, des ressources et des politiques de sécurité sur l'ensemble de ses sites géographiques.

Pour y répondre, les rôles ADDS, DNS, DHCP ont été déployés et configurés, complétés par un service de fichiers distribués (DFS/DFSR) et un modèle de sécurité par tiering garantissant un environnement robuste et évolutif.

1.1. Présentation Oasis

L'entreprise Oasis est une société parisienne spécialisée dans la conception de voyages sur mesure pour une clientèle exigeante, à la recherche d'expériences uniques, loin des circuits touristiques classiques.

Créée en 2017, elle s'est rapidement imposée comme un acteur innovant dans le secteur du tourisme personnalisé, grâce à une approche centrée sur l'écoute client, la connaissance culturelle approfondie des destinations, et un réseau de partenaires locaux dans plus de 30 pays.

Après plusieurs années de forte croissance, Oasis a décidé d'ouvrir une nouvelle agence à Marseille, pour mieux couvrir le sud de la France et répondre à une demande croissante dans cette zone. L'agence parisienne reste le siège social et le cœur de la stratégie de conception et de relation client haut de gamme.

En 2024, Oasis a atteint un chiffre d'affaires de 2,3 millions d'euros, et ambitionne désormais de renforcer sa structure numérique afin d'améliorer la coordination entre les sites, la sécurité des données clients, et la fluidité de l'expérience interne.

C'est dans ce contexte de croissance que NTxSystem a été sollicitée pour concevoir et déployer une infrastructure informatique adaptée aux besoins d'Oasis que ce soit pour l'agence parisienne, le siège social où pour l'agence de Marseille.

1.2. Présentation NTxSystem

NTxSystem est une entreprise prestataire spécialisée dans les solutions informatiques pour les professionnels. Dans le cadre de l'expansion d'Oasis, NTxSystem a été chargé de concevoir et déployer l'ensemble de l'infrastructure réseau des agences Paris et Marseille.

Les enjeux de ce projet sont multiples : centralisation des services, virtualisation des ressources, gestion des utilisateurs, sécurisation des communications inter-sites et mise en place d'un environnement stable et évolutif.

Pour répondre aux différentes exigences d'Oasis, l'ensemble de l'infrastructure est déployé dans un environnement virtualisé VMware ESXi.

1.3. Problématique

Oasis a mandaté NTxSystem pour concevoir et déployer une infrastructure d'annuaire centralisée, capable de couvrir l'ensemble de ses sites tout en répondant à des exigences opérationnelles et de sécurité stricte.

Les attentes de la direction portent sur plusieurs axes : centraliser la gestion des utilisateurs et des machines, assurer la réplication de l'annuaire entre les différents sites, automatiser la distribution des adresses IP, mettre à disposition des partages de fichiers répliqués et limiter les risques d'escalade de privilèges via un modèle de sécurité adapté. L'ensemble devait être déployé dans un environnement de test isolé avant mise en production.
La mission confiée comprenait le déploiement du domaine Active Directory oasis.local, intégrant les rôles ADDS, DNS, DHCP, DFS/DFSR ainsi que le modèle de tiering.

1.4. Analyse du besoin

Avant toute mise en œuvre, une phase de veille a été conduite afin d'identifier les solutions disponibles correspondant à notre contexte.

Trois solutions ont été comparées (Microsoft Active Directory, Samba AD et FreeIPA) :

Étude de solutions — Annuaire d'entreprise

Critère	✓ Solution retenue Microsoft ADDS	Samba AD	FreeIPA
Faisabilité technique	✓ Intégré nativement à Windows Server 2022, maintenu par Microsoft jusqu'en 2031	~ Compatible Windows mais fonctionnalités avancées partiellement supportées (LAPS, niveau fonctionnel 2016)	✗ Orienté Linux — compatibilité Windows très limitée, configurations complexes requises
Besoins RH	Interne	Interne	Interne
Besoin matériel & immatériel	Hyperviseur VMware ESXi ISO Windows Server 2022	Hyperviseur VMware ESXi ISO Samba	Hyperviseur VMware ESXi ISO FreeIPA
Coût total estimé	Inclus licence Windows Server	0 €	0 €
Temps (J/H)	3 J/H	4 J/H	5 J/H
Durée estimée	3 semaines	4 semaines	5 semaines
Points forts	• Support officiel Microsoft • Compatibilité native GPO, RSAT, LAPS, DFS/DFSR • Documentation exhaustive	• Gratuit • Déployable sur Linux • Compatible clients Windows	• Gratuit • Robuste en environnement Linux • Intègre LDAP
Points faibles	• Nécessite une licence Windows Server	• Fonctionnalités avancées incomplètes • Documentation fragmentée	• Incompatible avec notre parc Windows • Mise en œuvre très complexe • Aucun support des outils Microsoft

Au regard de cette analyse, Microsoft ADDS s'impose comme la solution la plus adaptée : compatibilité totale avec l'infrastructure Windows existante, support officiel garanti et intégration native de l'ensemble des services requis.

1.5. Planification

1) Analyse de la problématique : Compréhension du cahier des charges et définition des besoins en centralisation des identités et sécurisation des accès sur un environnement multi-sites.

2) Étude de solutions : Comparaison des solutions d'annuaire disponibles et justification du choix retenu.

3) Réalisation du GANTT : Planification des tâches, estimation des durées et identification des intervenants.

4) Installation de Windows Server 2022 : Déploiement des machines virtuelles sur VMware ESXi et installation du système d'exploitation.

5) Configuration ADDS / DNS / DHCP : Promotion des serveurs en contrôleurs de domaine, configuration des zones DNS intégrées AD et création des étendues DHCP.

6) Réplication inter-sites : Création des sites AD, des liens de sites avec leurs coûts et intervalles, et association des sous-réseaux.

7) Déploiement des DC secondaires en Server Core : Configuration des contrôleurs secondaires via PowerShell avec mise en place du DHCP Load Balancing.

8) DFS / DFSR : Déploiement des serveurs de fichiers, création de l'espace de noms et configuration de la réplication entre sites.

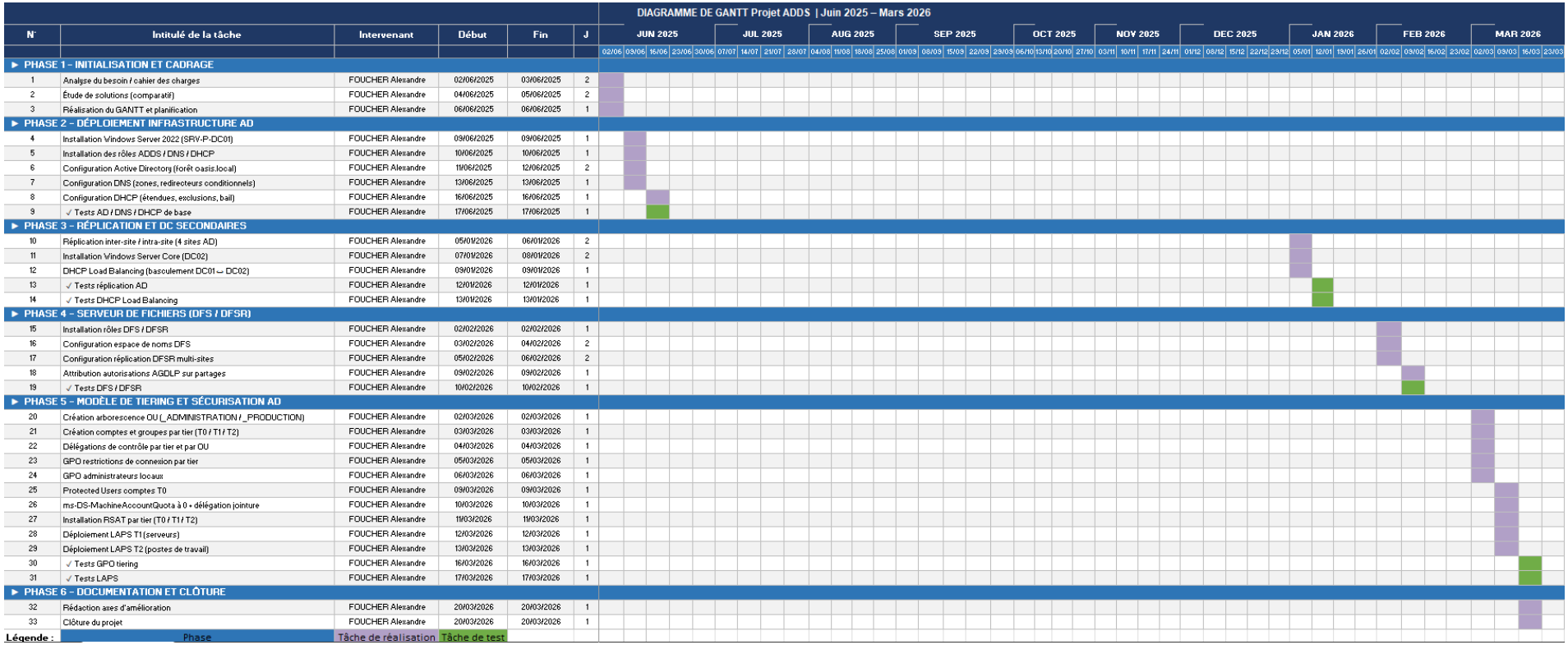
9) Modèle de tiering : Structuration des OU, création des comptes et groupes d'administration par tier, délégations et GPO de restriction de connexion.

10) RSAT et LAPS : Déploiement des outils d'administration à distance et de la gestion des mots de passe administrateurs locaux.

11) Tests et validation : Vérification de chaque service, tests de réplication, de basculement DHCP et de cloisonnement inter-tiers.

12) Clôture : Contrôle de conformité avec le cahier des charges.

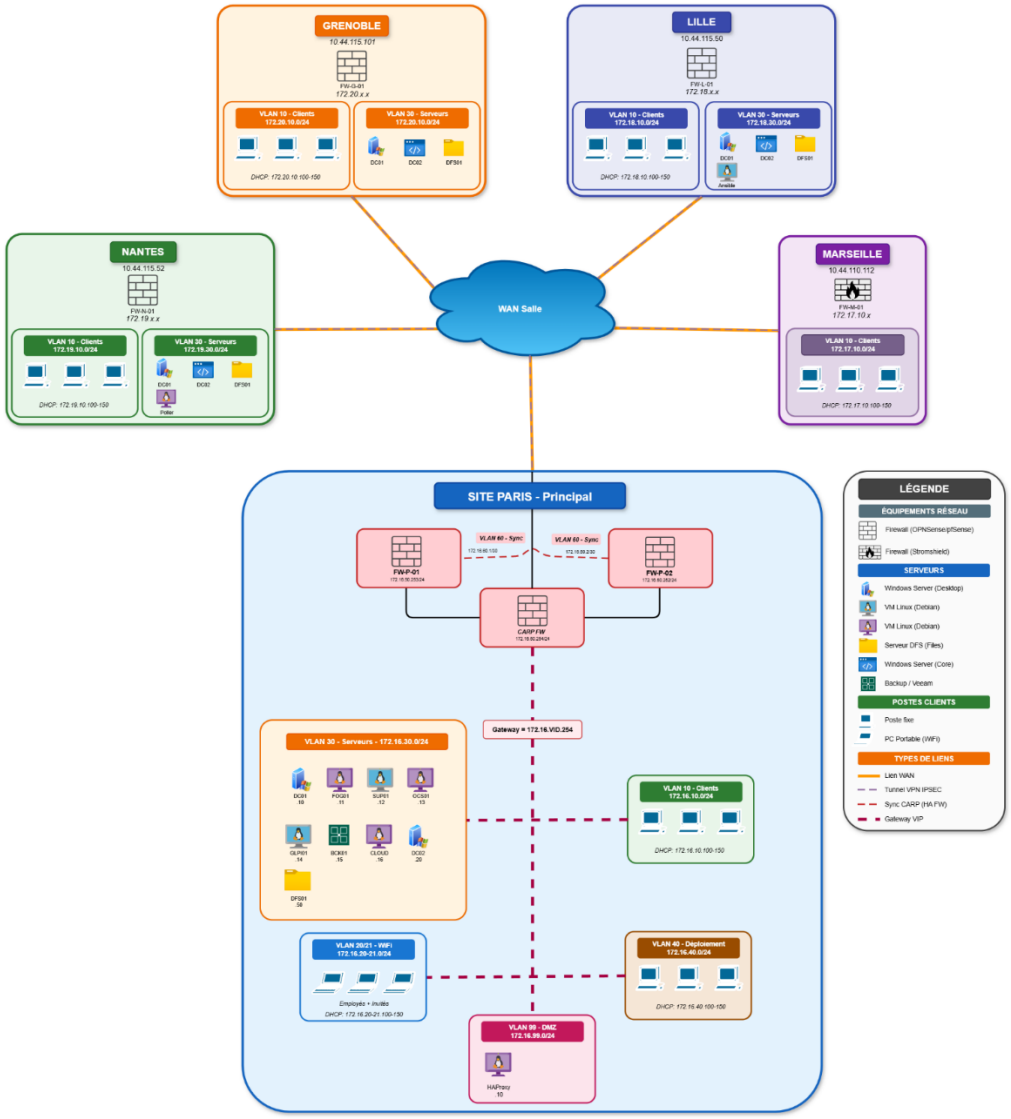
Le diagramme de GANTT ci-dessous présente la planification détaillée du projet, avec les différentes phases, leur durée estimée et leur ordre de réalisation.



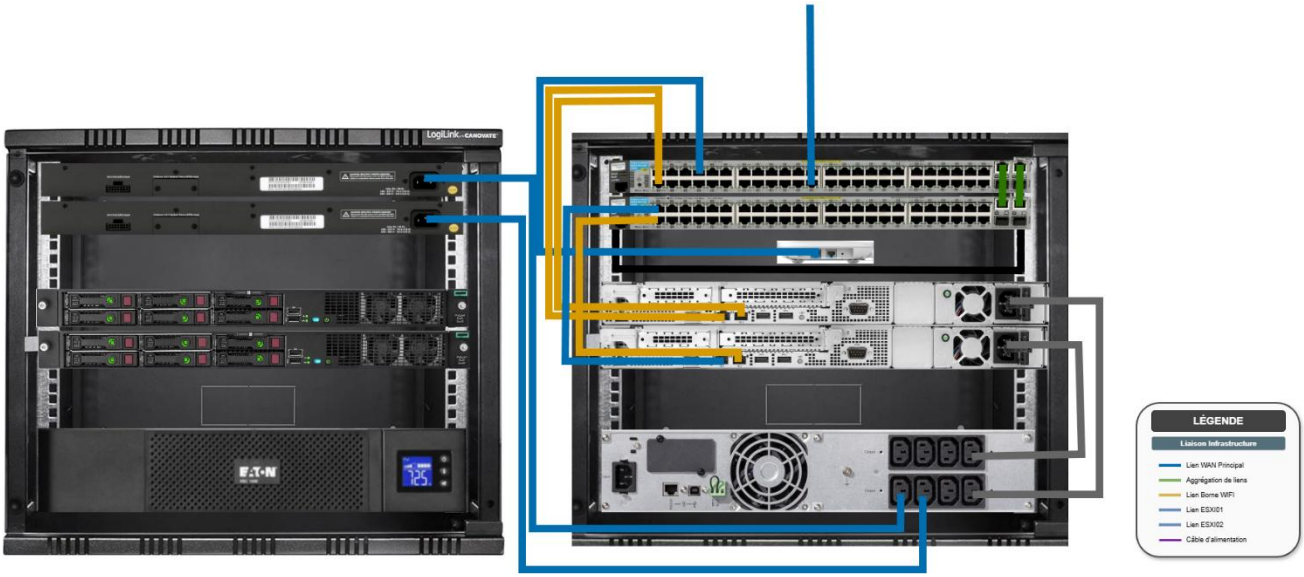
N°	Intitulé de la tâche	Intervenant	Début	Fin	J
►	PHASE 1 – INITIALISATION ET CADRAGE				
1	Analyse du besoin / cahier des charges	FOUCHER Alexandre	02/06/2025	03/06/2025	2
2	Étude de solutions (comparatif)	FOUCHER Alexandre	04/06/2025	05/06/2025	2
3	Réalisation du GANTT et planification	FOUCHER Alexandre	06/06/2025	06/06/2025	1
►	PHASE 2 – DÉPLOIEMENT INFRASTRUCTURE AD				
4	Installation Windows Server 2022 (SRV-P-DC01)	FOUCHER Alexandre	09/06/2025	09/06/2025	1
5	Installation des rôles ADDS / DNS / DHCP	FOUCHER Alexandre	10/06/2025	10/06/2025	1
6	Configuration Active Directory (forêt oasis.local)	FOUCHER Alexandre	11/06/2025	12/06/2025	2
7	Configuration DNS (zones, redirecteurs conditionnels)	FOUCHER Alexandre	13/06/2025	13/06/2025	1
8	Configuration DHCP (étendues, exclusions, bail)	FOUCHER Alexandre	16/06/2025	16/06/2025	1
9	✓ Tests AD / DNS / DHCP de base	FOUCHER Alexandre	17/06/2025	17/06/2025	1
►	PHASE 3 – RÉPLICATION ET DC SECONDAIRES				
10	Réplication inter-site / intra-site (4 sites AD)	FOUCHER Alexandre	05/01/2026	06/01/2026	2
11	Installation Windows Server Core (DC02)	FOUCHER Alexandre	07/01/2026	08/01/2026	2
12	DHCP Load Balancing (basculement DC01 ↔ DC02)	FOUCHER Alexandre	09/01/2026	09/01/2026	1
13	✓ Tests réplication AD	FOUCHER Alexandre	12/01/2026	12/01/2026	1
14	✓ Tests DHCP Load Balancing	FOUCHER Alexandre	13/01/2026	13/01/2026	1
►	PHASE 4 – SERVEUR DE FICHIERS (DFS / DFSR)				
15	Installation rôles DFS / DFSR	FOUCHER Alexandre	02/02/2026	02/02/2026	1
16	Configuration espace de noms DFS	FOUCHER Alexandre	03/02/2026	04/02/2026	2
17	Configuration réplication DFSR multi-sites	FOUCHER Alexandre	05/02/2026	06/02/2026	2
18	Attribution autorisations AGDLP sur partages	FOUCHER Alexandre	09/02/2026	09/02/2026	1
19	✓ Tests DFS / DFSR	FOUCHER Alexandre	10/02/2026	10/02/2026	1
►	PHASE 5 – MODÈLE DE TIERING ET SÉCURISATION AD				
20	Création arborescence OU (_ADMINISTRATION / _PRODUCTION)	FOUCHER Alexandre	02/03/2026	02/03/2026	1
21	Création comptes et groupes par tier (T0 / T1 / T2)	FOUCHER Alexandre	03/03/2026	03/03/2026	1
22	Délégations de contrôle par tier et par OU	FOUCHER Alexandre	04/03/2026	04/03/2026	1
23	GPO restrictions de connexion par tier	FOUCHER Alexandre	05/03/2026	05/03/2026	1
24	GPO administrateurs locaux	FOUCHER Alexandre	06/03/2026	06/03/2026	1
25	Protected Users comptes T0	FOUCHER Alexandre	09/03/2026	09/03/2026	1
26	ms-DS-MachineAccountQuota à 0 + délégation jointure	FOUCHER Alexandre	10/03/2026	10/03/2026	1
27	Installation RSAT par tier (T0 / T1 / T2)	FOUCHER Alexandre	11/03/2026	11/03/2026	1
28	Déploiement LAPS T1 (serveurs)	FOUCHER Alexandre	12/03/2026	12/03/2026	1
29	Déploiement LAPS T2 (postes de travail)	FOUCHER Alexandre	13/03/2026	13/03/2026	1
30	✓ Tests GPO tiering	FOUCHER Alexandre	16/03/2026	16/03/2026	1
31	✓ Tests LAPS	FOUCHER Alexandre	17/03/2026	17/03/2026	1
►	PHASE 6 – DOCUMENTATION ET CLÔTURE				
32	Rédaction axes d'amélioration	FOUCHER Alexandre	20/03/2026	20/03/2026	1
33	Clôture du projet	FOUCHER Alexandre	20/03/2026	20/03/2026	1
Légende :	Phase	Tâche de réalisation	Tâche de test		

2. Architecture

2.1. Schéma logique



2.2. Schéma physique



2.3. Plan d'adressage des contrôleurs de domaine

DC Paramètres Réseaux

Nom Machine	IP	DNS1	DNS2	Description
SRV-P-DC01	172.16.30.10	172.16.30.20	172.16.30.10	DC01 Paris
SRV-P-DC02	172.16.30.20	172.16.30.10	172.16.30.20	DC02 Paris
SRV-L-DC01	172.18.30.10	172.18.30.20	172.18.30.10	DC01 Lille
SRV-L-DC02	172.18.30.20	172.18.30.10	172.18.30.20	DC02 Core Lille
SRV-N-DC01	172.19.30.10	172.19.30.20	172.19.30.10	DC01 Nantes
SRV-N-DC02	172.19.30.20	172.19.30.10	172.19.30.20	DC02 Core Nantes
SRV-G-DC01	172.20.30.10	172.20.30.20	172.20.30.10	DC01 Grenoble
SRV-G-DC02	172.20.30.20	172.20.30.10	172.20.30.20	DC02 Core Grenoble

2.4. Ports utilisés

Les communications entre les différents composants de l'infrastructure nécessitent l'ouverture de ports spécifiques sur le pare-feu. Le tableau ci-dessous récapitule les ports utilisés pour le bon fonctionnement des services déployés.

Ports utilisés — Infrastructure Active Directory

Port	Protocole	Usage
53	TCP/UDP	DNS, résolution de noms
88	TCP/UDP	Kerberos, authentification
135	TCP	RPC Endpoint Mapper
389	TCP/UDP	LDAP
445	TCP	SMB, réplication SYSVOL / GPO
49152–65535	TCP	RPC dynamique, réplication AD

3. Définition et abréviations

ADDS (Active Directory Domain Services) : service permettant la gestion centralisée des utilisateurs, ordinateurs et ressources d'un réseau.

DHCP (Dynamic Host Configuration Protocol) : protocole réseau attribuant automatiquement des adresses IP aux machines d'un réseau.

DNS (Domain Name System) : service de résolution de noms qui traduit les noms de domaine en adresses IP.

DFS (Distribued File System) : service de rôle dans Windows Server utiliser pour regrouper des dossiers partagés situés sur des serveurs différents en un ou plusieurs espaces de noms logiquement structurés. Cela permet de donner aux utilisateurs une vue virtuelle des dossiers partagés, où un seul chemin d'accès mène aux fichiers situés sur plusieurs serveurs

DFSR (Distribued File System Replication) : service de rôle Windows Server qui vous permet de synchroniser efficacement des dossiers partagés sur plusieurs serveurs et sites.

AGDLP (Account, Global, Domain Local, Permission) **:** méthode d'attribution des permissions dans Active Directory. Les comptes utilisateurs (A) sont ajoutés dans des groupes globaux (G), eux-mêmes imbriqués dans des groupes de domaine local (DL), auxquels on attribue les permissions (P) sur les ressources.

GPO (Group Policy Object) : objet de stratégie de groupe permettant de définir et d'appliquer des configurations et des restrictions sur les utilisateurs et les ordinateurs d'un domaine Active Directory.

RSAT (Remote Server Administration Tools) : outils d'administration de serveur à distance permettant de gérer les rôles et fonctionnalités d'un serveur Windows (AD, DNS, DHCP, GPO, etc.) depuis un poste client sans se connecter directement au serveur.

PAW (Privileged Access Workstation) : poste d'administration à accès privilégié, dédié et durci, utilisé exclusivement pour les tâches d'administration sensibles afin de réduire la surface d'attaque.

KCC (Knowledge Consistency Checker) : processus intégré à Active Directory qui génère et maintient automatiquement la topologie de réplication entre les contrôleurs de domaine.

DSRM (Directory Services Restore Mode) : mode de démarrage spécial d'un contrôleur de domaine permettant la restauration ou la réparation de la base de données Active Directory en cas de défaillance.

ADUC (Active Directory Users and Computers) : console d'administration graphique intégrée à Windows Server permettant de gérer les objets de l'annuaire Active Directory : utilisateurs, ordinateurs, groupes et unités d'organisation.

LAPS (Local Administrator Password Solution) : solution Microsoft permettant de gérer automatiquement les mots de passe des comptes administrateurs locaux des machines du domaine. Chaque machine dispose d'un mot de passe unique, stocké dans Active Directory et renouvelé automatiquement.

JIT (Just-In-Time Administration) : méthode d'administration qui n'accorde les droits élevés qu'à la demande et pour une durée limitée, plutôt que de manière permanente. Réduit significativement la surface d'attaque en cas de compromission d'un compte privilégié.

OU (Organizational Unit) : unité d'organisation, conteneur logique dans Active Directory permettant de regrouper des objets (utilisateurs, ordinateurs, groupes) afin d'y appliquer des délégations de contrôle et des stratégies de groupe de manière granulaire.

DC (Domain Controller) : serveur Windows hébergeant le rôle Active Directory Domain Services. Il assure l'authentification des utilisateurs, la gestion des stratégies de groupe et la réplication de l'annuaire entre les sites.

NTDS (NT Directory Services) : base de données Active Directory. Elle contient l'ensemble des objets de l'annuaire : utilisateurs, groupes, ordinateurs et stratégies.

SYSVOL : dossier partagé présent sur chaque contrôleur de domaine, utilisé pour stocker et répliquer les stratégies de groupe et les scripts de démarrage entre les DC du domaine.

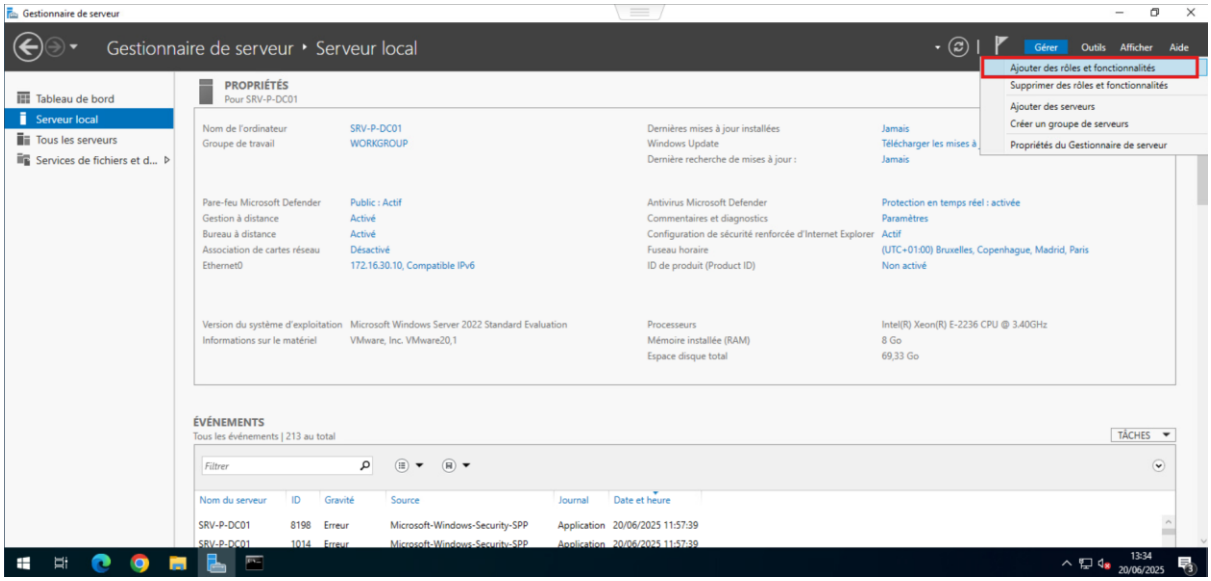
Server Core : mode d'installation de Windows Server sans interface graphique. Il réduit la consommation de ressources, la surface d'attaque et les temps de redémarrage. L'administration s'effectue via PowerShell ou à distance depuis un poste équipé de RSAT.

VMware ESXi : hyperviseur de type 1 développé par VMware, installé directement sur le matériel physique. Il permet de créer et gérer des machines virtuelles indépendamment d'un système d'exploitation hôte.

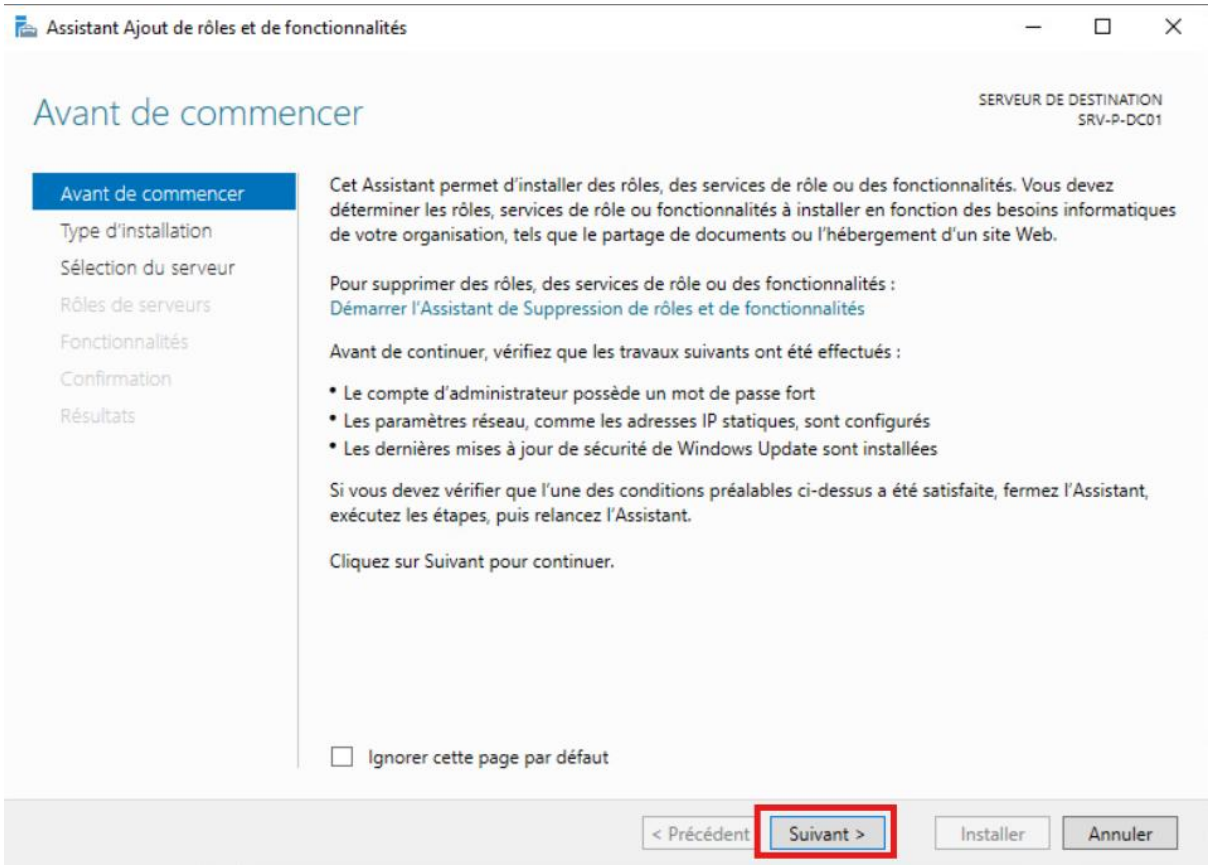
LDAP (Lightweight Directory Access Protocol) : protocole standard permettant d'interroger et de modifier un annuaire d'entreprise. Active Directory expose ses données via LDAP, utilisé notamment par les applications tierces pour l'authentification et la recherche d'objets.

4. Installation des rôles ADDS & DNS & DHCP

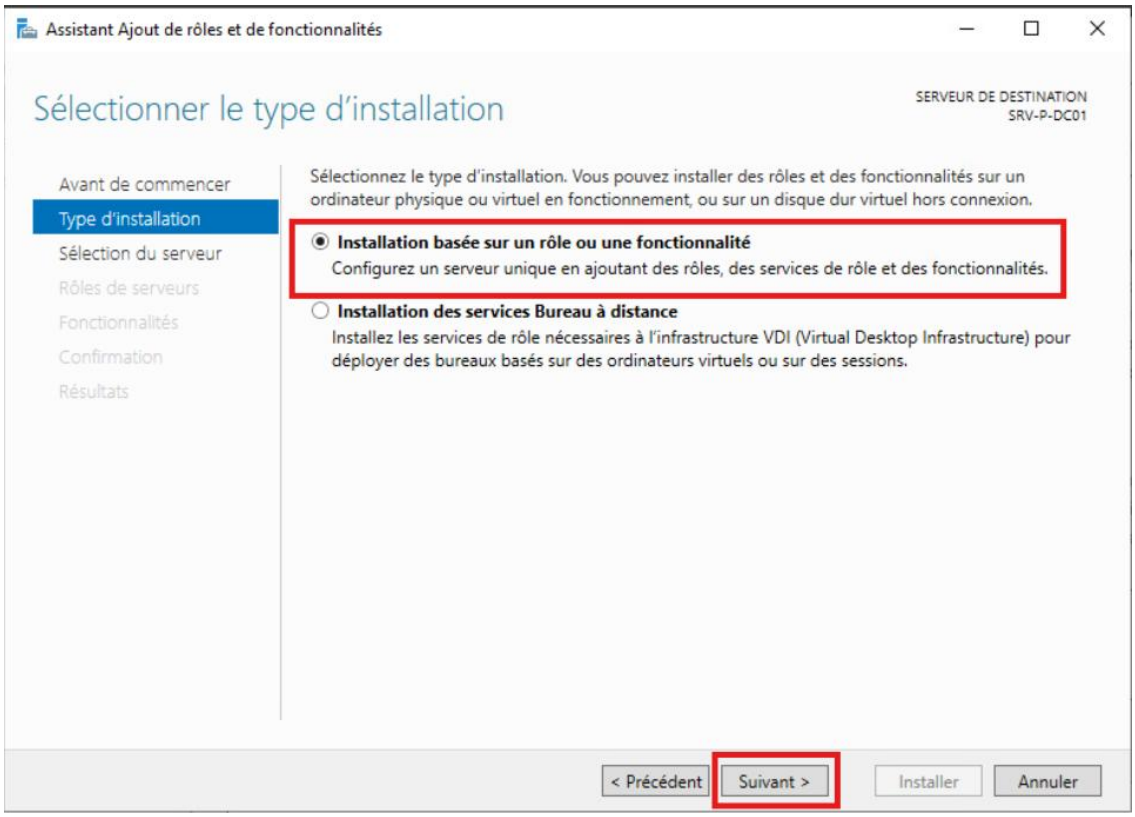
Sur le gestionnaire de serveur, se rendre sur « Gérer », puis « Ajouter des rôles et fonctionnalités »



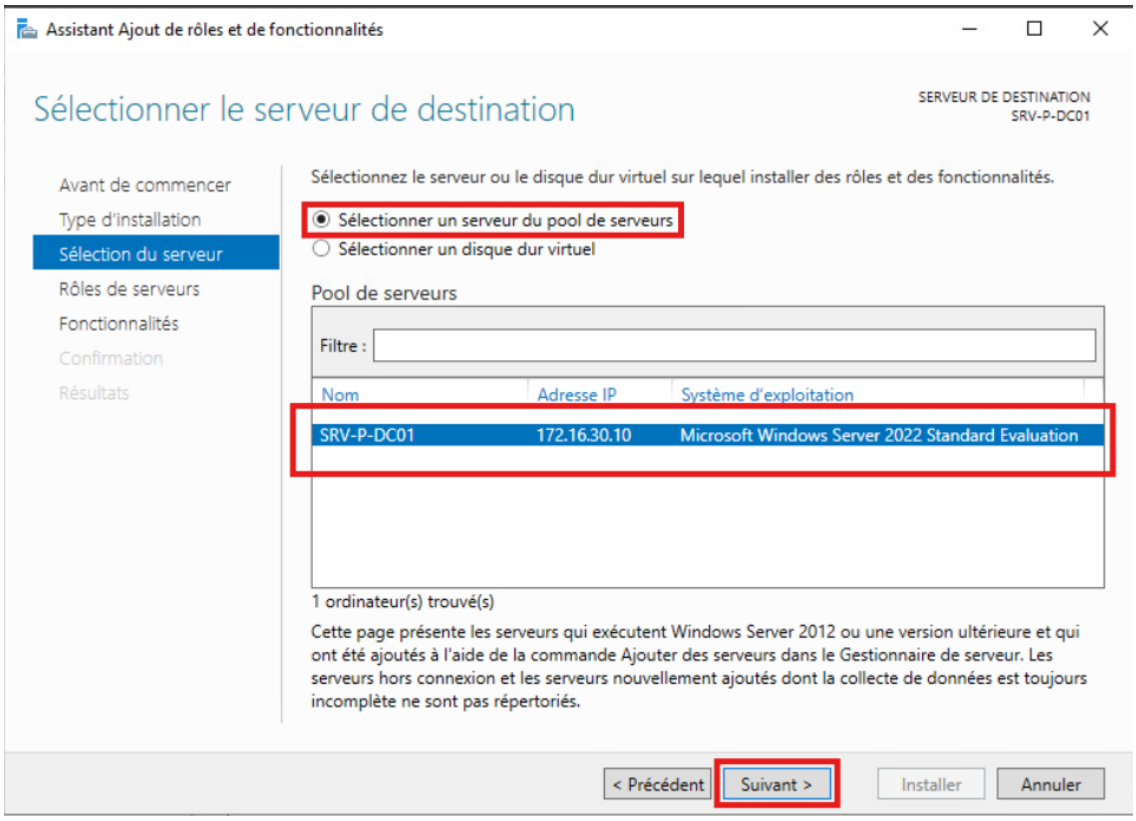
Puis, cliquer sur « Suivant »



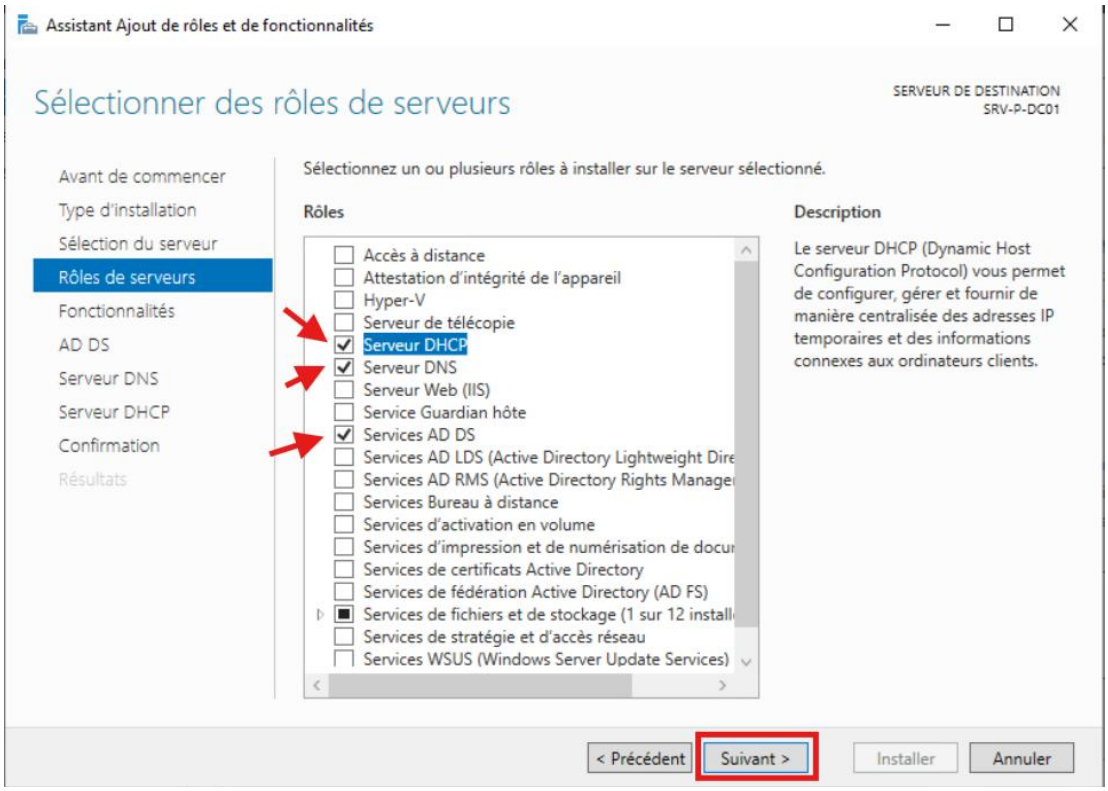
Sélectionner le type d'installation « Basée sur un rôle ou une fonctionnalité »



Choisir « Sélectionner un serveur du pool de serveurs », puis sélectionner le serveur cible.

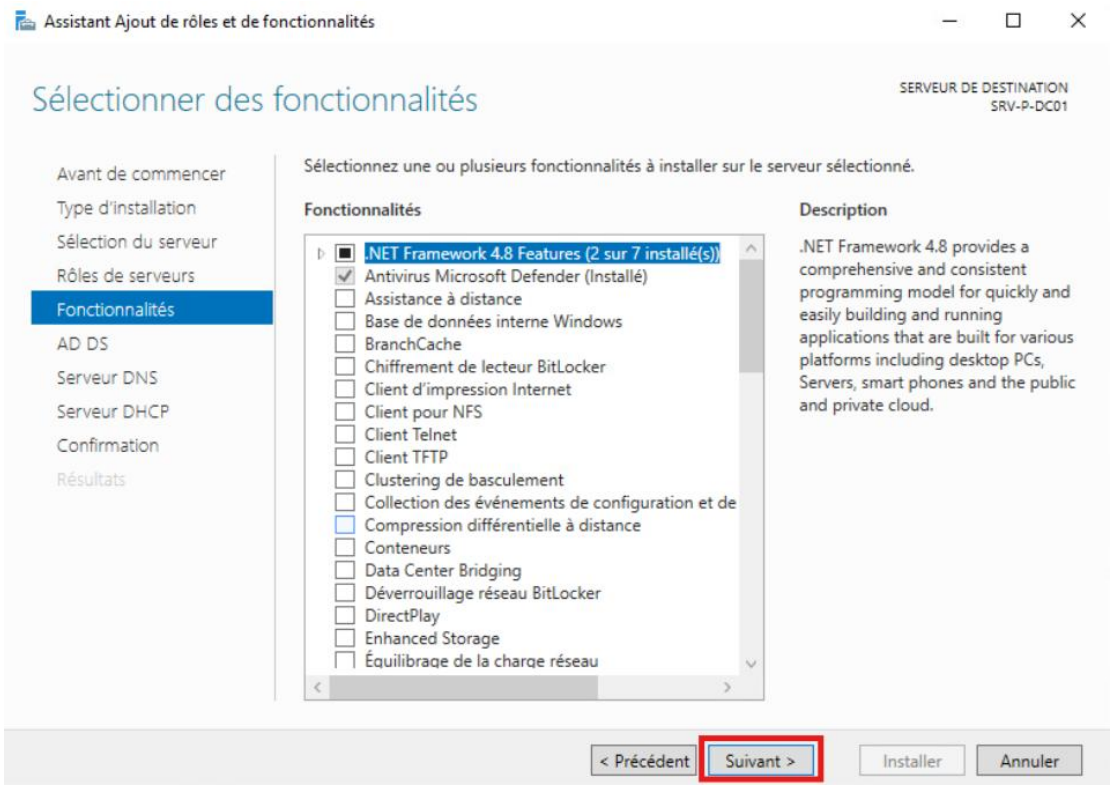


Choisir « Serveur DHCP », « Serveur DNS », et « Services AD DS »

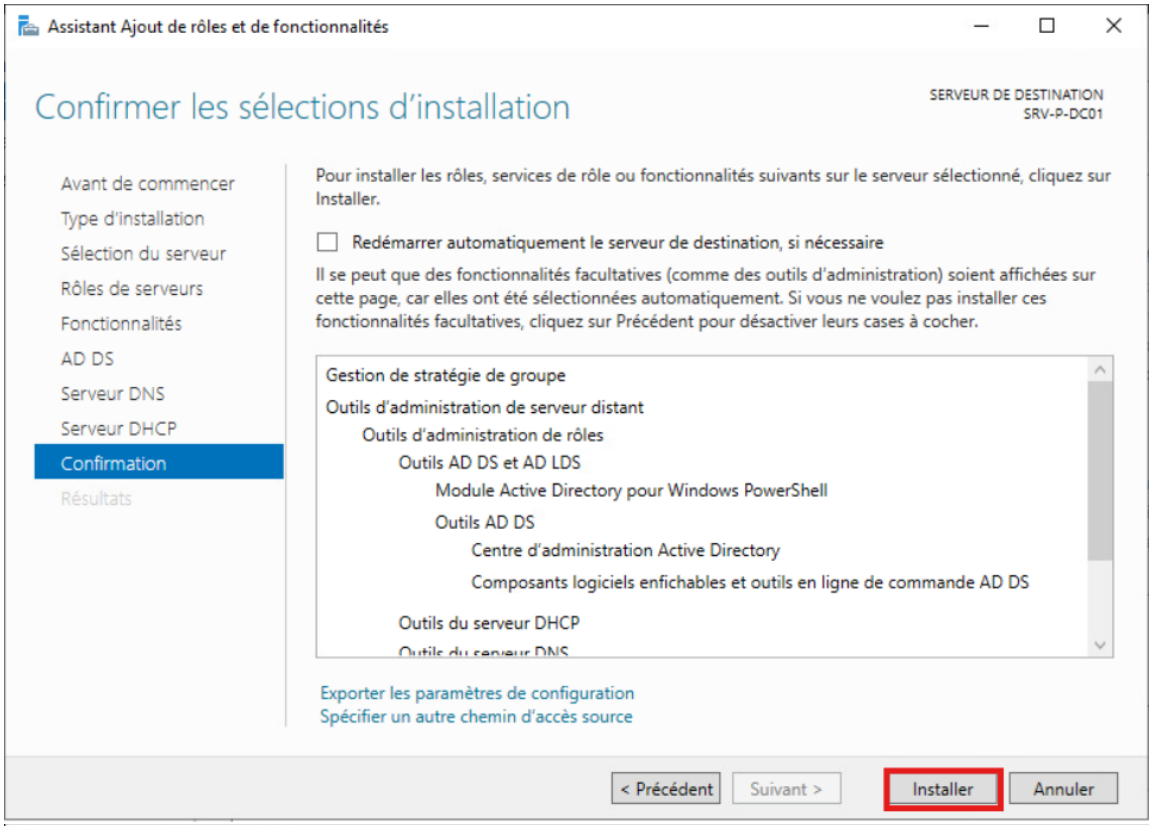


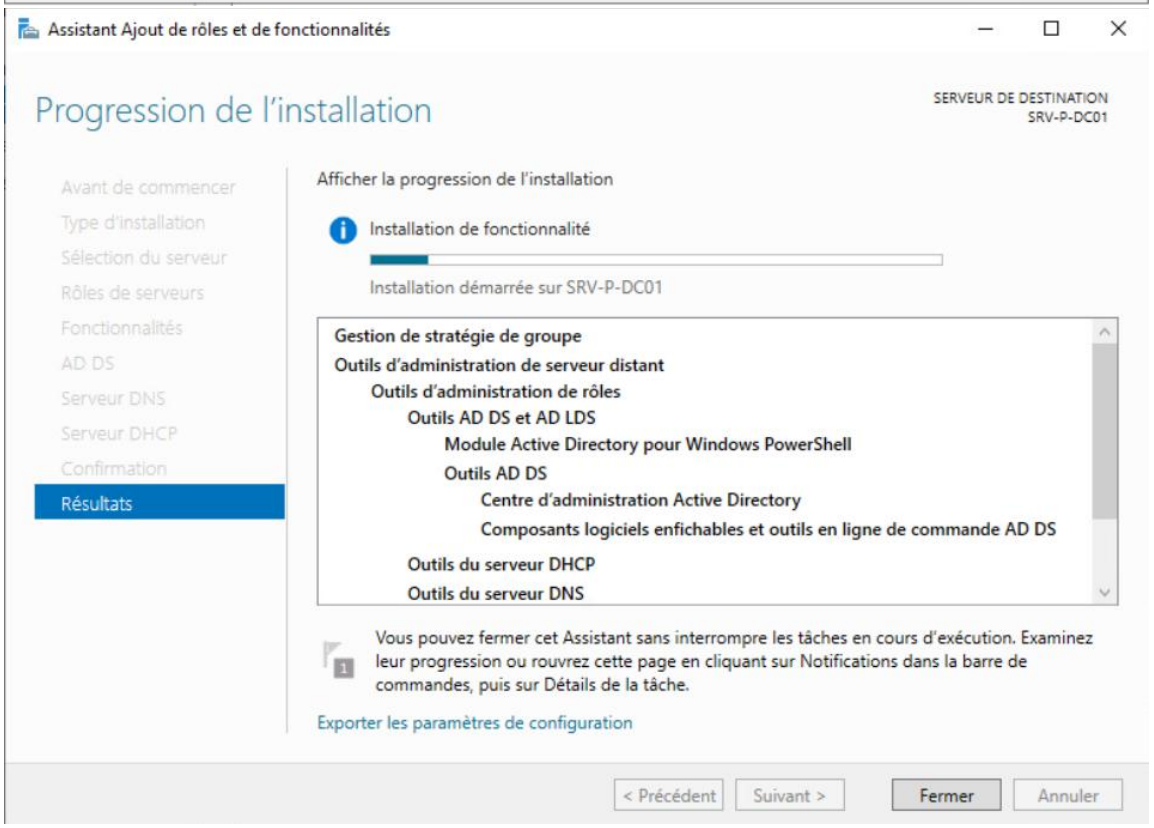
Ne pas choisir de fonctionnalités supplémentaires

Cliquer sur suivant jusqu'à « Confirmation »



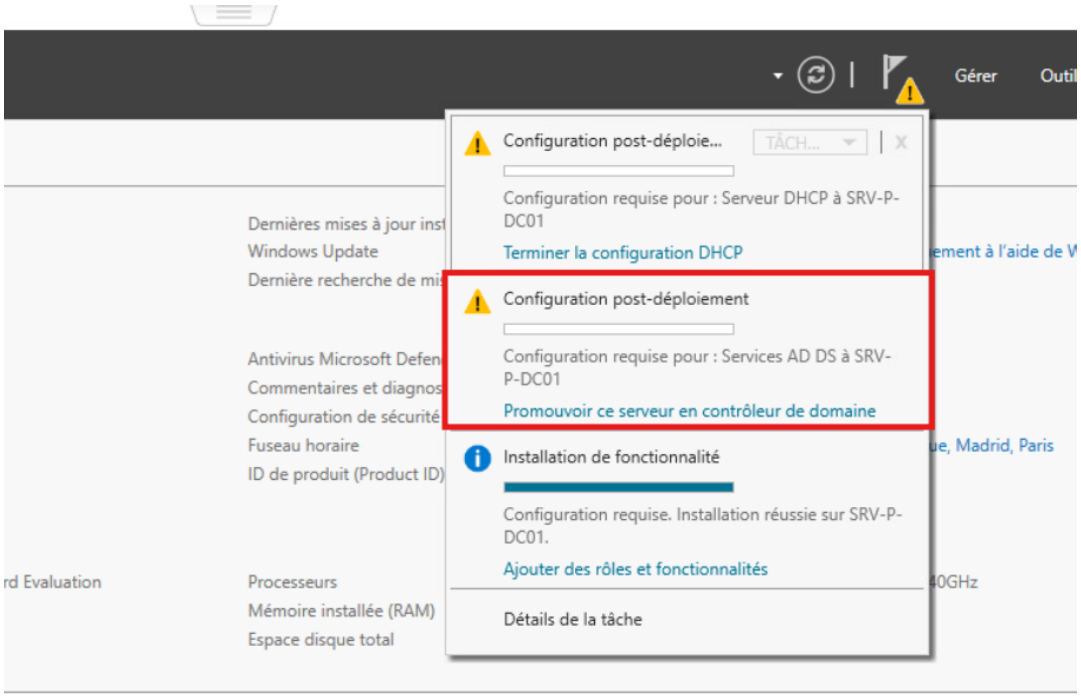
Puis un récapitulatif, cliquer sur « Installer »


Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
SRV-P-DC01
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Serveur DNS
Serveur DHCP
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
Centre d'administration Active Directory
Composants logiciels enfichables et outils en ligne de commande AD DS
Outils du serveur DHCP
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

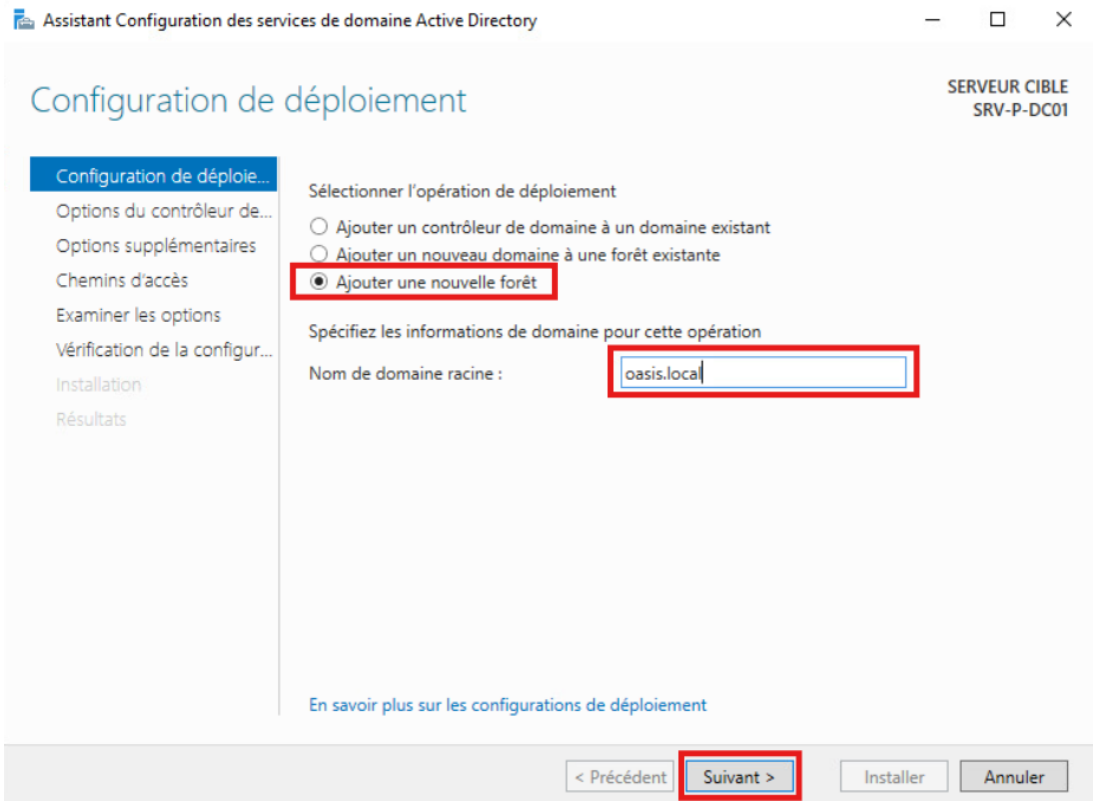

Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
SRV-P-DC01
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Serveur DNS
Serveur DHCP
Confirmation
Résultats
Afficher la progression de l'installation
Installation de fonctionnalité
Installation démarrée sur SRV-P-DC01
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
Centre d'administration Active Directory
Composants logiciels enfichables et outils en ligne de commande AD DS
Outils du serveur DHCP
Outils du serveur DNS
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.
Exporter les paramètres de configuration
< Précédent
Suivant >
Fermer
Annuler

4.1. Configuration Active Directory

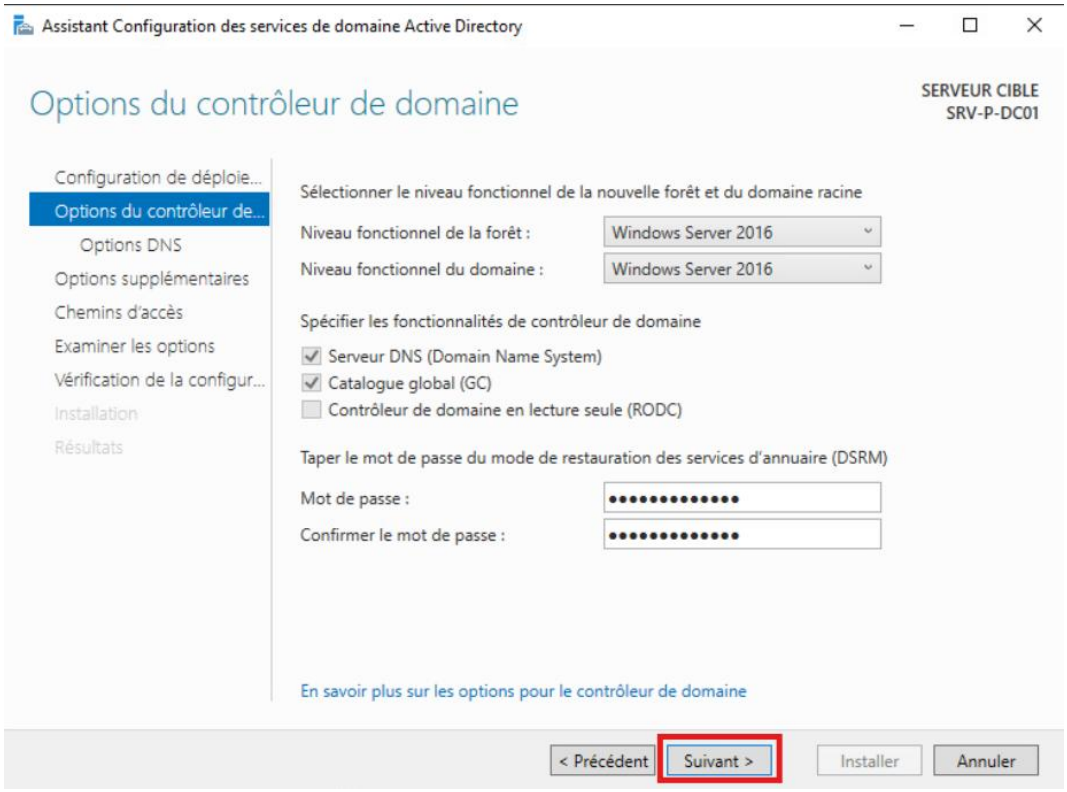
Sur le Gestionnaire de serveur, pour la fonctionnalité AD DS, cliquer sur « Promouvoir ce serveur en contrôleur de domaine »



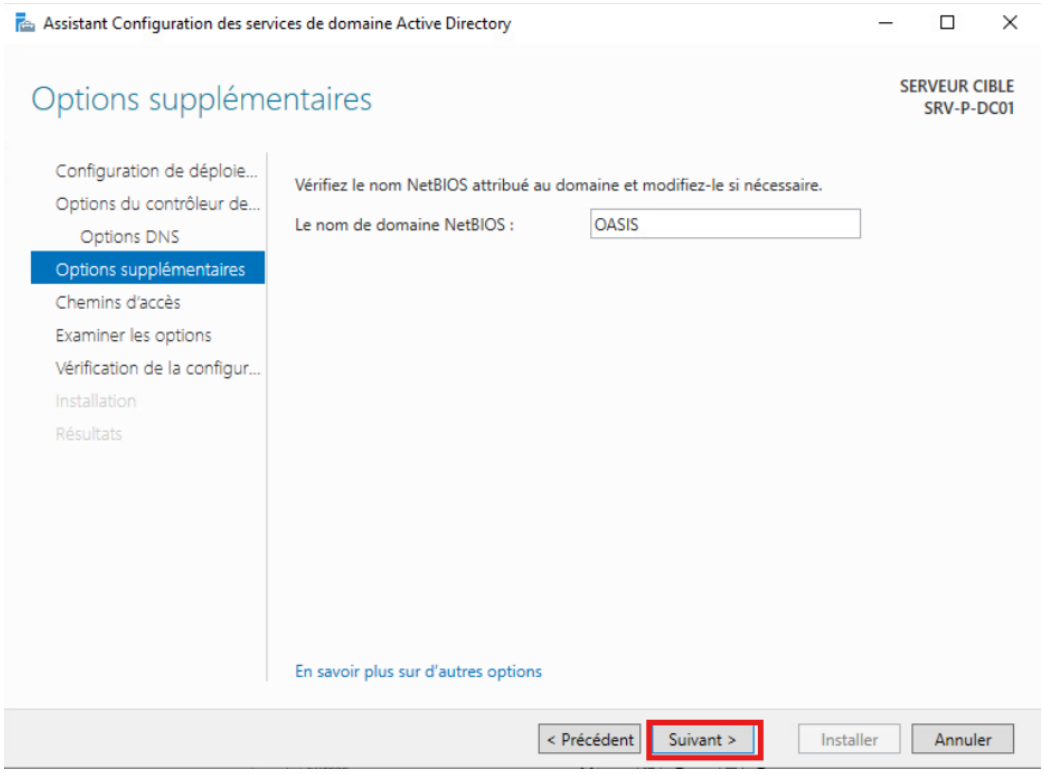
Ensuite, sélectionner « Ajouter une nouvelle forêt », et spécifier un nom de domaine racine, ici « oasis.local »



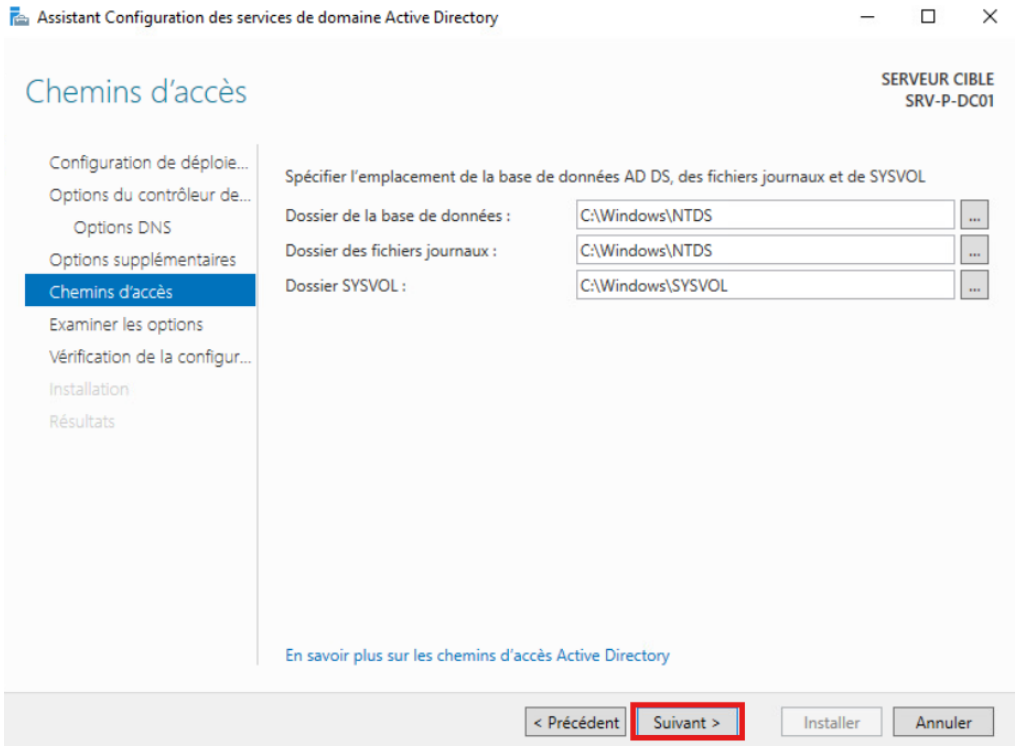
Définir le niveau fonctionnel de la forêt et du domaine en « Windows Server 2016 »
Spécifier les fonctionnalités du contrôleur de domaine avec « Serveur DNS » ainsi que « Catalogue Global »
Enfin, définir un mot de passe du mode de restauration des services d'annuaire (Directory Services Restore Mode = DSRM)



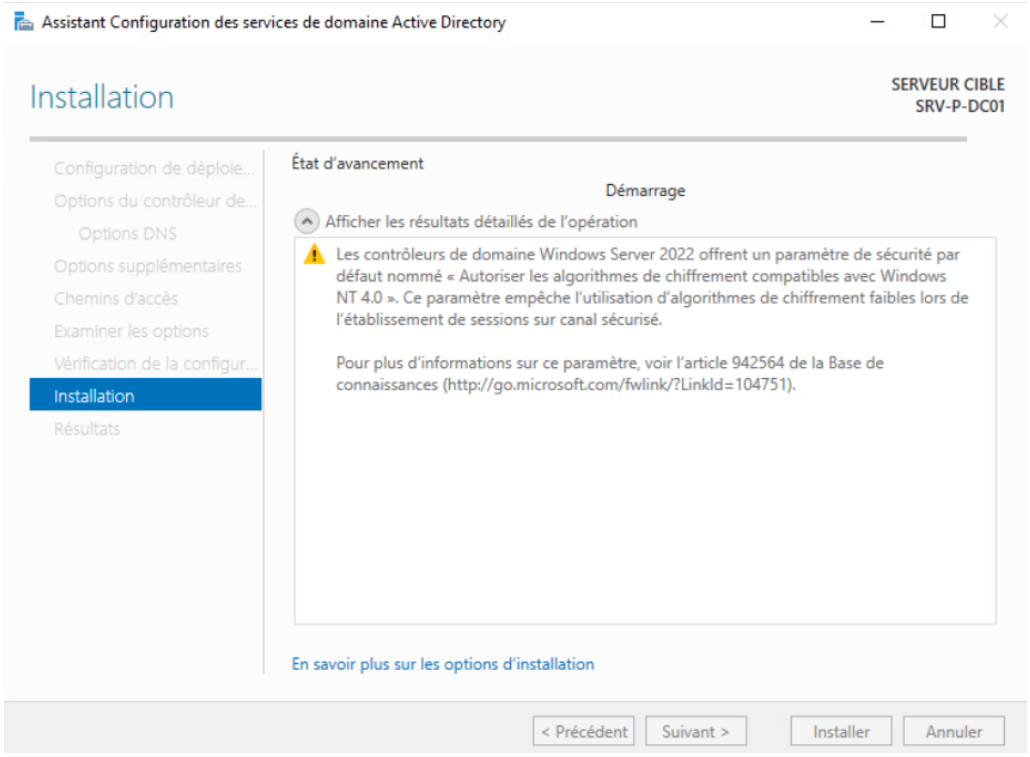
Passer les options DNS, puis définir le nom de domaine NetBIOS, ici « OASIS »



Si on suit les bonnes pratiques de l'ANSSI, il est important de mettre le dossier SYSVOL & NETLOGON sur une autre partition que celle occupée par le système (C:).
Dans notre cas, laisser par défaut l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL.

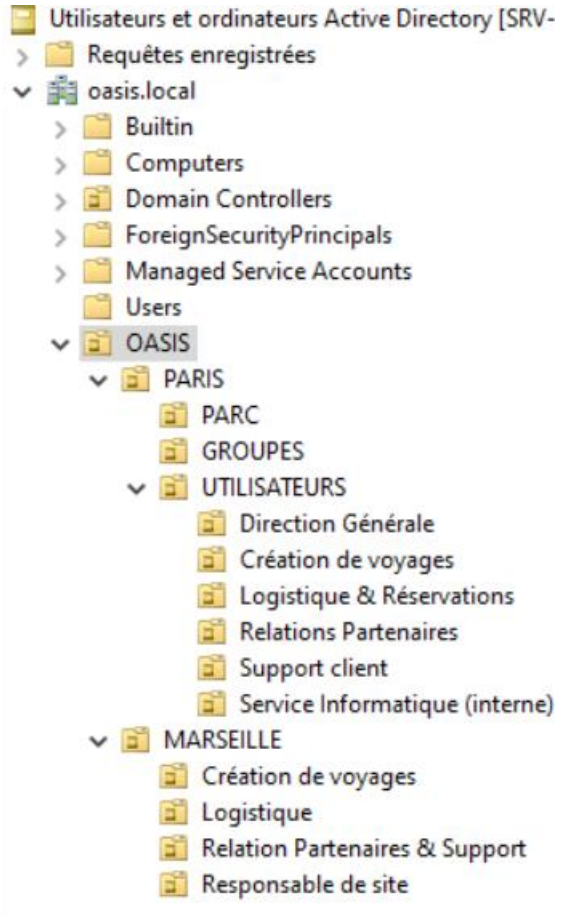


Ensuite, vient un récapitulatif, puis « Installer »



Le serveur effectue un redémarrage une fois terminé.

L'Active Directory est mis en place, la création d'objets dans l'annuaire est donc désormais fonctionnelle.



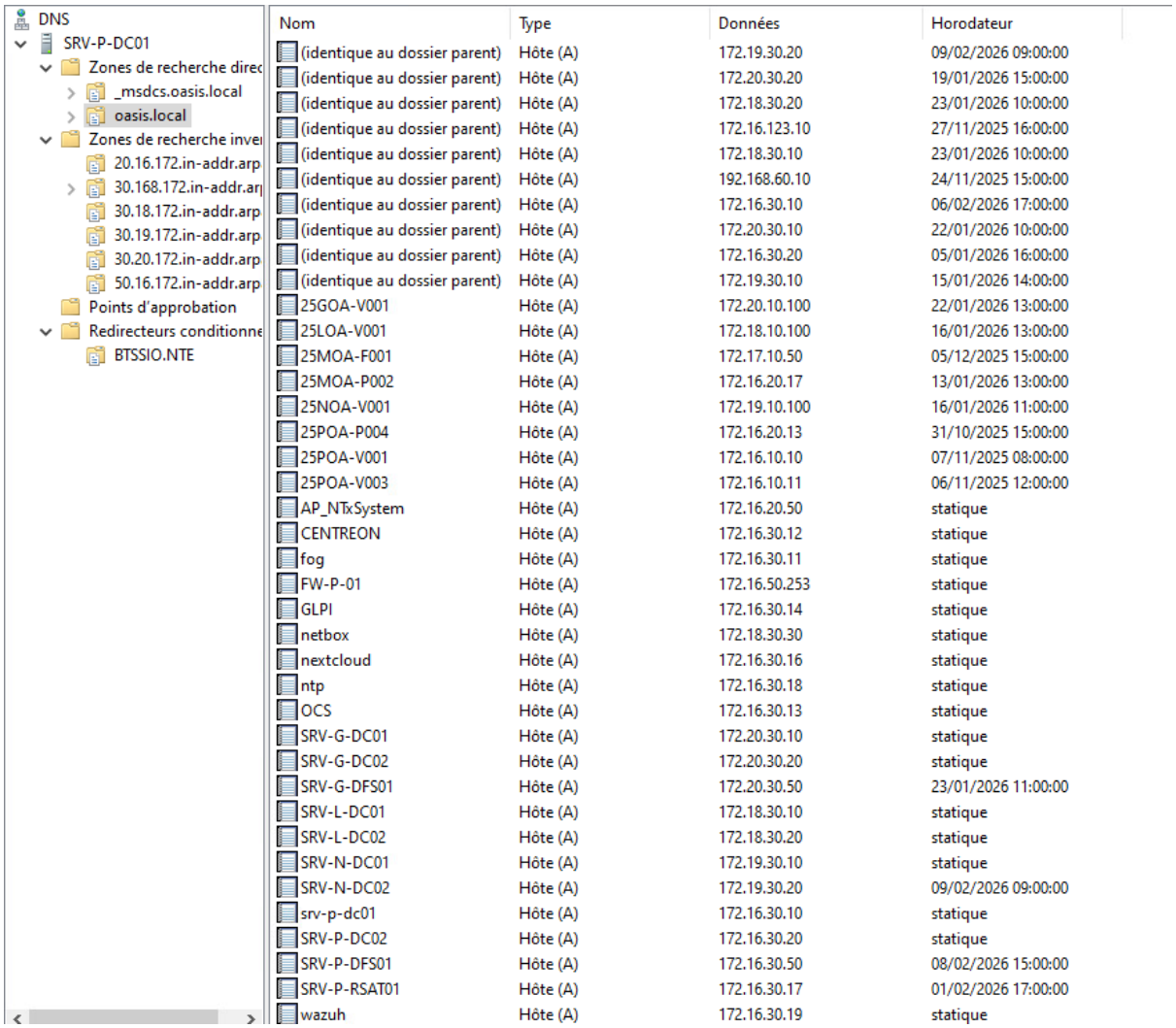
4.2. Configuration DNS

Le rôle DNS est automatiquement configuré lors de la promotion du serveur en contrôleur de domaine. La zone DNS oasis.local est intégrée à Active Directory, ce qui signifie que les enregistrements DNS sont stockés directement dans la base AD et répliqués automatiquement sur l'ensemble des contrôleurs de domaine du domaine.

Les enregistrements essentiels au bon fonctionnement d'Active Directory sont les suivants :

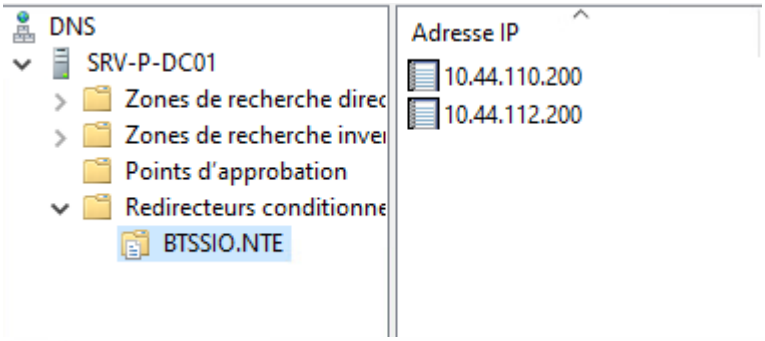
- Enregistrements SRV : ils permettent aux postes clients de localiser automatiquement les contrôleurs de domaine, le catalogue global…
- Enregistrements A (Host) : chaque contrôleur de domaine est enregistré avec son adresse IP.
- Enregistrements SOA et NS : ils définissent l'autorité de la zone et les serveurs de noms.

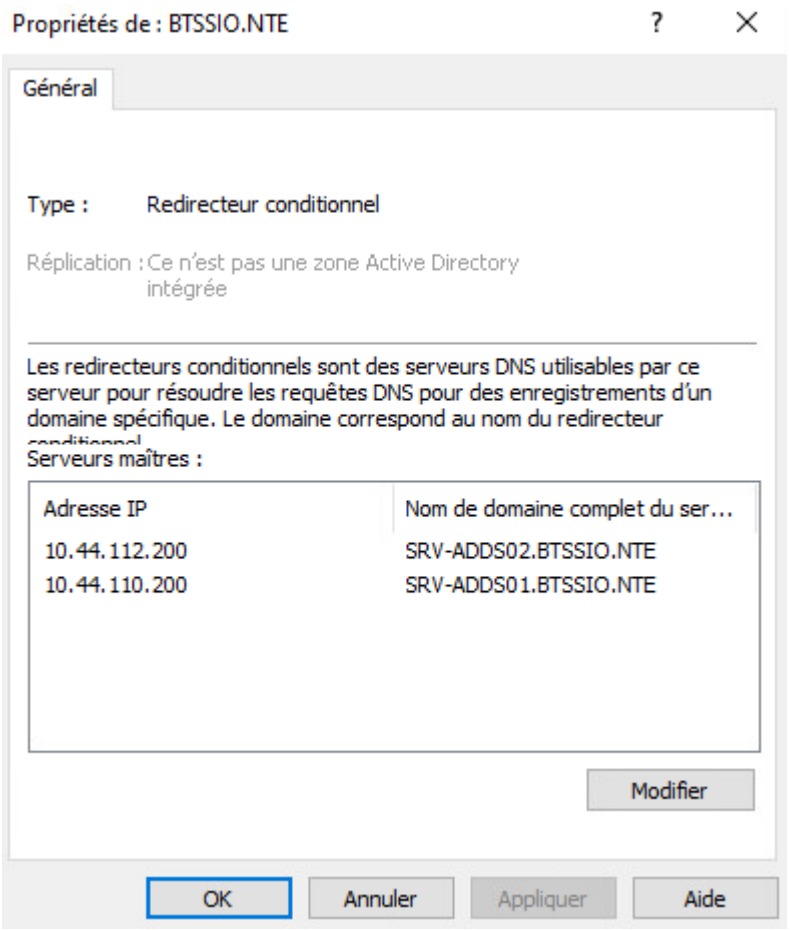
Il est également possible de créer une zone de recherche inversée afin de résoudre une adresse IP vers un nom de machine (enregistrements PTR).



Nom	Type	Données	Horodateur
(identique au dossier parent)	Hôte (A)	172.19.30.20	09/02/2026 09:00:00
(identique au dossier parent)	Hôte (A)	172.20.30.20	19/01/2026 15:00:00
(identique au dossier parent)	Hôte (A)	172.18.30.20	23/01/2026 10:00:00
(identique au dossier parent)	Hôte (A)	172.16.123.10	27/11/2025 16:00:00
(identique au dossier parent)	Hôte (A)	172.18.30.10	23/01/2026 10:00:00
(identique au dossier parent)	Hôte (A)	192.168.60.10	24/11/2025 15:00:00
(identique au dossier parent)	Hôte (A)	172.16.30.10	06/02/2026 17:00:00
(identique au dossier parent)	Hôte (A)	172.20.30.10	22/01/2026 10:00:00
(identique au dossier parent)	Hôte (A)	172.16.30.20	05/01/2026 16:00:00
(identique au dossier parent)	Hôte (A)	172.19.30.10	15/01/2026 14:00:00
25GOA-V001	Hôte (A)	172.20.10.100	22/01/2026 13:00:00
25LOA-V001	Hôte (A)	172.18.10.100	16/01/2026 13:00:00
25MOA-F001	Hôte (A)	172.17.10.50	05/12/2025 15:00:00
25MOA-P002	Hôte (A)	172.16.20.17	13/01/2026 13:00:00
25NOA-V001	Hôte (A)	172.19.10.100	16/01/2026 11:00:00
25POA-P004	Hôte (A)	172.16.20.13	31/10/2025 15:00:00
25POA-V001	Hôte (A)	172.16.10.10	07/11/2025 08:00:00
25POA-V003	Hôte (A)	172.16.10.11	06/11/2025 12:00:00
AP_NTxSystem	Hôte (A)	172.16.20.50	statique
CENTREON	Hôte (A)	172.16.30.12	statique
fog	Hôte (A)	172.16.30.11	statique
FW-P-01	Hôte (A)	172.16.50.253	statique
GLPI	Hôte (A)	172.16.30.14	statique
netbox	Hôte (A)	172.18.30.30	statique
nextcloud	Hôte (A)	172.16.30.16	statique
ntp	Hôte (A)	172.16.30.18	statique
OCS	Hôte (A)	172.16.30.13	statique
SRV-G-DC01	Hôte (A)	172.20.30.10	statique
SRV-G-DC02	Hôte (A)	172.20.30.20	statique
SRV-G-DFS01	Hôte (A)	172.20.30.50	23/01/2026 11:00:00
SRV-L-DC01	Hôte (A)	172.18.30.10	statique
SRV-L-DC02	Hôte (A)	172.18.30.20	statique
SRV-N-DC01	Hôte (A)	172.19.30.10	statique
SRV-N-DC02	Hôte (A)	172.19.30.20	09/02/2026 09:00:00
srv-p-dc01	Hôte (A)	172.16.30.10	statique
SRV-P-DC02	Hôte (A)	172.16.30.20	statique
SRV-P-DFS01	Hôte (A)	172.16.30.50	08/02/2026 15:00:00
SRV-P-RSAT01	Hôte (A)	172.16.30.17	01/02/2026 17:00:00
wazuh	Hôte (A)	172.16.30.19	statique

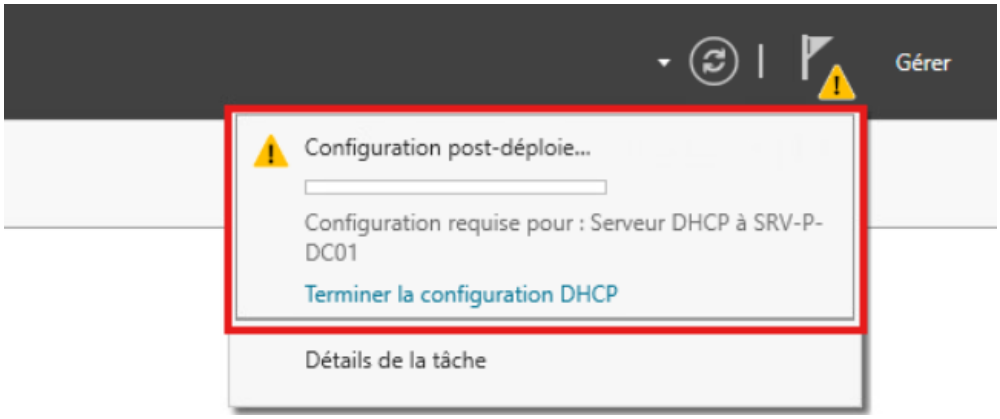
Configurer des redirecteurs conditionnels afin de diriger les requêtes DNS destinées à des domaines spécifiques vers des serveurs DNS définis. Cela permet par exemple de résoudre des noms de domaines externes ou partenaires sans passer par les redirecteurs classiques.



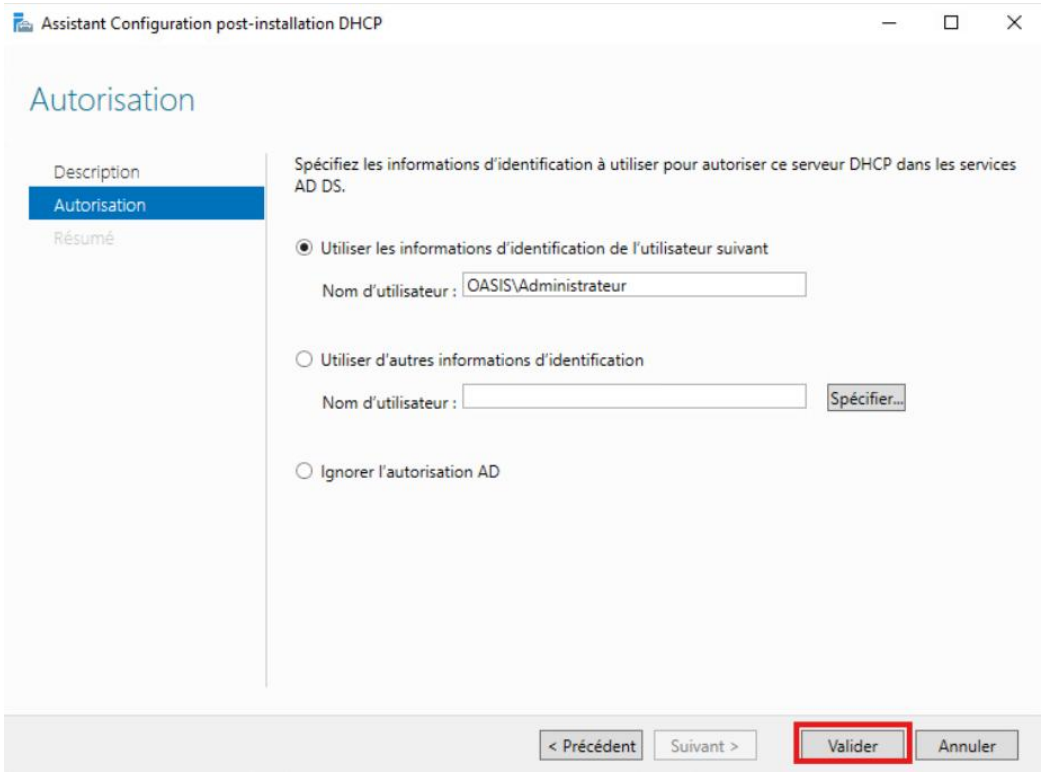


4.3. Configuration DHCP

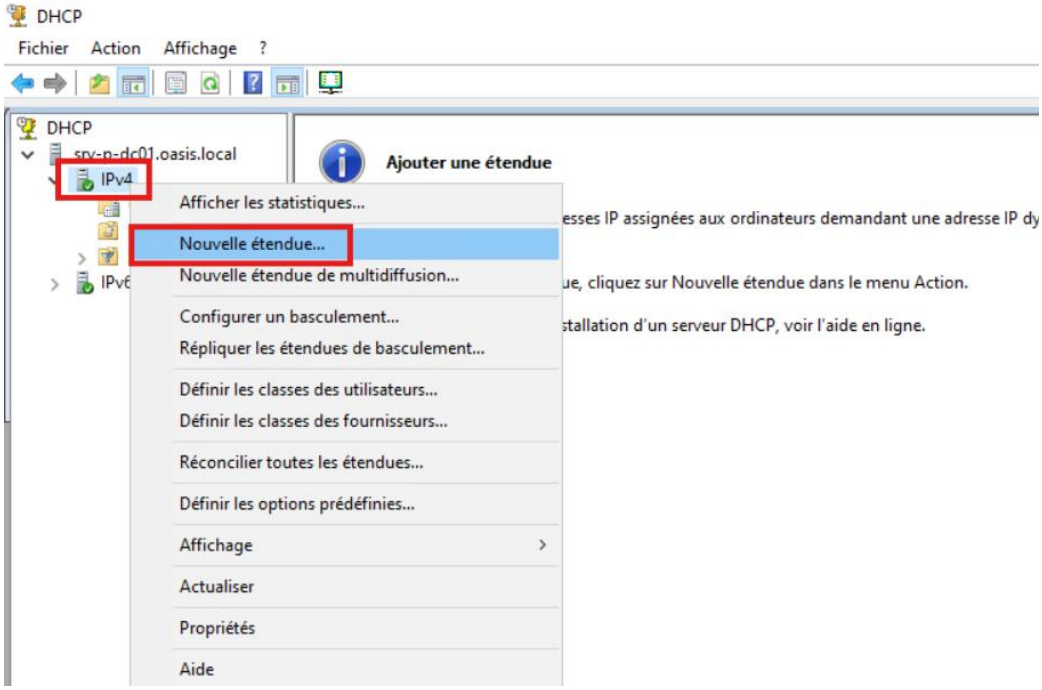
De retour sur le Gestionnaire de serveur, se rendre dans « Terminer la configuration DHCP »



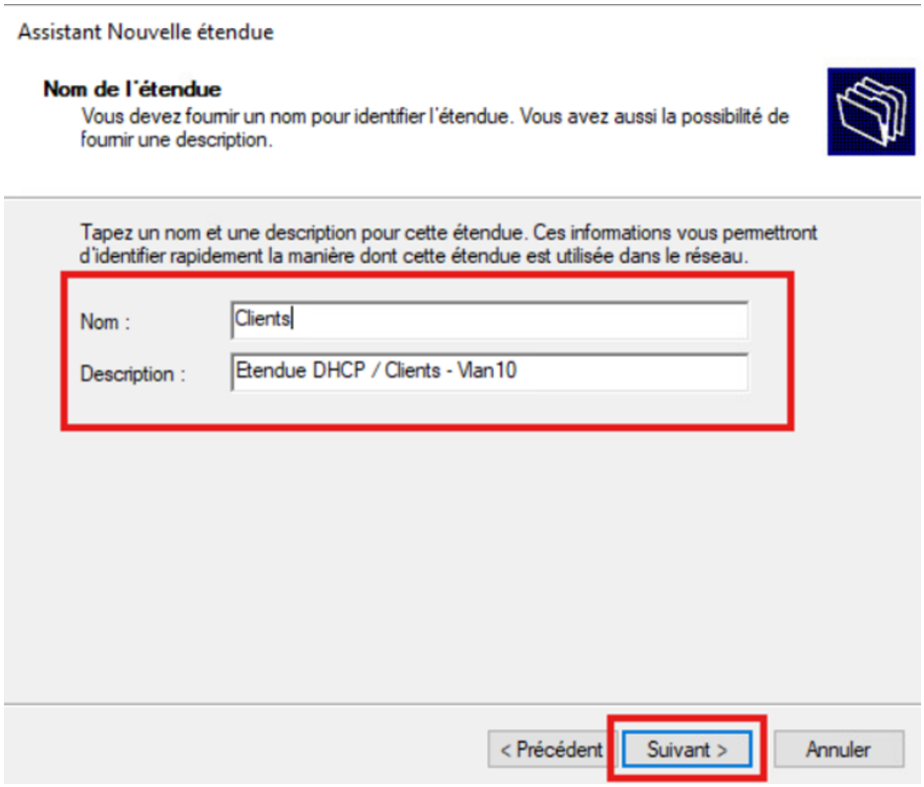
Utiliser l'administrateur du domaine pour autoriser ce serveur DHCP dans les services AD DS



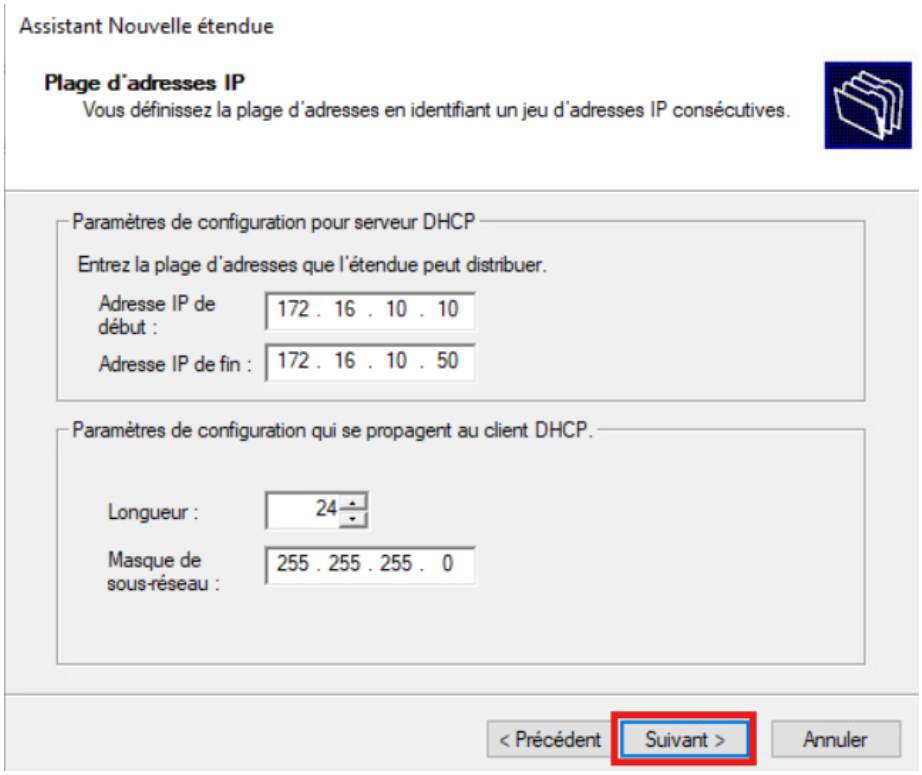
Une fois installé, démarrer l'applicatif « DHCP », développer le serveur « srv-p-dc01.oasis.local », puis sur « IPv4 », et enfin « Nouvelle étendue » afin de créer une plage DHCP.



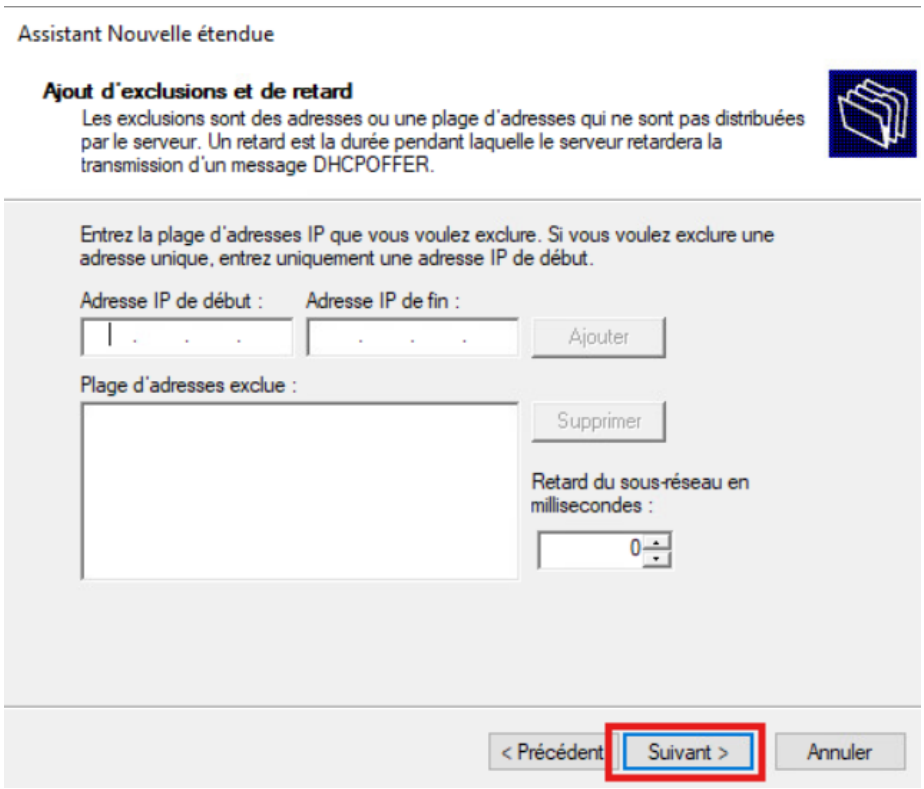
Nommer l'étendue, ainsi que le décrire pour une meilleure clarté.



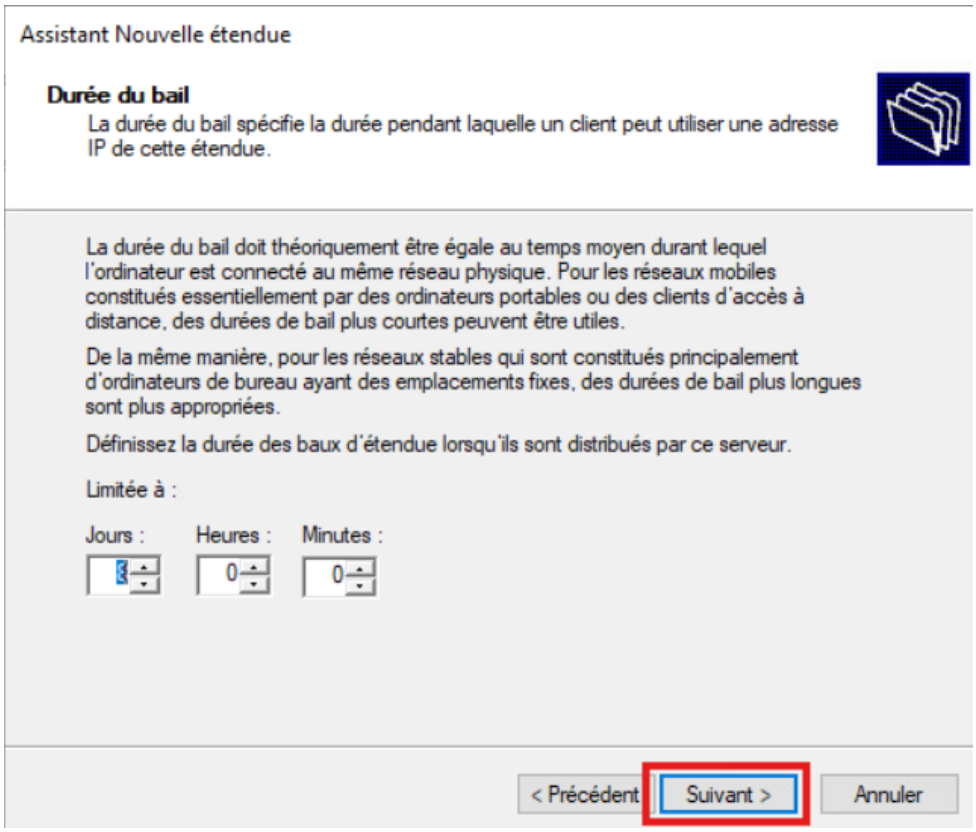
Définir une plage d'adresses DHCP, une adresse IP de début de plage ainsi qu'une adresse IP de fin de plage. Définir également un masque de sous réseau.



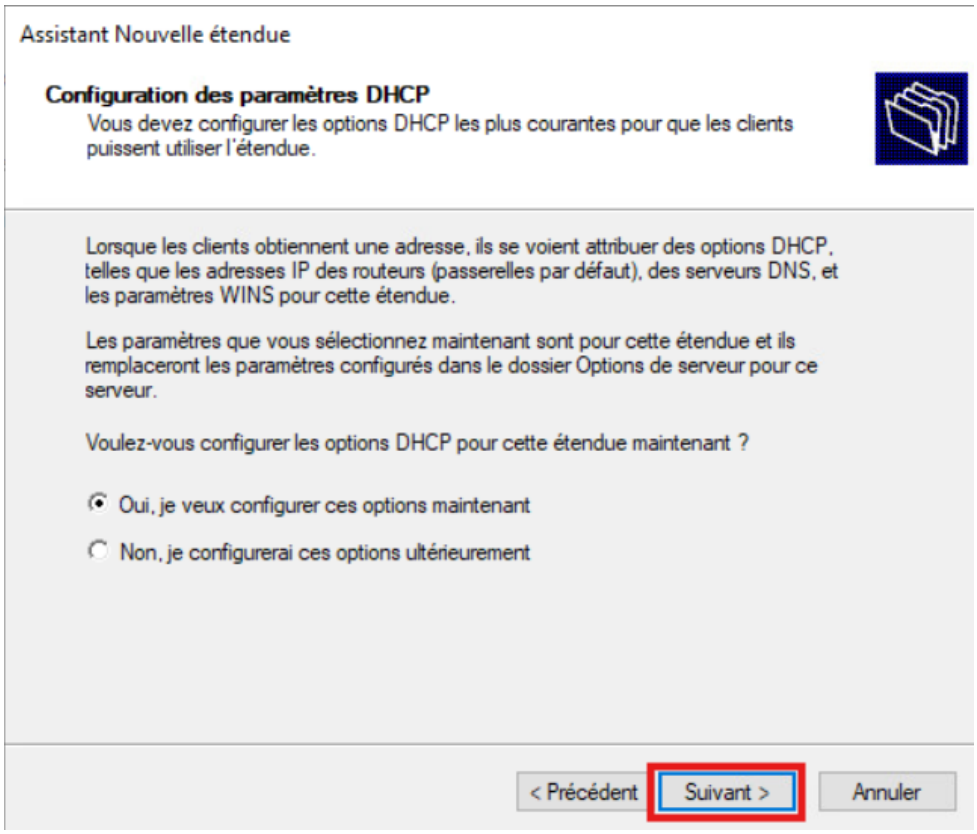
Si l'on souhaite avoir une grande plage DHCP mais que des IP fixes sont destinés dans cette plage, il est possible d'ajouter des exclusions.



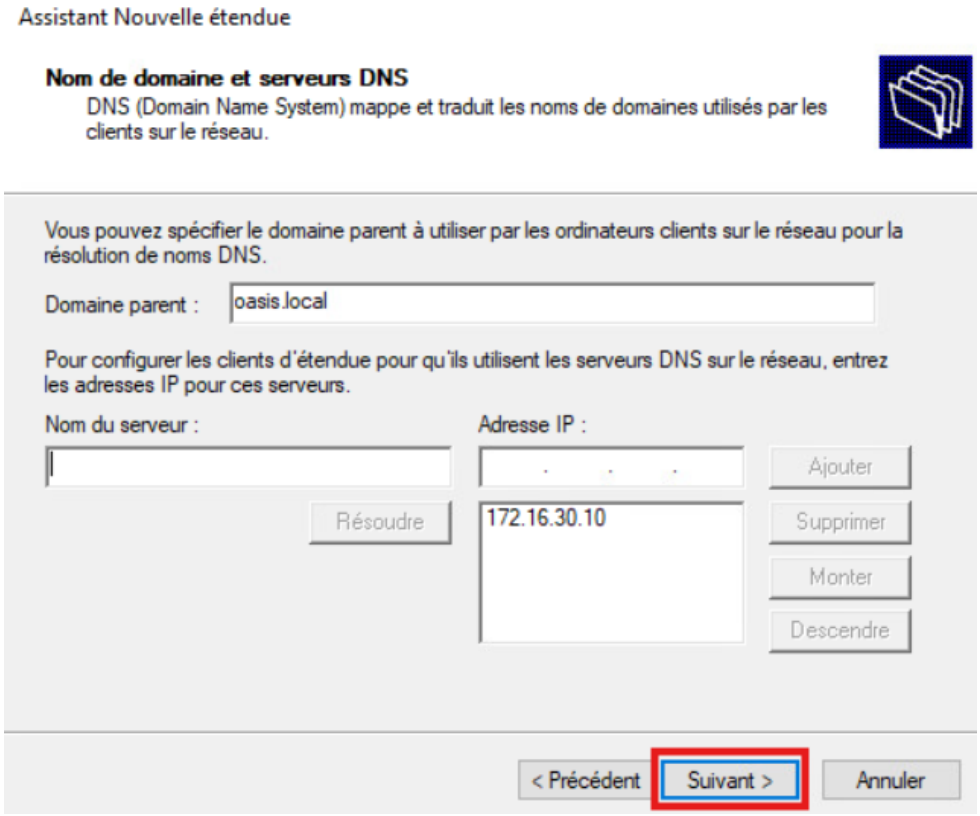
Définir une durée de bail pour cette plage.



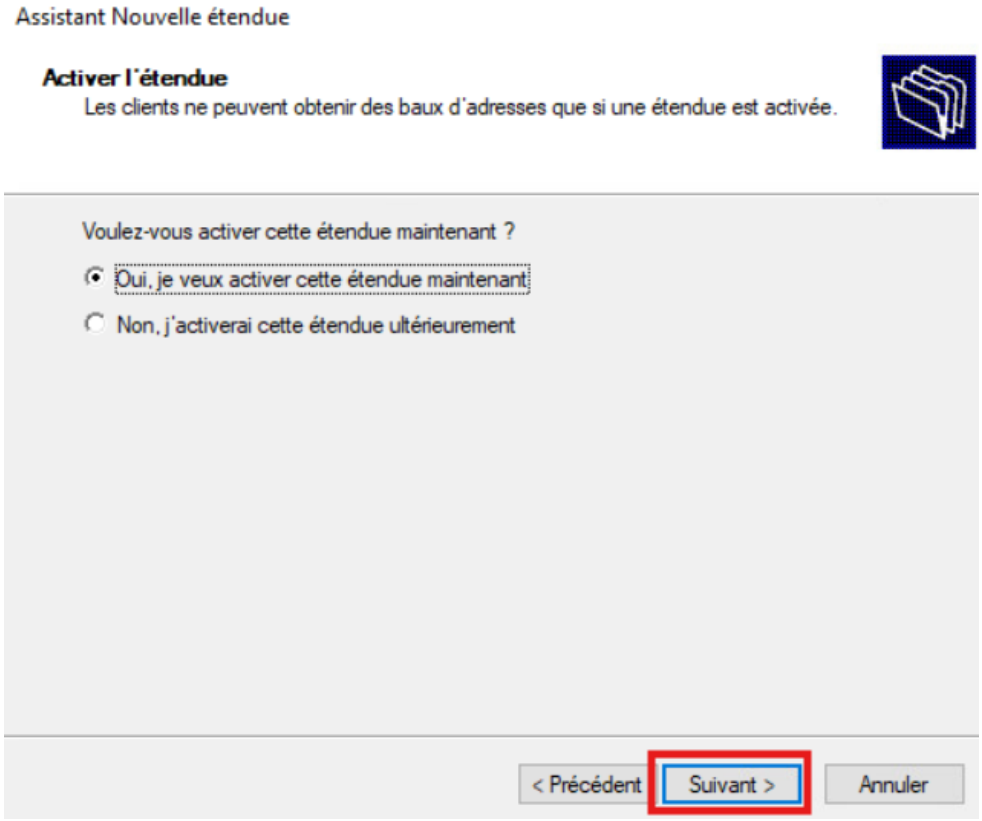
Sélectionner « Oui » afin de configurer maintenant le DNS ainsi que la passerelle pour cette étendue DHCP.



Définir l'adresse du serveur DNS souhaitée pour l'étendue.



Ne pas définir de Serveur WINS (Windows Internet Name Service), car ceci est obsolète, alors privilégier un serveur DNS.
Et enfin activer l'étendue DHCP.



4.4. Conclusion

L'installation de Windows Server 2022 et le déploiement des rôles ADDS, DNS et DHCP ont été validés avec succès. Le serveur SRV-P-DC01 est opérationnel en tant que contrôleur de domaine principal de la forêt oasis.local, avec le niveau fonctionnel défini à Windows Server 2016.

La résolution de noms est fonctionnelle et les redirecteurs conditionnels permettent la résolution des domaines externes.

Le service DHCP distribue correctement les adresses IP aux clients des étendues configurées, avec les options passerelle et serveur DNS transmises automatiquement aux postes.

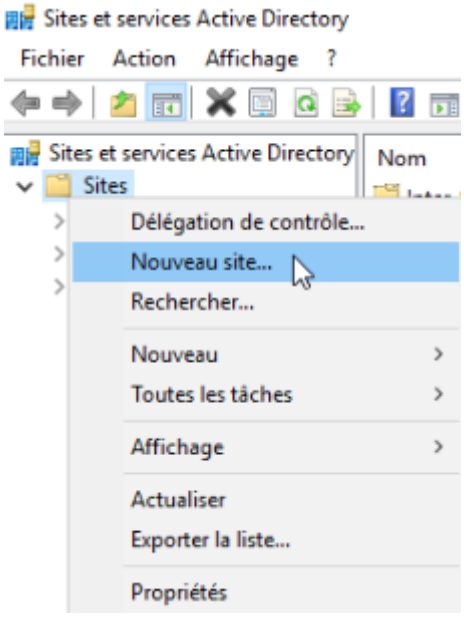
Une première ouverture de session avec un compte du domaine sur un poste client confirme que l'authentification Active Directory est fonctionnelle et que les stratégies de groupe de base s'appliquent correctement.

5. Réplication inter-site/intra-site

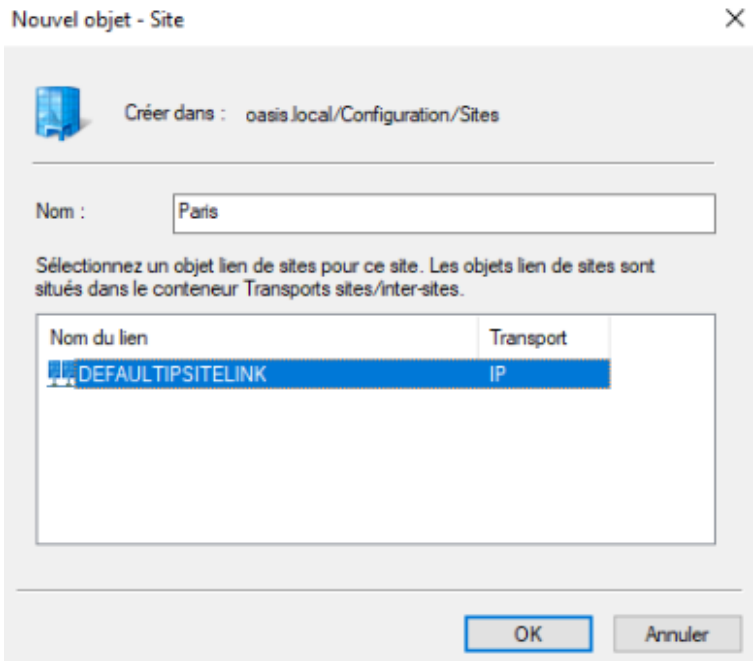
La réplication Active Directory permet de synchroniser les données de l'annuaire (comptes utilisateurs, groupes, GPO, zones DNS intégrées) entre les différents contrôleurs de domaine.
On distingue deux types de réplication :

- **Réplication intra-site :** réplication automatique entre les DC d'un même site, déclenchée quasi instantanément à chaque modification.
- **Réplication inter-site :** réplication planifiée entre les DC de sites différents, configurable en termes de coût et d'intervalle.

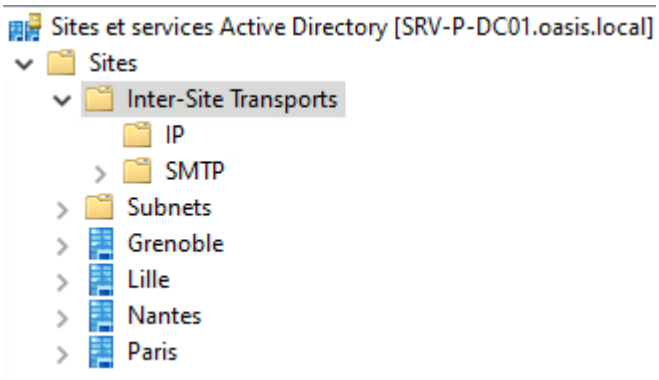
La configuration s'effectue depuis l'applicatif « Sites et services Active Directory ».
Créer le premier site, pour ce faire un clic droit sur « Sites » → « Nouveau site »



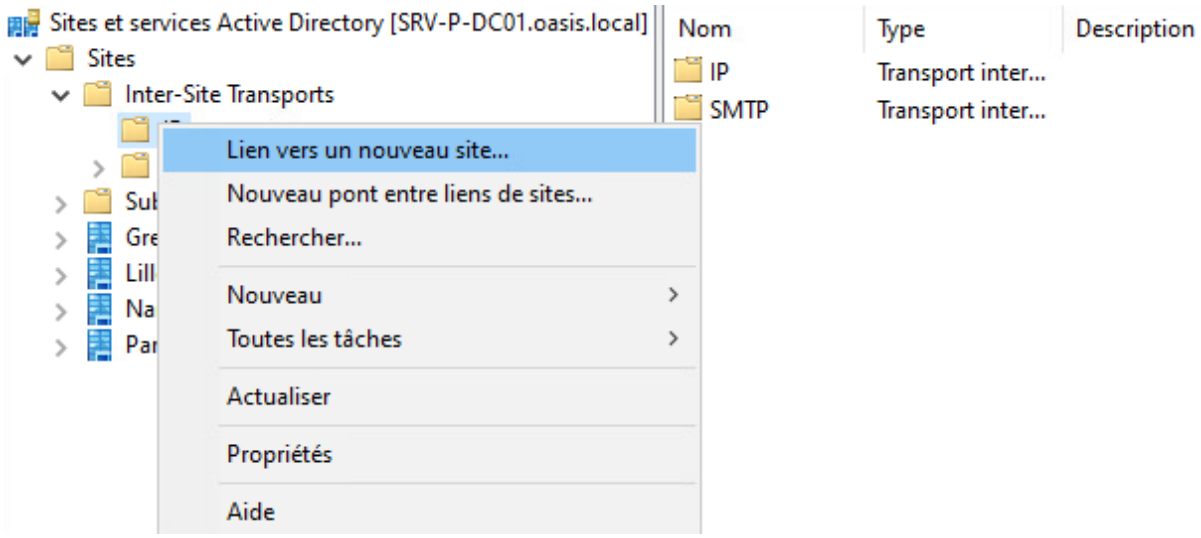
Renseigner le nom du site, ici « Paris », puis sélectionner le lien de site par défaut (DEFAULTIPSITELINK).
Répéter l'opération pour chaque site de l'infrastructure.



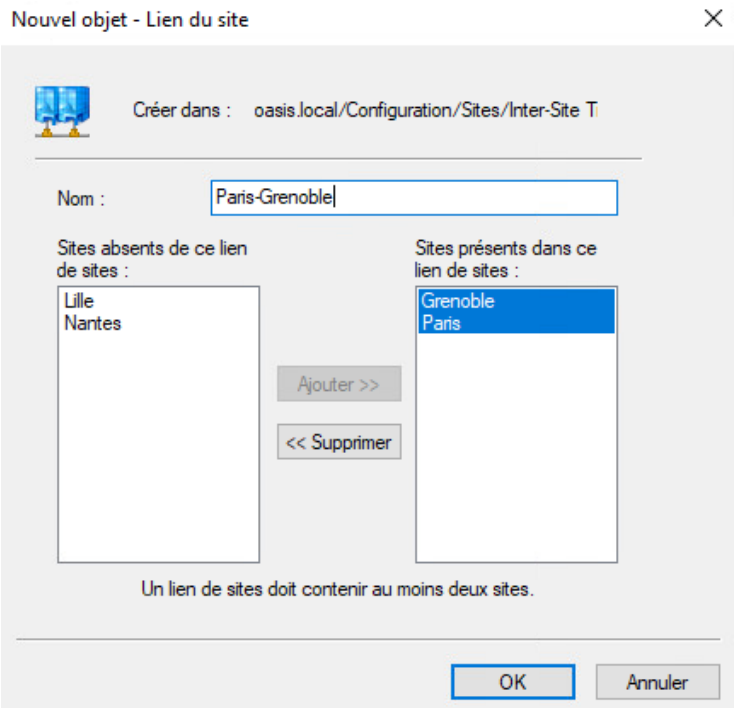
Une fois les sites créés, on retrouve les quatre sites : Grenoble, Lille, Nantes, Paris ainsi que le site par défaut qui est à supprimer.



Les liens de site définissent les chemins de réplication entre les sites. Pour créer un lien, se rendre dans « Inter-Site Transports » → « IP », clic droit puis « Lien vers un nouveau site »



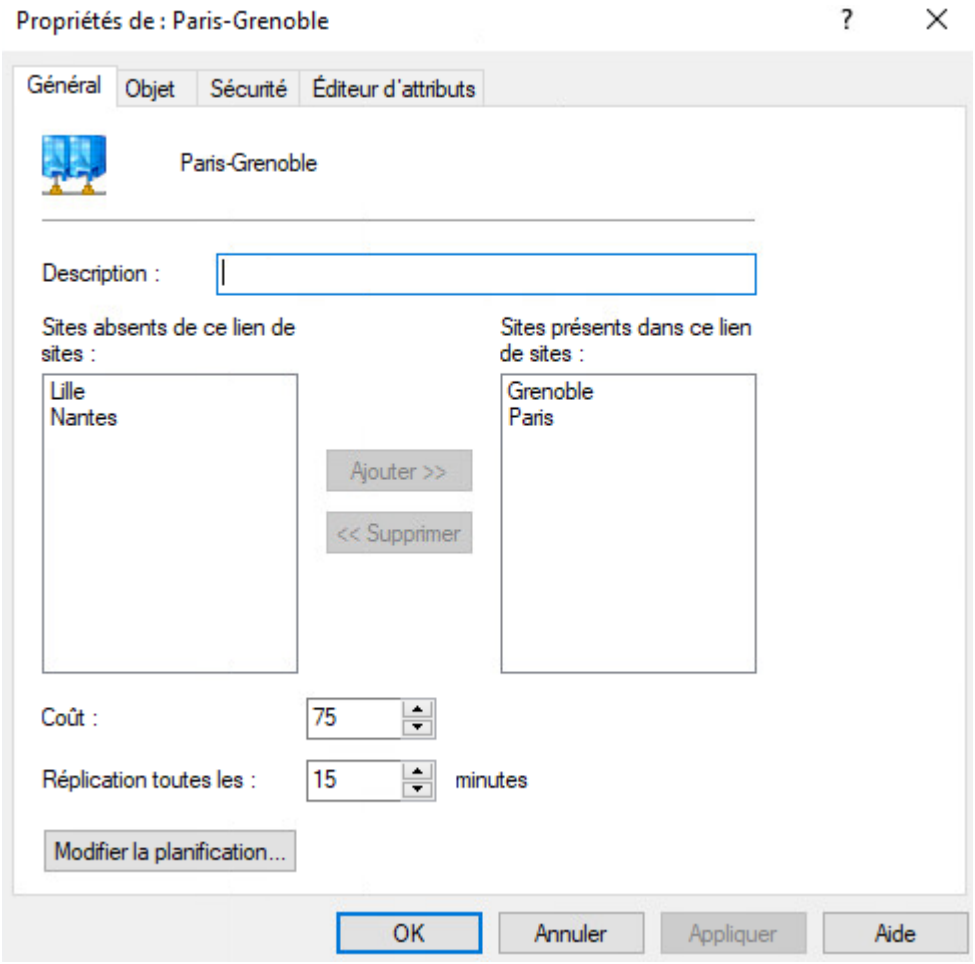
Nommer le lien selon la convention « Site1-Site2 », par exemple « Paris-Grenoble », puis sélectionner les deux sites concernés en les déplaçant dans la liste de droite.



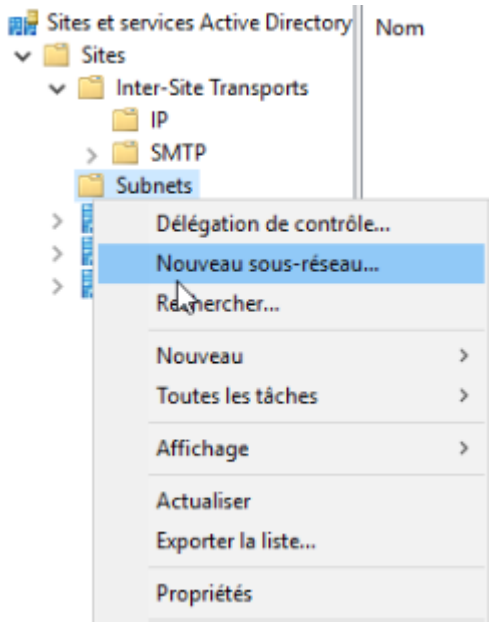
Au total, six liens de site sont créés pour couvrir l'ensemble des interconnexions. Les liens depuis Paris (site principal) ont un coût de 75 (prioritaire), tandis que les liens entre sites secondaires ont un coût de 100 (redondance). L'intervalle de réplication est fixé à 15 minutes pour tous les liens.

Nom	Type	Description	Coût	Intervalle de réplication
Grenoble-Lille	Lien du site		100	15
Grenoble-Nantes	Lien du site		100	15
Nantes-Lille	Lien du site		100	15
Paris-Grenoble	Lien du site		75	15
Paris-Lille	Lien du site		75	15
Paris-Nantes	Lien du site		75	15

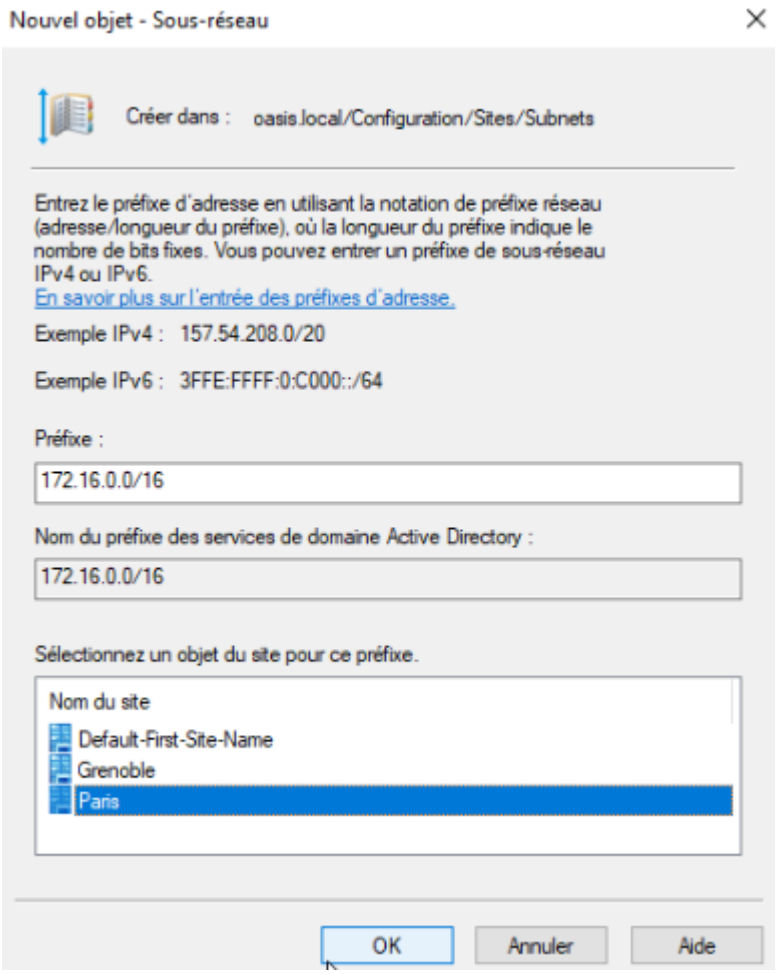
Les propriétés d'un lien de site permettent de modifier le coût, l'intervalle de réplication et la planification horaire si nécessaire.



Afin que les postes clients et serveurs soient automatiquement rattachés au bon site AD, il faut associer chaque sous-réseau à son site. Clic droit sur « Subnets » → « Nouveau sous-réseau »



Renseigner le préfixe réseau en notation CIDR, puis sélectionner le site correspondant. Par exemple, le sous-réseau 172.16.0.0/16 est associé au site Paris. Afin de ne pas créer plusieurs subnets par site, opter pour un /16 au lieu d'un /24 qui n'est pas forcément utile dans notre cas.



L'ensemble des sous-réseaux associés à leurs sites respectifs :

Nom	Site	Em...	Type	Description
172.16.0.0/16	Paris		Sous-réseau	Réseau Paris
172.17.0.0/16	Paris		Sous-réseau	Réseau Marseille
172.18.0.0/16	Lille		Sous-réseau	Réseau Lille
172.19.0.0/16	Nantes		Sous-réseau	Réseau Nantes
172.20.0.0/16	Grenoble		Sous-réseau	Réseau Grenoble

Une fois la configuration terminée, il est possible de forcer le recalcul de la topologie de réplication via le KCC (Knowledge Consistency Checker), car celle-ci peut prendre un certain temps avant de générer la topologie, puis de déclencher une synchronisation complète entre tous les partenaires :
Cette commande force le KCC à recalculer les connexions de réplication sur l'ensemble des contrôleurs de domaine :

*repadmin /kcc * /async*

```
PS C:\Users\Administrateur> repadmin /kcc * /async
```

Cette commande synchronise tous les partenaires de réplication de manière récursive. Les paramètres /A (tous les partenaires), /d (identification par DN), /e (inter-sites) et /P (push) garantissent une réplication complète et immédiate.

repadmin /syncall /AdeP

```
PS C:\Users\Administrateur> repadmin /syncall /AdeP
```

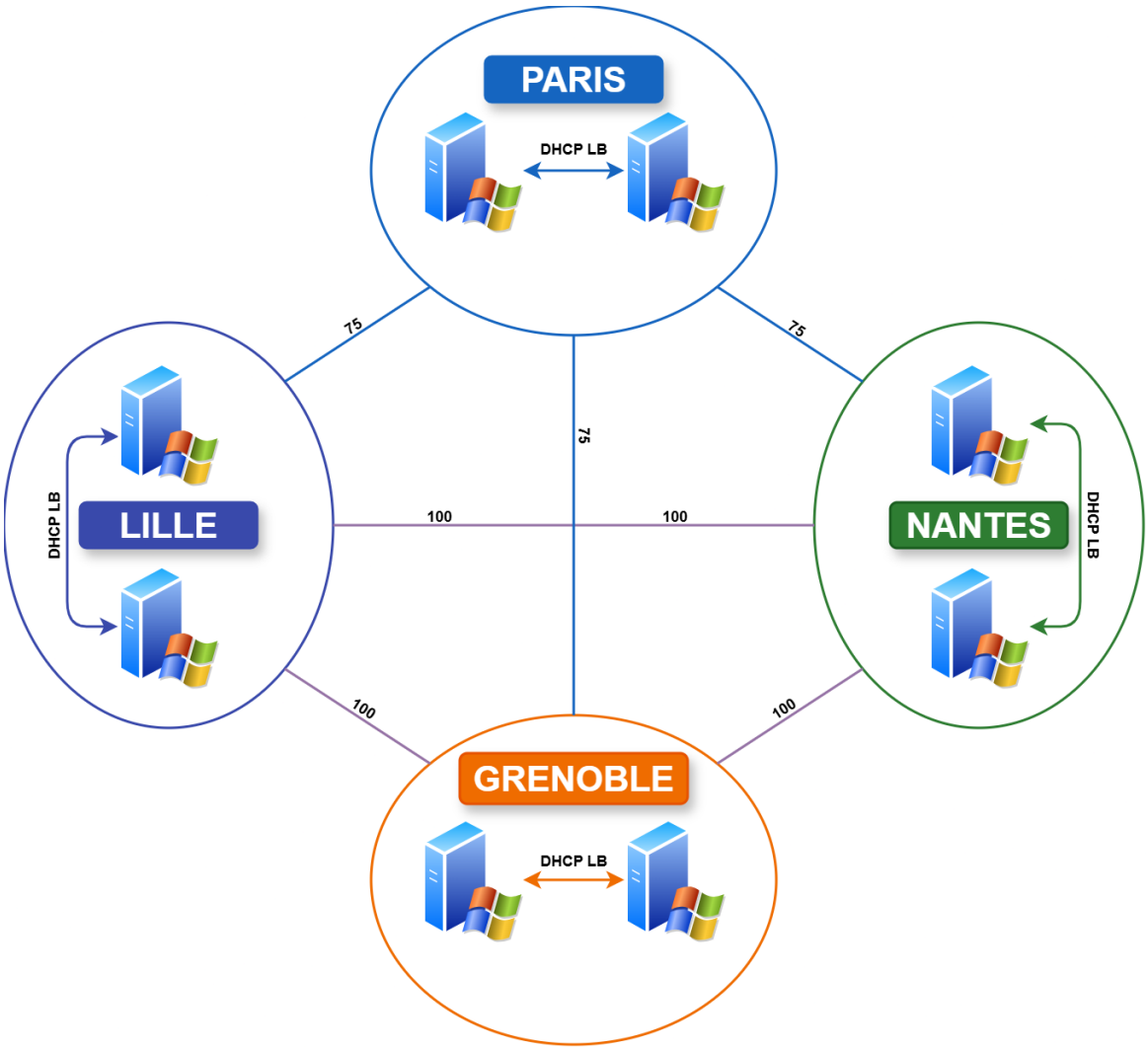
5.1. Conclusion

La réplication Active Directory a été validée sur l'ensemble des quatre sites de l'infrastructure. Les sites Paris, Grenoble, Lille et Nantes sont bien créés dans la console Sites et Services Active Directory, chacun associé à son sous-réseau en notation CIDR.

Les six liens de site couvrent l'ensemble des interconnexions, les liens depuis Paris ont un coût de 75 et les liens entre sites secondaires un coût de 100, avec un intervalle de réplication fixé à 15 minutes sur l'ensemble des liens.

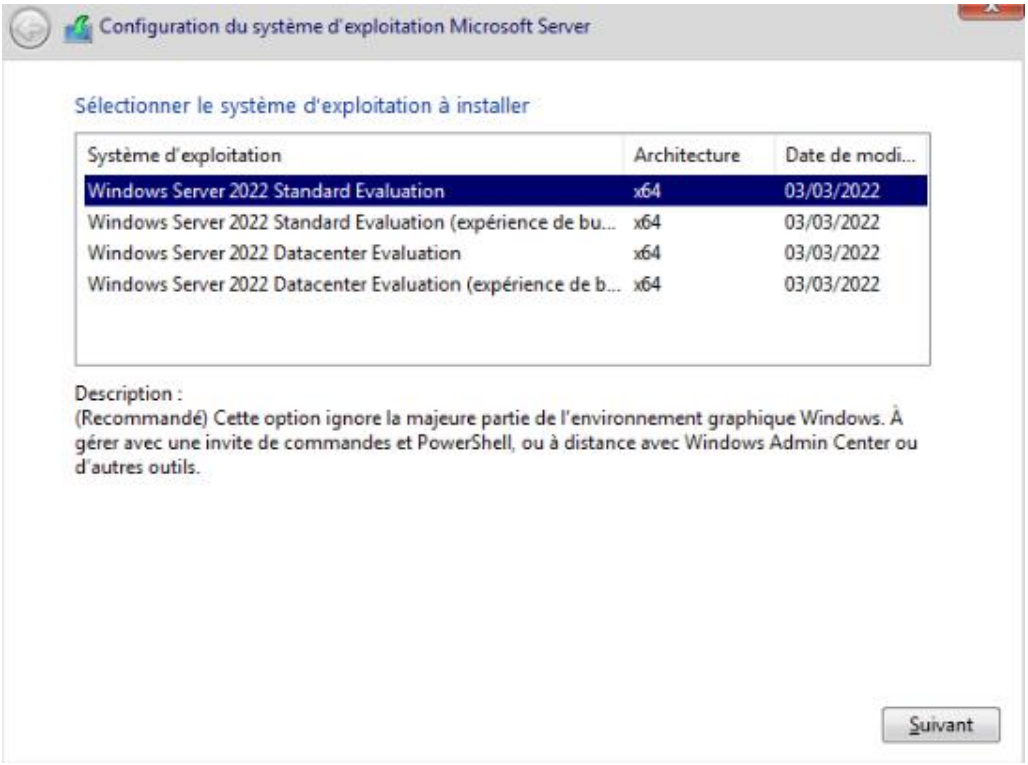
La synchronisation forcée via les commandes « repadmin /kcc * /async » et « repadmin /syncall /AdeP » s'est exécutée sans erreur, confirmant que les données de l'annuaire sont bien répliquées entre les contrôleurs de domaine sur l'ensemble des partitions.

5.2. Schéma de réplication

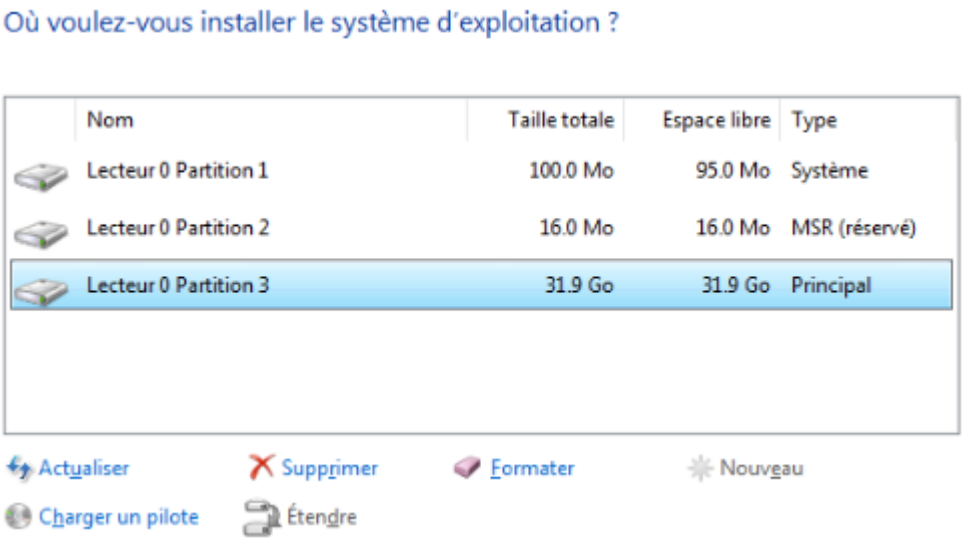


6. Installation Windows Server Core

Les contrôleurs de domaine secondaires (DC02) sont installés en mode Server Core, c'est-à-dire sans interface graphique. Ce choix présente plusieurs avantages : consommation de ressources moindre (RAM et CPU), un temps d'installation et de redémarrage plus court.
Démarrer sur un disque d'installation Windows Server, puis installation basique jusqu'au choix du système d'exploitation. Sélectionner « Windows Server 2022 Standard ».

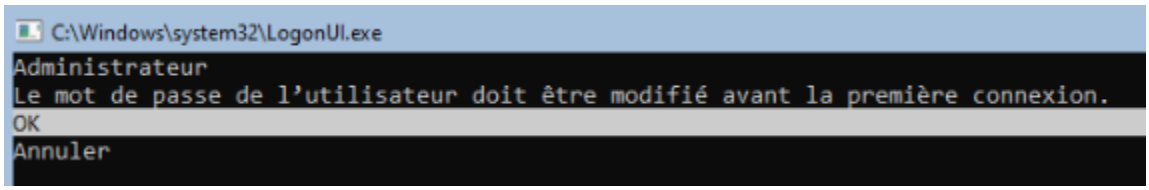


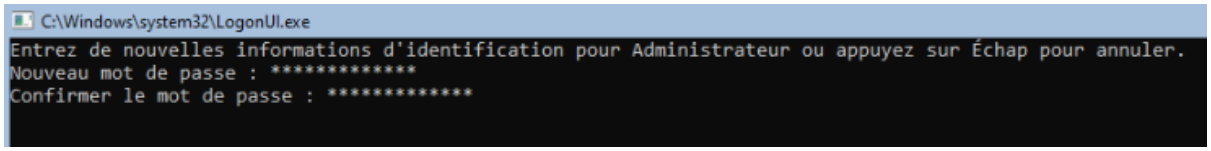
Puis initialiser le(s) disque(s), et créer les partitions.



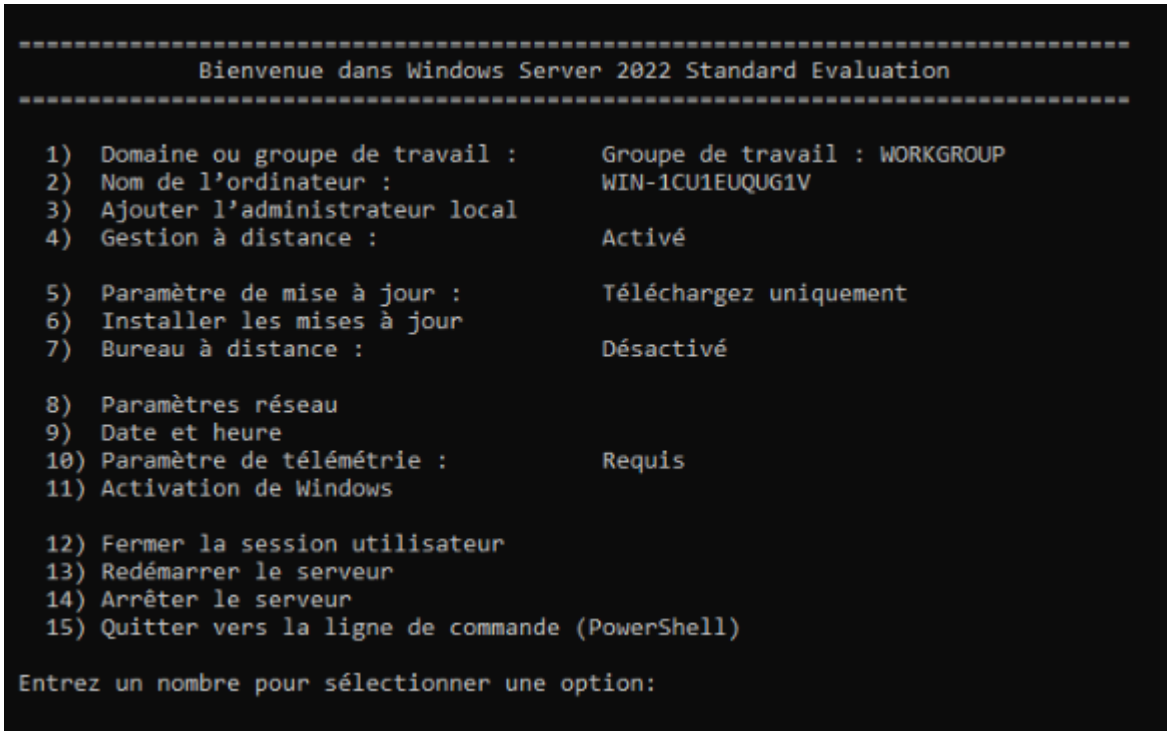
L'installation se poursuit, attendre la fin de l'installation.

Premier démarrage sans interface graphique : Définir un mot de passe pour l'administrateur local





Ensuite le serveur démarre dans un menu « SCONFIG »



La configuration initiale est possible via le menu « SCONFIG », cependant pour des paramètres avancés, l'utilisation du Powershell est obligatoire.

6.1. Configuration SCONFIG (Optionnel)

Saisir le chiffre « 1 » afin de modifier le nom de la machine

```
================================================================================
                            Nom de l'ordinateur
================================================================================

Nom de l'ordinateur actuel : WIN-1CU1EUQUG1V

Entrer un nouveau nom d'ordinateur (Vide = annuler): SRV-G-DC02
```

Saisir le chiffre « 8 » afin de modifier les paramètres réseaux. Puis choisir la carte réseau en saisissant l'index correspondant. Ici « 1 ».

```
================================================================================
                            Paramètres réseau
================================================================================

Cartes réseau disponibles :

Index numéro | Adresse IP      | Description
1            | 169.254.208.175 | Intel(R) PRO/1000 MT Network Connection

Sélectionnez le numéro d'index de la carte réseau (Vide = annuler): 1
```

Ensuite, saisir le chiffre « 1 », pour modifier les adresses de la carte réseau :

- Adresse Statique / Adresse dynamique (DHCP)
- Adresse IP
- Masque de sous-réseau
- Passerelle par défaut

```
================================================================================
                        Paramètres de carte réseau
================================================================================

Index NIC :                1
Description :              Intel(R) PRO/1000 MT Network Connection
Adresse IP :               169.254.208.175,
                           fe80::d4e2:7494:1da8:d0af
Masque de sous-réseau :    255.255.0.0
DHCP activé :              True

Passerelle par défaut :
Serveur DNS préféré :
Serveur DNS auxiliaire :

  1) Définir l'adresse de la carte réseau
  2) Définir les serveurs DNS
  3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler): 1
Sélectionnez le protocole (D)HCP ou l'adresse IP (S)tatique (Vide = annuler): S
Entrer une adresse IP statique : (Vide = annuler): 172.20.30.20
Entrer un masque de sous-réseau (Vide=255.255.255.0):
Entrez la passerelle par défaut (Vide = annuler): 172.20.30.254
```

Désormais on peut quitter le mode SCONFIG et basculer en Powershell en saisissant le nombre « 15 ».
On peut d'ailleurs vérifier la configuration réseau via la commande :

Get-NetIPConfiguration

```
PS C:\Users\Administrateur> Get-NetIPConfiguration


InterfaceAlias       : Ethernet
InterfaceIndex       : 4
InterfaceDescription : Intel(R) PRO/1000 MT Network Connection
NetProfile.Name      : Réseau
IPv4Address          : 172.20.30.20
IPv6DefaultGateway   :
IPv4DefaultGateway   : 172.20.30.254
DNSServer            : 172.16.30.10
                       172.20.30.10
```

On vérifie qu'on arrive à résoudre le domaine oasis.local qui sera ensuite le domaine à rejoindre :

nslookup oasis.local

On retrouve tous les hôtes répondant ou qui ont répondu au nom de oasis.local

```
PS C:\Users\Administrateur> nslookup oasis.local
Serveur :   UnKnown
Address:  172.16.30.10

Nom :    oasis.local
Addresses:  172.20.30.10
          172.16.30.20
          172.16.30.10
          192.168.60.10
          172.18.30.10
          172.16.123.10
          172.19.30.10
```

Il est aussi possible d'ajouter une machine dans le domaine depuis le menu « SCONFIG ».

6.2. Configuration Powershell (Préféré)

La méthode PowerShell est plus rapide et reproductible. Elle permet également de scripter l'ensemble de la configuration pour la déployer sur plusieurs serveurs.
Renommer l'ordinateur :

Rename-Computer 'SRV-N-DC02'

```
PS C:\Users\Administrateur> Rename-Computer 'SRV-N-DC02'
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-4BUT3NHV446.
```

On peut redémarrer la machine maintenant mais ce n'est pas obligatoire pour le moment :

Restart-Computer

```
PS C:\Users\Administrateur> Restart-Computer
```

Définition de la configuration IP :

Récupérer des informations de la carte réseau

```
$adapter = Get-NetAdapter -Name 'Ethernet'
$adapter | Remove-NetIPAddress -Confirm:$false
$adapter | Remove-NetRoute -Confirm:$false
```

```
PS C:\Users\Administrateur> $adaptater = Get-NetAdapter -Name 'Ethernet'
PS C:\Users\Administrateur> $adaptater | Remove-NetIPAddress -Confirm:$false
PS C:\Users\Administrateur> $adaptater | Remove-NetRoute -Confirm:$false
```

Définir l'adresse IP statique, le masque et la passerelle :

```
$param = @{
  IfIndex = $adapter.ifIndex
  IPAddress = '172.19.30.20'
  AddressFamily = 'IPv4'
  PrefixLength = 24
  DefaultGateway = '172.19.30.254'
}
```

```
PS C:\Users\Administrateur> $param = @{
>> Ifindex = $adaptater.ifIndex
>> IPAddress = '172.19.30.20'
>> AddressFamily = 'IPv4'
>> PrefixLength = 24
>> DefaultGateway = '172.19.30.254'
>> }
```

Appliquer la configuration IP :

New-NetIPAddress @param

```
PS C:\Users\Administrateur> New-NetIPAddress @param


IPAddress         : 172.19.30.20
InterfaceIndex    : 5
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 172.19.30.20
InterfaceIndex    : 5
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Définition des serveurs DNS :

```
$param = @{
   InterfaceIndex  = $adapter.ifIndex
   ServerAddresses = '172.19.30.10', '172.19.30.20'
}
```

```
PS C:\Users\Administrateur> $param = @{
>> InterfaceIndex = $adaptater.ifIndex
>> ServerAddresses = '172.19.30.10', '172.19.30.20'
>> }
```

Appliquer la configuration DNS :

Set-DnsClientServerAddress @param

```
PS C:\Users\Administrateur> Set-DnsClientServerAddress @param
PS C:\Users\Administrateur> nslookup google.fr
Serveur :   SRV-N-DC01.oasis.local
Address:  172.19.30.10

Réponse ne faisant pas autorité :
Nom :    google.fr
Addresses:  2a00:1450:4007:805::2003
          172.217.18.195
```

On évite d'utiliser l'adresse de loopback 127.0.0.1 pour le serveur DNS d'un contrôleur de domaine.
Vérifier que la configuration reseau est correcte :

Get-NetIPConfiguration -InterfaceIndex $adapter.ifIndex

```
PS C:\Users\Administrateur> Get-NetIPConfiguration -InterfaceIndex $adaptater.ifIndex


InterfaceAlias       : Ethernet
InterfaceIndex       : 5
InterfaceDescription : Intel(R) PRO/1000 MT Network Connection
NetProfile.Name      : Réseau
IPv4Address          : 172.19.30.20
IPv6DefaultGateway   :
IPv4DefaultGateway   : 172.19.30.254
DNSServer            : 172.19.30.10
                       172.19.30.20
```

Le serveur dispose bien de l'adresse 172.19.30.20, de la passerelle 172.19.30.254 et des DNS 172.19.30.10 | 172.19.30.20.
Installer le rôle Active Directory Domain Services (ADDS) et redémarrer le serveur :

Install-WindowsFeature -Name AD-Domain-Services –Restart

```
PS C:\Users\Administrateur> Install-WindowsFeature -Name AD-Domain-Services -Restart

Collecte des données en cours...
    2 %
    [oo
```

Si on suit les bonnes pratiques de l'ANSSI, il est important de mettre le dossier SYSVOL & NETLOGON sur une autre partition que celle occupée par le système (C:). Alors, créer une partition depuis un disque virtuel vierge. Pour la taille du disque, tabler sur 10 Go.
Dans cet exemple, utiliser la lettre F:\
Lister les disques :

Get-Disk

```
PS C:\Users\Administrateur> Get-Disk

Number Friendly Name Serial Number                 HealthStatus         OperationalStatus      Total Size Partition
                                                                                                           Style
------ ------------- -------------                 ------------         -----------------      ---------- ----------
0      QEMU QEMU ...                               Healthy              Online                     32 GB GPT
1      QEMU QEMU ...                               Healthy              Offline                    10 GB RAW
```

Le disque 1 (10 Go, RAW) est disponible. L'initialiser, le partitionner et le formater :

Initialize-Disk –Number 1

```
PS C:\Users\Administrateur> Initialize-Disk -Number 1
```

New-Partition -DiskNumber 1 -UseMaximumSize -AssignDriveLetter

```
PS C:\Users\Administrateur> New-Partition -DiskNumber 1 -UseMaximumSize -AssignDriveLetter


   DiskPath : \\?\scsi#disk&ven_qemu&prod_qemu_harddisk#6&32a8f6f9&0&000001#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
2                F           16777216                                    9.98 GB Basic
```

La partition est créée sur le lecteur (F:), formater la partition :

Get-Partition -DriveLetter 'F' |
Format-Volume -FileSystem NTFS -NewFileSystemLabel 'NTDS'

```
PS C:\Users\Administrateur> Get-Partition -DriveLetter 'F' |
>> Format-Volume -FileSystem NTFS -NewFileSystemLabel 'NTDS'
```

Vérifier la présence du nouveau disque avec la commande suivante :
Get-PSDrive

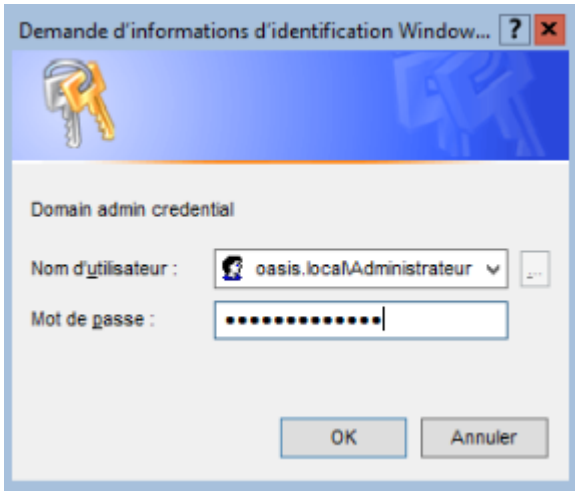
```
PS C:\Users\Administrateur> Get-PSDrive

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Alias                                  Alias
C                   6,85         24,47 FileSystem    C:\                                                Users\Administrateur
Cert                                   Certificate   \
D                   0,74          0,00 FileSystem    D:\
E                   4,71          0,00 FileSystem    E:\
Env                                    Environment
F                   0,04          9,95 FileSystem    F:\
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USER
HKLM                                   Registry      HKEY_LOCAL_MACHINE
Variable                               Variable
WSMan                                  WSMan
```

Préparer les paramètres de promotion en contrôleur de domaine en pointant les chemins NTDS et SYSVOL vers le lecteur (F:) :

```
$splat = @{
   DomainName    = 'oasis.local'
   Credential    = (Get-Credential -Message 'Domain admin credential')
   LogPath       = 'F:\NTDS'
   DatabasePath = 'F:\NTDS'
   SysvolPath    = 'F:\SYSVOL'
}
```

```
PS C:\Users\Administrateur> $splat = @{
>> DomainName = 'oasis.local'
>> Credential = (Get-Credential -Message 'Domain admin credential')
>> LogPath = 'F:\NTDS'
>> DatabasePath = 'F:\NTDS'
>> SysvolPath = 'F:\SYSVOL'
>> }
```

Renseigner les identifiants d'un administrateur du domaine (oasis.local\Administrateur).



Lancer la promotion :

Install-ADDSDomainController @splat

Définir le mot de passe DSRM (SafeModeAdministratorPassword), puis confirmer l'opération en saisissant « O » (Oui).

```
PS C:\Users\Administrateur> Install-ADDSDomainController @splat
SafeModeAdministratorPassword: ************
Confirmer SafeModeAdministratorPassword: ************

Le serveur cible sera configuré en tant que contrôleur de domaine et redémarré à la fin de cette opération.
Voulez-vous continuer en procédant à cette opération ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») :
```

L'opération s'est déroulée avec succès. Le serveur redémarrera automatiquement et sera désormais contrôleur de domaine du domaine oasis.local.

```
Message                                Context          RebootRequired  Status
-------                                -------          --------------  ------
L'opération s'est déroulée avec succès. DCPromo.General.3          False Success
```

6.3. Configuration DHCP Load Balancing

Le DHCP Load Balancing permet de répartir la charge d'attribution des adresses IP entre deux serveurs DHCP. En cas de défaillance de l'un des deux, l'autre prend automatiquement le relais sans interruption de service.
Sur le DC02 (Server Core), installer le rôle DHCP :

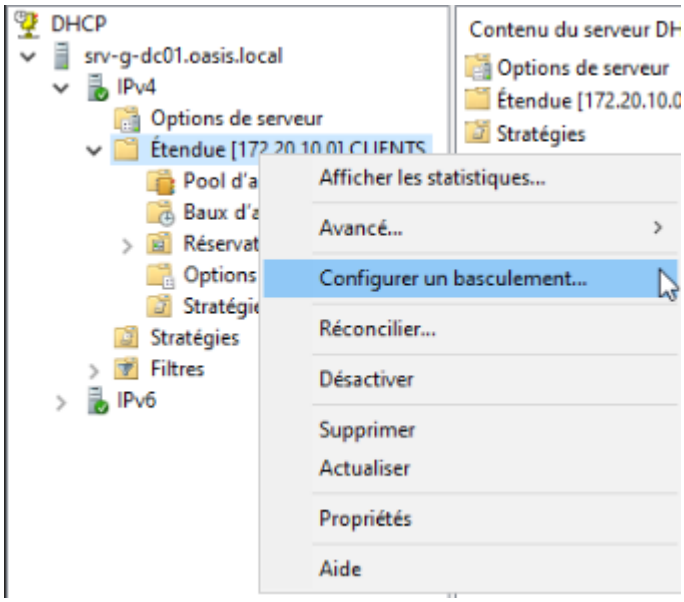
Install-WindowsFeature -Name DHCP -IncludeManagementTool

```
PS C:\Users\Administrateur.OASIS> Install-WindowsFeature -Name DHCP -IncludeManagementTool
```

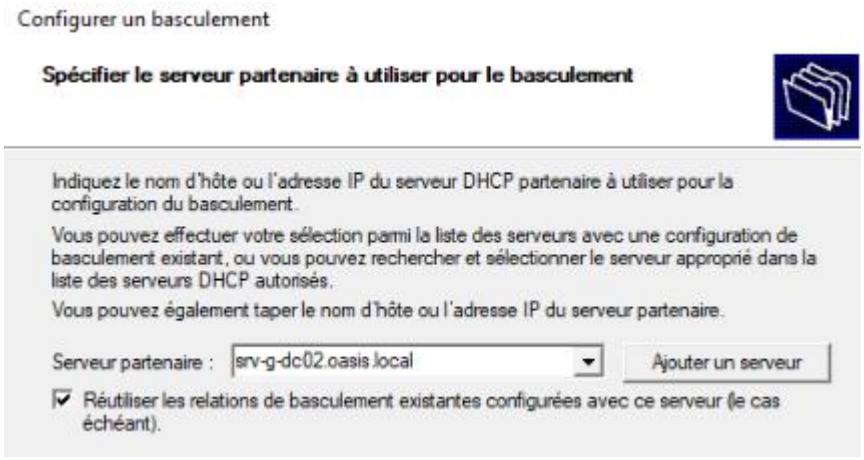
Le rôle DHCP est installé avec succès.

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Serveur DHCP}
```

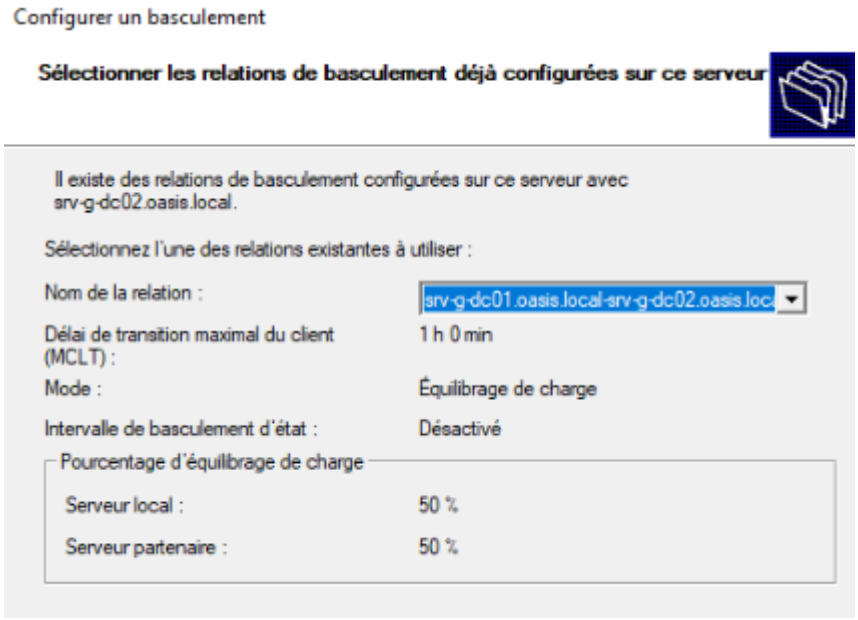
La configuration du basculement se fait depuis la console DHCP du DC01 (qui possède l'interface graphique). Sur l'étendue DHCP existante, effectuer un clic droit puis « Configurer un basculement »



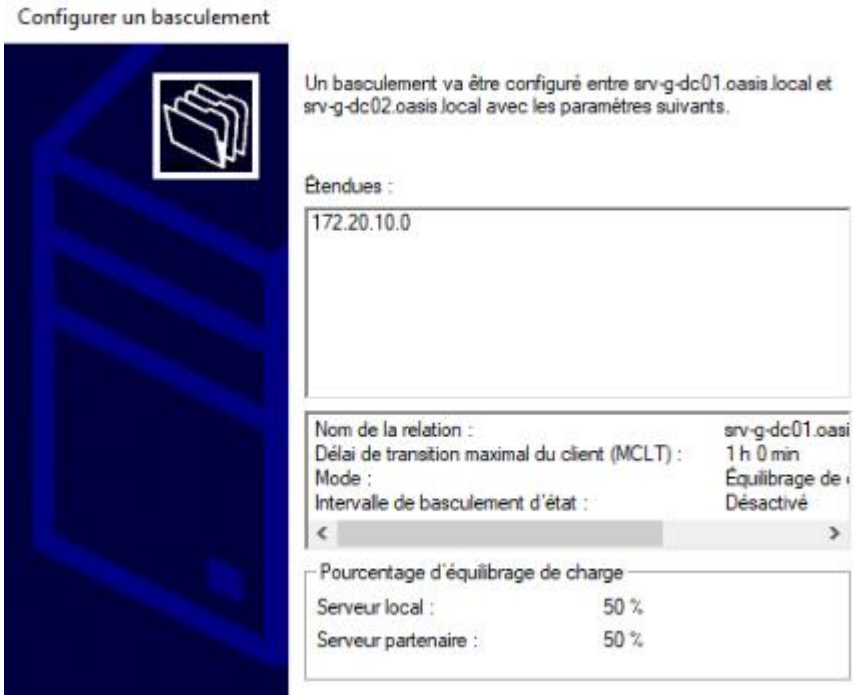
Spécifier le serveur partenaire : ici « srv-g-dc02.oasis.local », le DC02 du site Grenoble.



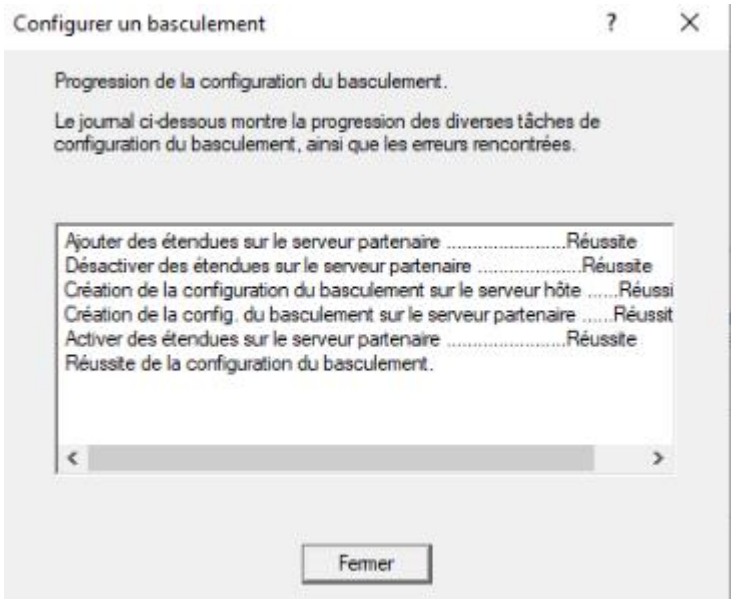
Configurer les paramètres de basculement :



Un récapitulatif affiche l'ensemble des paramètres de basculement avant validation.



La configuration du basculement se termine avec succès : les étendues sont répliquées sur le serveur partenaire et le mode d'équilibrage de charge est actif.



6.4. Conclusion

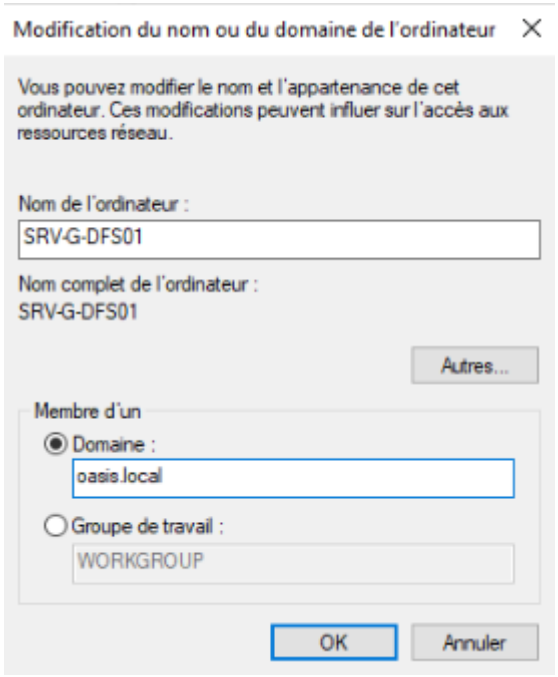
Le contrôleur de domaine secondaire DC02, installé en mode Server Core, a rejoint le domaine oasis.local avec succès. Conformément aux recommandations de l'ANSSI, les dossiers NTDS et SYSVOL ont été placés sur une partition dédiée F: distincte de la partition système.

La promotion en contrôleur de domaine s'est déroulée sans erreur. Le serveur réplique correctement et apparaît bien dans la console Sites et Services Active Directory rattaché à son site respectif.

Le DHCP Load Balancing entre DC01 et DC02 a été testé en simulant une indisponibilité du serveur principal. Les postes clients ont continué à obtenir des adresses IP sans interruption depuis le serveur partenaire, confirmant que la continuité de service est assurée en cas de défaillance d'un des deux serveurs DHCP.

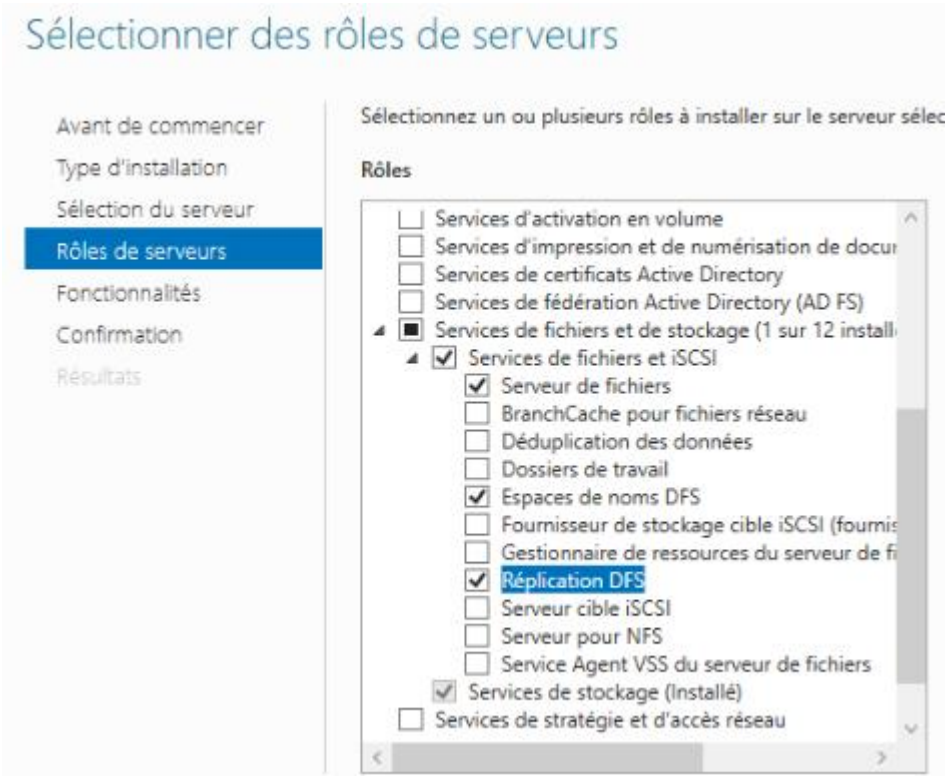
7. Serveur de fichiers (DFS & DFSR)

Le service de fichiers distribués (DFS) permet de regrouper des dossiers partagés situés sur des serveurs différents sous un chemin d'accès unique et unifié (espace de noms). Associé à la réplication DFS (DFSR), il assure la synchronisation automatique des fichiers entre les sites, offrant aux utilisateurs un accès transparent et redondant aux données.
Il est conseillé de dédier un serveur de fichiers distinct, sans rôle Active Directory, afin d'isoler les services et de limiter la surface d'attaque sur les contrôleurs de domaine.
Configurer les paramètres réseaux, le nom de machine, puis joindre le serveur au domaine « oasis.local ».

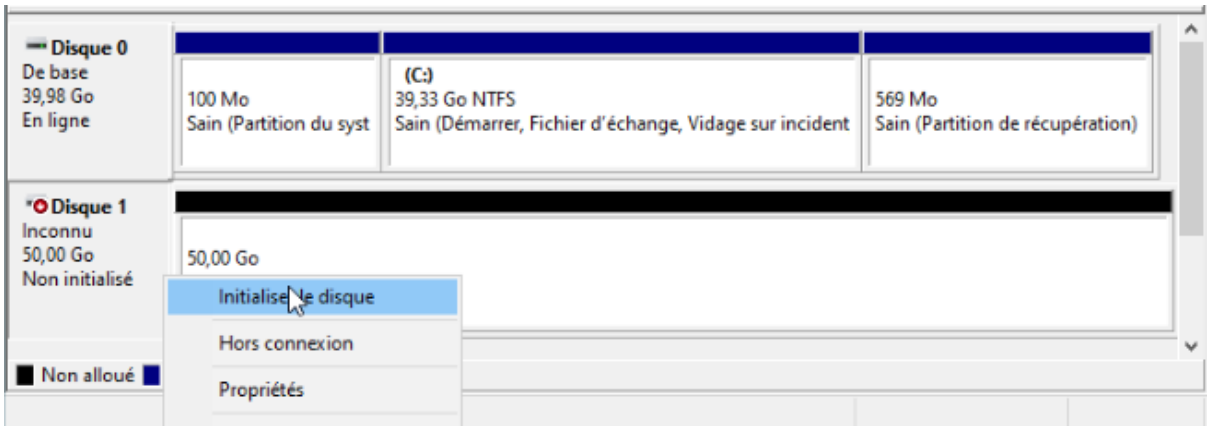


Dans le Gestionnaire de serveur, se rendre dans « Gérer » → « Ajouter des rôles et fonctionnalités ».

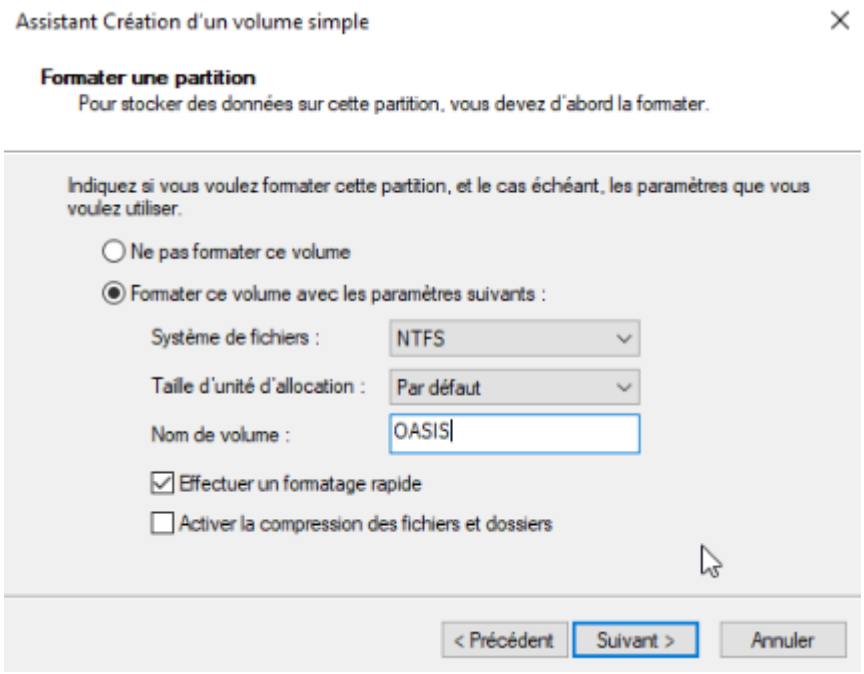
Sélectionner le serveur, puis dans les rôles de serveurs, choisir « Services de fichiers et de stockage » → « Services de fichiers et iSCSI », et cocher « Espaces de noms DFS » ainsi que « Réplication DFS ».



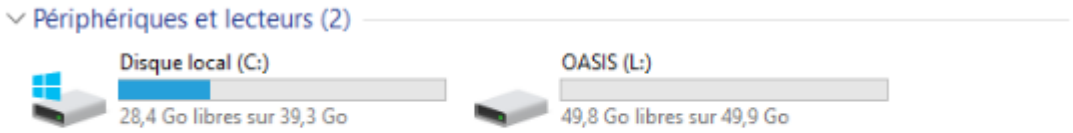
Il est préférable de stocker les partages de fichiers sur un disque distinct de celui contenant le système d'exploitation. Dans le Gestionnaire de disques, effectuer un clic droit sur le disque non initialisé → « Initialiser le disque ».



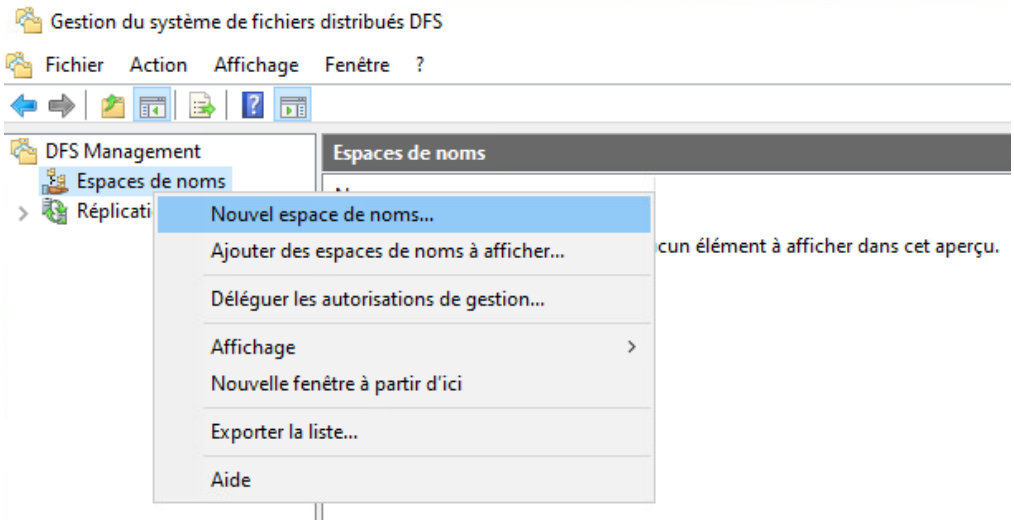
Formater le disque en volume NTFS avec le nom de volume « OASIS ».



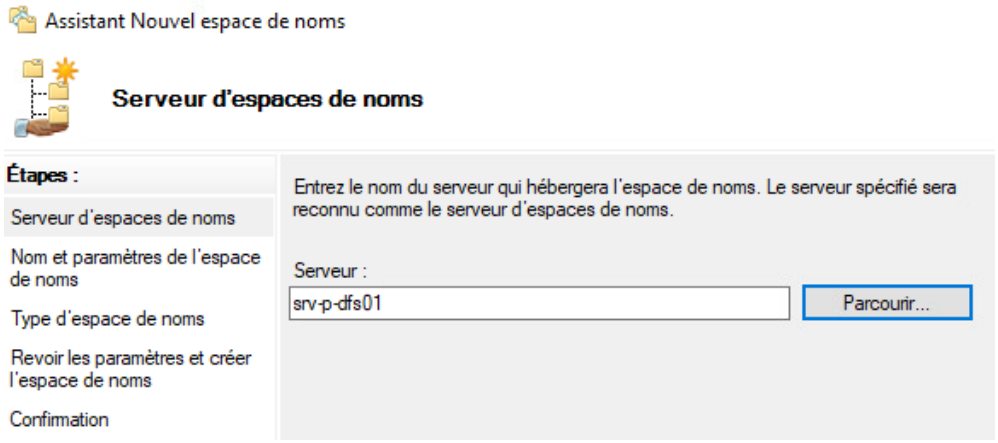
On retrouve bien les deux volumes : le disque système (C:) et le disque de données OASIS (L:).



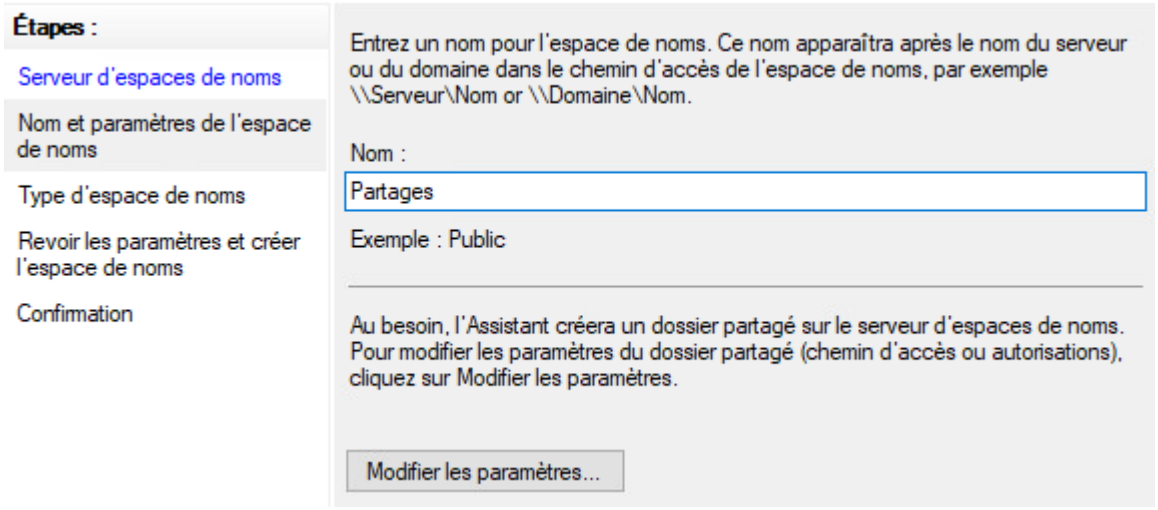
Lancer l'applicatif « Gestion du système de fichiers distribués DFS ». Effectuer un clic droit sur « Espaces de noms » → « Nouvel espace de noms »



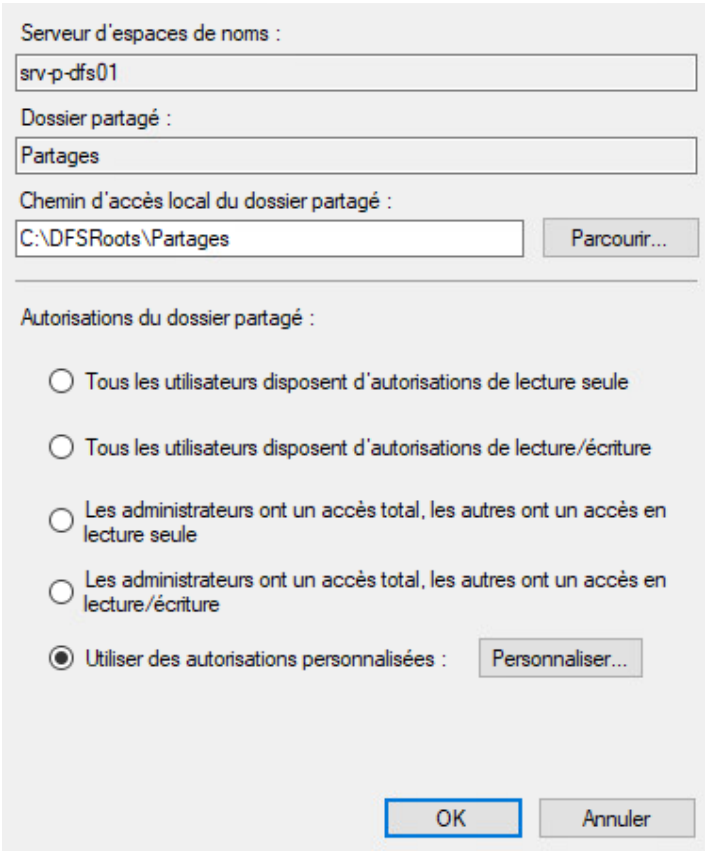
Sélectionner le serveur qui hébergera l'espace de noms. Ici « SRV-P-DFS01 » (serveur de fichiers du site de Paris).



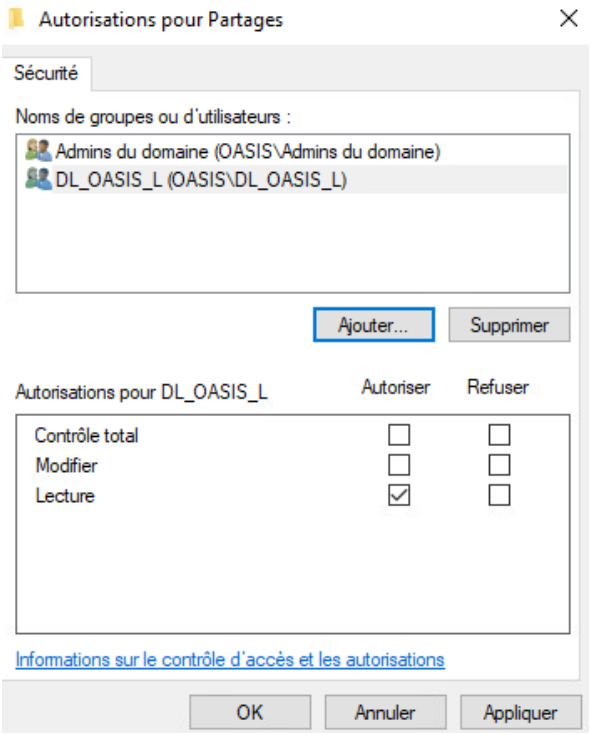
Nommer l'espace de noms « Partages ». L'assistant créera automatiquement un dossier partagé sur le serveur. Cliquer sur « Modifier les paramètres » pour personnaliser les autorisations.



Laisser le chemin d'accès local du dossier partagé par défaut, et afin de respecter la méthode AGDLP, sélectionner « Utiliser des autorisations personnalisées » puis « Personnaliser ».

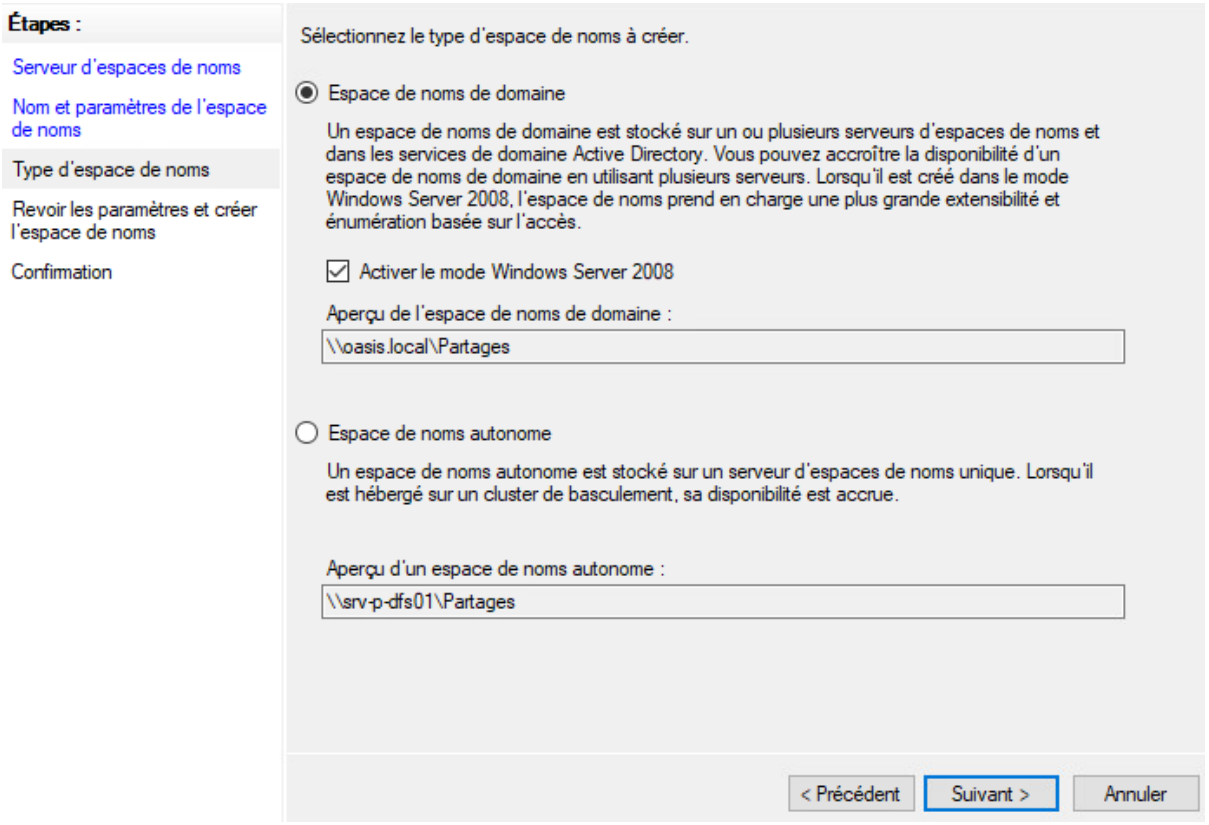


Attribuer au groupe Domaine Local « DL_OASIS_L » les droits de lecture sur ce dossier, et conserver le contrôle total pour les Admins du domaine.

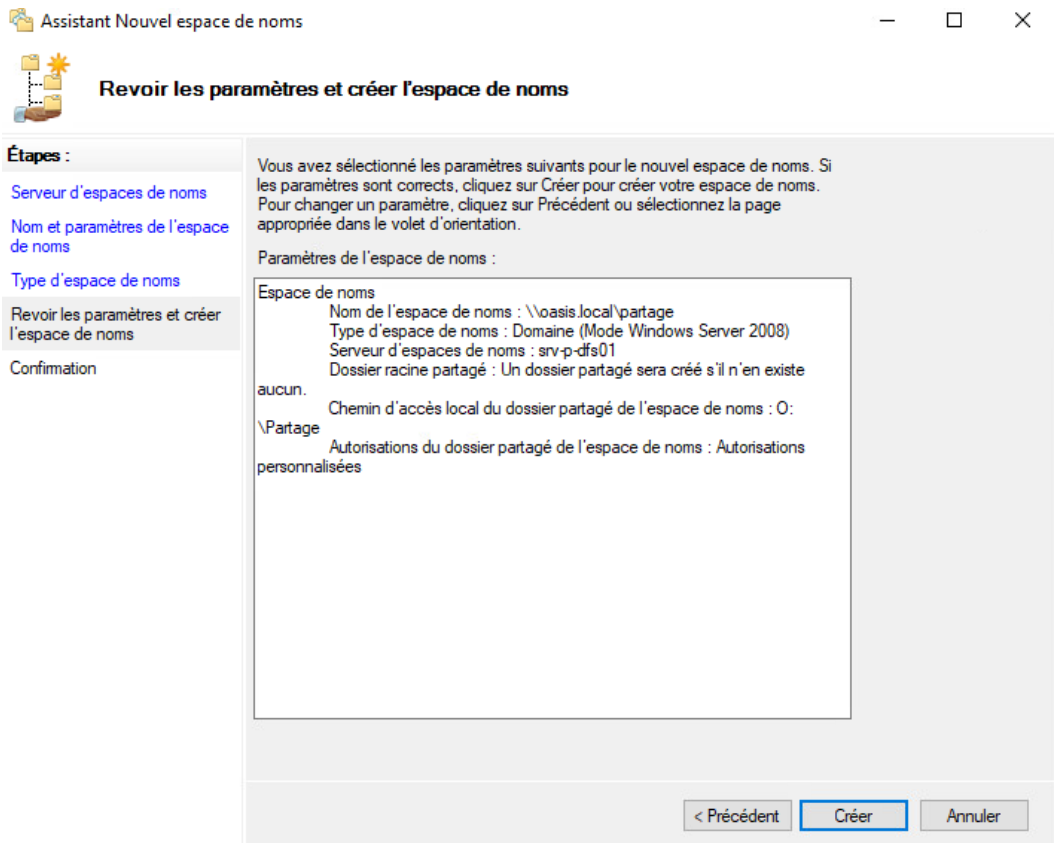


En type d'espace de noms, choisir « Espace de noms de domaine » et cocher « Activer le mode Windows Server 2008 ». Ce mode offre une meilleure extensibilité et une énumération basée sur l'accès.

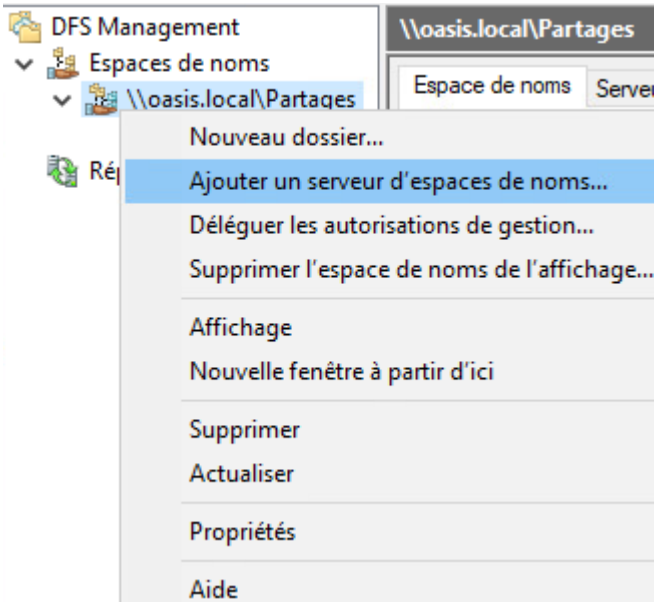
Le chemin d'accès sera alors « \\oasis.local\Partages ».



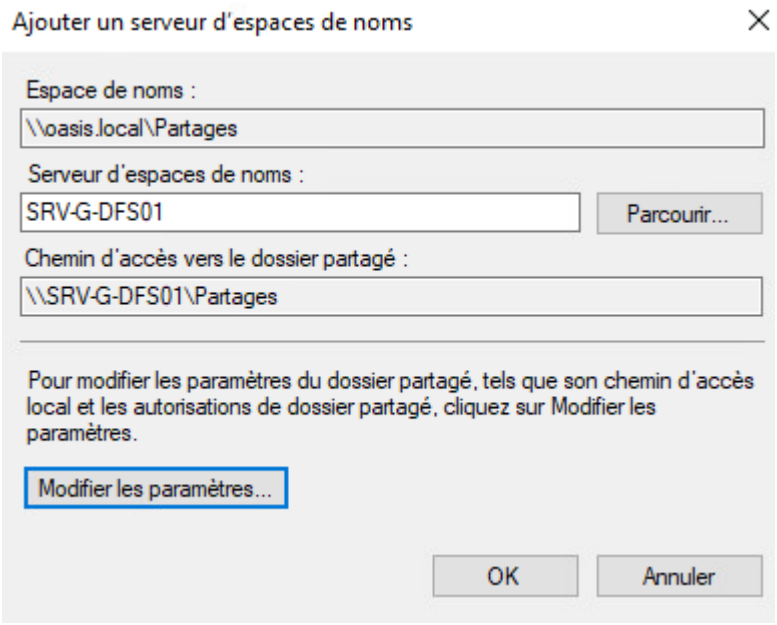
Un récapitulatif s'affiche avec l'ensemble des paramètres. Si tout est conforme, cliquer sur « Créer ».



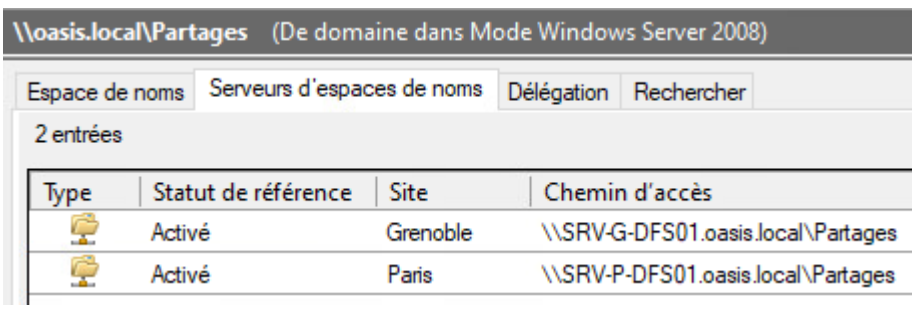
Pour assurer la disponibilité de l'espace de noms sur un autre site, effectuer un clic droit sur « \\oasis.local\Partages » puis « Ajouter un serveur d'espaces de noms ».



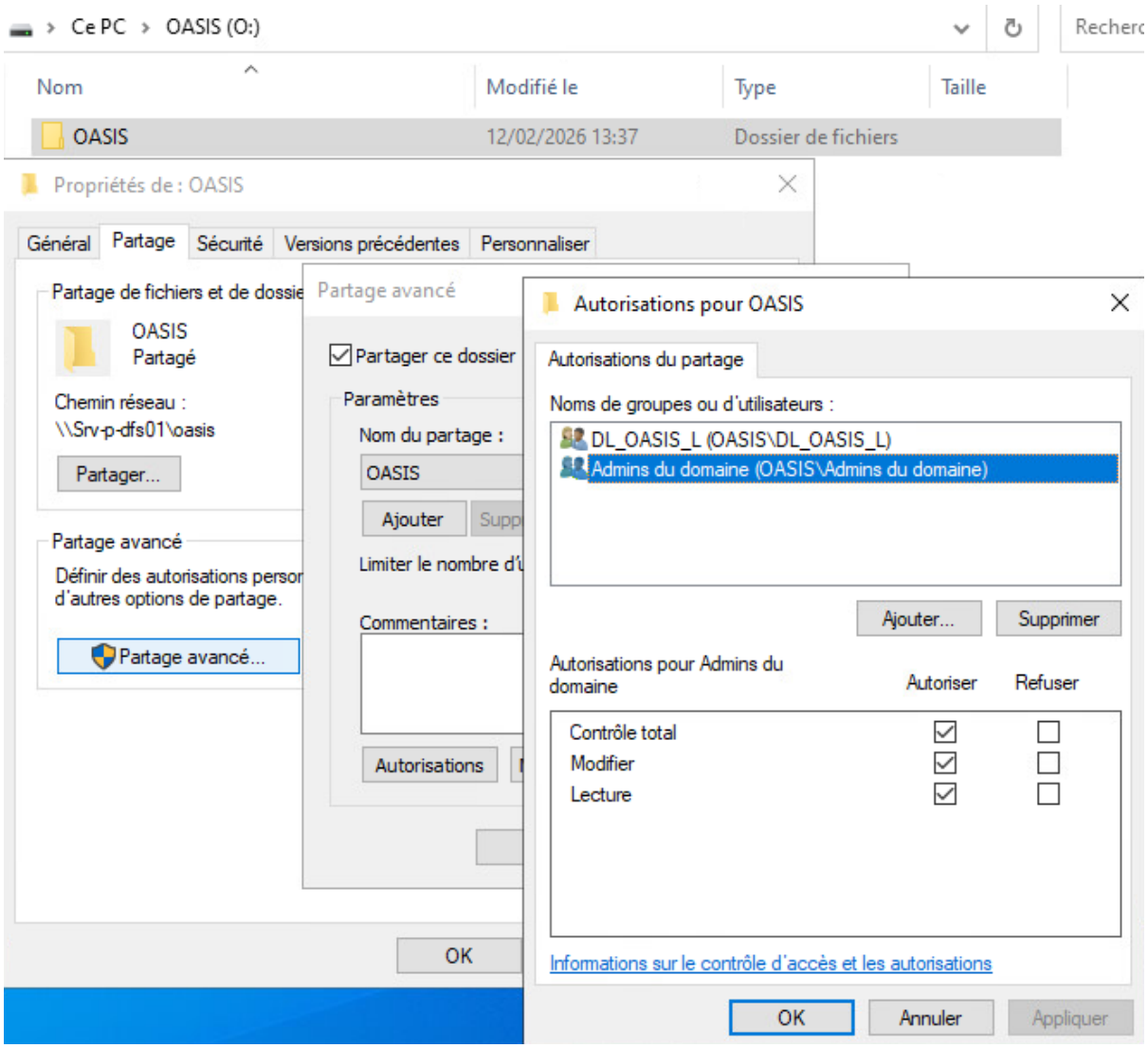
Renseigner le serveur de fichiers du site distant, ici « SRV-G-DFS01 » (Grenoble). L'espace de noms sera désormais accessible localement depuis ce site.



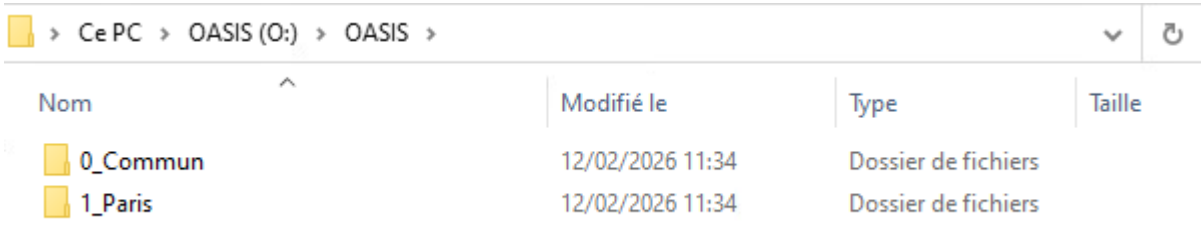
On retrouve bien les deux serveurs d'espaces de noms actifs : SRV-G-DFS01 (Grenoble) et SRV-P-DFS01 (Paris).



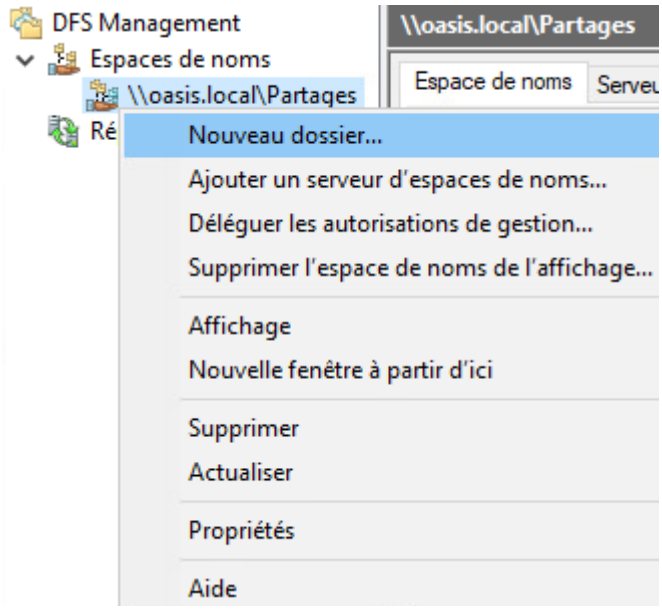
Sur le serveur SRV-P-DFS01, créer un dossier « OASIS » sur le disque O:(anciennement L:), puis configurer le partage avancé. Les autorisations de partage suivent la méthode AGDLP : « DL_OASIS_L » en lecture et « Admins du domaine » en contrôle total.



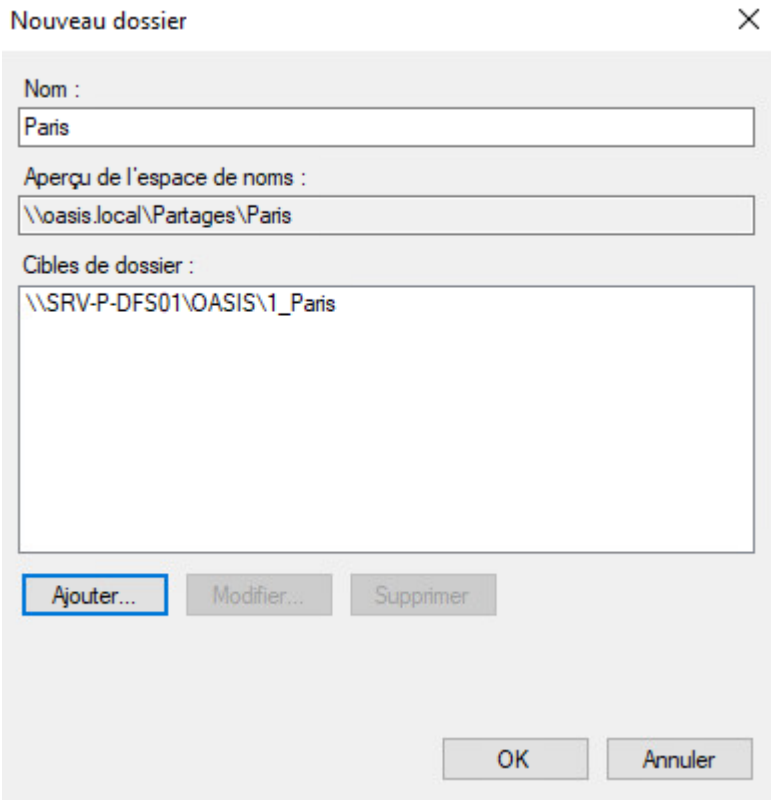
Créer l'arborescence de dossiers à l'intérieur du partage. Ici, deux dossiers sont créés : « 0_Commun » (dossier commun à tous les sites) et « 1_Paris » (dossier spécifique au site de Paris).



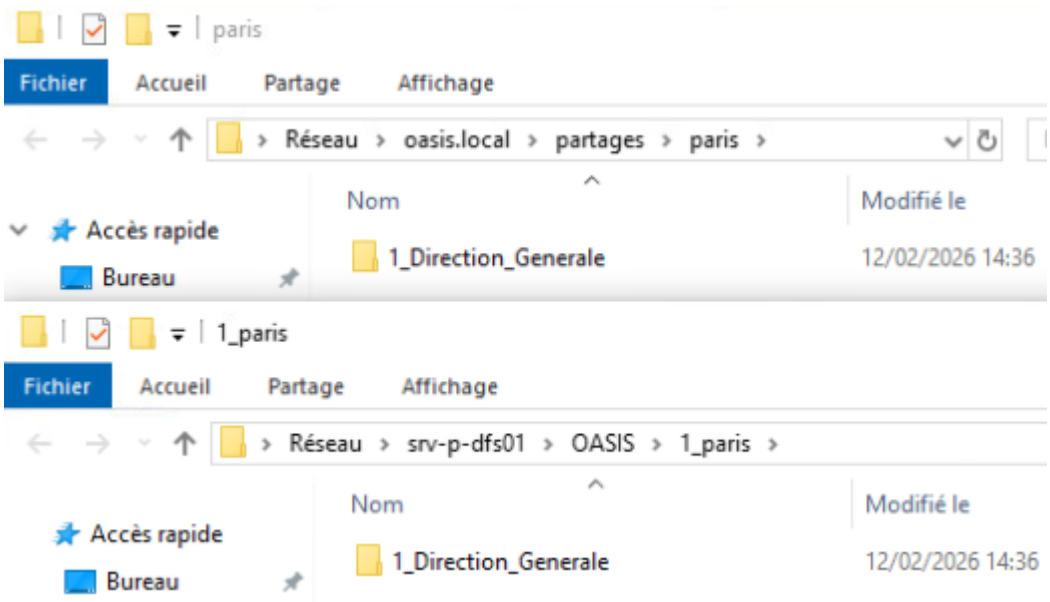
De retour dans la console DFS, effectuer un clic droit sur « \\oasis.local\Partages » → « Nouveau dossier »



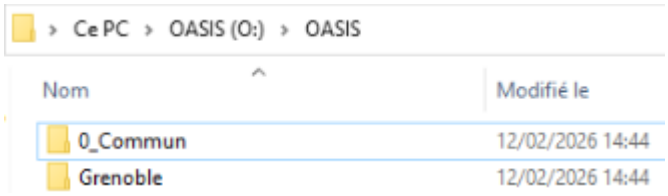
Créer un dossier « Paris » pointant vers la cible « \\SRV-P-DFS01\OASIS\1_Paris ».



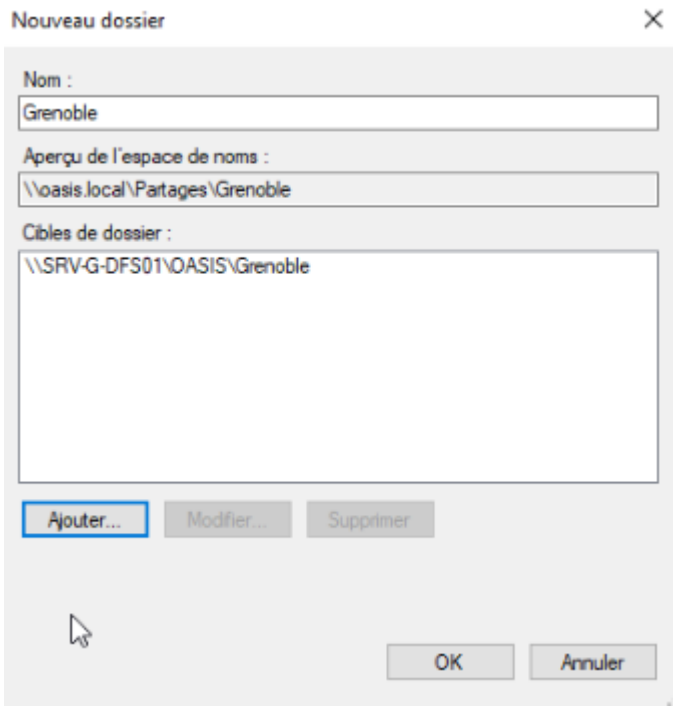
Vérifier l'accès via le chemin DFS : les utilisateurs peuvent désormais accéder au dossier via « \\oasis.local\partages\paris », qui redirige de manière transparente vers le dossier physique sur SRV-P-DFS01.



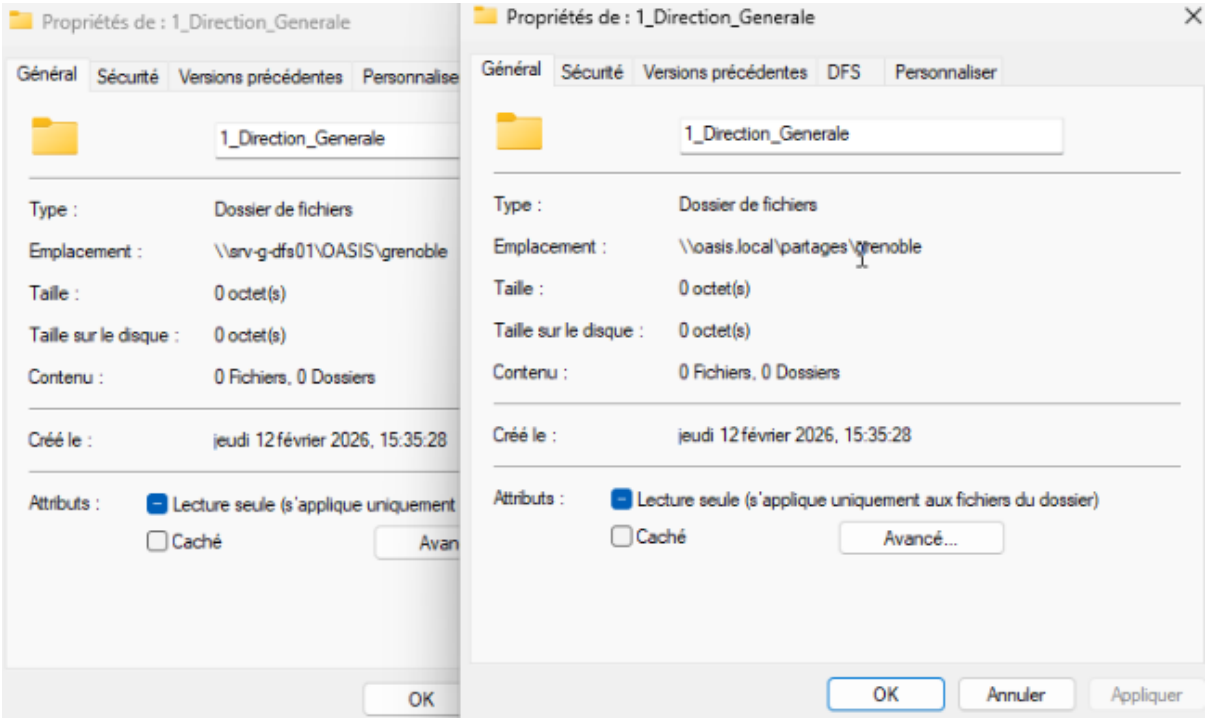
Reproduire la même arborescence sur le serveur de fichiers du site de Grenoble (SRV-G-DFS01) : créer les dossiers « 0_Commun » et « Grenoble » sur le disque de données.



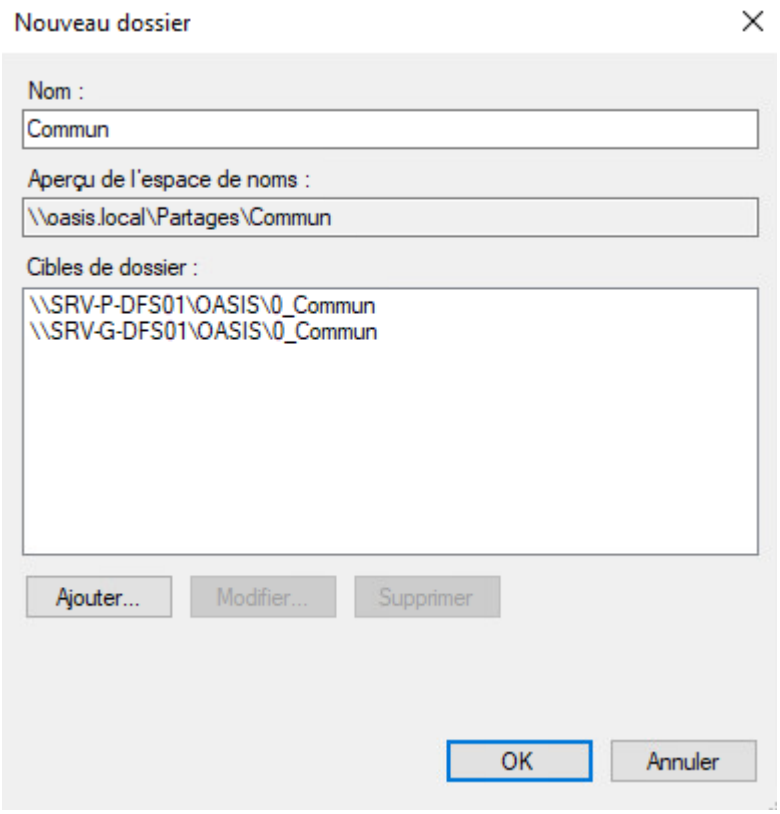
Créer le dossier DFS « Grenoble » pointant vers « \\SRV-G-DFS01\OASIS\Grenoble ».



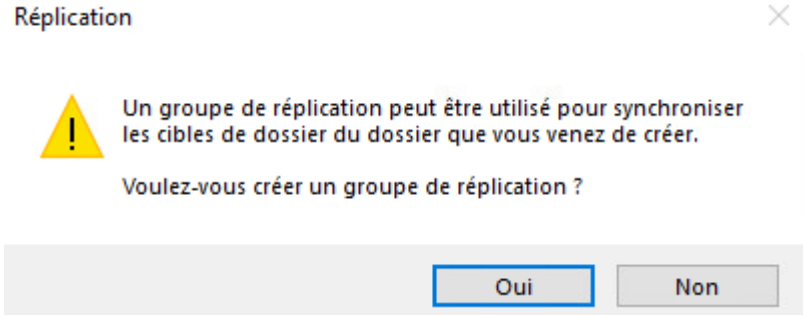
On peut vérifier que les propriétés du dossier sont identiques, que l'on y accède via le chemin local (\\srv-g-dfs01\OASIS\grenoble) ou via l'espace de noms DFS (\\oasis.local\partages\grenoble).



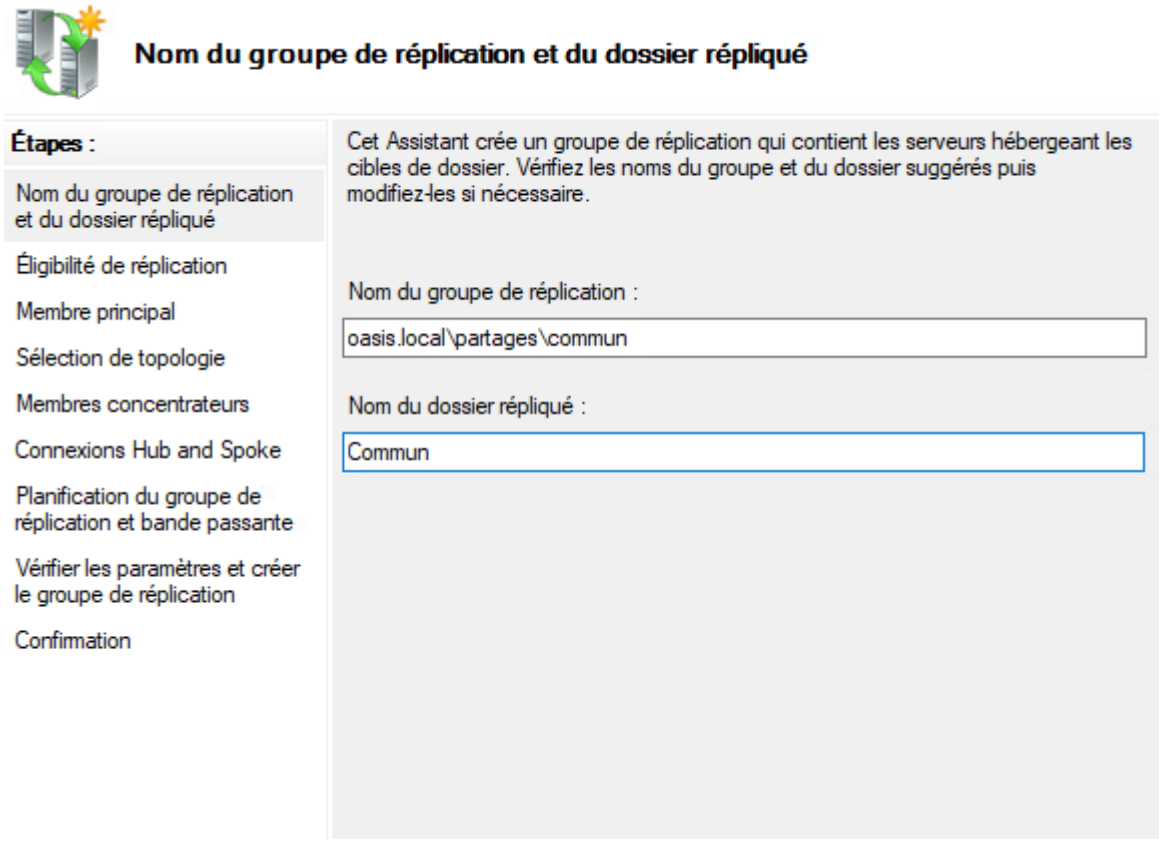
Le dossier « Commun » a la particularité de posséder deux cibles de dossier : une sur SRV-P-DFS01 (Paris) et une sur SRV-G-DFS01 (Grenoble). Cela permet aux utilisateurs des deux sites d'accéder au même contenu via un serveur local.



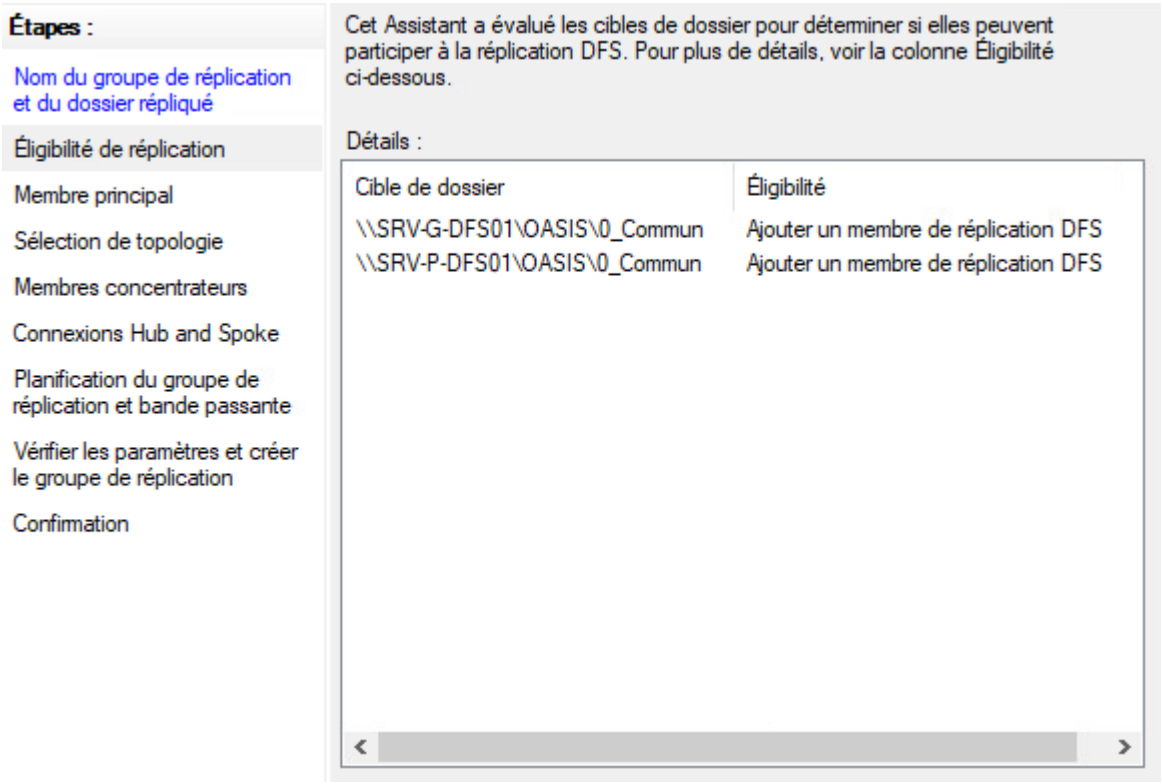
Lorsqu'un dossier DFS possède plusieurs cibles, l'assistant propose de créer un groupe de réplication pour synchroniser automatiquement le contenu. Cliquer sur « Oui ».



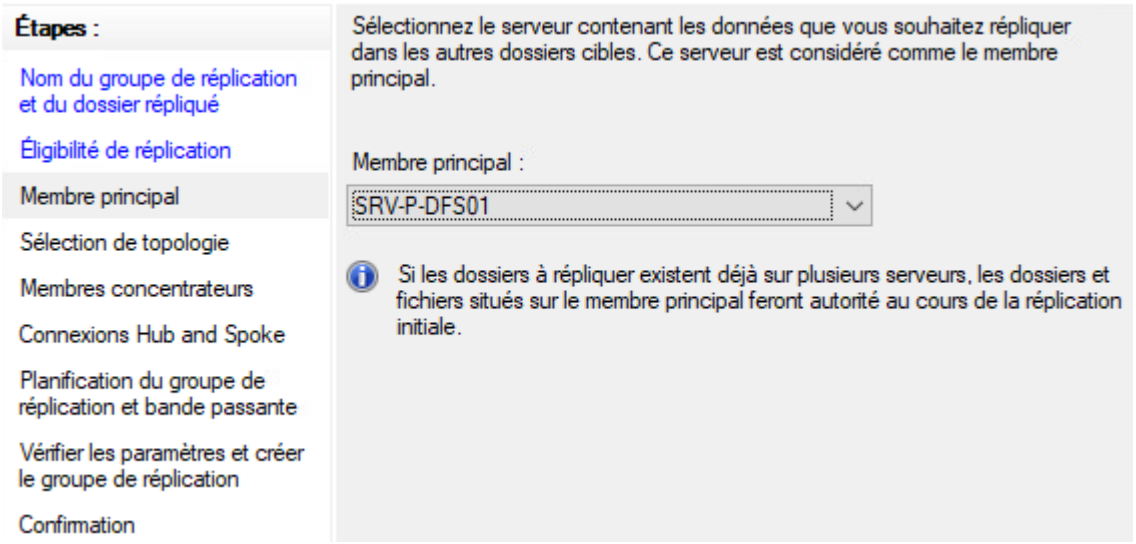
L'assistant de réplication s'ouvre. Le nom du groupe de réplication est automatiquement défini : « oasis.local\partages\commun », et le dossier répliqué est nommé « Commun ».



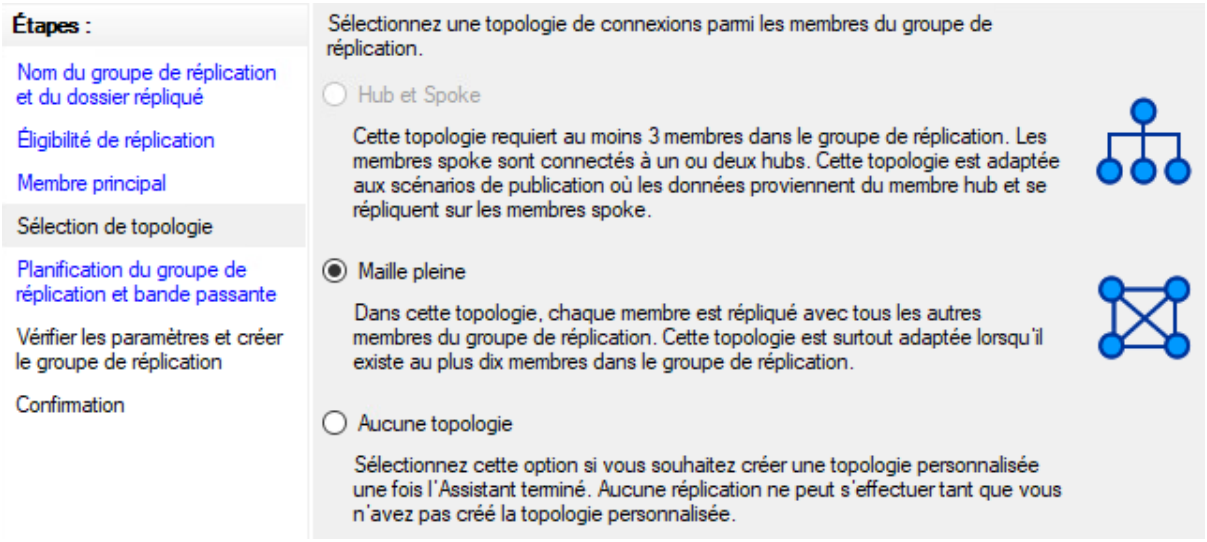
L'assistant vérifie l'éligibilité des cibles de dossier. Les deux serveurs (SRV-G-DFS01 et SRV-P-DFS01) sont éligibles à la réplication.



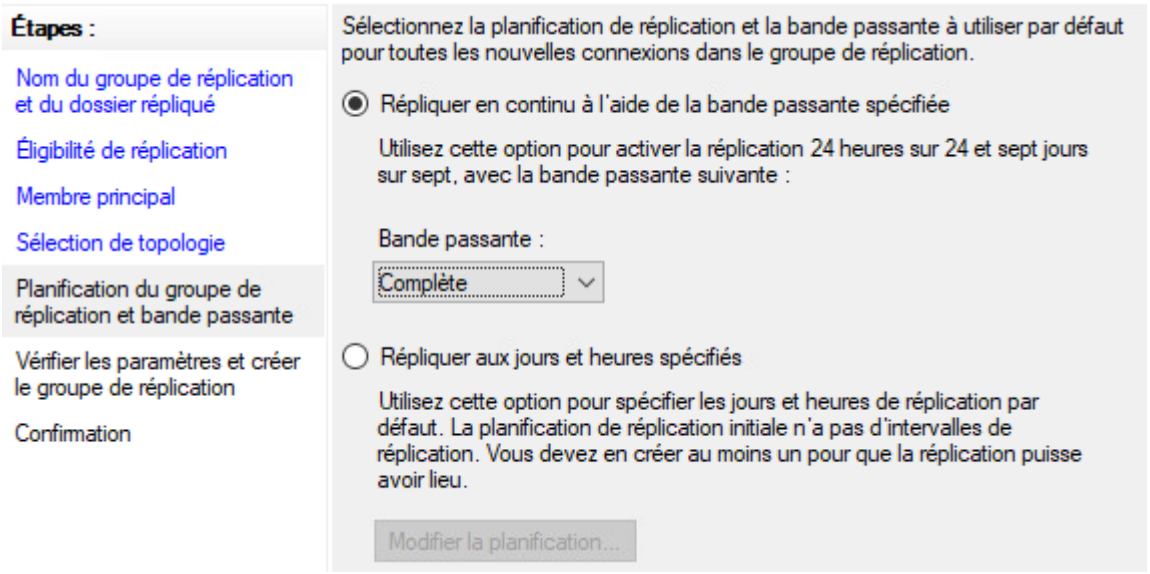
Sélectionner le membre principal : « SRV-P-DFS01 ». En cas de conflit de données entre les serveurs, les fichiers du membre principal feront autorité lors de la réplication initiale.



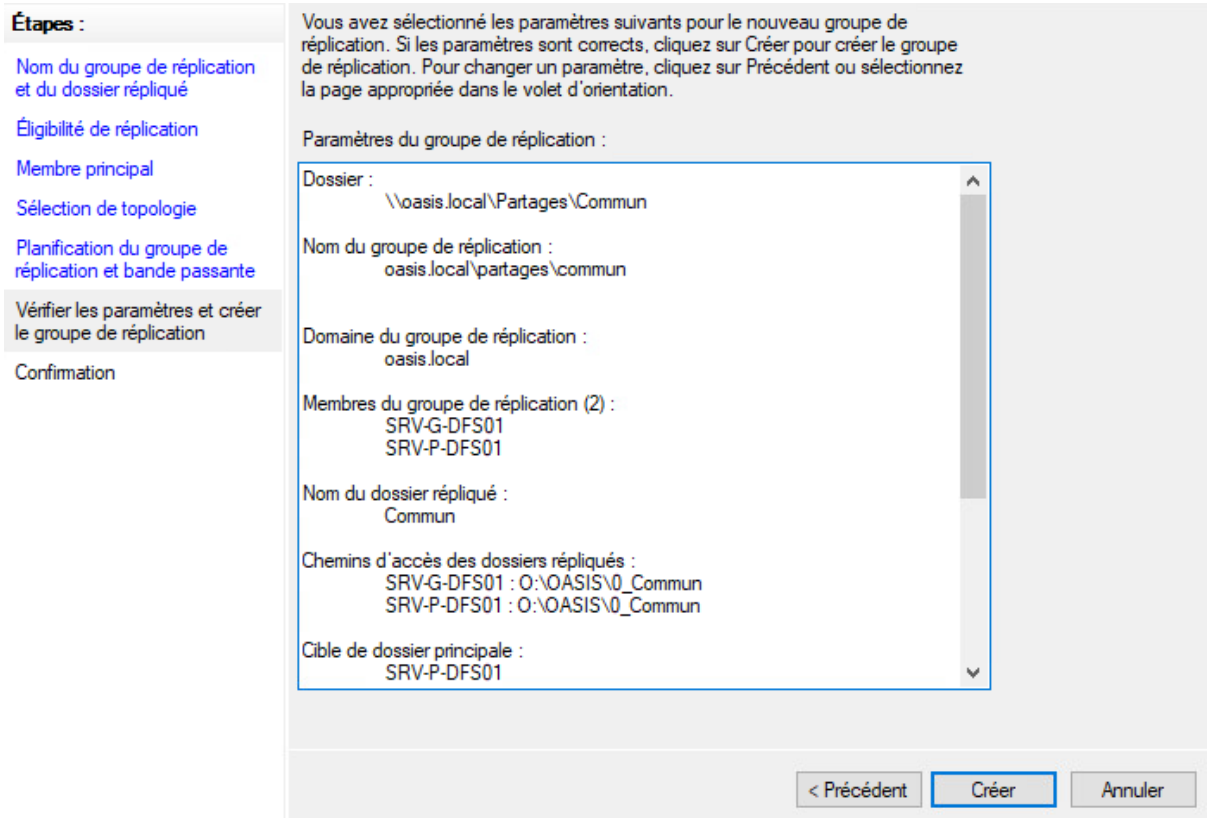
Pour la topologie de réplication, choisir « Maille pleine ». Dans cette topologie, chaque membre réplique directement avec tous les autres, ce qui est adapté lorsque le groupe comprend peu de membres.



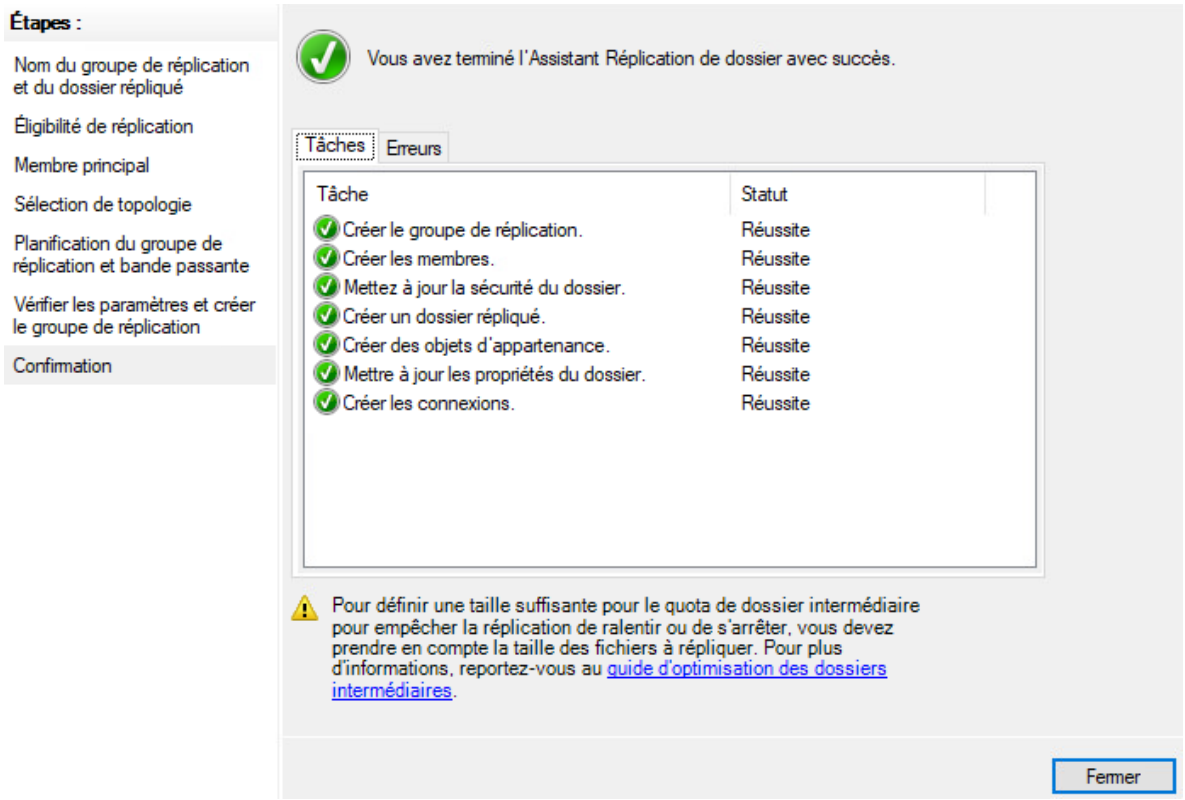
Configurer la planification de la réplication : sélectionner « Répliquer en continu… » avec la bande passante « Complète ». Les modifications seront ainsi synchronisées en temps réel sans limitation de débit.



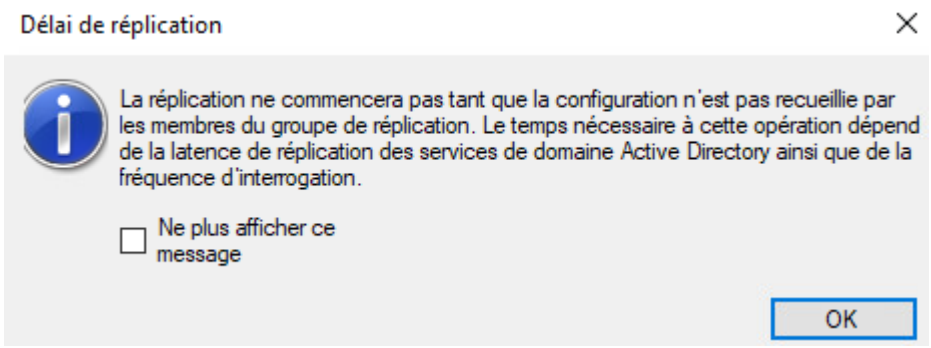
Un récapitulatif affiche l'ensemble des paramètres : dossier « \\oasis.local\Partages\Commun », membres SRV-G-DFS01 et SRV-P-DFS01, chemins d'accès « O:\OASIS\0_Commun » sur chaque serveur, et cible principale SRV-P-DFS01.



La création du groupe de réplication se termine avec succès (toutes les tâches au statut « Réussite »).

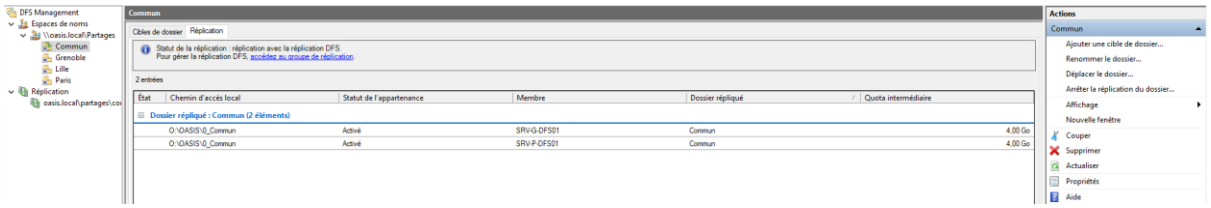


Un message informe que la réplication ne commencera pas immédiatement : il faut attendre que la configuration soit propagée à tous les membres via la réplication Active Directory.

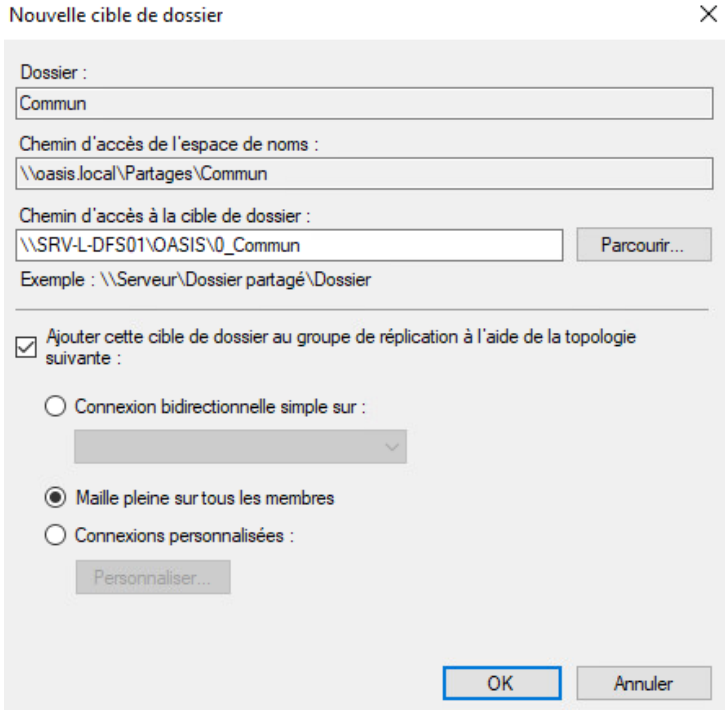


Dans la console DFS, le dossier répliqué « Commun » apparaît bien dans la section « Réplication », lié à l'espace de noms « \\oasis.local\Partages\Commun ».

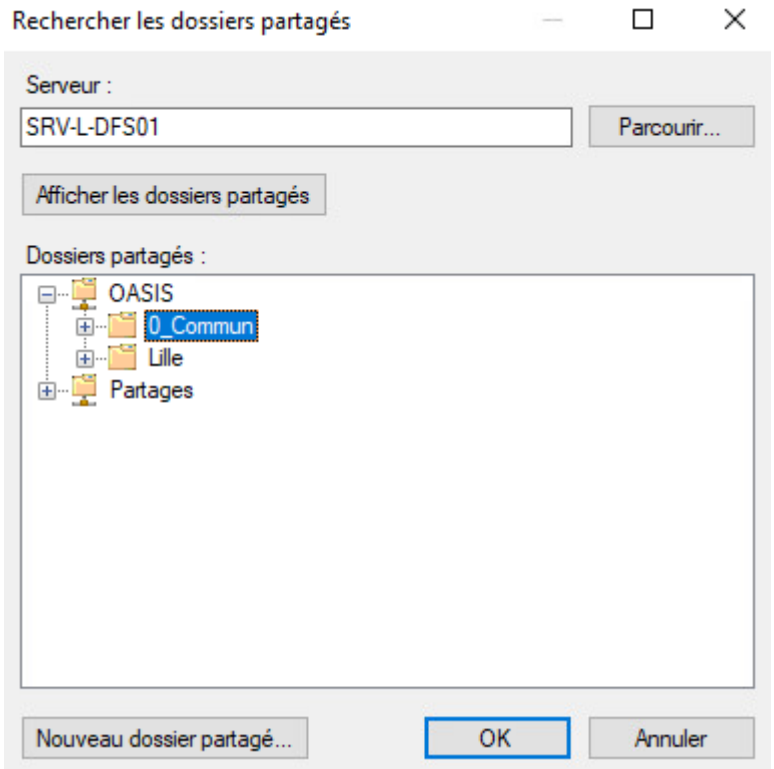
On peut vérifier dans l'onglet « \\oasis.local\Partages » → « Commun » → « Réplication » que les deux serveurs sont bien actifs et que le dossier est répliqué entre eux.



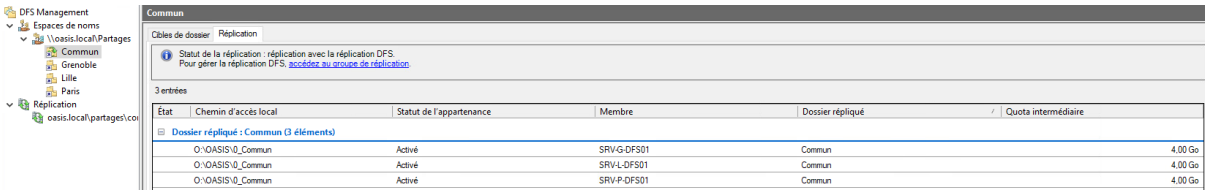
Pour étendre la réplication sur un autre site tel que Lille, cliquer sur « ajouter une nouvelle cible de dossier » sur le dossier « Commun » pointant vers « \\SRV-L-DFS01\OASIS\0_Commun », en sélectionnant la topologie « Maille pleine sur tous les membres ».
(Il faut d'abord créer le dossier partagé en local sur le serveur du site Lille)



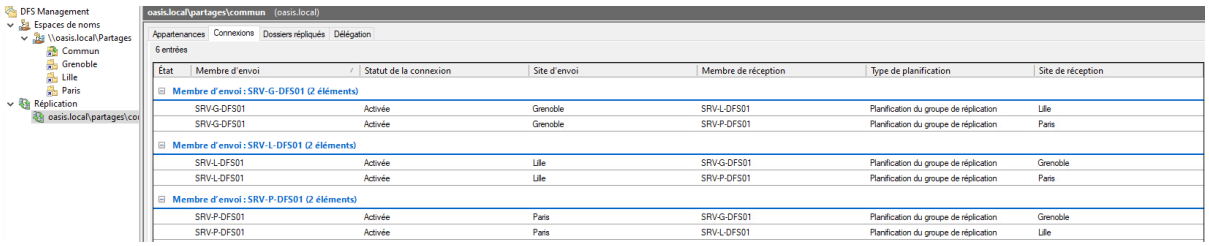
Parcourir les dossiers partagés sur SRV-L-DFS01 et sélectionner « 0_Commun ».



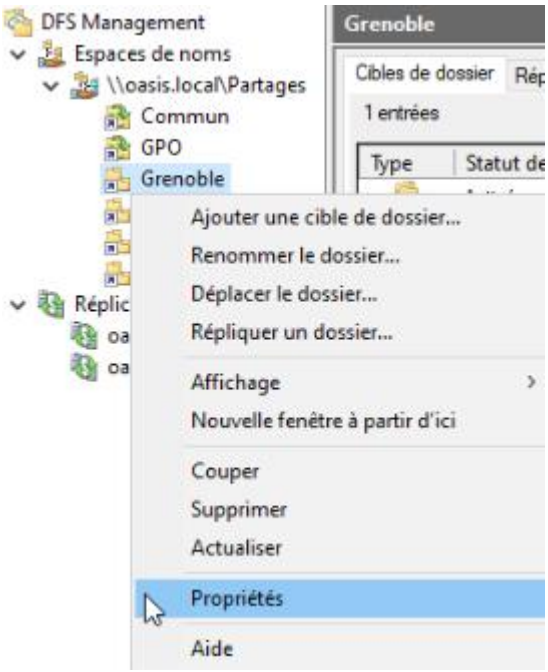
Le dossier « Commun » dispose désormais de trois cibles actives : SRV-G-DFS01 (Grenoble), SRV-L-DFS01 (Lille) et SRV-P-DFS01 (Paris).



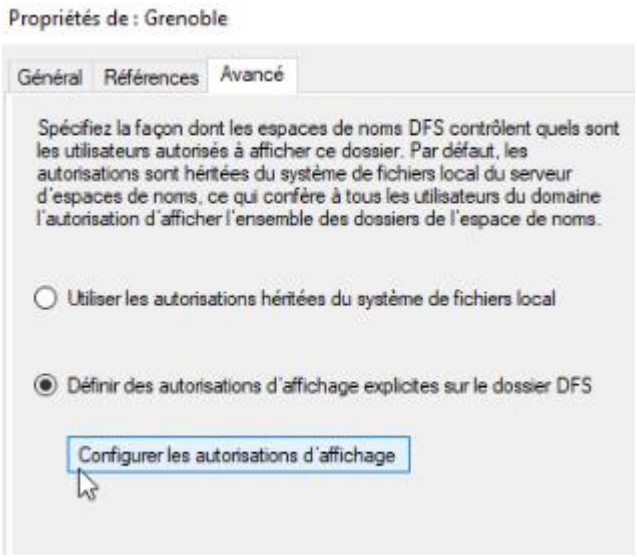
Dans l'onglet « Connexions » du groupe de réplication, on retrouve les six connexions en maille pleine : chaque serveur réplique vers les deux autres de manière bidirectionnelle.



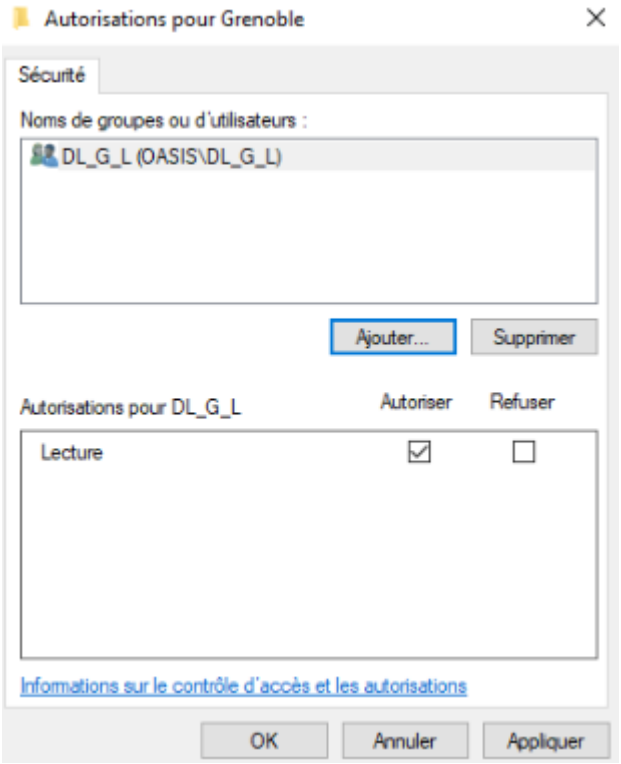
Afin de restreindre la visibilité des dossiers selon les sites, il est possible de configurer des autorisations d'affichage explicites sur chaque dossier DFS. Clic droit sur le dossier → « Propriétés »



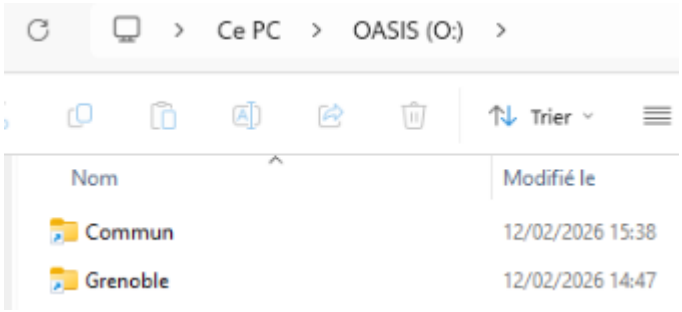
Aller dans l'onglet « Avancé », puis sélectionner « Définir des autorisations d'affichage explicites sur le dossier DFS », cliquer sur « Configurer les autorisations d'affichage ».



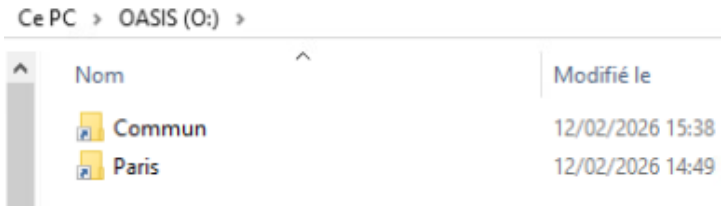
Attribuer les droits de lecture au groupe Domaine Local correspondant au site. Par exemple, pour le dossier « Grenoble », seul le groupe « DL_G_L » aura un droit de lecture, ce qui empêchera les utilisateurs des autres sites de voir ce dossier dans l'espace de noms.



Sur le serveur de Grenoble (SRV-G-DFS01), on retrouve les dossiers « Commun » et « Grenoble » sur le disque OASIS.



Sur le serveur de Paris (SRV-P-DFS01), on retrouve les dossiers « Commun » et « Paris ».



Chaque site dispose ainsi de son dossier local (visible uniquement par les utilisateurs du site) et d'un dossier commun répliqué sur l'ensemble des sites. Les utilisateurs accèdent à l'ensemble des données via le chemin unique « \\oasis.local\Partages », sans avoir besoin de connaître le serveur physique qui héberge les fichiers.

7.1. Conclusion

L'espace de noms DFS \\oasis.local\Partages est accessible depuis les postes clients des quatre sites. Les deux serveurs d'espaces de noms SRV-P-DFS01 et SRV-G-DFS01 sont actifs et assurent la disponibilité locale de l'espace de noms sur leurs sites respectifs.

Les dossiers Paris et Grenoble sont correctement visibles depuis le chemin DFS unifié et redirigent de manière transparente vers le serveur physique du site correspondant. Les autorisations d'affichage explicites configurées sur chaque dossier garantissent que les utilisateurs d'un site ne voient pas les dossiers des autres sites dans l'espace de noms.

La réplication DFSR du dossier Commun a été validée entre tous les sites : une modification effectuée sur SRV-P-DFS01 est bien répliquée sur SRV-G-DFS01 dans les délais attendus. Les connexions en maille pleine sont visibles dans la console DFS et toutes les cibles du dossier Commun sont actives.

Les autorisations AGDLP sont fonctionnelles : un compte utilisateur membre de DL_OASIS_L accède bien au partage en lecture.

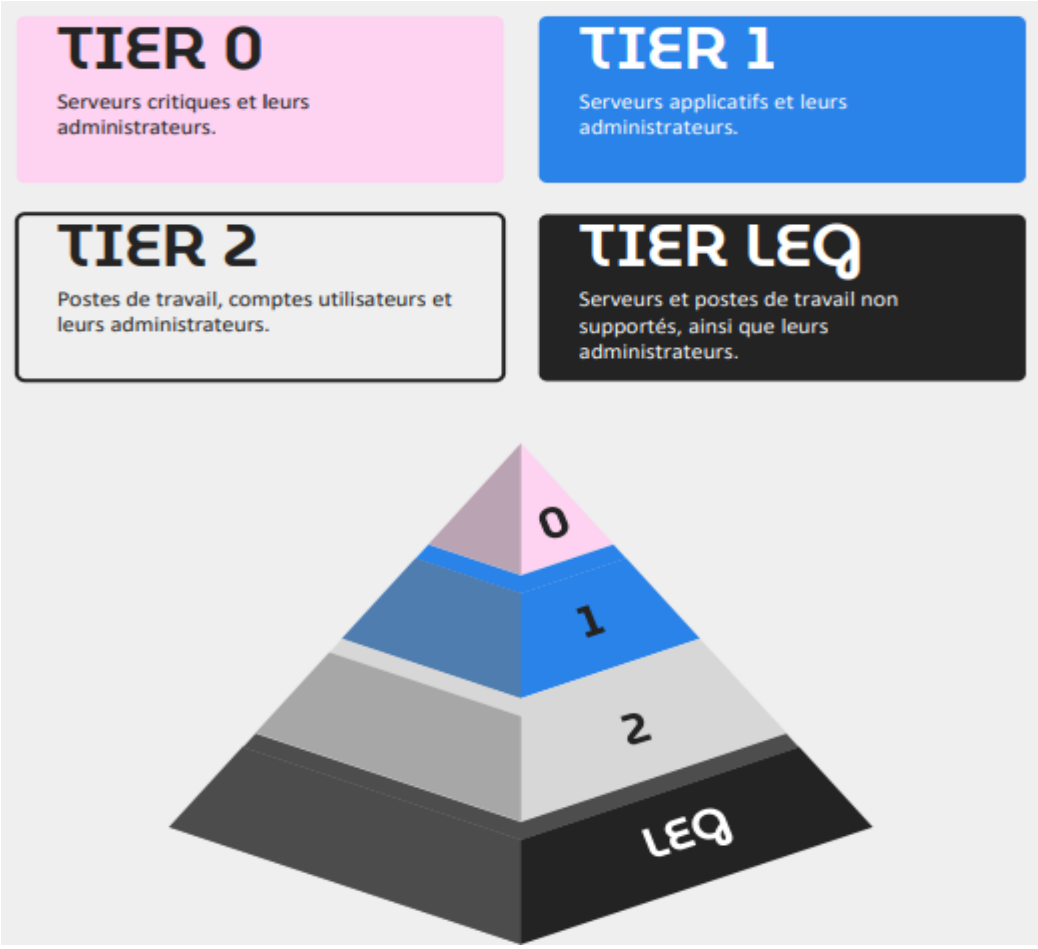
8. Modèle de Tiering

Le modèle de tiering est un modèle de sécurité Active Directory recommandé par Microsoft et l'ANSSI. Il segmente les comptes et ressources en niveaux (Tiers) afin de contenir les escalades de privilèges et les mouvements latéraux en cas de compromission d'un compte.

Le principe fondamental est simple : un compte d'administration ne peut se connecter qu'aux systèmes de son propre tier. Un administrateur du Tier 0 ne peut pas se connecter sur un poste du Tier 2, et inversement. Cela empêche qu'un attaquant ayant compromis un poste utilisateur puisse récupérer des identifiants d'un administrateur ayant accès aux contrôleurs de domaine.

L'infrastructure est découpée en quatre niveaux :

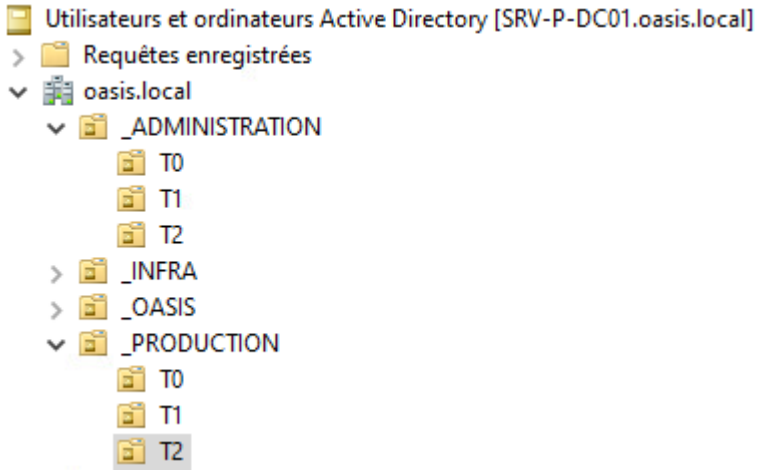
- **Tier 0 :** serveurs critiques (contrôleurs de domaine) et leurs administrateurs. C'est le niveau le plus sensible.
- **Tier 1 :** serveurs applicatifs (fichiers, supervision, déploiement, etc.) et leurs administrateurs.
- **Tier 2 :** postes de travail, comptes utilisateurs et administrateurs locaux.
- **Tier Legacy :** serveurs et postes de travail qui ne sont plus supportés (anciennes versions de Windows, systèmes obsolètes).



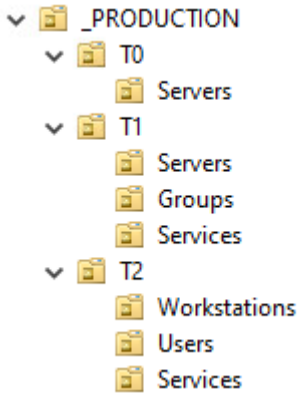
La mise en place du tiering repose sur une organisation rigoureuse des unités d'organisation (OU). Deux OU principales sont créées à la racine du domaine :

- **_ADMINISTRATION :** contient la partie administration (comptes admins, groupes d'administration, délégations) organisée par tier (T0, T1, T1L, T2, T2L).
- **_PRODUCTION :** contient les objets de production (serveurs, postes de travail, utilisateurs, groupes) organisés par tier.

Dans notre cas nous n'aurons pas à nous occuper des Tiers Legacy.

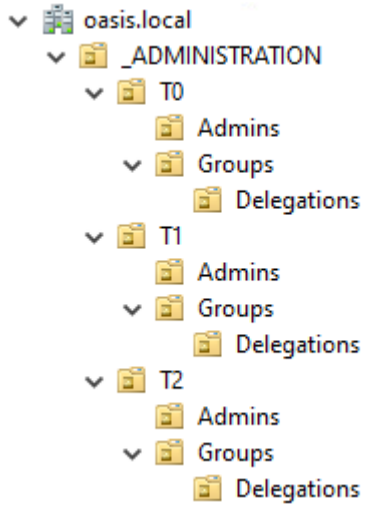


À l'intérieur de chaque tier de production, on crée des sous-OU par type d'objet. Pour les tiers serveurs (T0, T1,), on retrouve : Servers, Groups et Services. Pour les tiers utilisateurs (T2), on retrouve : Workstations, Users et Groups.
Cette séparation permet d'appliquer des délégations de contrôle granulaires sur chaque type d'objet.



Chaque tier dans _ADMINISTRATION possède les sous-OU suivantes :

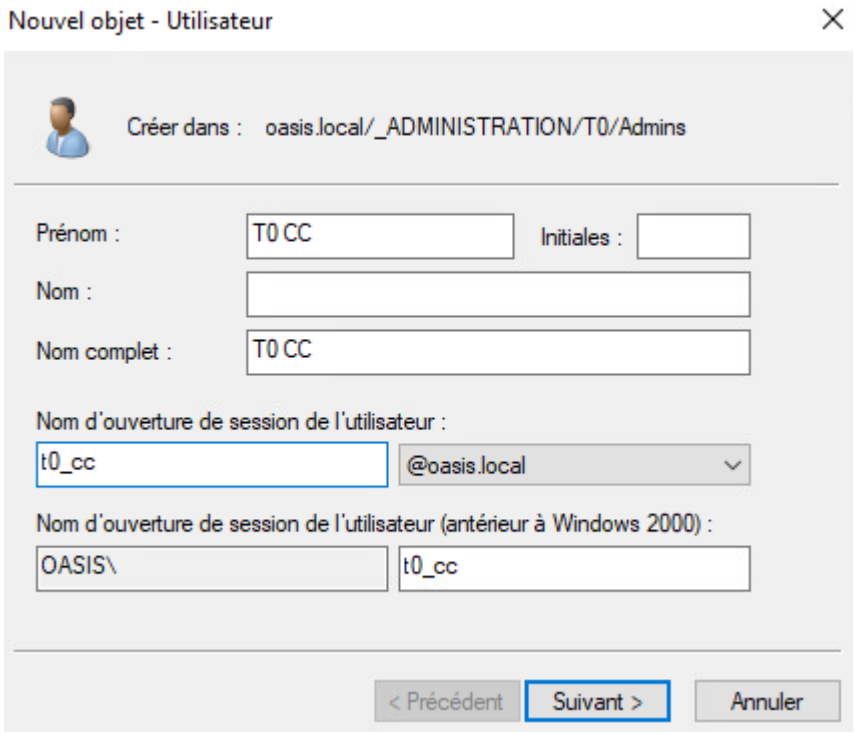
- **Admins :** contient les comptes d'administration du tier.
- **Groups :** contient les groupes de rôles et une sous-OU « Delegations » pour les groupes de délégation de contrôle.
- **Devices :** contient les postes d'administration du tier.

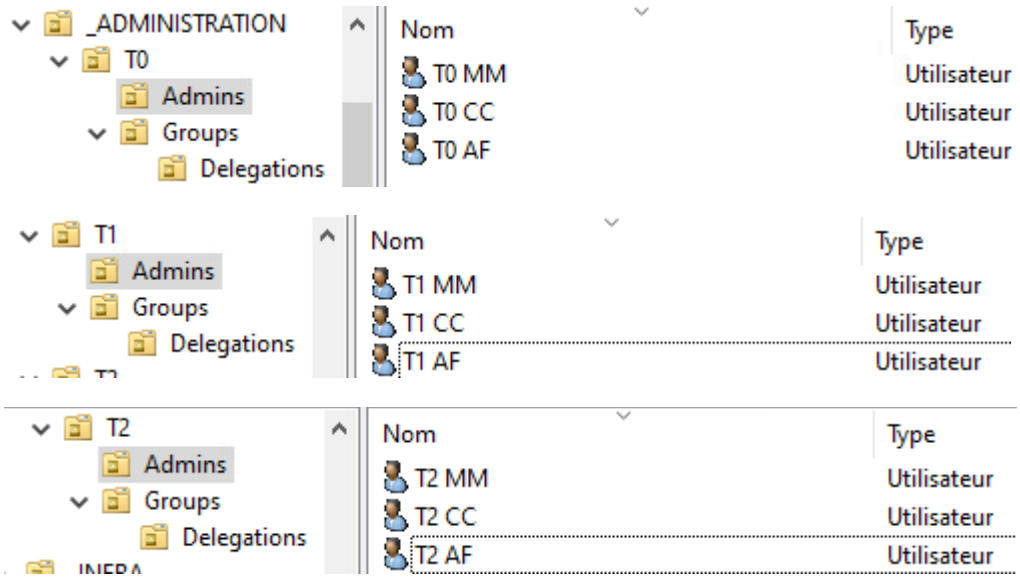


Un compte d'administration dédié est créé par personne et par tier (cela dépend des missions de l'administrateur). Par exemple, pour un administrateur « AF » :

- **t0_af** dans _ADMINISTRATION/T0/Admins (accès aux DC uniquement)
- **t1_af** dans _ADMINISTRATION/T1/Admins (accès aux serveurs applicatifs)
- **t2_af** dans _ADMINISTRATION/T2/Admins (accès aux postes de travail)

Ces comptes sont distincts du compte utilisateur standard de la personne. Cela garantit une séparation claire entre les activités d'administration et les activités quotidiennes.





Trois rôles sont définis pour structurer les droits d'administration au sein de chaque tier :

Managers

- Ce rôle est le plus privilégié. Il permet de gérer tout le Tier associé: la partie **Production** et la partie **Administration**.
- Il permet de créer, modifier et supprimer des objets ordinateurs, des groupes, des comptes de services, des utilisateurs (y compris d'administration).

Administrators

- Ce rôle permet de gérer uniquement la partie Production associé au Tier.
- Il permet de créer, modifier et supprimer des objets ordinateurs, des groupes, des comptes de services, des utilisateurs ,etc.

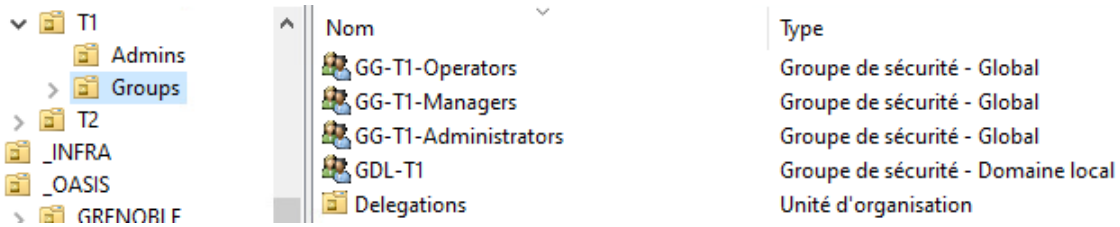
Operators

- Ce rôle n'a aucun droit dans l'AD.
- Il permet uniquement d'être administrateur local d'une ou plusieurs machines.

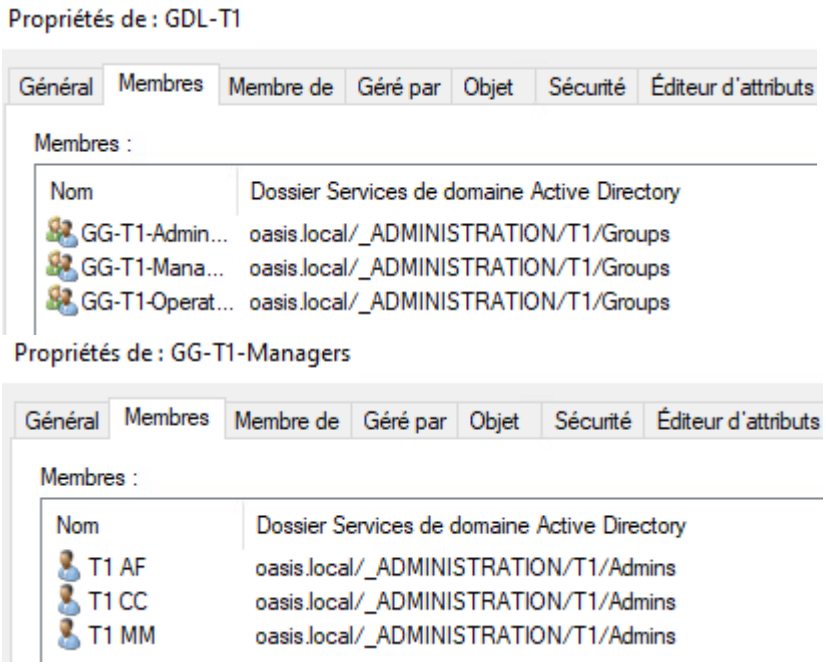
Pour chaque tier (sauf le Tier 0), on crée quatre groupes :

- **GG-T{x}-Managers** (Groupe Global)
- **GG-T{x}-Administrators** (Groupe Global)
- **GG-T{x}-Operators** (Groupe Global)
- **GDL-T{x}** (Groupe Domaine Local) : regroupe les trois groupes globaux ci-dessus.

Les administrateurs sont ajoutés dans les groupes correspondant à leur responsabilité.



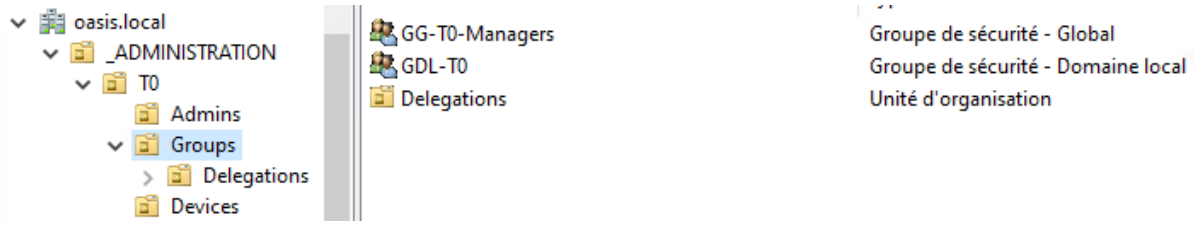
Les trois groupes globaux sont imbriqués dans le groupe Domaine Local du tier, conformément à la méthode AGDLP.

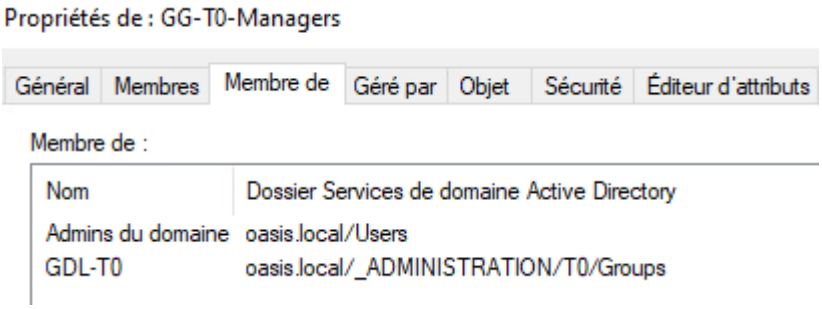


Le Tier 0 étant la partie la plus critique de l'infrastructure, sa configuration est différente. Il suffit de créer :

- Un groupe Domaine Local GDL-T0
- Un groupe Global GG-T0-Managers

Il n'y a pas d'Administrators ni d'Operators au Tier 0 : les quelques administrateurs habilités sont tous Managers. Le groupe GG-T0-Managers est ajouté au groupe « Administrateurs du domaine » et dans GDL-T0.





Important :

Cette approche est fonctionnelle mais n'est pas recommandée sur le long terme. Placer le groupe GG-T0-Managers dans « Admins du domaine » accorde un accès permanent au plus haut niveau de privilèges du domaine, ce qui va à l'encontre du principe du moindre privilège et augmente la surface d'attaque en cas de compromission.
Des approches plus robustes existent, notamment le JIT (Just-In-Time Administration) qui n'accorde les droits élevés que temporairement à la demande (via MIM/PAM ou des solutions tierces), ou encore le maintien du groupe « Admins du domaine » vide en permanence, en n'y ajoutant un compte que ponctuellement lorsqu'une opération l'exige. L'utilisation de PAW (Privileged Access Workstations) dédiés et durcis renforce également la sécurité du Tier 0.
Dans le cadre de ce projet, la configuration actuelle a été mise en place à des fins de fonctionnalité et de démonstration, mais elle constitue un axe d'amélioration prioritaire pour renforcer la sécurité du Tier 0.

Les groupes de délégation permettent d'attribuer des permissions granulaires sur les OU. Pour chaque tier (sauf le T0), on crée 6 groupes de type Domaine Local dans l'OU Delegations :

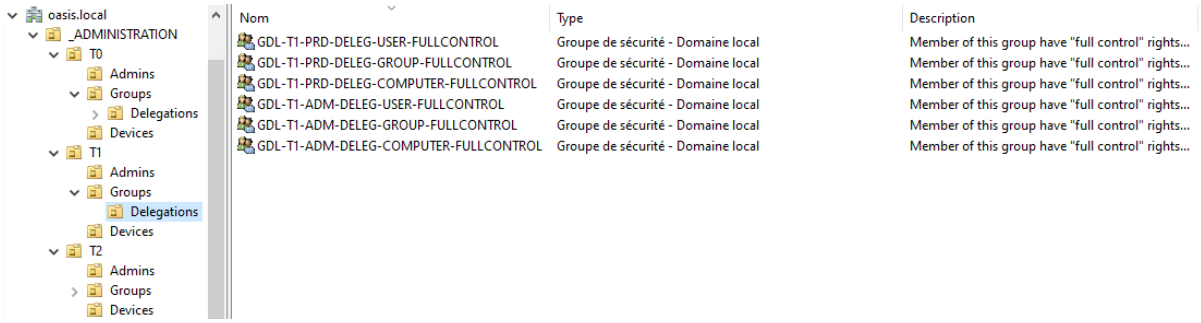
3 groupes pour la **Production** :

- GDL-T{x}-PRD-DELEG-COMPUTER-FULLCONTROL
- GDL-T{x}-PRD-DELEG-GROUP-FULLCONTROL
- GDL-T{x}-PRD-DELEG-USER-FULLCONTROL

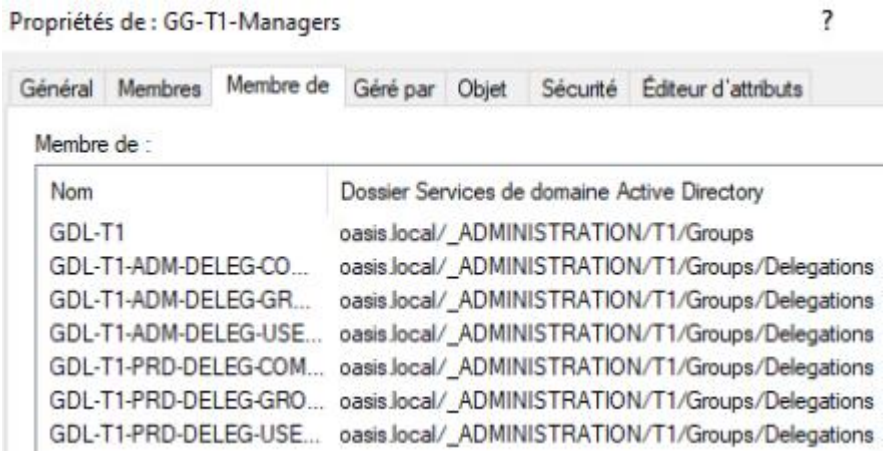
3 groupes pour l'**Administration** :

- GDL-T{x}-ADM-DELEG-COMPUTER-FULLCONTROL
- GDL-T{x}-ADM-DELEG-GROUP-FULLCONTROL
- GDL-T{x}-ADM-DELEG-USER-FULLCONTROL

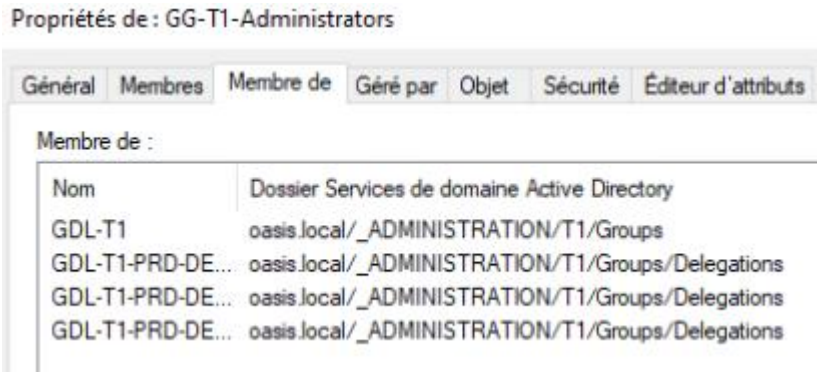
Chaque groupe représente un type d'objet (Computer, Group ou User) et sera utilisé pour déléguer le contrôle sur l'OU correspondante.



Le **Manager** est membre des 6 groupes de délégation (3 Production + 3 Administration), car il doit pouvoir gérer l'intégralité du tier.

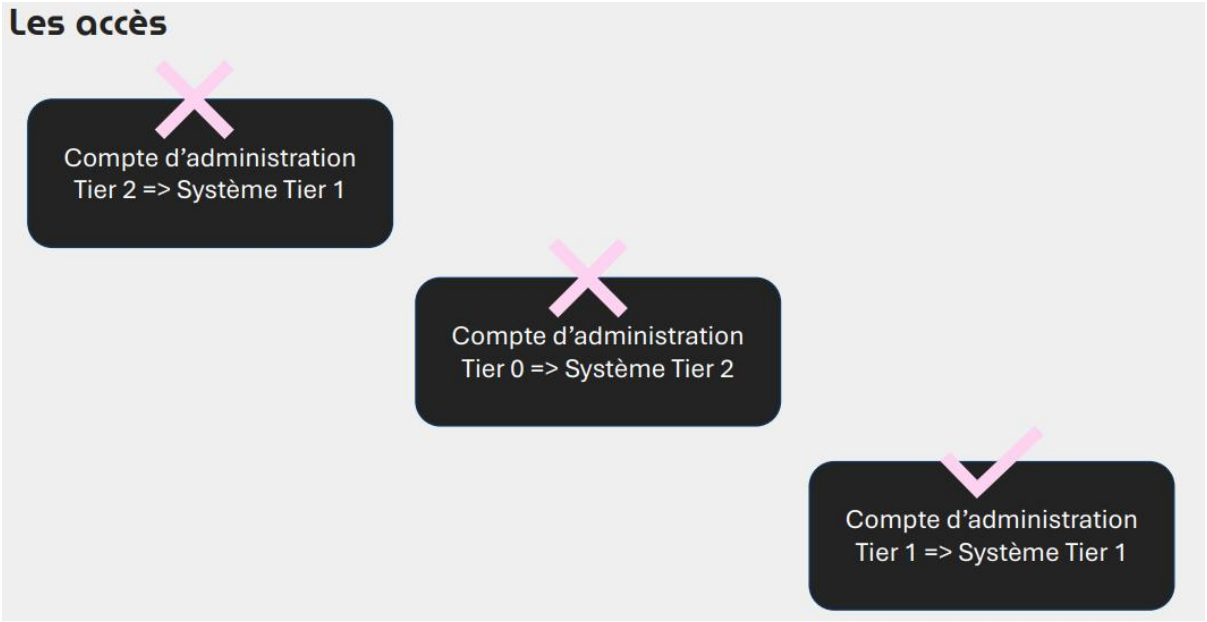


L'**Administrator** est membre uniquement des 3 groupes de délégation Production, car il n'a pas vocation à modifier les objets d'administration.

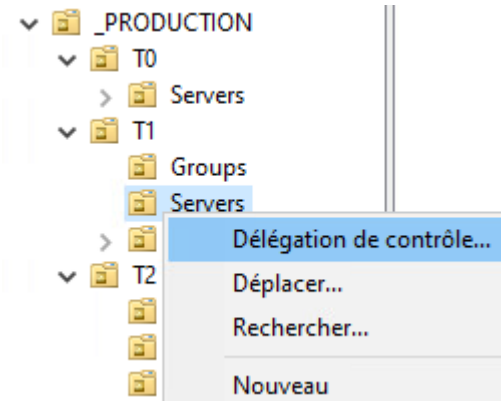


Reproduire la même logique pour les autres tiers (T2).

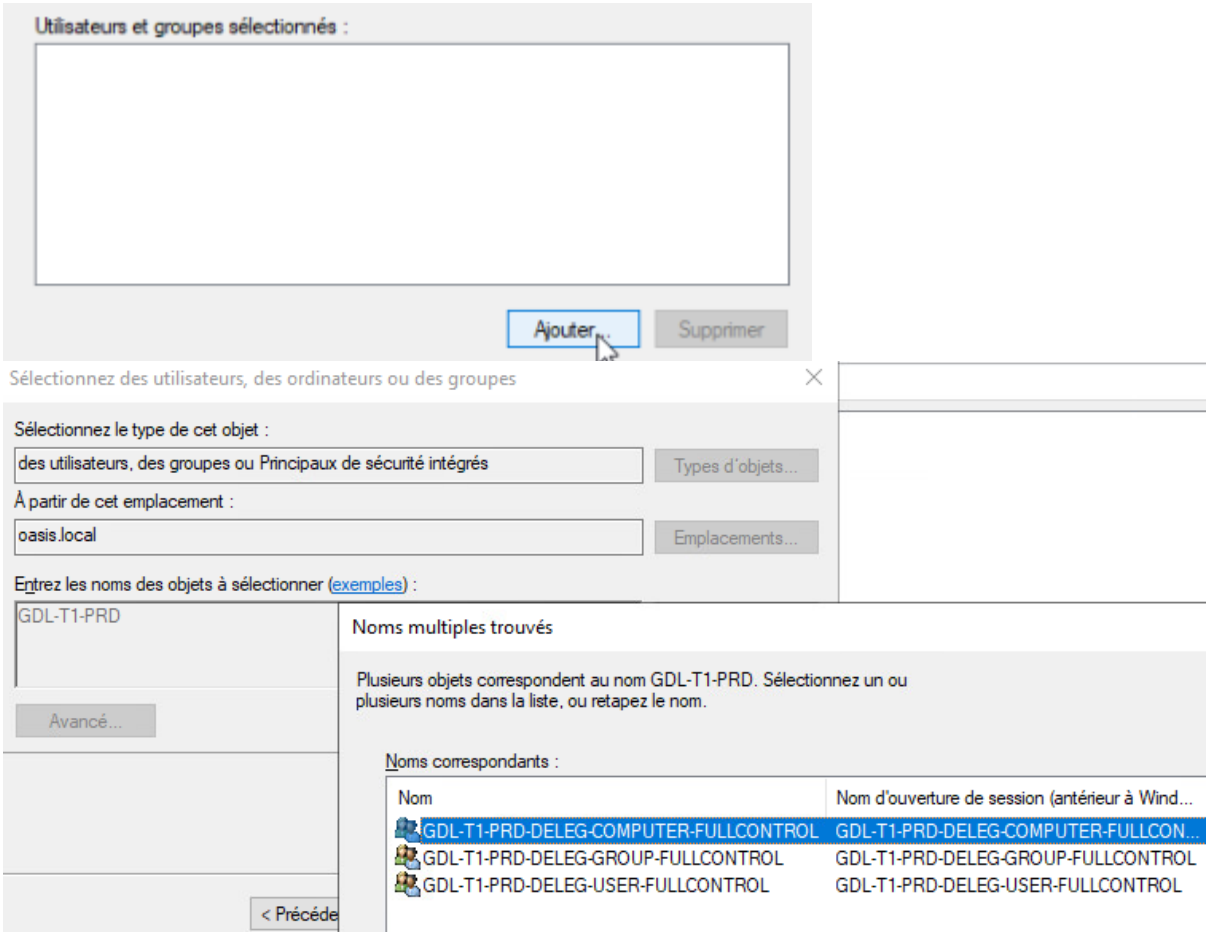
Maintenant que tous les groupes sont créés, il faut configurer les permissions sur chaque OU de production et d'administration. Par défaut, seuls les administrateurs du Tier 0 (Administrateurs du domaine) ont accès à l'AD. La logique d'accès est la suivante : un compte d'administration ne peut agir que sur les objets de son propre tier.



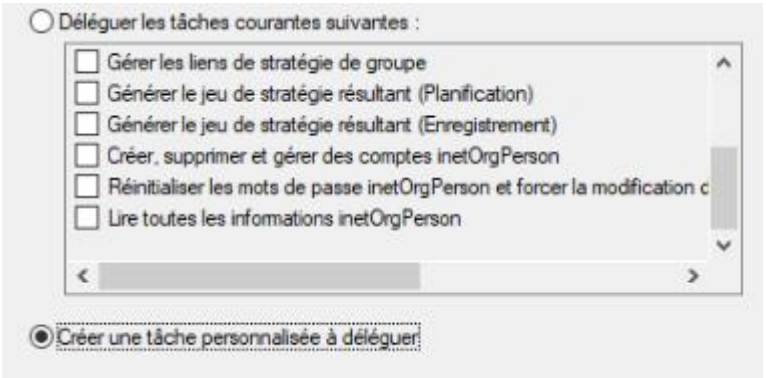
Pour configurer les permissions, effectuer un clic droit sur l'OU cible → « Délégation de contrôle »



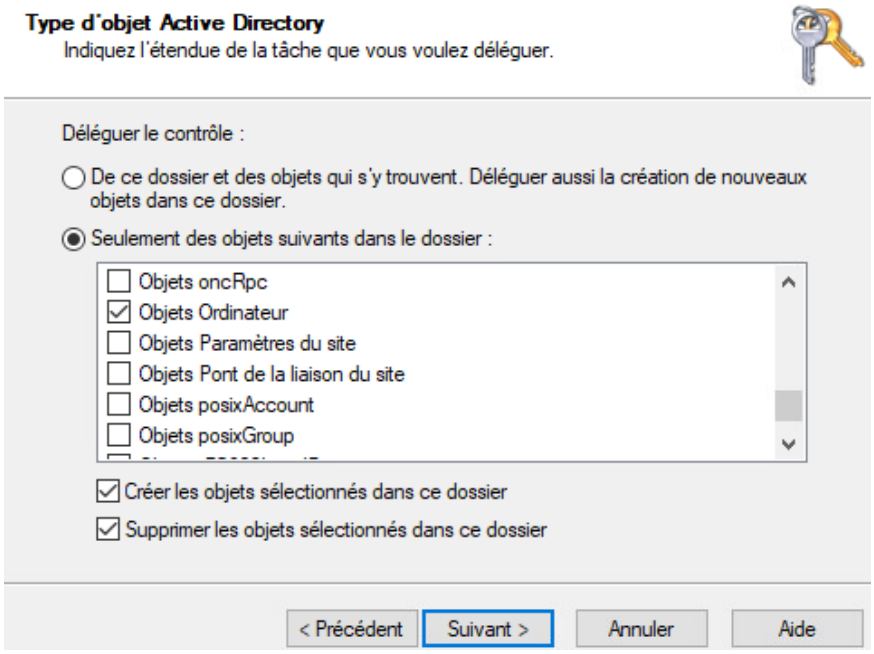
Ajouter le groupe de délégation correspondant. Par exemple, pour l'OU « Servers » dans « _PRODUCTION/T1 », sélectionner « GDL-T1-PRD-DELEG-COMPUTER-FULLCONTROL ».



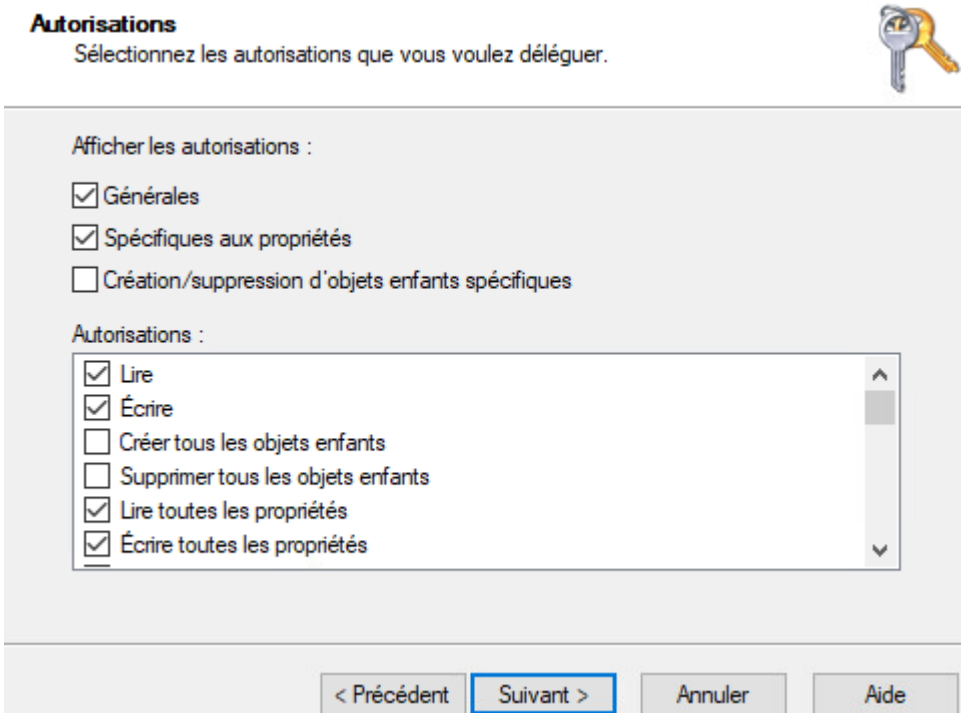
Choisir « Créer une tâche personnalisée à déléguer » afin de configurer des permissions.



Sélectionner « Seulement des objets suivants dans le dossier », puis cocher le type d'objet correspondant (ici « Objets Ordinateur »). Cocher également « Créer les objets sélectionnés dans ce dossier » et « Supprimer les objets sélectionnés dans ce dossier ».



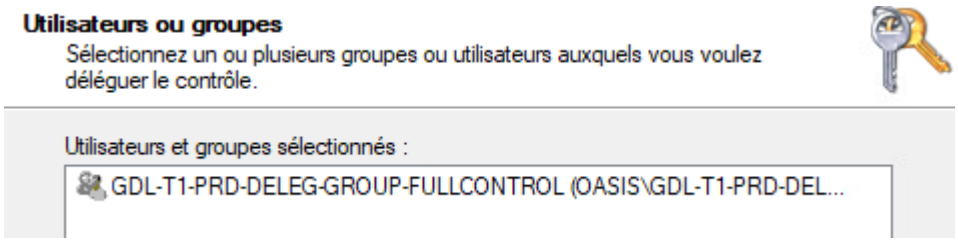
Attribuer les autorisations : cocher « Générales » et « Spécifiques aux propriétés », puis sélectionner « Lire », « Écrire », « Lire toutes les propriétés » et « Écrire toutes les propriétés ».



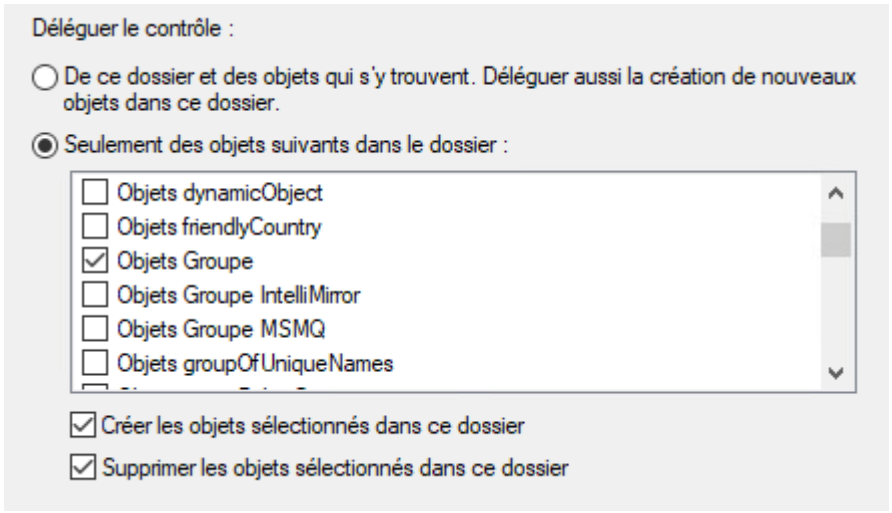
Répéter cette opération pour chaque OU et chaque type d'objet :

- OU Servers / Workstations → groupe DELEG-COMPUTER-FULLCONTROL
- OU Groups → groupe DELEG-GROUP-FULLCONTROL
- OU Users / Admins → groupe DELEG-USER-FULLCONTROL

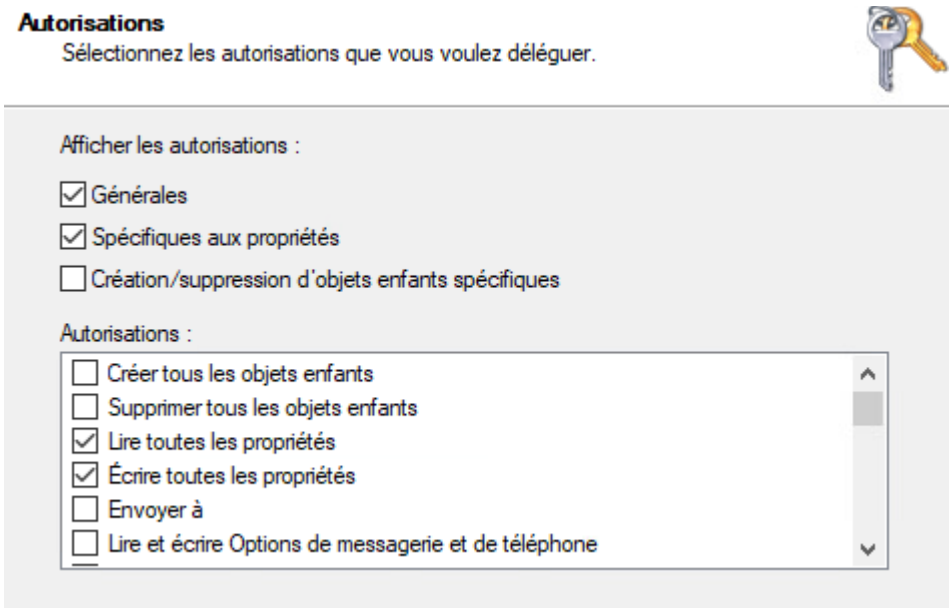
Pour la délégation sur l'OU Groups, sélectionner le groupe GDL-T{x}-PRD-DELEG-GROUP-FULLCONTROL.



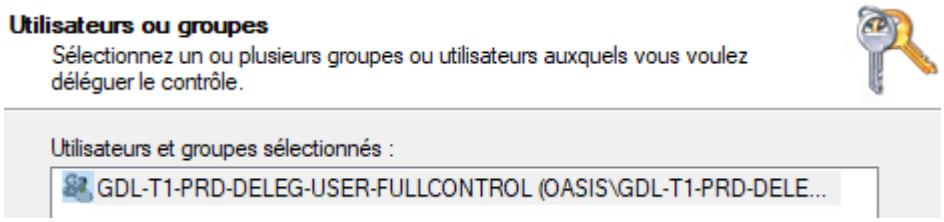
Choisir « Seulement des objets suivants dans le dossier », cocher « Objets Groupe » ainsi que « Créer les objets sélectionnés dans ce dossier » et « Supprimer les objets sélectionnés dans ce dossier ».



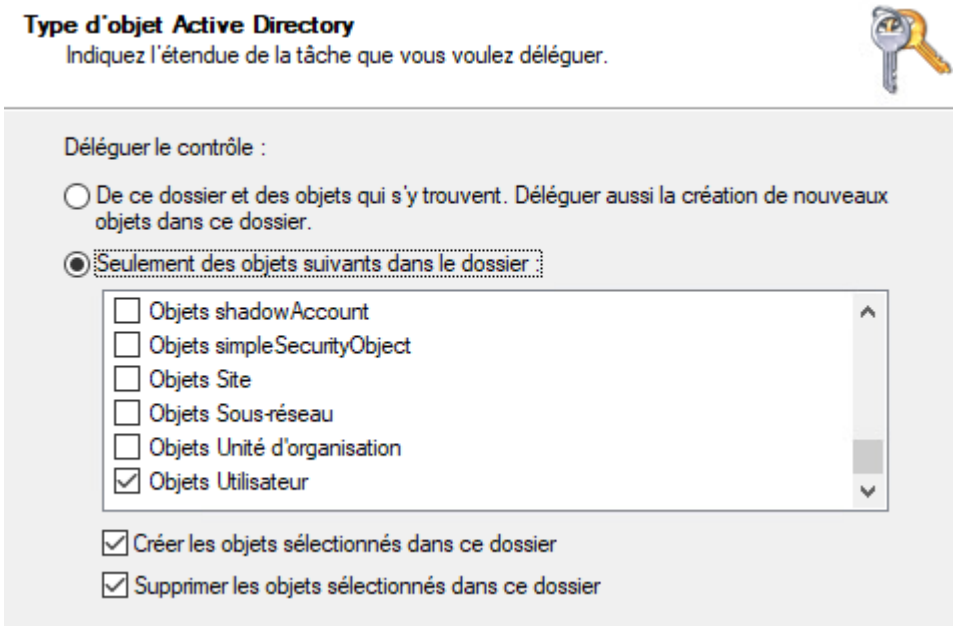
Dans les autorisations, cocher « Générales » et « Spécifiques aux propriétés », puis sélectionner « Lire », « Écrire », « Lire toutes les propriétés » et « Écrire toutes les propriétés ».



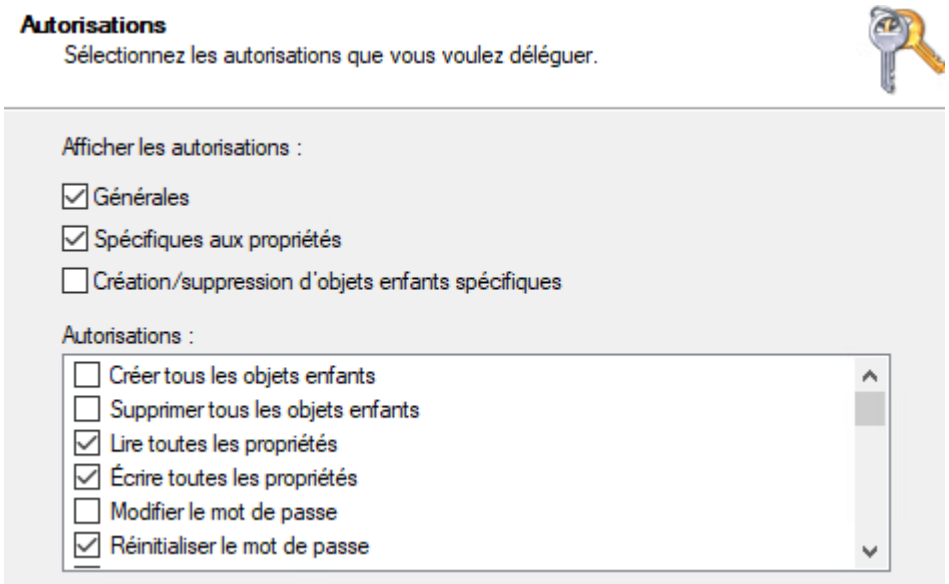
Pour les délégations sur les OU Users, sélectionner le groupe GDL-T{x}-PRD-DELEG-USER-FULLCONTROL.



Puis cocher « Objets Utilisateur », « Créer les objets sélectionnés dans ce dossier » et « Supprimer les objets sélectionnés dans ce dossier ».

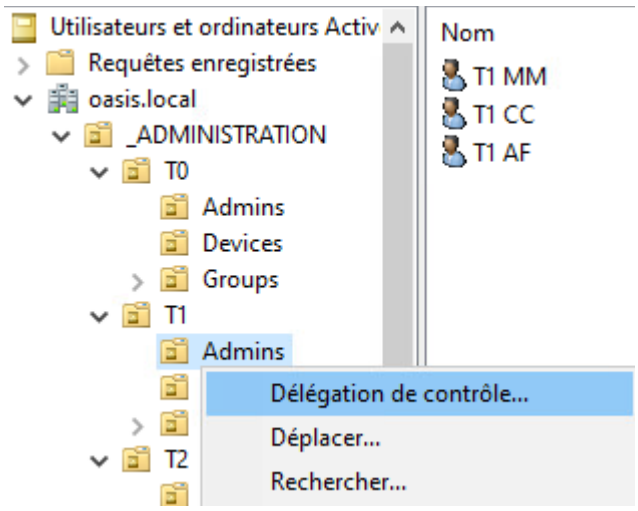


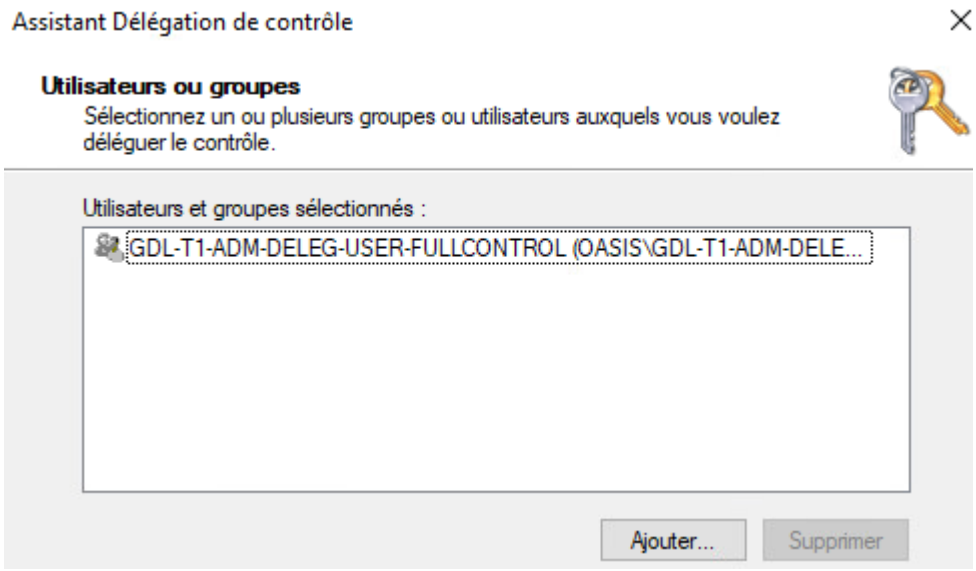
Dans les autorisations, choisir « Spécifiques aux propriétés », puis sélectionner « Lire toutes les propriétés », « Écrire toutes les propriétés » ainsi que « Réinitialiser les mots de passe ».

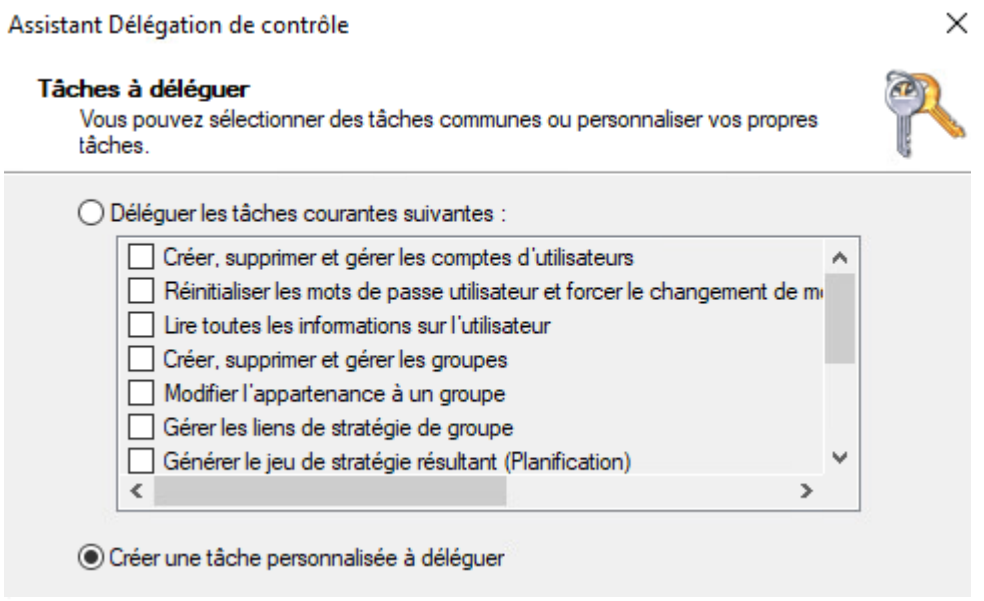


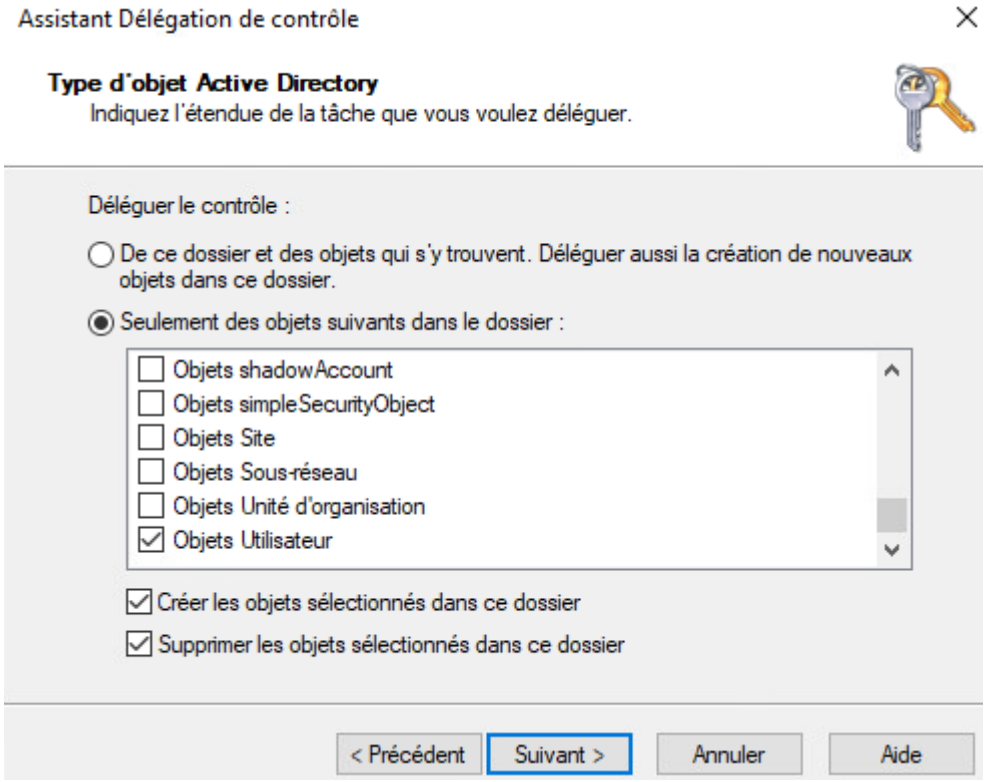
La même logique s'applique pour les groupes de délégation de la partie Administration. Pour chaque tier, répéter les opérations ci-dessus sur les OUs correspondantes en utilisant les groupes :

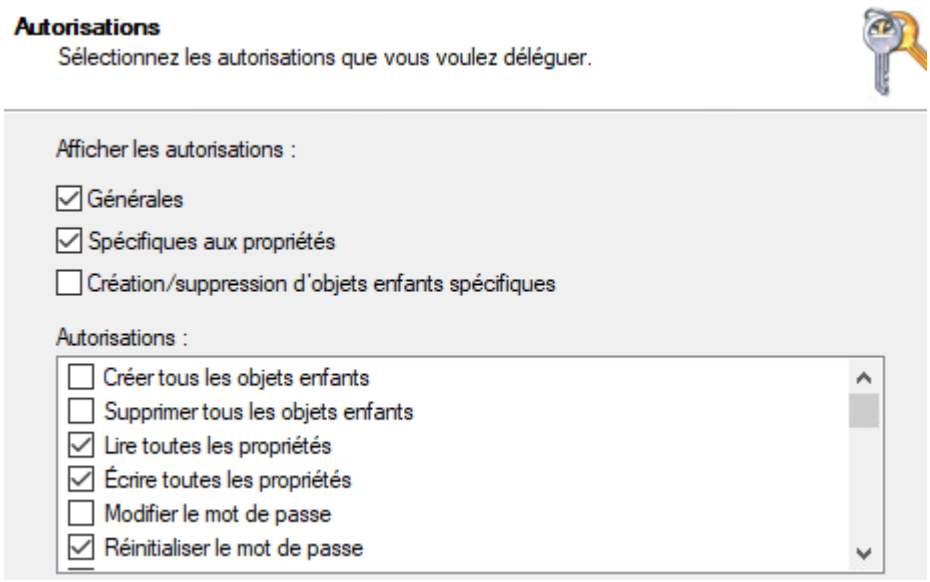
GDL-T{x}-ADM-DELEG-COMPUTER-FULLCONTROL,
GDL-T{x}-ADM-DELEG-GROUP-FULLCONTROL,
GDL-T{x}-ADM-DELEG-USER-FULLCONTROL.





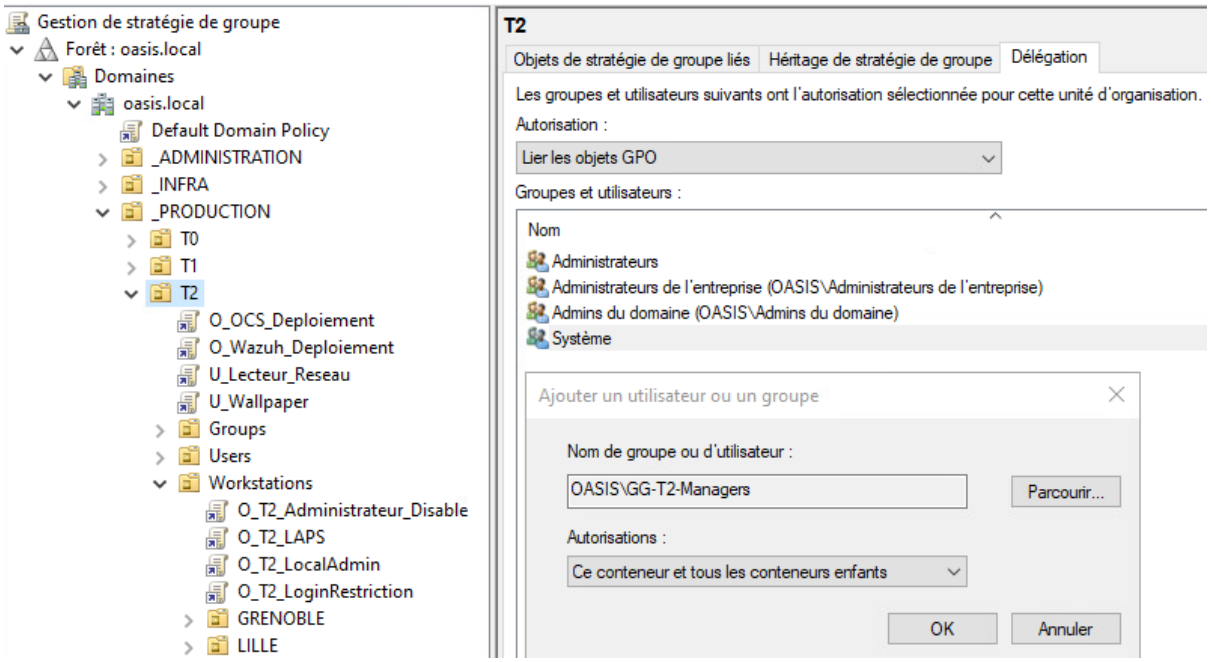

Assistant Délégation de contrôle
Tâches à déléguer
Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.
Déléguer les tâches courantes suivantes :
Créer, supprimer et gérer les comptes d'utilisateurs
Réinitialiser les mots de passe utilisateur et forcer le changement de m
Lire toutes les informations sur l'utilisateur
Créer, supprimer et gérer les groupes
Modifier l'appartenance à un groupe
Gérer les liens de stratégie de groupe
Générer le jeu de stratégie résultant (Planification)
Créer une tâche personnalisée à déléguer

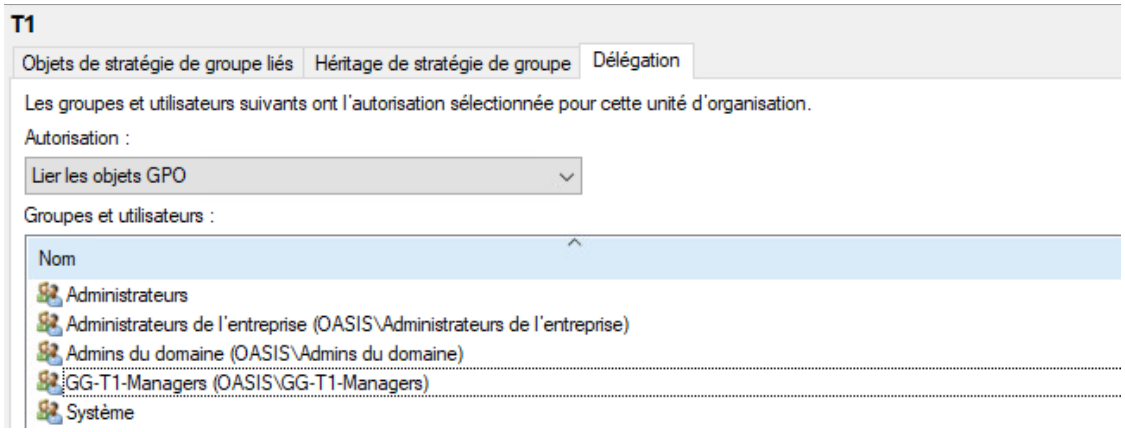

Assistant Délégation de contrôle
Type d'objet Active Directory
Indiquez l'étendue de la tâche que vous voulez déléguer.
Déléguer le contrôle :
De ce dossier et des objets qui s'y trouvent. Déléguer aussi la création de nouveaux objets dans ce dossier.
Seulement des objets suivants dans le dossier :
Objets shadowAccount
Objets simpleSecurityObject
Objets Site
Objets Sous-réseau
Objets Unité d'organisation
Objets Utilisateur
Créer les objets sélectionnés dans ce dossier
Supprimer les objets sélectionnés dans ce dossier
< Précédent
Suivant >
Annuler
Aide



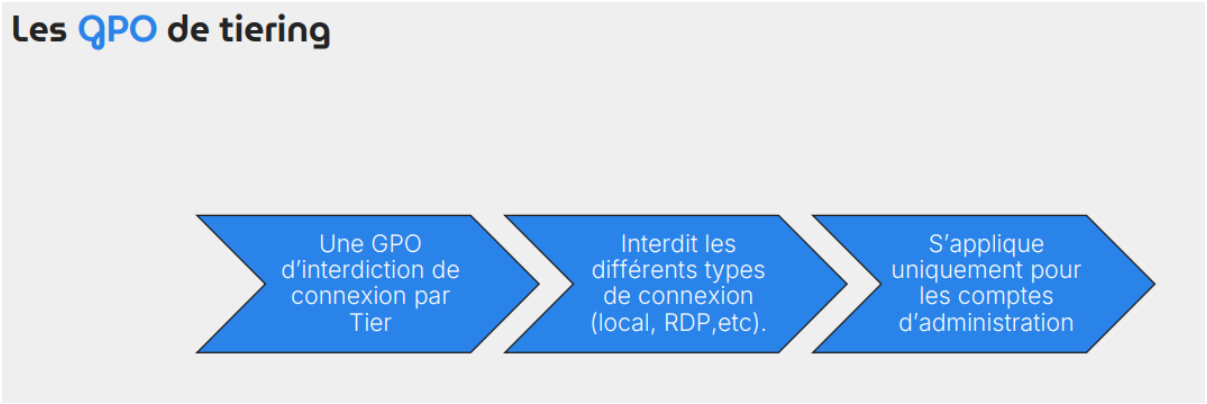
Avant de configurer les GPO de restriction, il faut donner aux Managers de chaque tier le droit de lier des GPO sur leurs OUs.

Dans l'onglet « Délégation » de chaque OU (_PRODUCTION/T1, _PRODUCTION/T2, etc.), ajouter le groupe GG-T1-Managers ou GG-T2-Managers avec l'autorisation « Lier les objets GPO ».



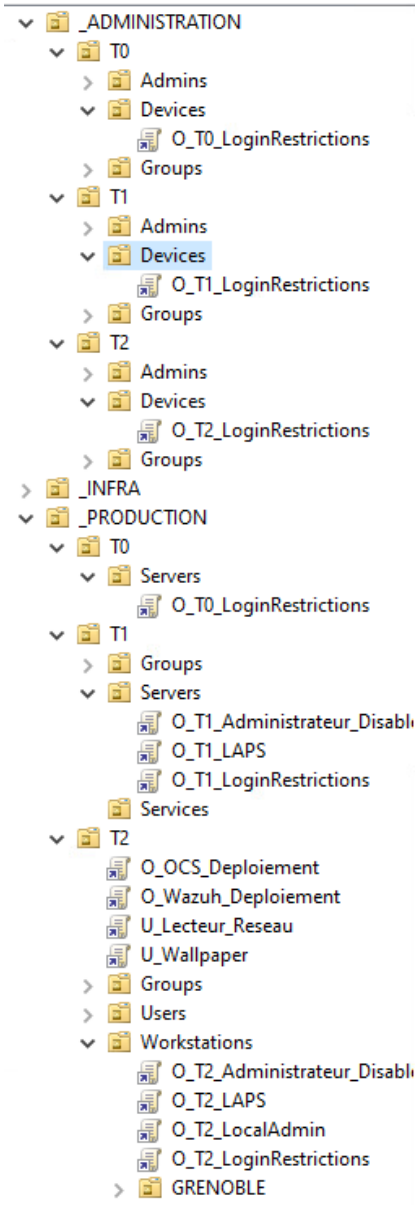


Les GPO de tiering reposent sur un principe simple : une GPO d'interdiction de connexion est créée par tier, interdit les différents types de connexion (locale, RDP, service, tâche planifiée) et s'applique uniquement aux comptes d'administration.

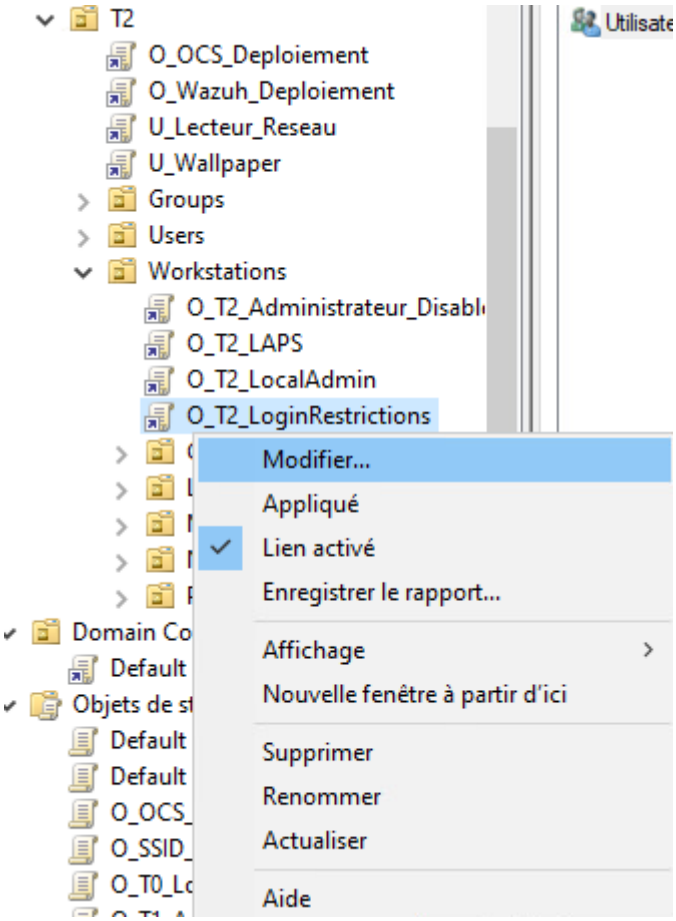


Dans la console « Gestion de stratégie de groupe », créer une GPO par tier et la lier aux OUs correspondantes :

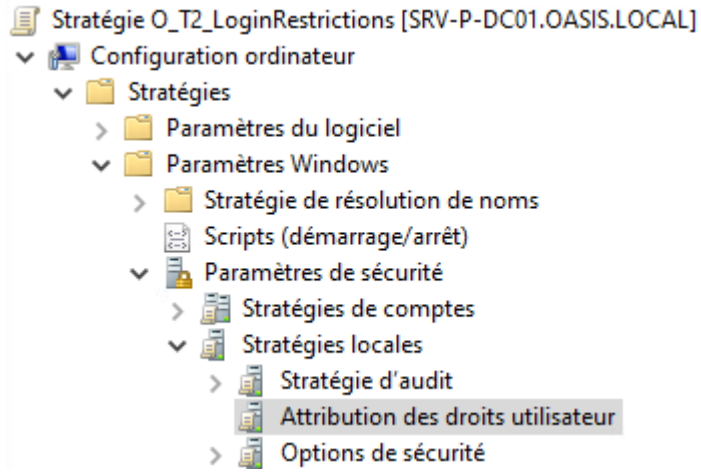
- O_T0_LoginRestrictions : liée à _ADMINISTRATION/T0/Devices et _PRODUCTION/T0/Servers
- O_T1_LoginRestrictions liée à _ADMINISTRATION/T1/Devices et _PRODUCTION/T1/Servers
- O_T2_LoginRestrictions : liée à _ADMINISTRATION/T2/Devices et _PRODUCTION/T2/Workstations



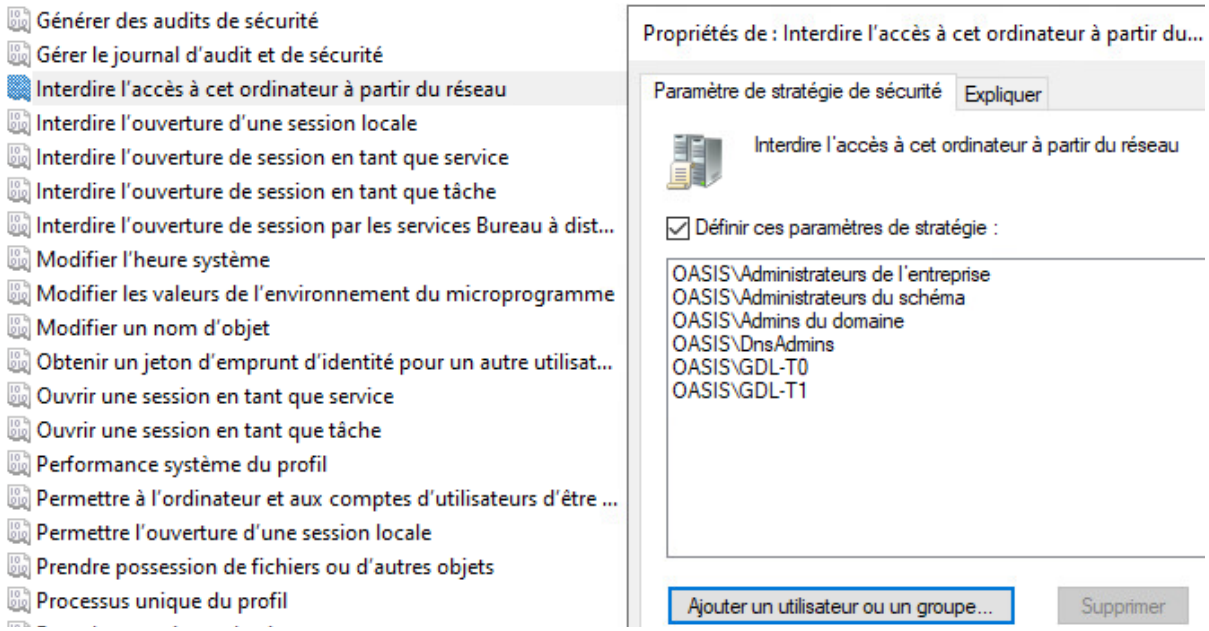
Pour éditer une GPO, effectuer un clic droit → « Modifier ».



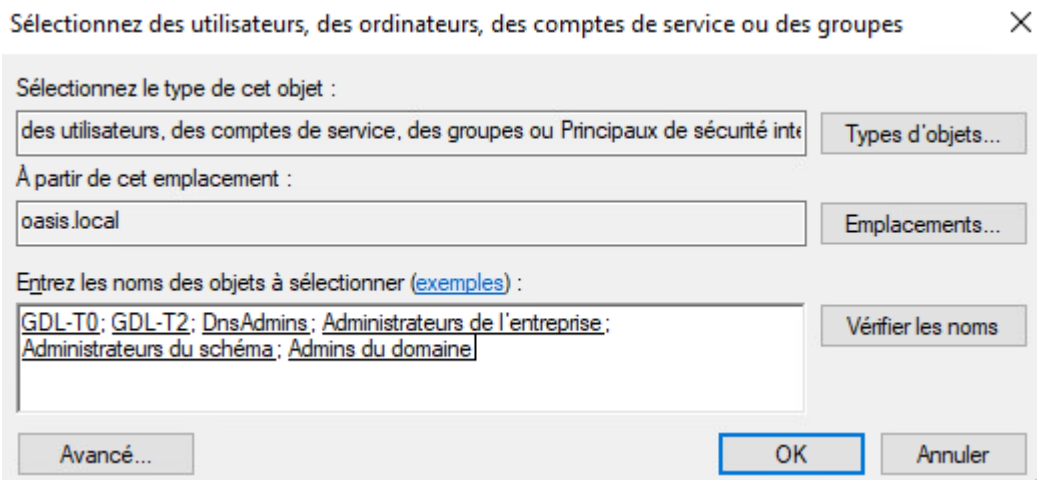
Se rendre dans Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies locales → Attribution des droits utilisateurs.



Pour le Tier 1, ajouter dans chaque paramètre d'interdiction de connexion les groupes GDL-T0, GDL-T1, GDL-T2, DnsAdmin, Administrateurs de l'entreprise, Administrateurs du schéma et Admins du domaine.

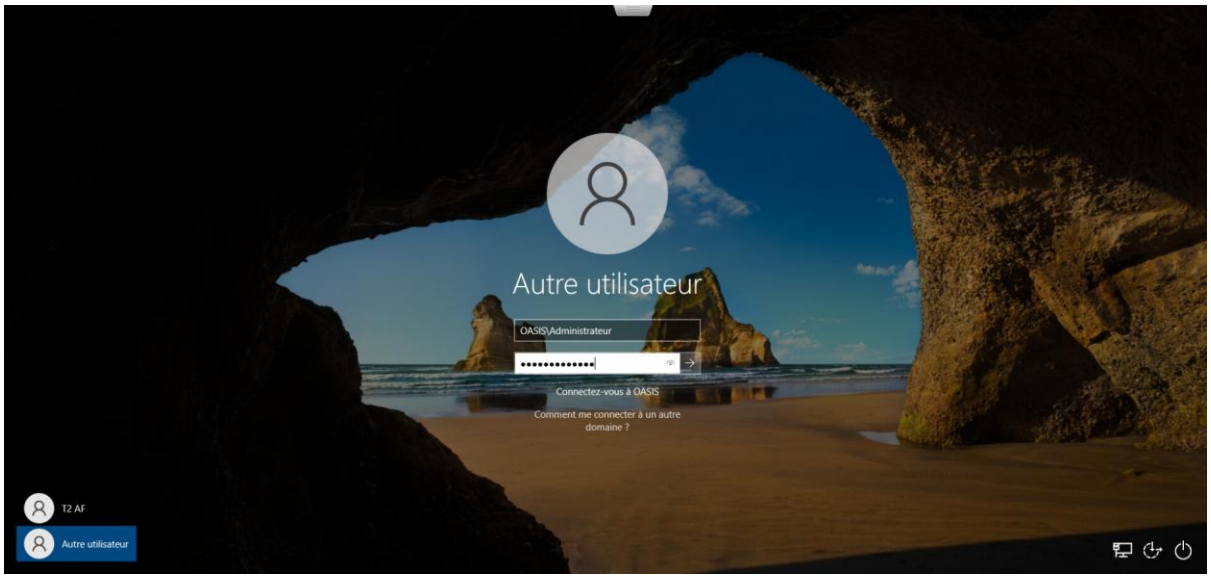


Répéter la même opération pour les GPO des autres tiers.

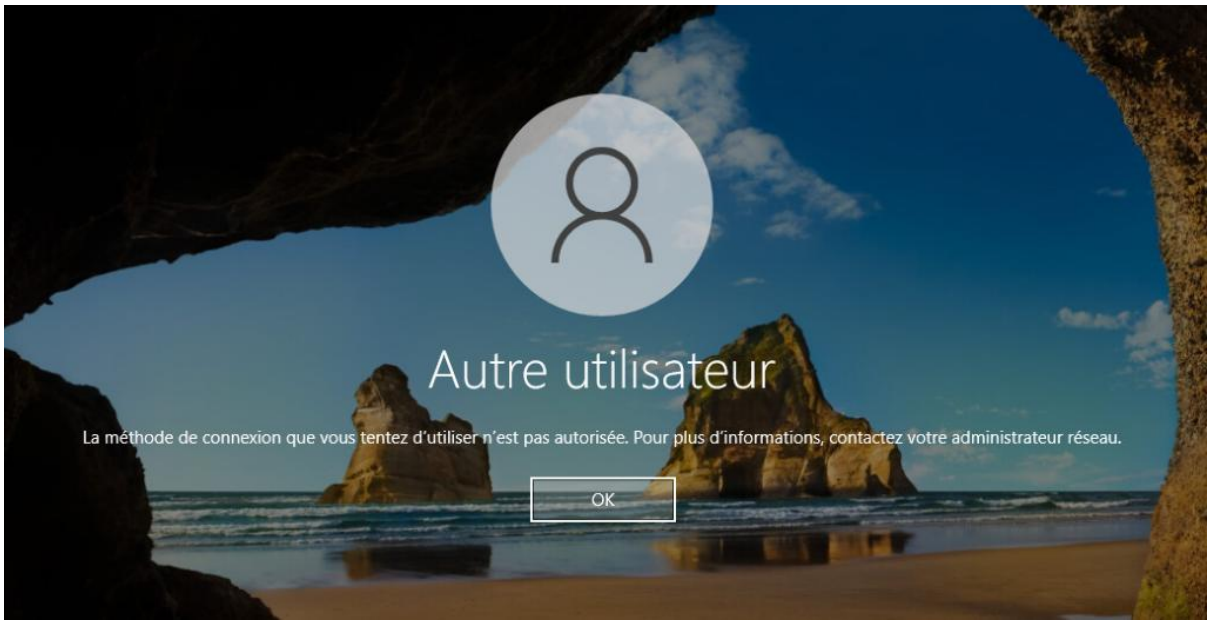


Pour vérifier le bon fonctionnement des GPO de tiering, effectuer les tests suivants depuis un poste du tier T2.
Premier test : connexion avec un compte Administrateur du domaine :

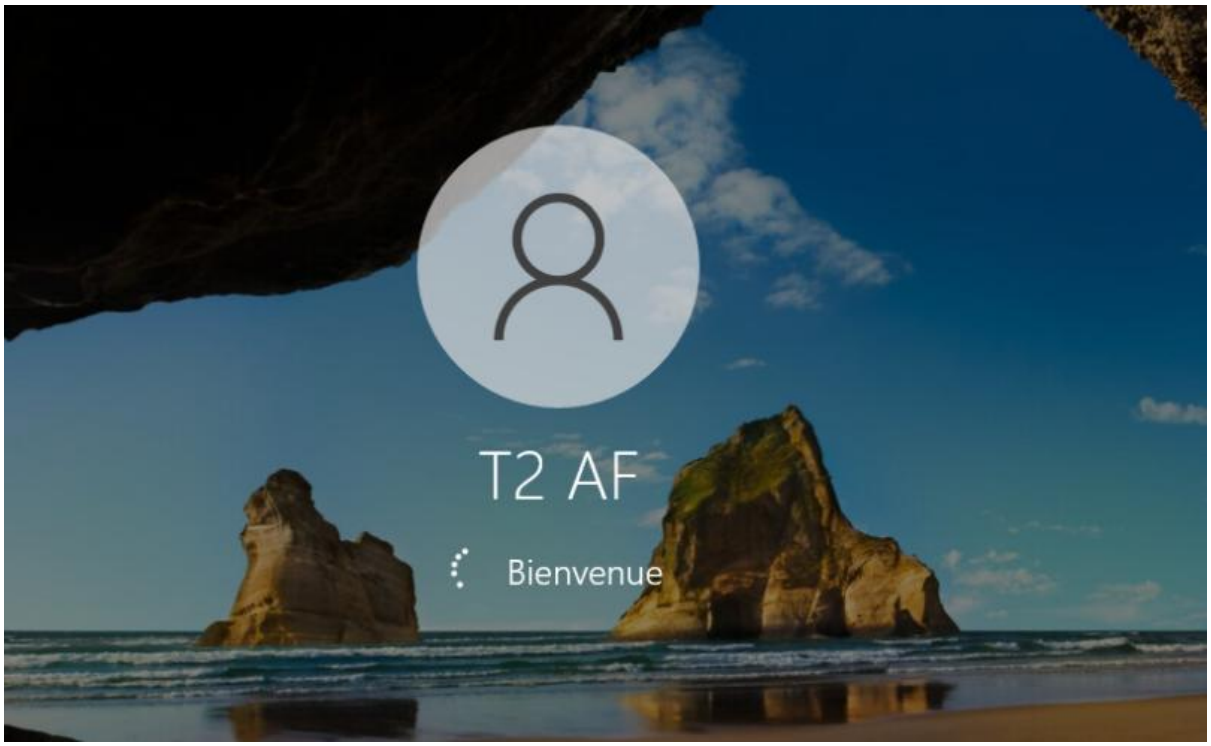
Tenter de se connecter sur un poste T2 avec le compte OASIS\Administrateur.



La tentative doit être bloquée avec le message : « La méthode de connexion que vous tentez d'utiliser n'est pas autorisée. Pour plus d'informations, contactez votre administrateur réseau. »



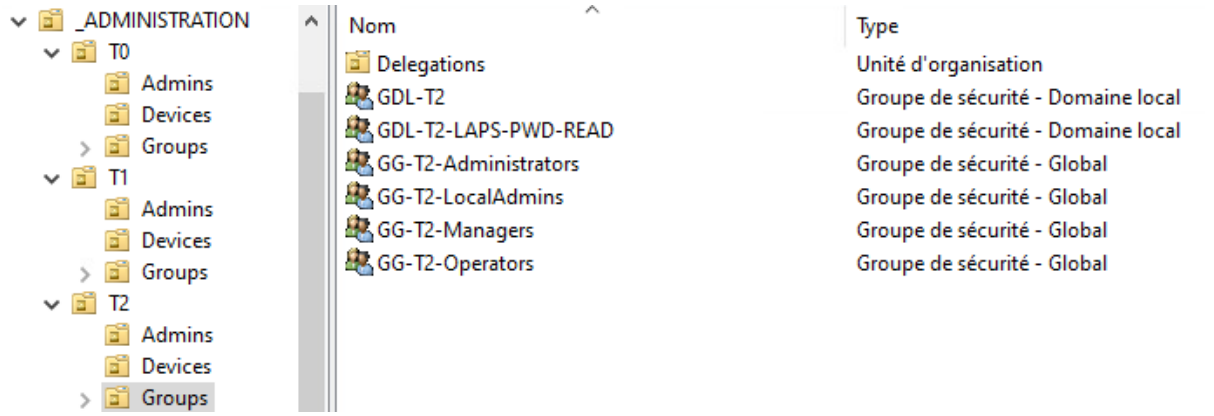
Second test : connexion avec un compte administrateur du tier T2 :
Se connecter sur le même poste avec le compte t2_af. La session s'ouvre normalement le compte T2 est bien autorisé sur les machines de son tier.



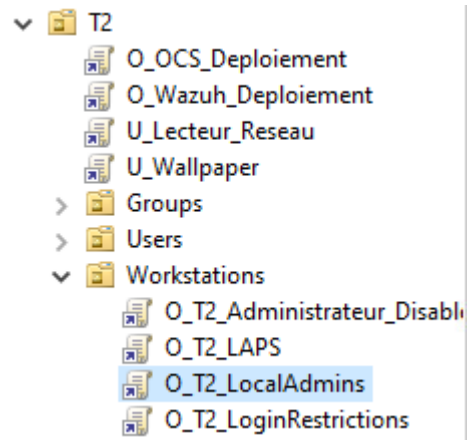
La configuration des accès est fonctionnelle. Il est impossible de se connecter avec un administrateur d'un tier plus élevé. De même, un administrateur d'un tier inférieur au T0 ne peut pas se connecter sur les DC car il n'est pas administrateur du domaine.

S'assurer que les deux GPO par défaut Default Domain Controllers Policy et Default Domain Policy sont bien appliquées depuis la console « Gestion de stratégie de groupe » → « Objets de stratégie de groupe ».

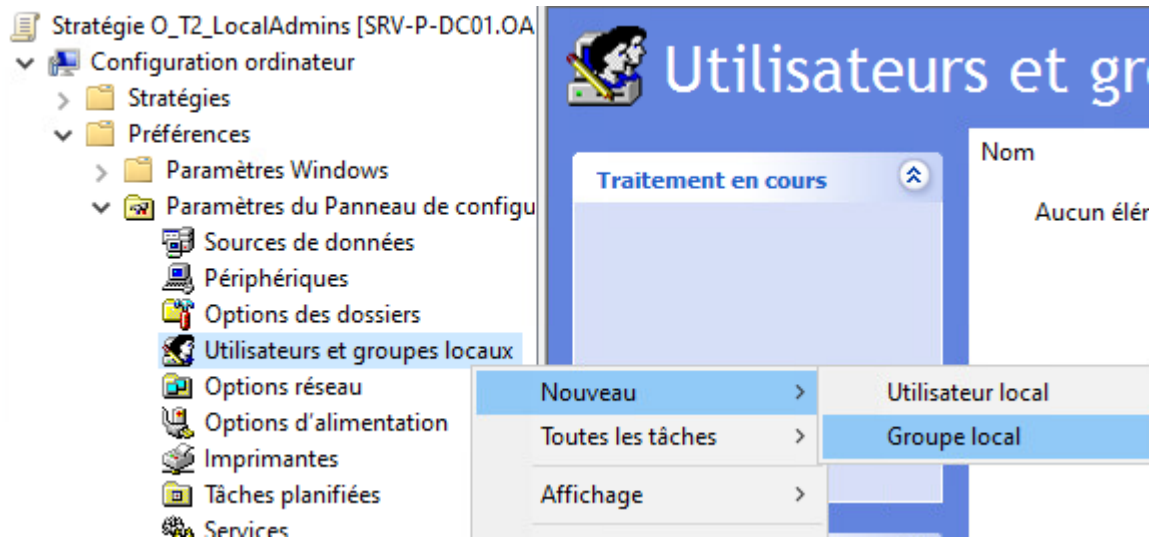
Désormais, il faut faire en sorte que les administrateurs soient administrateur local des postes qu'ils ont à administrer. Pour cela, créer un groupe GG-T2-LocalAdmins dans _ADMINISTRATION/T2/Groups et y ajouter les utilisateurs devant disposer des droits d'administrateur local sur les machines du Tier 2.



Dans la console « Gestion de stratégie de groupe », créer une GPO liée à l'OU _PRODUCTION/T2/Workstations nommée O_T2_LocalAdmins.

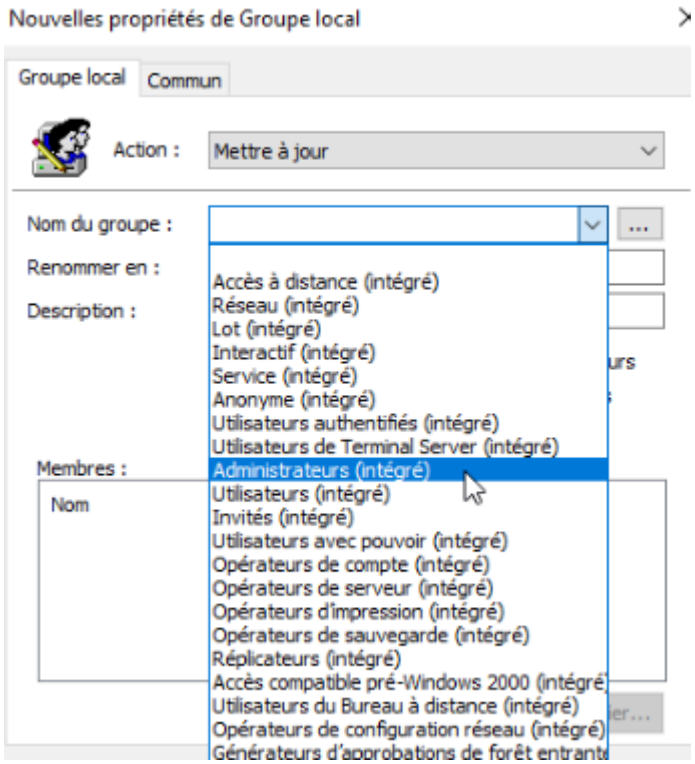


Dans l'éditeur de la GPO, se rendre dans Configuration ordinateur → Préférences → Paramètres du Panneau de configuration → Utilisateurs et groupes locaux. Effectuer un clic droit → Nouveau → Groupe local.

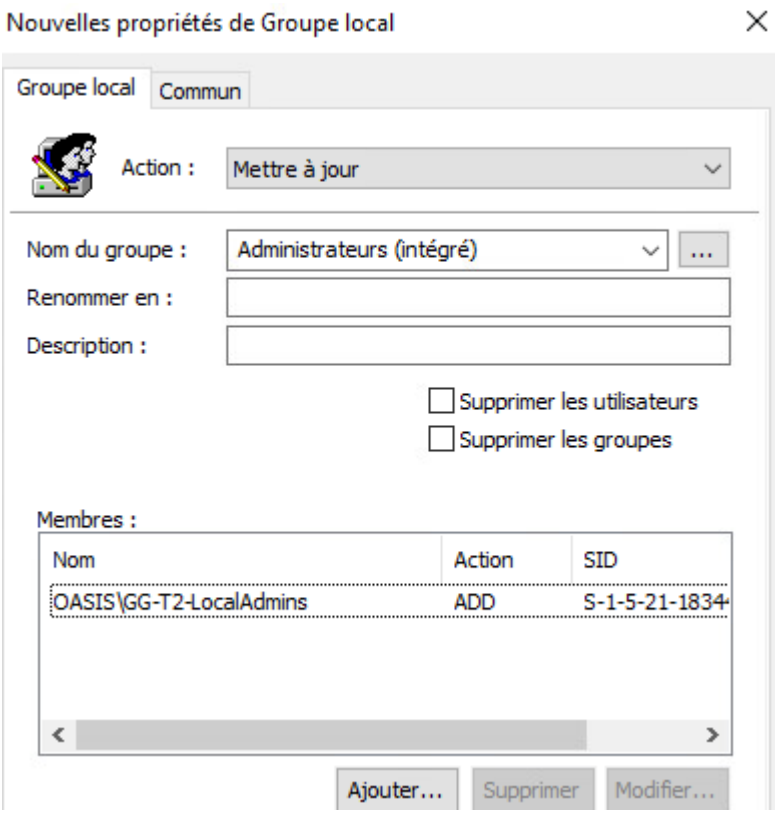


Configurer les paramètres suivants :

- Action : Mettre à jour
- Nom du groupe : Administrateurs (intégré)
- Dans la section Membres, cliquer sur « Ajouter »



Dans la section Membres, cliquer sur « Ajouter » et renseigner le groupe OASIS\GG-T2-LocalAdmins avec l'action ADD



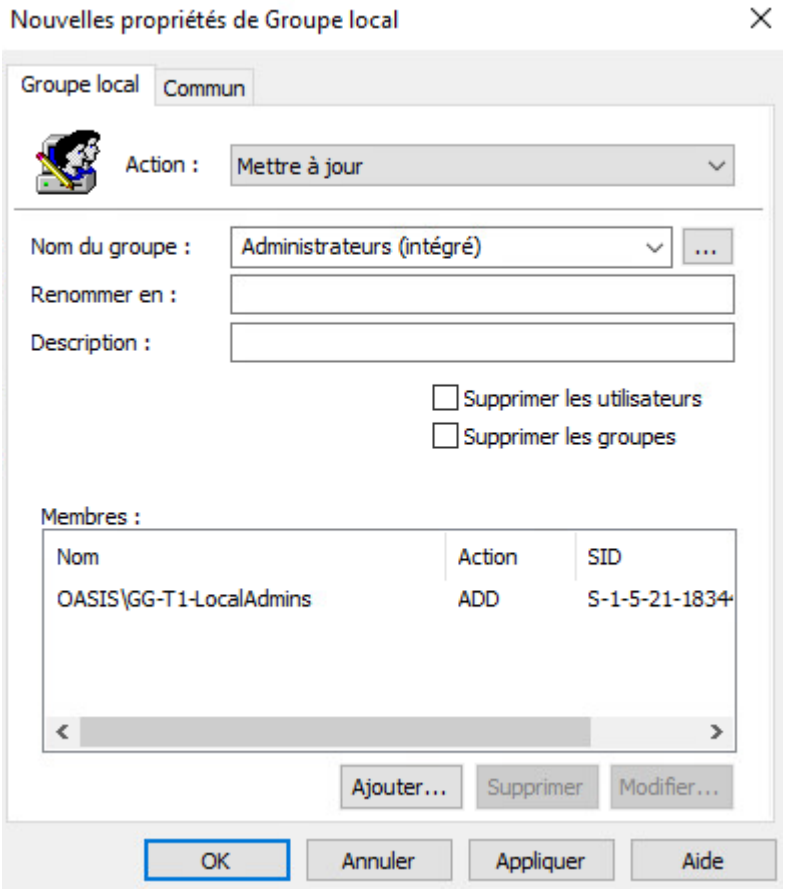
Une fois la GPO appliquée, vérifier la présence du groupe dans les administrateurs locaux d'un poste T2 via la commande :

net localgroup Administrateurs

Le groupe OASIS\GG-T2-LocalAdmins apparaît bien dans le groupe local Administrateurs, aux côtés du compte Administrateur local et du compte de service TechNTx.

```
C:\Windows\system32>net localgroup administrateurs
Nom alias       administrateurs
Commentaire

Membres

-------------------------------------------------------
Administrateur
OASIS\Admins du domaine
OASIS\GG-T2-LocalAdmins
TechNTx
La commande s'est terminée correctement.
```

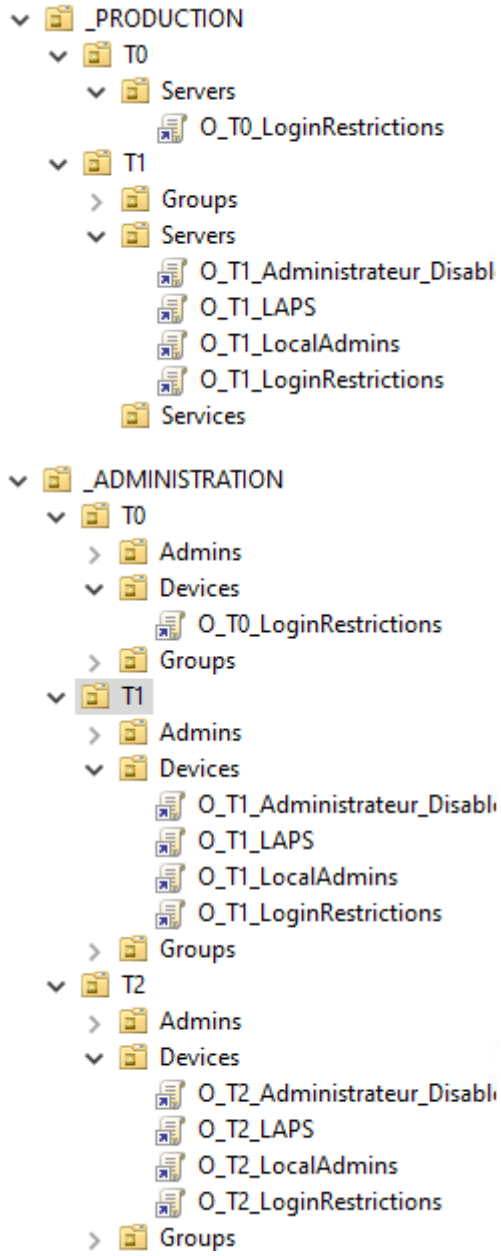
Pour le Tier 1, reproduire la même logique en créant un groupe GG-T1-LocalAdmins dans _ADMINISTRATION/T1/Groups et une GPO O_T1_LocalAdmins liée à l'OU _PRODUCTION/T1/Servers, avec le groupe OASIS\GG-T1-LocalAdmins ajouté en action ADD dans le groupe local Administrateurs (intégré).



La vérification sur le serveur SRV-P-DFS01 confirme le bon fonctionnement via la commande net localgroup Administrateurs : le groupe OASIS\GG-T1-LocalAdmins est bien présent aux côtés du compte Administrateur local et du compte SrvNTx.

```
C:\Windows\system32>net localgroup administrateurs
Nom alias       administrateurs
Commentaire

Membres

-------------------------------------------------------------------------------
Administrateur
OASIS\Admins du domaine
OASIS\GG-T1-LocalAdmins
SrvNTx
La commande s'est terminée correctement.
```

Les OUs _ADMINISTRATION/T0/Devices, _ADMINISTRATION/T1/Devices et _ADMINISTRATION/T2/Devices accueilleront les GPO dédiées aux postes d'administration RSAT de chaque tier. Ces GPO permettront d'appliquer les restrictions de connexion propres à chaque tier sur les postes RSAT, garantissant qu'un poste RSAT T2 ne peut pas être utilisé pour administrer des ressources T1 ou T0.



Par défaut, l'attribut ms-DS-MachineAccountQuota est fixé à 10, ce qui autorise n'importe quel utilisateur authentifié à joindre jusqu'à 10 machines au domaine.

```
PS C:\Users\Administrateur> Get-ADObject -Identity ((Get-ADDomain).distinguishedname) `
>> -Properties ms-DS-MachineAccountQuota


DistinguishedName          : DC=oasis,DC=local
ms-DS-MachineAccountQuota : 10
Name                       : oasis
ObjectClass                : domainDNS
ObjectGUID                 : c5c40292-75d3-49d2-b1bc-2476e872b3a8
```

Cet attribut est passé à 0 afin que seuls les comptes disposant d'une délégation explicite sur une OU puissent joindre des machines.

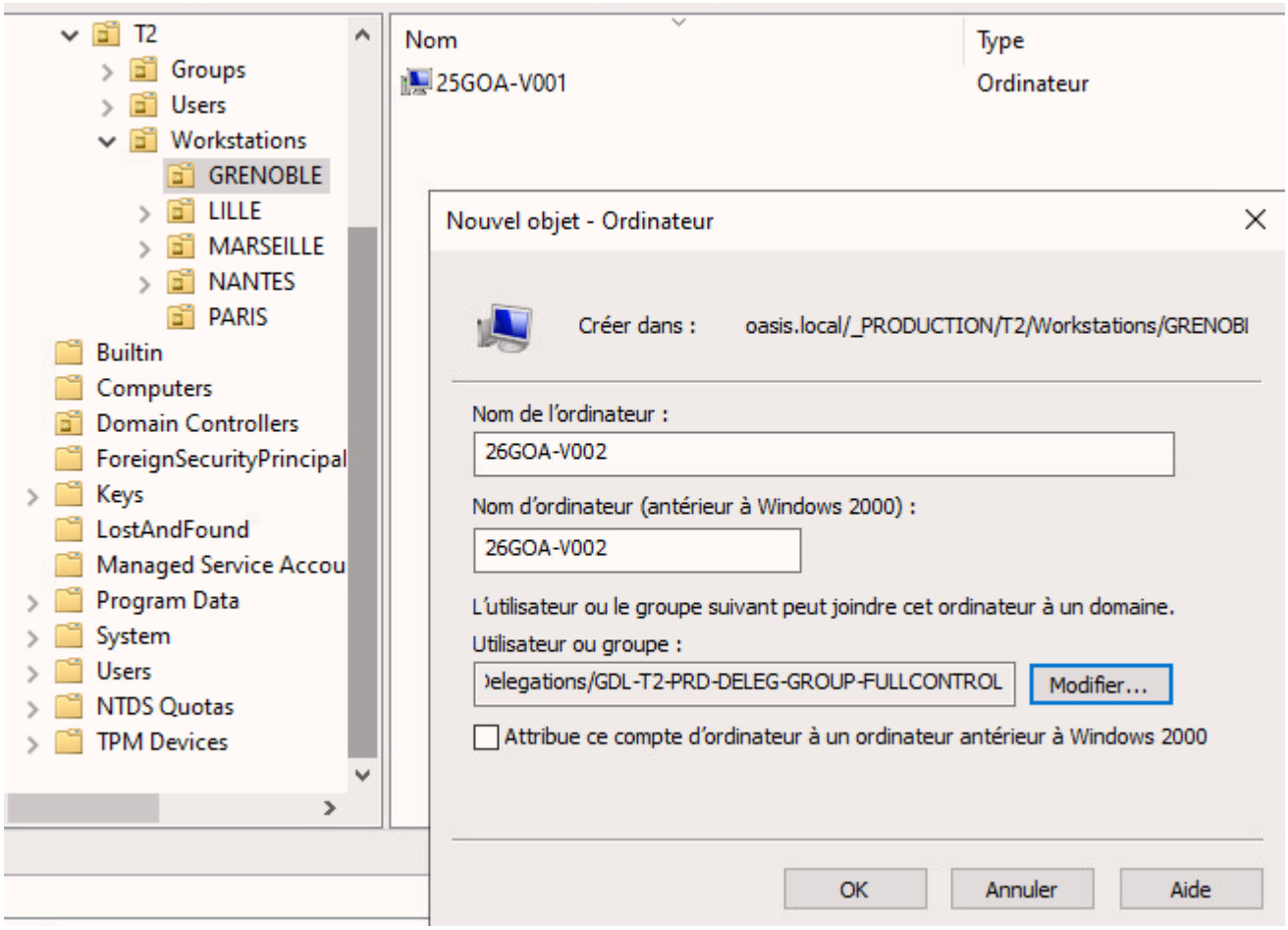
Set-ADDomain -Identity "Oasis.local" `
-Replace @{"ms-DS-MachineAccountQuota" = "0"}

La vérification confirme que la valeur est bien passée à 0 sur le domaine DC=oasis,DC=local.

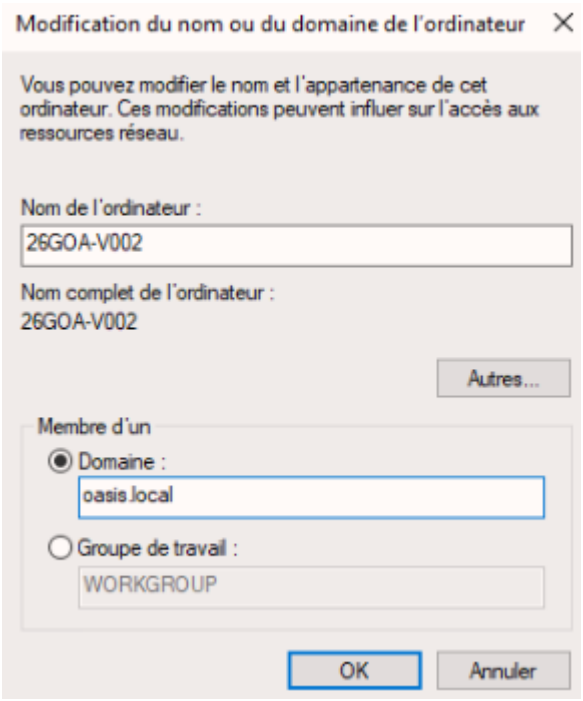
```
PS C:\Users\Administrateur> Set-ADDomain -Identity "Oasis.local" `
>> -Replace @{"ms-DS-MachineAccountQuota" = "0"}
PS C:\Users\Administrateur> Get-ADObject -Identity ((Get-ADDomain).distinguishedname) `
>> -Properties ms-DS-MachineAccountQuota


DistinguishedName          : DC=oasis,DC=local
ms-DS-MachineAccountQuota : 0
Name                       : oasis
ObjectClass                : domainDNS
ObjectGUID                 : c5c40292-75d3-49d2-b1bc-2476e872b3a8
```

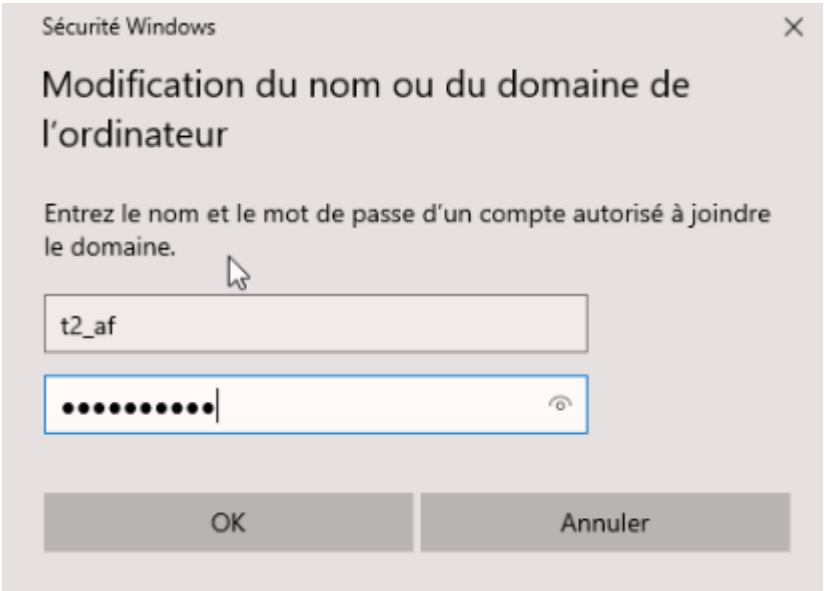
Conformément aux recommandations Microsoft, les comptes ordinateurs sont créés à l'avance (pré-staging) dans l'OU cible avant la jonction. Dans la console, effectuer un clic droit sur l'OU _PRODUCTION/T2/Workstations/GRENOBLE → Nouveau → Ordinateur.

Renseigner le nom de la machine, ici 26GOA-V002, puis dans le champ « L'utilisateur ou le groupe suivant peut joindre cet ordinateur à un domaine », cliquer sur « Modifier » et sélectionner GDL-T2-PRD-DELEG-COMPUTER-FULLCONTROL. Cela garantit que seul un membre de ce groupe de délégation peut effectuer la jointure sur ce compte, sans passer par un compte Admins du domaine.

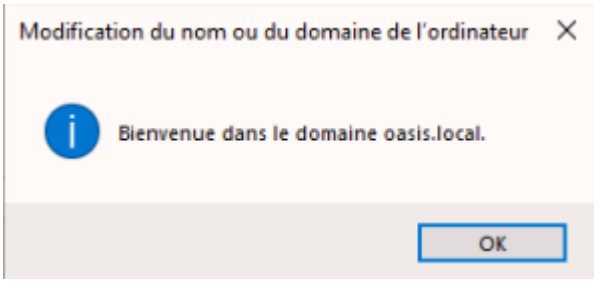


Pour joindre la machine, se rendre dans les propriétés système du poste → Modifier → Domaine : oasis.local, puis s'authentifier avec le compte t2_af.





Le message « Bienvenue dans le domaine oasis.local » confirme que la jointure s'est effectuée correctement et que la machine est bien placée dans l'OU cible.



8.1. Conclusion

Le modèle de tiering est fonctionnel sur l'ensemble de l'infrastructure. L'arborescence des OUs **_ADMINISTRATION** et **_PRODUCTION** est en place avec la séparation **T0**, **T1** et **T2**. Les comptes d'administration dédiés par tier et par personne sont créés et correctement placés dans leurs OUs respectives.

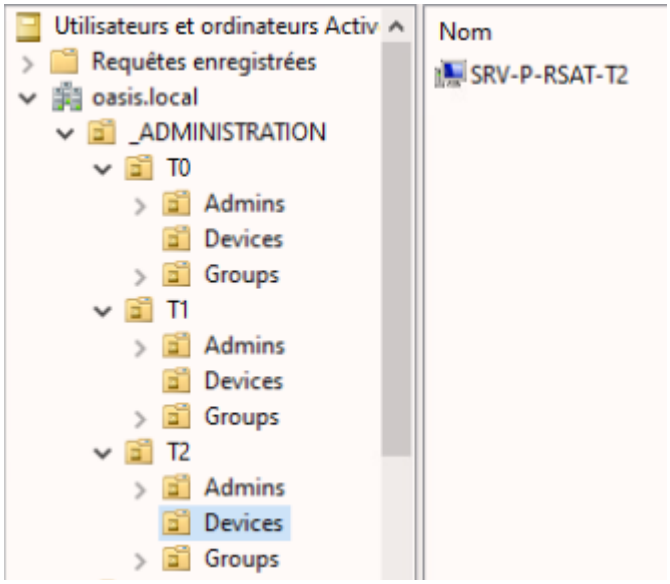
Les délégations de contrôle ont été appliquées sur chaque OU de production et d'administration. Les groupes de délégation **GDL-T{x}-PRD-DELEG-COMPUTER-FULLCONTROL, GDL-T{x}-PRD-DELEG-GROUP-FULLCONTROL et GDL-T{x}-PRD-DELEG-USER-FULLCONTROL** permettent aux administrateurs de chaque tier d'agir uniquement sur les objets qui leur sont rattachés.

Les GPO de restriction de connexion **O_T0_LoginRestrictions**, **O_T1_LoginRestrictions** et **O_T2_LoginRestrictions** sont liées aux OUs correspondantes et appliquées correctement. Les tests de connexion confirment le bon fonctionnement du cloisonnement : une tentative de connexion avec un compte Administrateur du domaine sur un poste T2 est refusée. Un compte T2 peut en revanche ouvrir une session normalement sur les machines de son tier.

La GPO **O_T2_LocalAdmins** est fonctionnelle : le groupe **GG-T2-LocalAdmins** apparaît bien dans le groupe local Administrateurs des postes T2, confirmé via la commande *net localgroup Administrateurs*. La même logique est validée pour le Tier 1 avec **GG-T1-LocalAdmins** sur les serveurs T1.

9. Installation RSAT

Les outils d'administration à distance (RSAT) sont installés sur des machines dédiées placées dans les OUs _ADMINISTRATION/T{x}/Devices de chaque tier. Ces postes permettent aux administrateurs de chaque tier d'administrer les ressources qui leur sont rattachées sans se connecter directement sur les serveurs.



L'installation des modules RSAT s'effectuera en PowerShell.
Lister les modules disponibles :

Get-WindowsCapability -Name RSAT -Online | Select-Object -Property Name, DisplayName*

```
PS C:\Windows\System32> Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property Name, DisplayName

Name                                                  DisplayName
----                                                  -----------
Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0          RSAT : outils Active Directory Domain Services Directory et services LDS (Lightweight Directory Services)
Rsat.AzureStack.HCI.Management.Tools~~~~0.0.1.0       RSAT: PowerShell module for Azure Stack HCI
Rsat.BitLocker.Recovery.Tools~~~~0.0.1.0              RSAT : utilitaires d'administration de chiffrement de lecteur BitLocker
Rsat.CertificateServices.Tools~~~~0.0.1.0             RSAT : outils des services de certificats Active Directory
Rsat.DHCP.Tools~~~~0.0.1.0                            RSAT : outils du serveur DHCP
Rsat.Dns.Tools~~~~0.0.1.0                             RSAT : outils du serveur DNS
Rsat.FailoverCluster.Management.Tools~~~~0.0.1.0      RSAT : outils de clustering de basculement
Rsat.FileServices.Tools~~~~0.0.1.0                    RSAT : outils de services de fichiers
Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0          RSAT : outils de gestion de stratégie de groupe
Rsat.IPAM.Client.Tools~~~~0.0.1.0                     RSAT : client Gestion des adresses IP (IPAM)
Rsat.LLDP.Tools~~~~0.0.1.0                            RSAT : outils LLDP Data Center Bridging
Rsat.NetworkController.Tools~~~~0.0.1.0               RSAT : outils de gestion du contrôleur de réseau
Rsat.NetworkLoadBalancing.Tools~~~~0.0.1.0            RSAT : outils d'équilibrage de charge réseau
Rsat.RemoteAccess.Management.Tools~~~~0.0.1.0         RSAT : outils de gestion de l'accès à distance
Rsat.RemoteDesktop.Services.Tools~~~~0.0.1.0          RSAT : outils des services Bureau à distance
Rsat.ServerManager.Tools~~~~0.0.1.0                   RSAT : gestionnaire de serveur
Rsat.StorageMigrationService.Management.Tools~~~~0.0.1.0 RSAT : Outils de gestion des services de migration du stockage
Rsat.StorageReplica.Tools~~~~0.0.1.0                  Outils d'administration de serveur distant : module de réplica de stockage pour Windows PowerShell
Rsat.SystemInsights.Management.Tools~~~~0.0.1.0       RSAT : module Informations système pour Windows PowerShell
Rsat.VolumeActivation.Tools~~~~0.0.1.0                RSAT : outils d'activation en volume
Rsat.WSUS.Tools~~~~0.0.1.0                            RSAT : outils Windows Server Update Services
```

Installer ensuite les modules nécessaires selon le tier.

Chaque installation retourne Online : True et RestartNeeded : False, confirmant que le module est bien activé sans nécessiter de redémarrage.

Pour le Tier 1 (administration des serveurs applicatifs et services de fichiers) :

Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"
Add-WindowsCapability -Online -Name "Rsat.FileServices.Tools~~~~0.0.1.0"
Add-WindowsCapability -Online -Name "Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0"

```
PS C:\Users\Administrateur> Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

```
PS C:\Windows\System32> Add-WindowsCapability -Online -Name "Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

```
PS C:\Users\Administrateur> Add-WindowsCapability -Online -Name "Rsat.FileServices.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

Pour le Tier 0 (administration des contrôleurs de domaine) :

Add-WindowsCapability -Online -Name "Rsat.DHCP.Tools~~~~0.0.1.0"
Add-WindowsCapability -Online -Name "Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0"
Add-WindowsCapability -Online -Name "Rsat.Dns.Tools~~~~0.0.1.0"

```
PS C:\Windows\System32> Add-WindowsCapability -Online -Name "Rsat.Dns.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

```
PS C:\Windows\System32> Add-WindowsCapability -Online -Name "Rsat.DHCP.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

```
PS C:\Users\Administrateur> Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

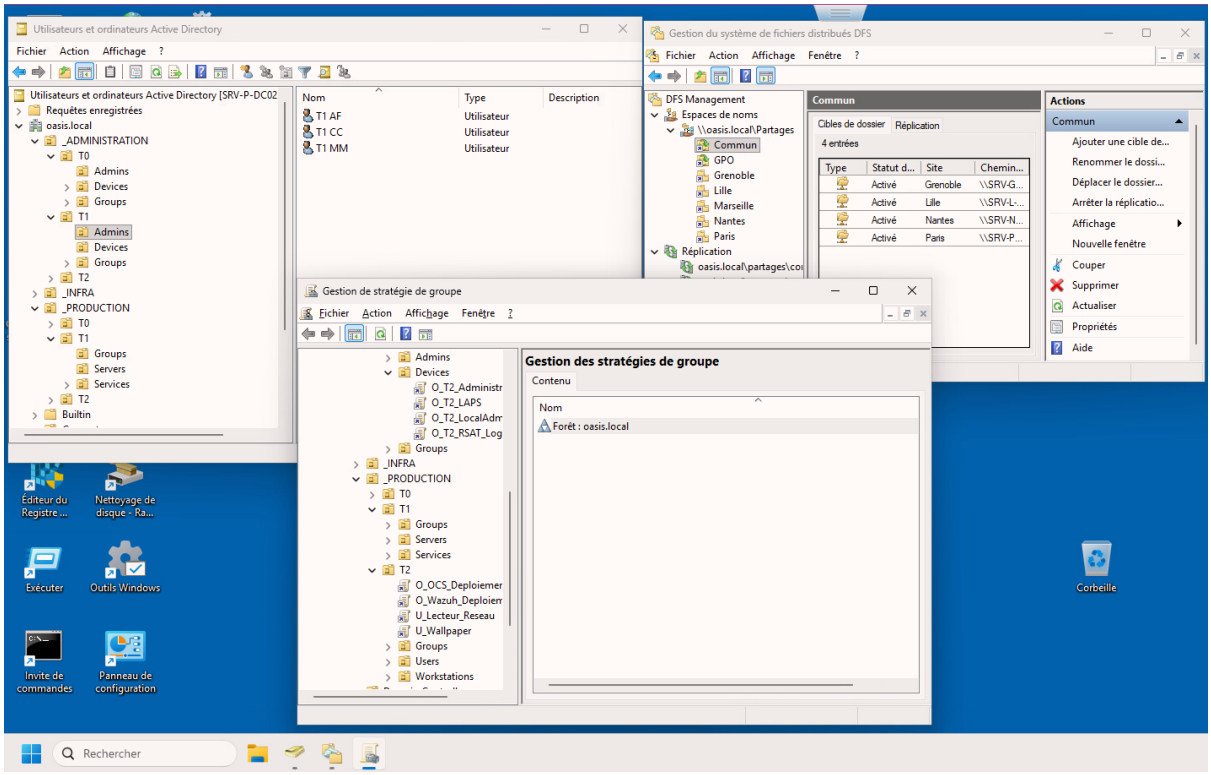
```
PS C:\Windows\System32> Add-WindowsCapability -Online -Name "Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

Pour le Tier 2 (administration des postes de travail) :

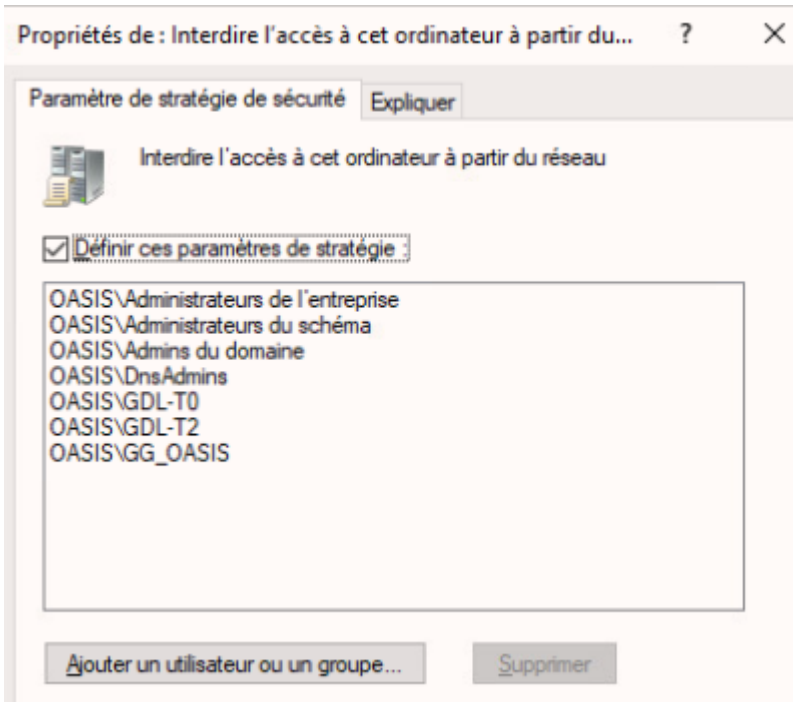
Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"

```
PS C:\Users\Administrateur> Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

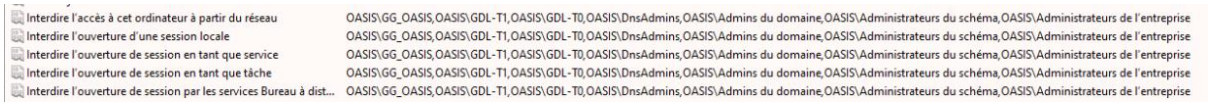
Administration depuis un poste RSAT T1 :

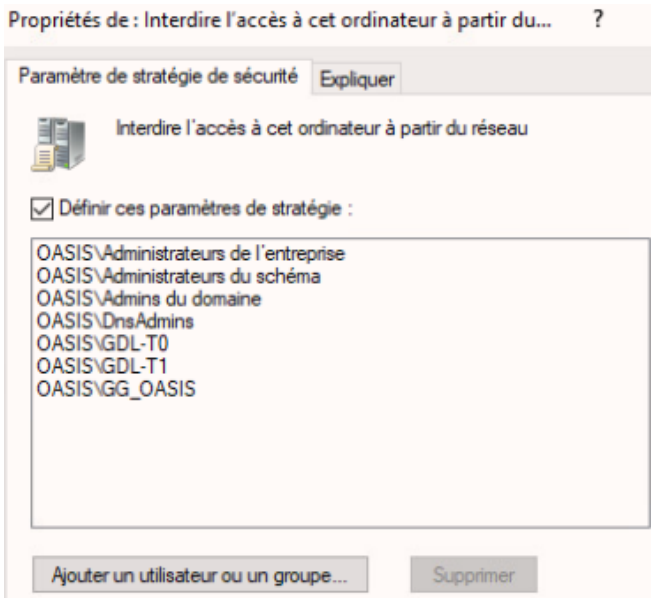


Afin d'interdire aux utilisateurs du domaine de se connecter sur les postes RSAT, les GPO de restriction de connexion sont complétées.
Pour les postes RSAT T1, ajouter dans chaque paramètre d'interdiction de connexion les groupes GG_OASIS, GDL-T0, GDL-T2, DnsAdmins, Administrateurs de l'entreprise, Administrateurs du schéma et Admins du domaine. Seuls les membres de GDL-T1 peuvent ainsi ouvrir une session sur ces postes.

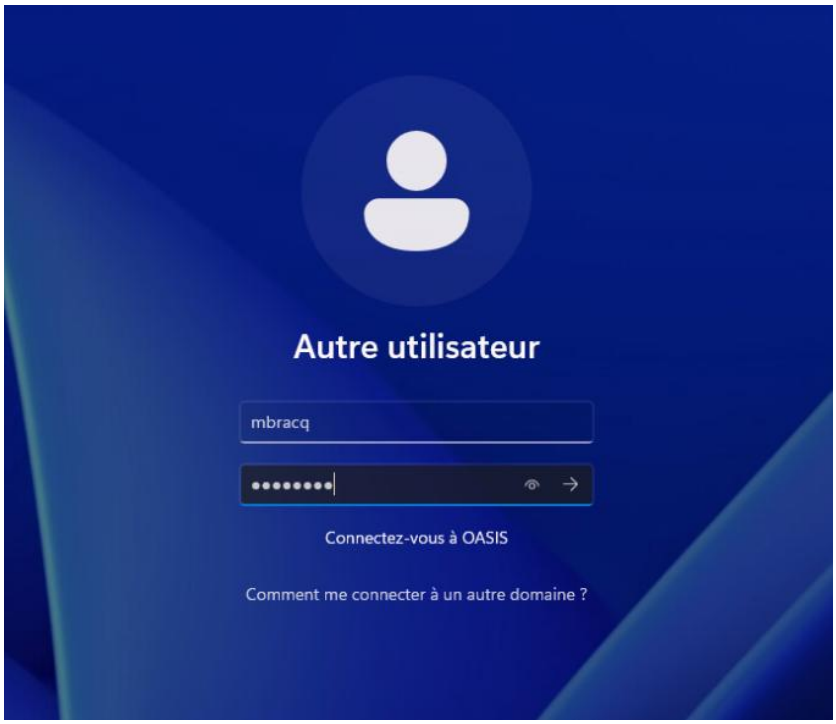


Pour les postes RSAT T2, créer une GPO dédiée et appliquer la même logique en remplaçant GDL-T2 par GDL-T1 dans la liste des groupes interdits. Seuls les membres de GDL-T2 peuvent se connecter sur les postes RSAT T2.

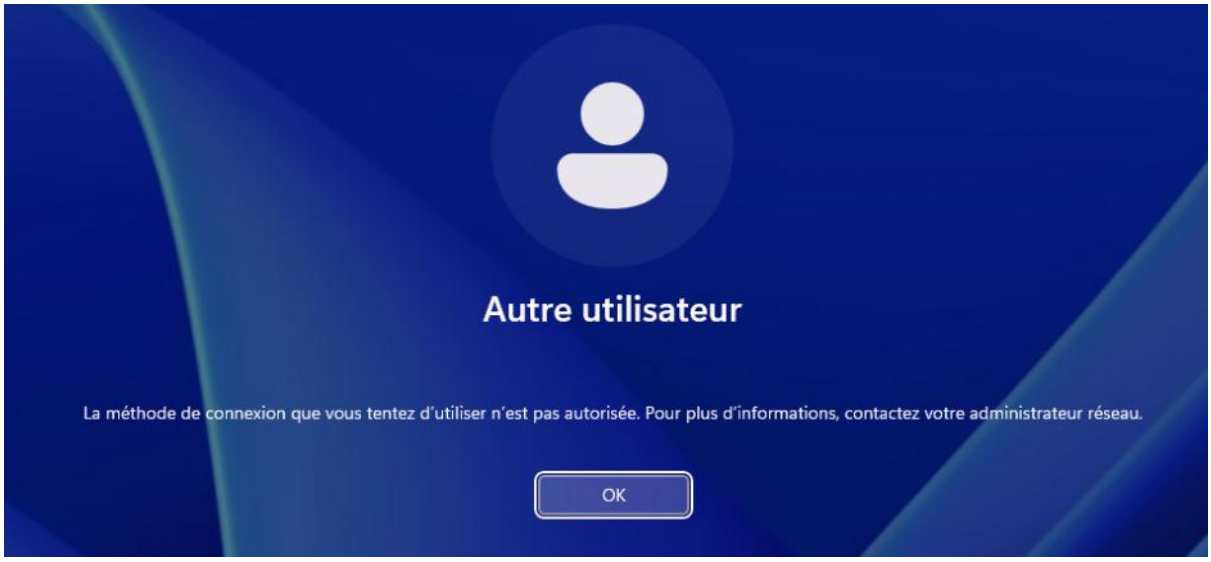




Tentative de connexion avec le compte utilisateur mbracq (compte domaine standard, hors de tout groupe d'administration) sur un poste RSAT.



La connexion est bloquée avec le message : « La méthode de connexion que vous tentez d'utiliser n'est pas autorisée. » La configuration est fonctionnelle.



9.1. Conclusion

Les outils RSAT sont installés et fonctionnels sur les postes dédiés de chaque tier, placés dans les OUs **_ADMINISTRATION/T{x}/Devices**. Les modules nécessaires à chaque tier ont été installés via PowerShell.

L'administration depuis un poste RSAT T1 est fonctionnelle, les consoles Utilisateurs et ordinateurs Active Directory, Gestion des stratégies de groupe et Gestion du système de fichiers distribués sont accessibles et opérationnelles depuis le compte t1.

Les GPO de restriction de connexion sur les postes RSAT sont effectives. Une tentative de connexion avec un compte utilisateur standard du domaine et administrateur du domaine sur un poste RSAT est refusée, confirmant que seuls les administrateurs du tier correspondant peuvent accéder à ces postes.

10. Mise en place de LAPS

LAPS (Local Administrator Password Solution) est une solution Microsoft intégrée nativement à Windows depuis la mise à jour d'avril 2023. Elle permet de gérer automatiquement le mot de passe d'un compte administrateur local sur chaque machine jointe au domaine, en le stockant de manière chiffrée dans Active Directory.

Vérifier la présence du module LAPS :

Get-Command -Module LAPS

Le module expose les cmdlets nécessaires :

Update-LapsADSchema, Set-LapsADComputerSelfPermission, Set-LapsADReadPasswordPermission, Set-LapsADResetPasswordPermission, Get-LapsADPassword, etc…

```
PS C:\Users\Administrateur> Get-Command -Module LAPS

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Get-LapsAADPassword                                1.0.0.0    LAPS
Function        Get-LapsDiagnostics                                1.0.0.0    LAPS
Cmdlet          Find-LapsADExtendedRights                          1.0.0.0    LAPS
Cmdlet          Get-LapsADPassword                                 1.0.0.0    LAPS
Cmdlet          Invoke-LapsPolicyProcessing                        1.0.0.0    LAPS
Cmdlet          Reset-LapsPassword                                 1.0.0.0    LAPS
Cmdlet          Set-LapsADAuditing                                 1.0.0.0    LAPS
Cmdlet          Set-LapsADComputerSelfPermission                   1.0.0.0    LAPS
Cmdlet          Set-LapsADPasswordExpirationTime                   1.0.0.0    LAPS
Cmdlet          Set-LapsADReadPasswordPermission                   1.0.0.0    LAPS
Cmdlet          Set-LapsADResetPasswordPermission                  1.0.0.0    LAPS
Cmdlet          Update-LapsADSchema                                1.0.0.0    LAPS
```

Importer le module puis étendre le schéma AD pour ajouter les attributs LAPS :

Import-Module LAPS
Update-LapsADSchema -Verbose

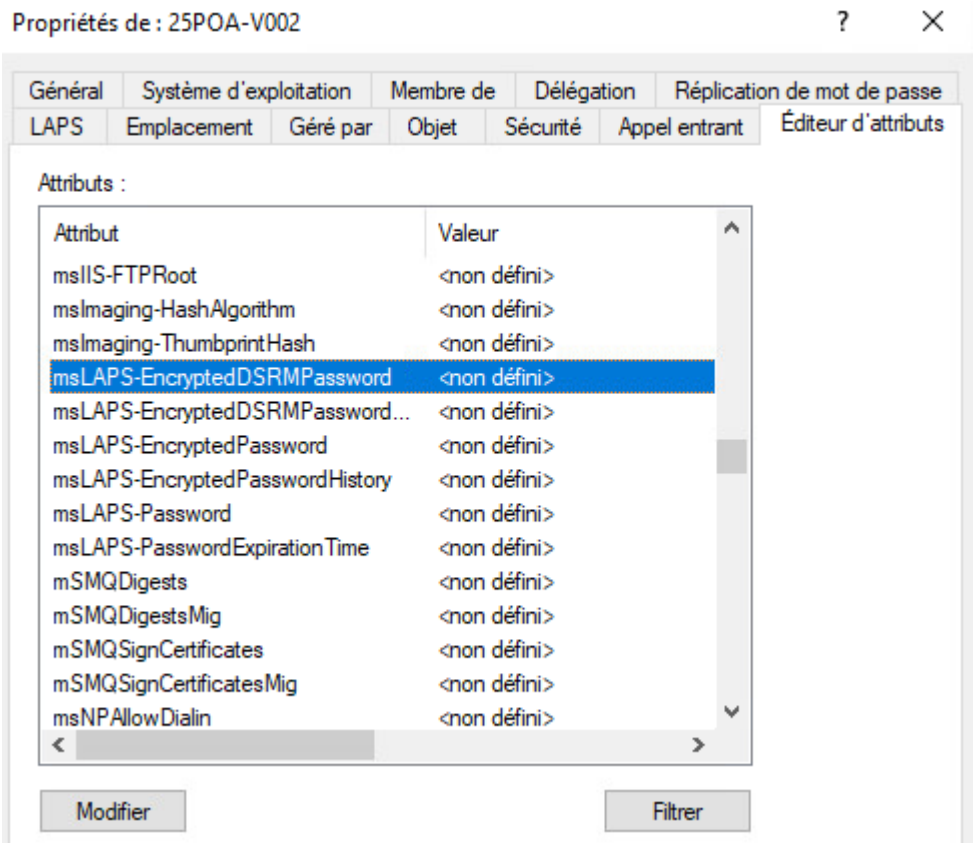
```
PS C:\Users\Administrateur> Import-Module LAPS
PS C:\Users\Administrateur> Update-LapsADSchema -Verbose
```

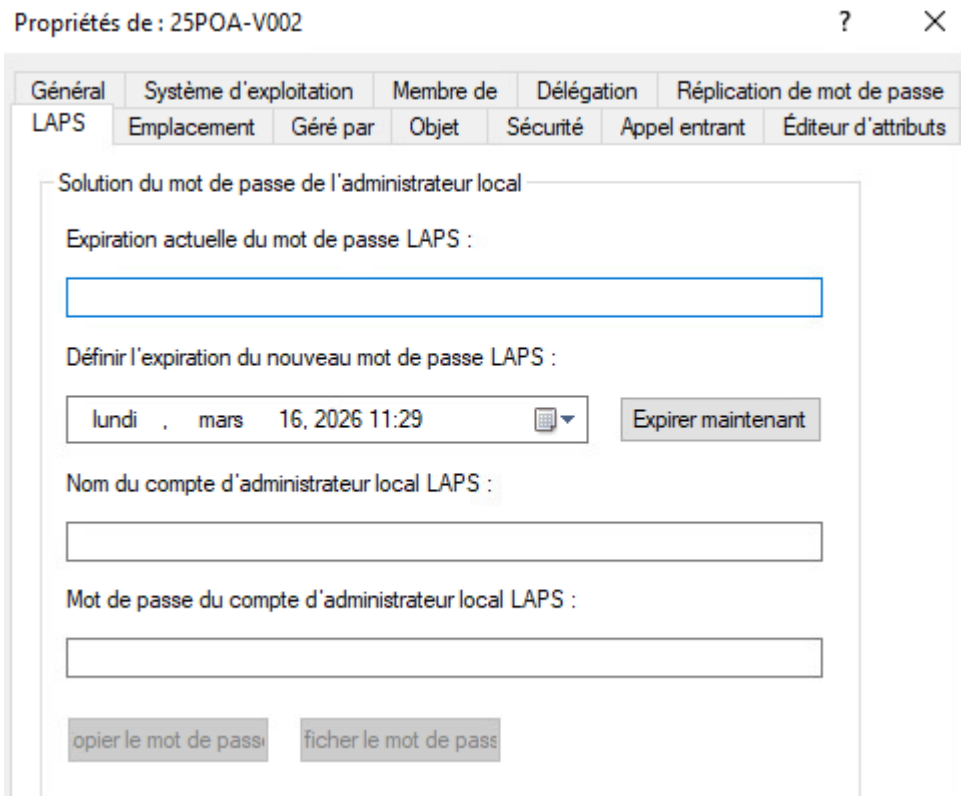
L'opération confirme que les attributs msLAPS-Password, msLAPS-EncryptedPassword, msLAPS-PasswordExpirationTime et msLAPS-EncryptedDSRMPassword ont bien été ajoutés au schéma du domaine oasis.local.

```
PS C:\Users\Administrateur> Import-Module LAPS
PS C:\Users\Administrateur> Update-LapsADSchema -Verbose
COMMENTAIRES : BeginProcessing started
COMMENTAIRES : Creating LDAP binding to specified domain controller 'localhost'
COMMENTAIRES : Port not specified - will default to 389
COMMENTAIRES : Successfully created LDAP binding
COMMENTAIRES : Verifying that current machine is AD domain-joined
COMMENTAIRES : Success: current machine is domain-joined to 'OASIS'
COMMENTAIRES : Running on a domain controller - verifying that the current process is elevated
COMMENTAIRES : Success: current process is elevated
COMMENTAIRES : Calling DC-locator to locate a DC in the  domain
COMMENTAIRES : DC-locator succeeded:
COMMENTAIRES : Name:SRV-P-DC01.oasis.local Address:\\172.16.30.10 AddressType:1 DomainGuid:c5c40292-75d3-49d2-b1bc-2476e872b3a8 DomainDnsName:oasis.local
ForestDnsName:oasis.local Flags:0xe003f3fd DcSiteName:Paris ClientSiteName:Paris
COMMENTAIRES : Binding to domain controller SRV-P-DC01.oasis.local
COMMENTAIRES : Bound LDAP connection to schema FSMO SRV-P-DC01.oasis.local
COMMENTAIRES : Successfully bound to domain controller:
COMMENTAIRES :  DC: SRV-P-DC01.oasis.local
COMMENTAIRES :  DC functional level: 7
COMMENTAIRES :  Domain info:
COMMENTAIRES :    Domain DNS name: oasis.local
COMMENTAIRES :    Domain NC: DC=oasis,DC=local
COMMENTAIRES :    Domain functional level: 7
COMMENTAIRES :  Forest info:
COMMENTAIRES :    Forest DNS name: oasis.local
COMMENTAIRES :    Forest NC: DC=oasis,DC=local
COMMENTAIRES :    Config NC: CN=Configuration,DC=oasis,DC=local
COMMENTAIRES :    Schema NC: CN=Schema,CN=Configuration,DC=oasis,DC=local
COMMENTAIRES :    Forest functional level: 7
COMMENTAIRES : BeginProcessing completed
COMMENTAIRES :
COMMENTAIRES : ProcessRecord started
COMMENTAIRES : Invoking schemaUpdateNow on DC
COMMENTAIRES : Successfully invoked schemaUpdateNow on DC
COMMENTAIRES :
COMMENTAIRES : Issuing LDAP search request for 'CN=ms-LAPS-Password,CN=Schema,CN=Configuration,DC=oasis,DC=local'
COMMENTAIRES : Did not find the 'CN=ms-LAPS-Password,CN=Schema,CN=Configuration,DC=oasis,DC=local' schema attribute in AD

The 'ms-LAPS-Password' schema attribute needs to be added to the AD schema.
Do you want to proceed?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») :
```

```
The 'ms-LAPS-Password' schema attribute needs to be added to the AD schema.
Do you want to proceed?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : T
```

Vérifier leur présence dans l'onglet « Éditeur d'attributs » d'un objet ordinateur, les attributs LAPS sont bien visibles, initialement non définis.





Donner aux machines le droit de mettre à jour leur propre mot de passe LAPS dans AD (T2) :

Set-LapsADComputerSelfPermission `
-Identity "OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local"

```
PS C:\Users\Administrateur> Set-LapsADComputerSelfPermission -Identity "OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local"

Name         DistinguishedName
----         -----------------
Workstations OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local
```

Donner au groupe GG-T2-Administrators le droit de lire les mots de passe LAPS T2 :

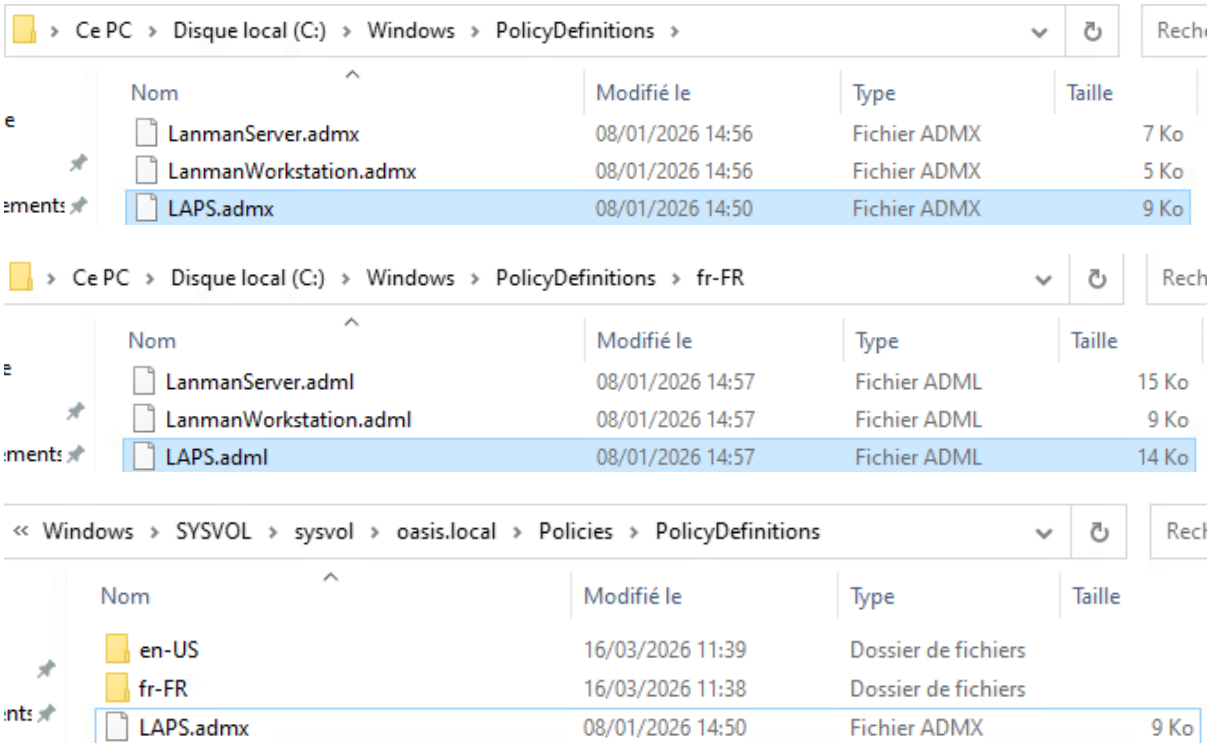
```
PS C:\Users\Administrateur.OASIS> Set-LapsADReadPasswordPermission `
>> -Identity "OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T2-Administrators"

Name         DistinguishedName
----         -----------------
Workstations OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local
```

Donner au groupe GG-T2-Managers le droit de lire et réinitialiser les mots de passe LAPS T2 :

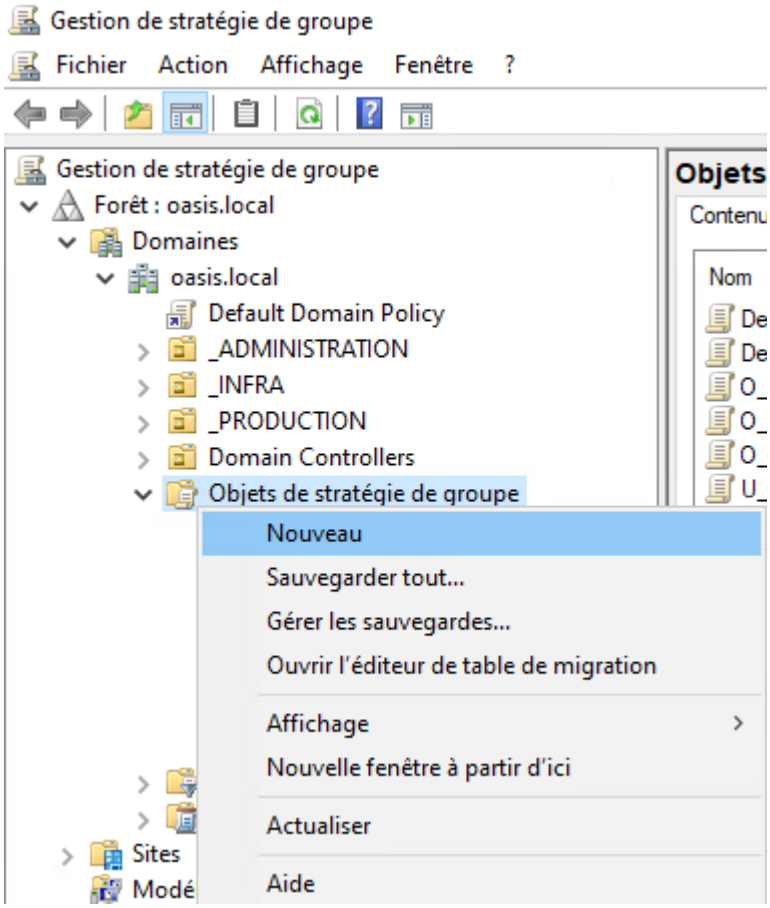
```
PS C:\Users\Administrateur.OASIS> Set-LapsADReadPasswordPermission `
>> -Identity "OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T2-Managers"

Name         DistinguishedName
----         -----------------
Workstations OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local
```

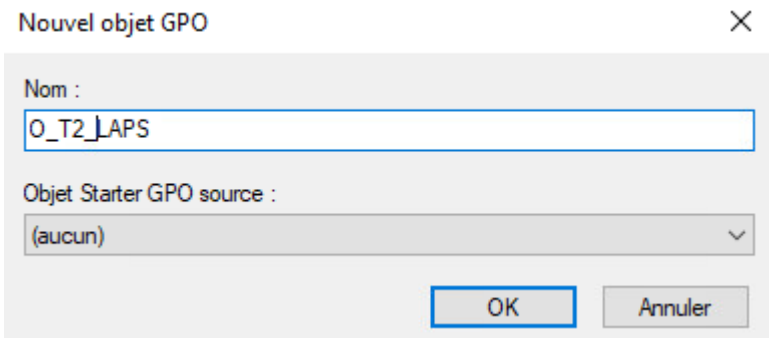
```
PS C:\Users\Administrateur.OASIS> Set-LapsADResetPasswordPermission `
>> -Identity "OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T2-Managers"

Name         DistinguishedName
----         -----------------
Workstations OU=Workstations,OU=T2,OU=_PRODUCTION,DC=oasis,DC=local
```

Importer les modèles d'administration LAPS dans le magasin central SYSVOL. Les fichiers LAPS.admx et LAPS.adml sont copiés respectivement dans SYSVOL\oasis.local\Policies\PolicyDefinitions et dans le sous-dossier de langue fr-FR.

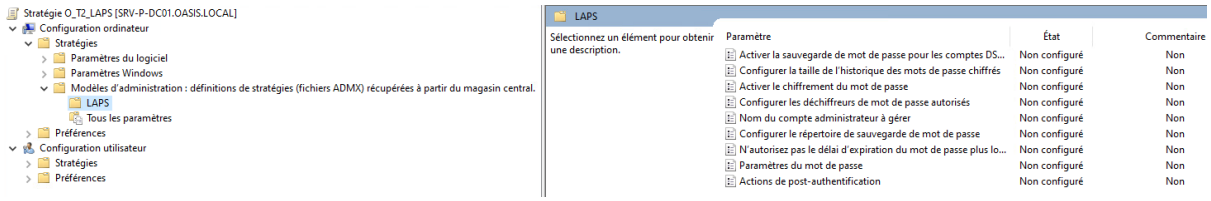


Dans la console « Gestion de stratégie de groupe », créer une GPO O_T2_LAPS liée à _PRODUCTION/T2/Workstations



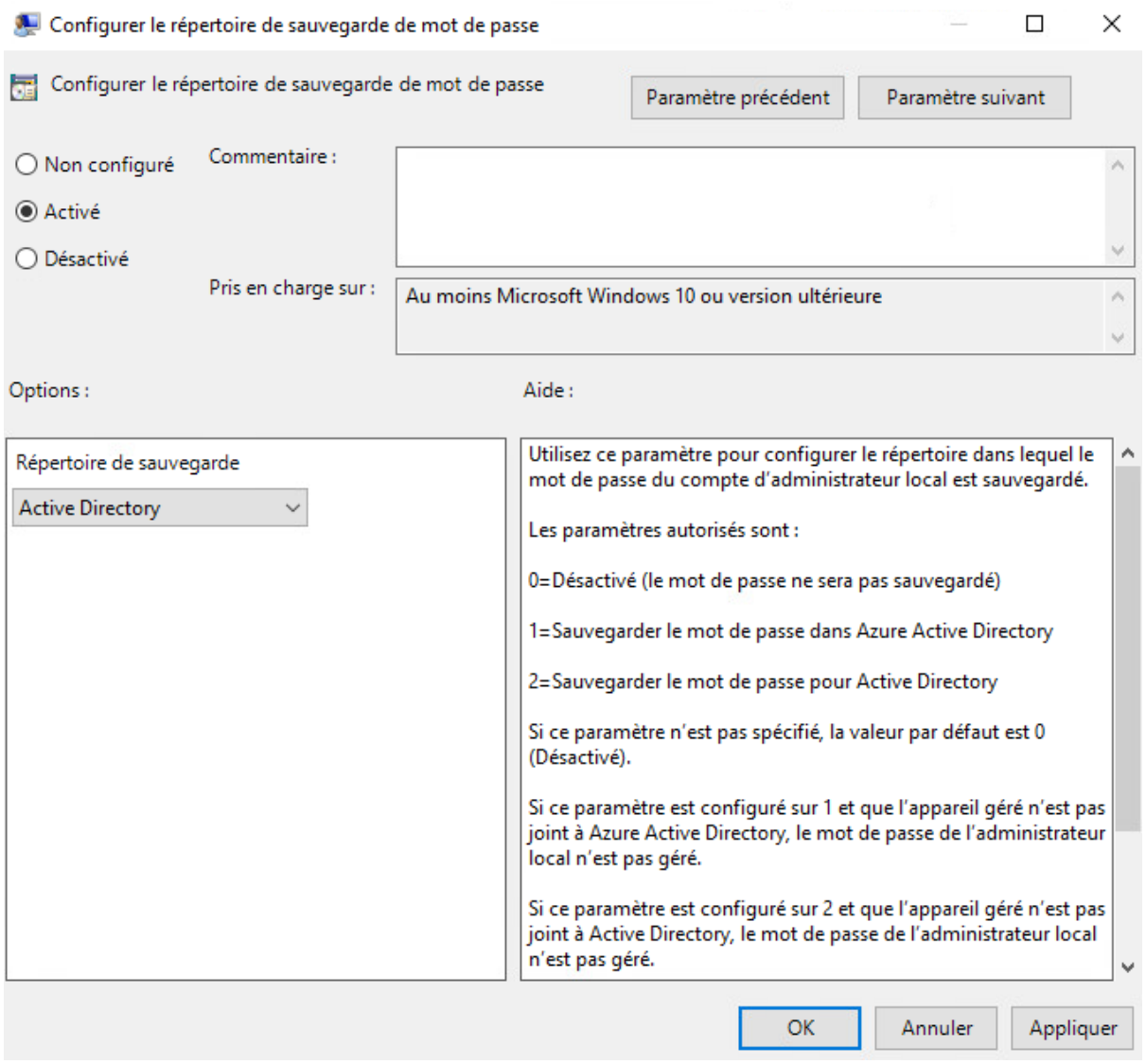


Se rendre dans Configuration ordinateur → Stratégies → Modèles d'administration → LAPS.



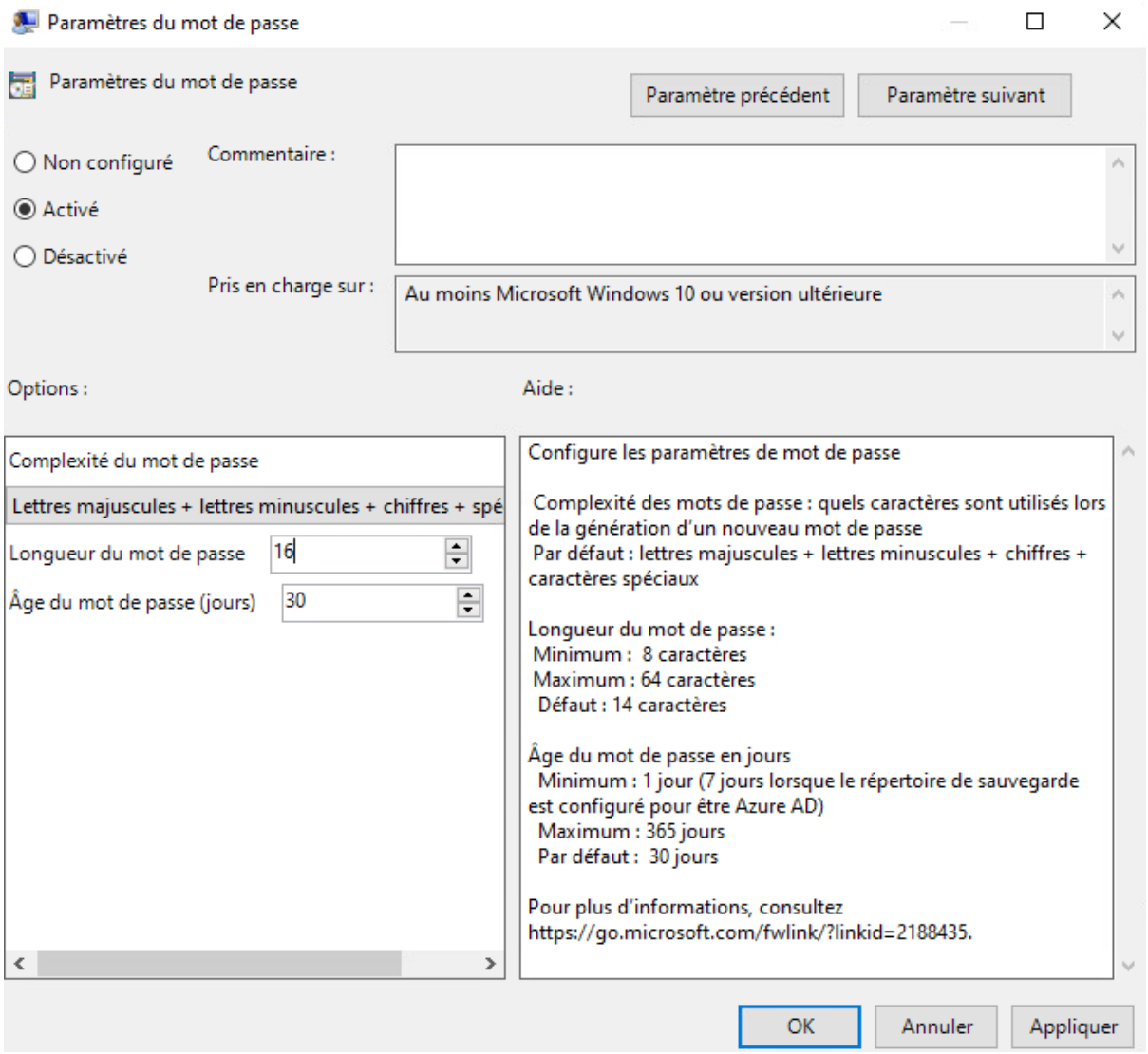
Configurer le répertoire de sauvegarde du mot de passe : Activé

- Active Directory



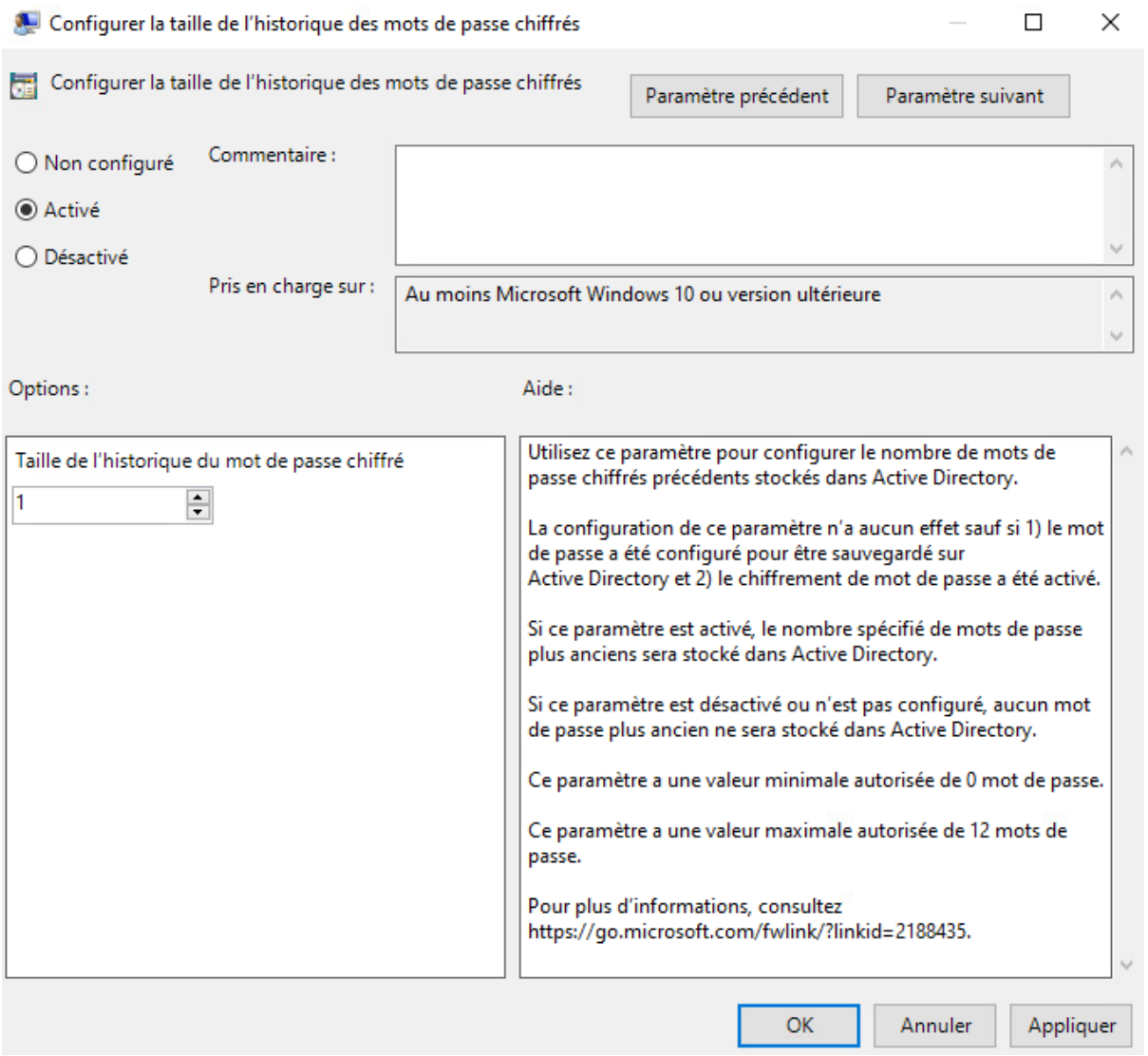
Paramètres du mot de passe : Activé

- Complexité : Lettres majuscules + lettres minuscules + chiffres + caractères spéciaux
- Longueur : 16 caractères
- Âge maximum : 30 jours

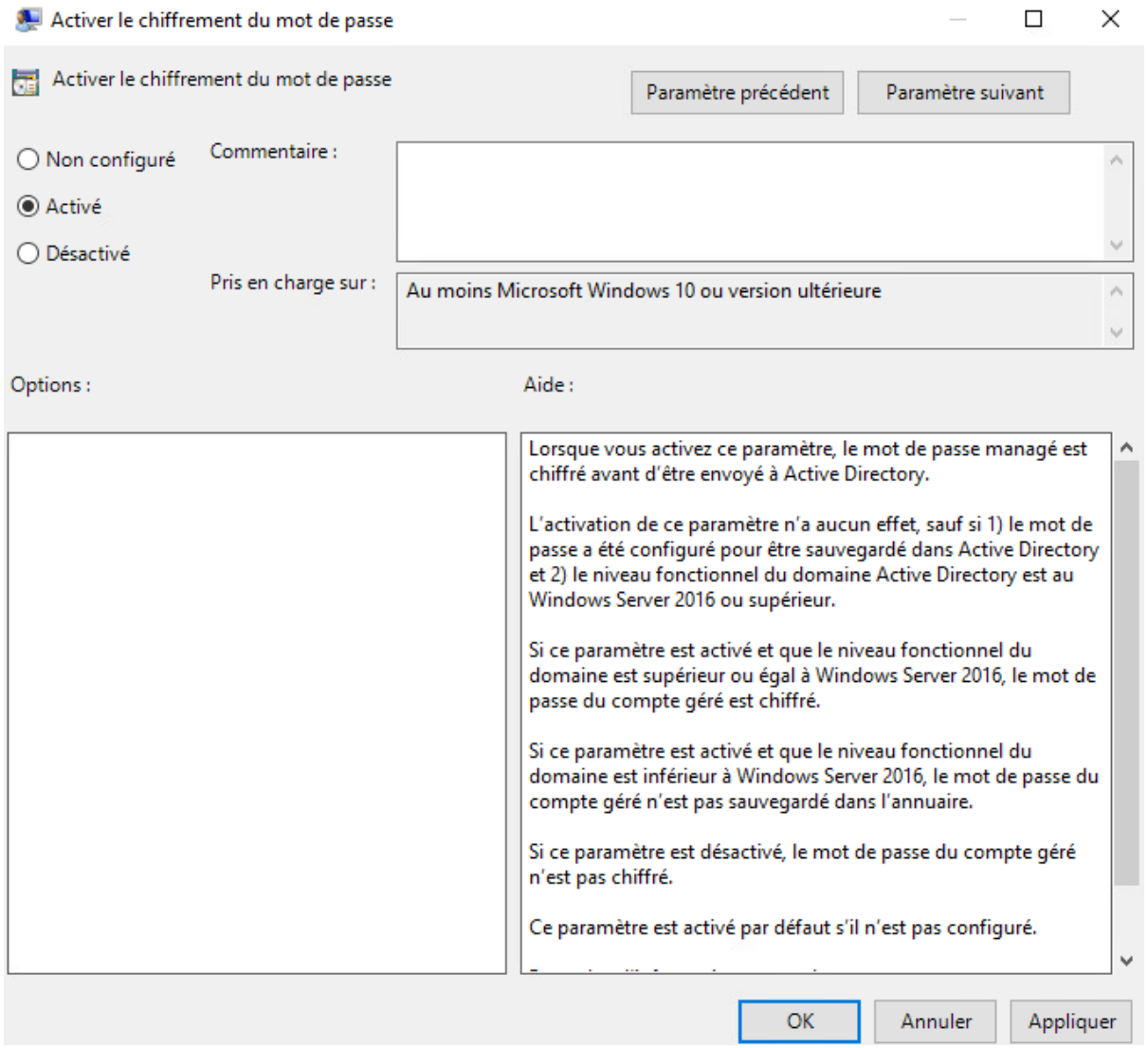


Configurer la taille de l'historique des mots de passe chiffrés : Activé

- Valeur : 1

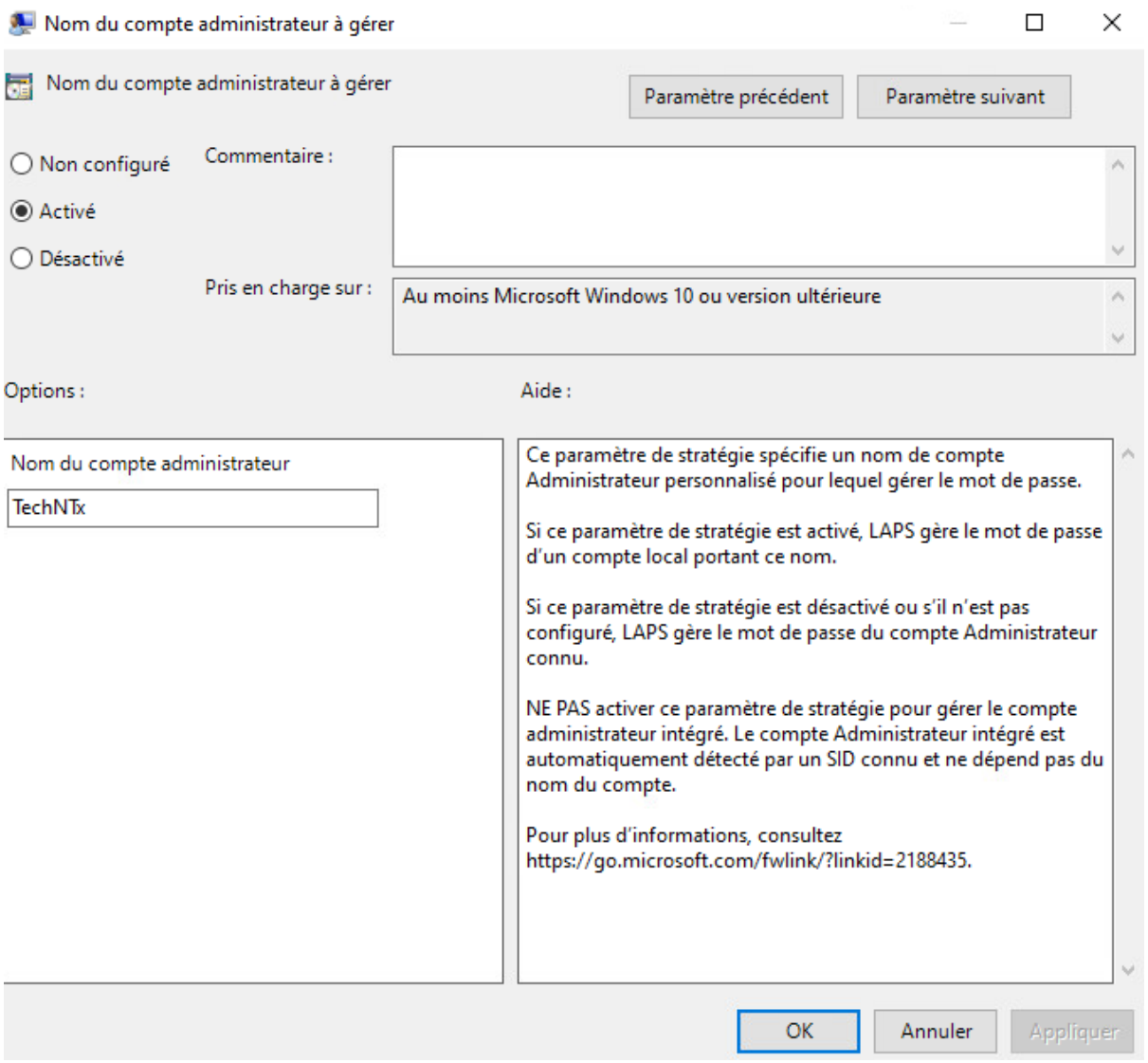


Activer le chiffrement du mot de passe : Activé



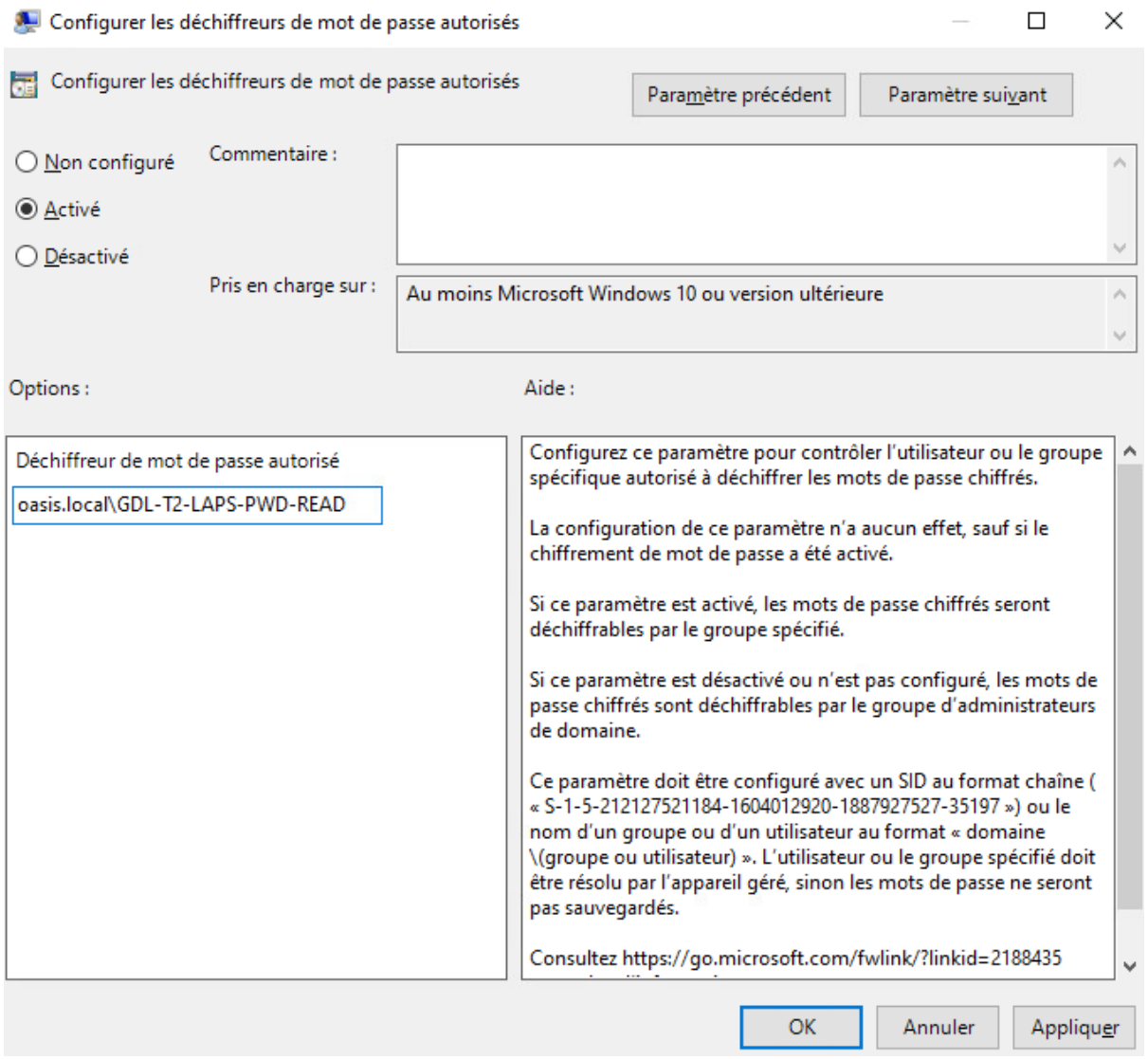
Nom du compte administrateur à gérer : Activé

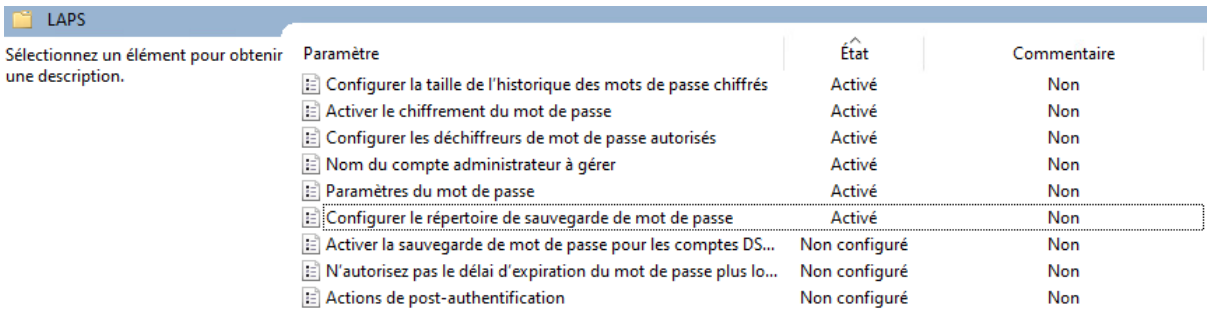
- TechNTx



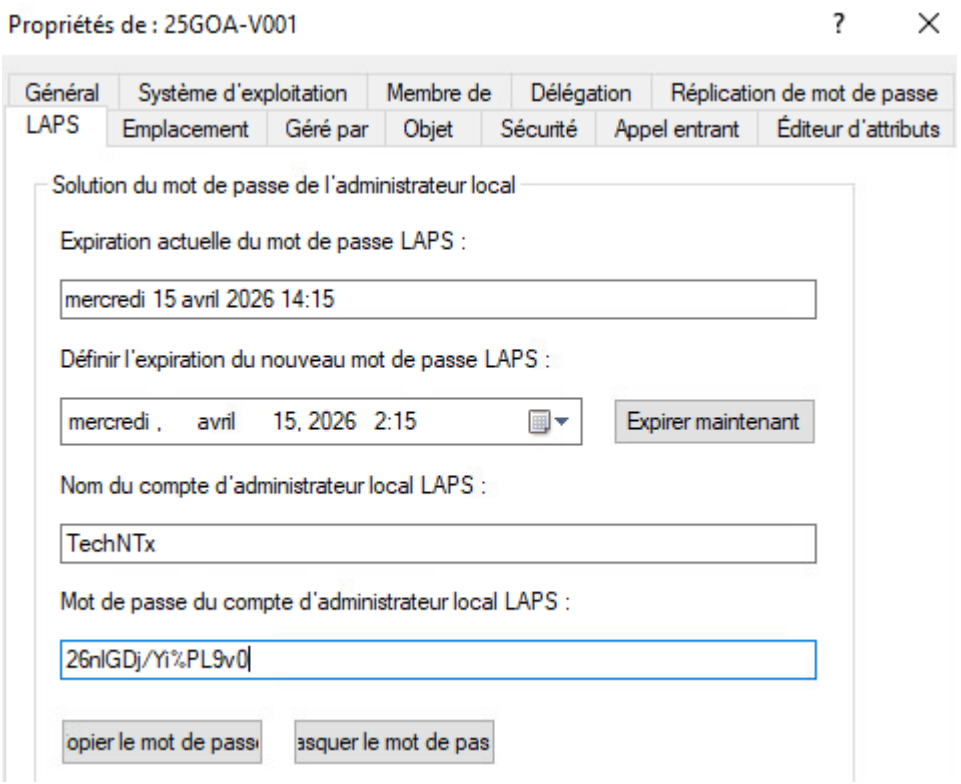
Configurer les déchiffreurs de mot de passe autorisés : Activé

- oasis.local\GDL-T2-LAPS-PWD-READ



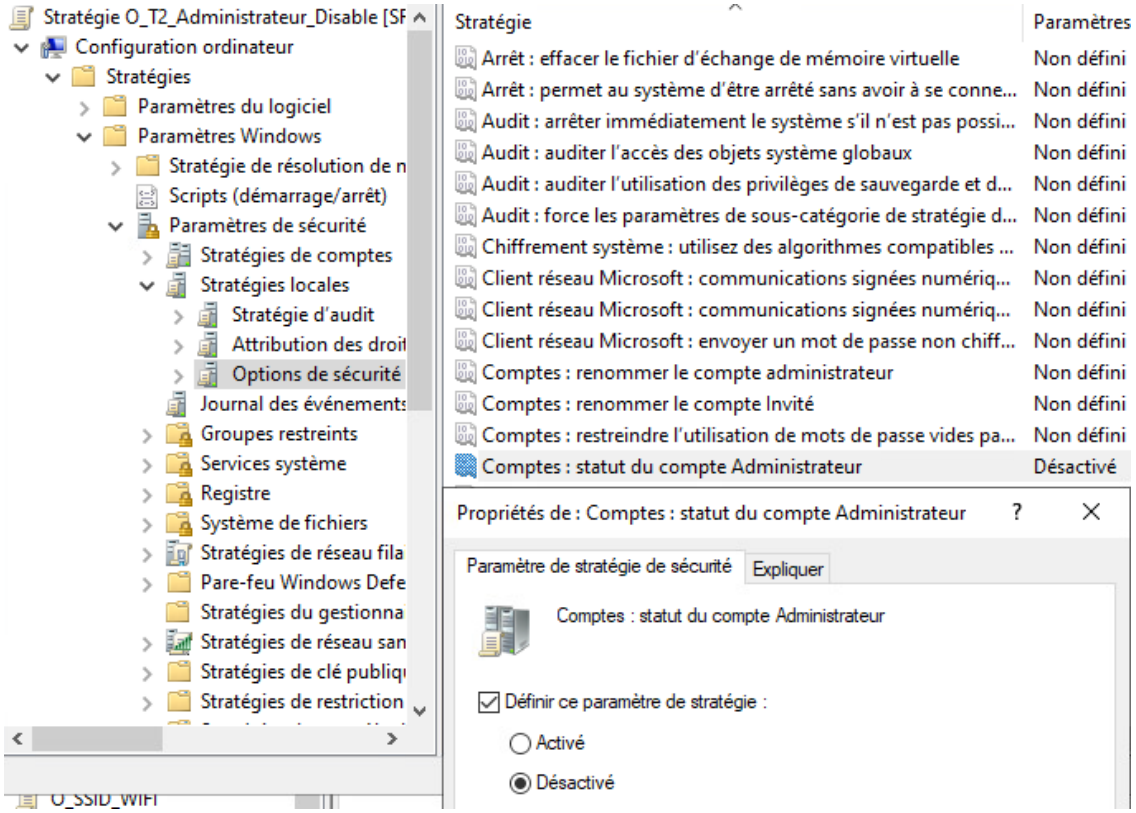


Sur le poste 25GOA-V001 (T2), l'onglet LAPS des propriétés de l'objet ordinateur dans ADUC (Active Directory Users and Computers) affiche :



Désactiver le compte Administrateur intégré : GPO O_T2_Administrateur_Disable :

Statut du compte Administrateur → Désactivé



LAPS est fonctionnel sur le Tier 2, le mot de passe du compte TechNTx est géré automatiquement et stocké chiffré dans Active Directory, accessible uniquement aux groupes habilités du tier.

Pour le Tier 1, appliquer les permissions LAPS sur l'OU _PRODUCTION/T1/Servers de la même façon que ci-dessus pour le Tier 2 :

Set-LapsADComputerSelfPermission `
-Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local"

```
PS C:\Users\Administrateur.OASIS> Set-LapsADComputerSelfPermission -Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local"

Name    DistinguishedName
----    -----------------
Servers OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local
```

Set-LapsADReadPasswordPermission `
-Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local" `
-AllowedPrincipals "OASIS.LOCAL\GG-T1-Administrators"

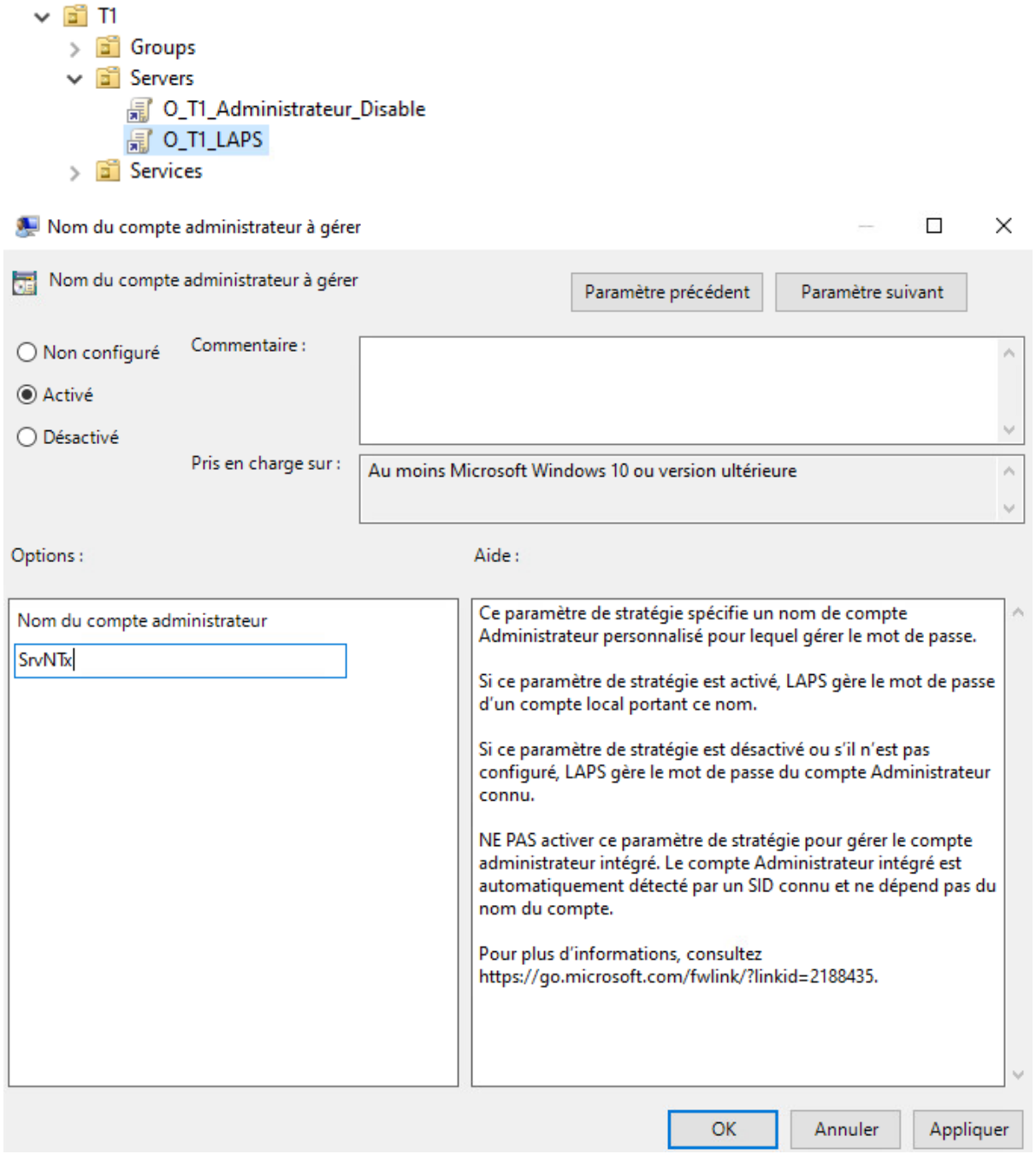
```
PS C:\Users\Administrateur.OASIS> Set-LapsADReadPasswordPermission `
>> -Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T1-Administrators"

Name    DistinguishedName
----    -----------------
Servers OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local
```

Set-LapsADReadPasswordPermission `
-Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local" `
-AllowedPrincipals "OASIS.LOCAL\GG-T1-Managers"

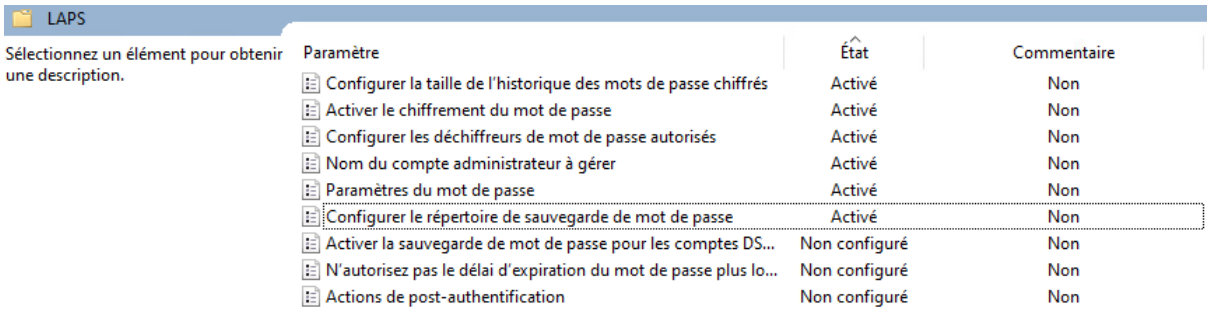
Set-LapsADResetPasswordPermission `
-Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local" `
-AllowedPrincipals "OASIS.LOCAL\GG-T1-Managers"

```
PS C:\Users\Administrateur.OASIS> Set-LapsADReadPasswordPermission `
>> -Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T1-Managers"

Name    DistinguishedName
----    -----------------
Servers OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local


PS C:\Users\Administrateur.OASIS> Set-LapsADResetPasswordPermission `
>> -Identity "OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T1-Managers"

Name    DistinguishedName
----    -----------------
Servers OU=Servers,OU=T1,OU=_PRODUCTION,DC=oasis,DC=local
```

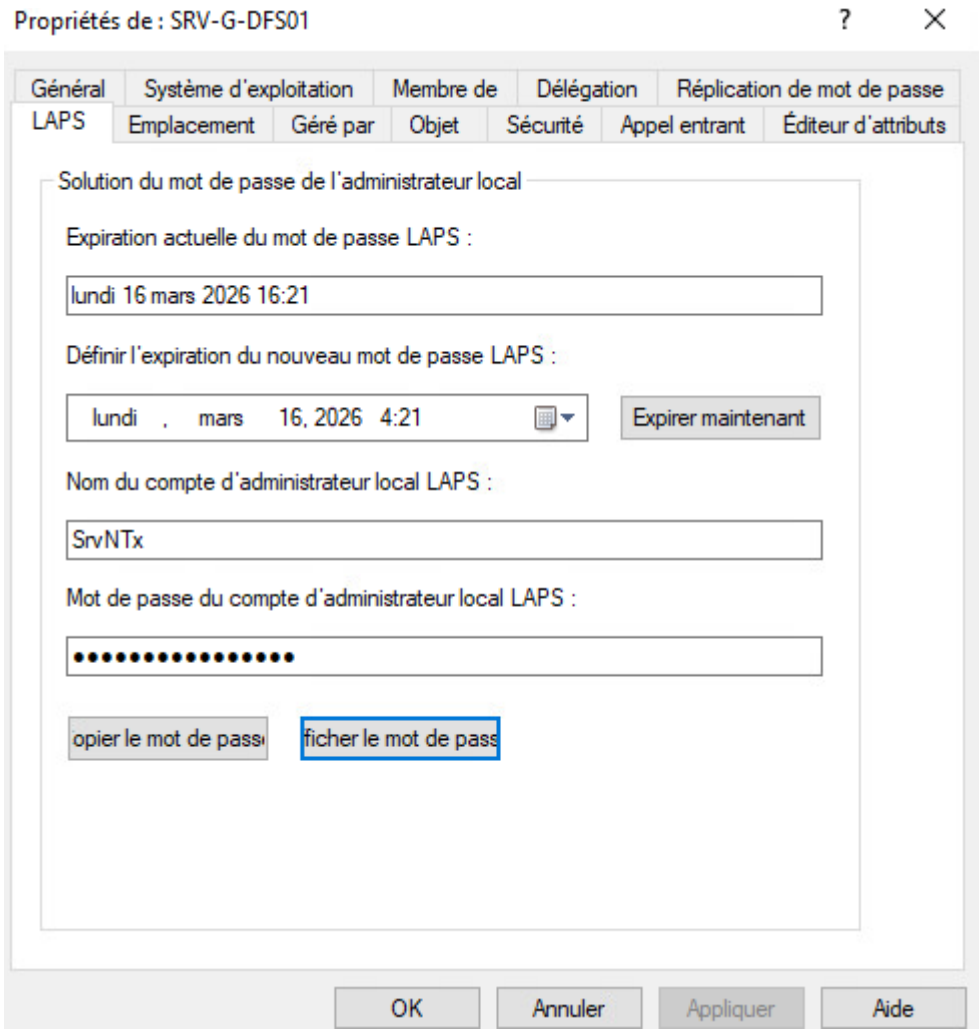
Créer la GPO O_T1_LAPS liée à _PRODUCTION/T1/Servers avec les mêmes paramètres que T2, en adaptant uniquement le nom du compte administrateur à gérer : SrvNTx.



Les paramètres actifs dans la GPO T1 sont identiques à T2 :
Chiffrement activé, historique à 1, longueur 16 caractères, complexité maximale, durée 30 jours, répertoire Active Directory, déchiffreur oasis.local\GDL-T1-LAPS-PWD-READ.



Sur le serveur SRV-G-DFS01, l'onglet LAPS des propriétés de l'objet ordinateur dans ADUC affiche :



Appliquer les mêmes permissions sur les postes RSAT T1 et T2 dans _ADMINISTRATION/T{x}/Devices :

```
PS C:\Users\Administrateur> Set-LapsADComputerSelfPermission -Identity "OU=Devices,OU=T1,OU=_ADMINISTRATION,DC=oasis,DC=local"

Name    DistinguishedName
----    -----------------
Devices OU=Devices,OU=T1,OU=_ADMINISTRATION,DC=oasis,DC=local
```

```
PS C:\Users\Administrateur> Set-LapsADReadPasswordPermission `
>> -Identity "OU=Devices,OU=T1,OU=_ADMINISTRATION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T1-managers"

Name    DistinguishedName
----    -----------------
Devices OU=Devices,OU=T1,OU=_ADMINISTRATION,DC=oasis,DC=local

PS C:\Users\Administrateur> Set-LapsADResetPasswordPermission `
>> -Identity "OU=Devices,OU=T1,OU=_ADMINISTRATION,DC=oasis,DC=local" `
>> -AllowedPrincipals "OASIS.LOCAL\GG-T1-managers"

Name    DistinguishedName
----    -----------------
Devices OU=Devices,OU=T1,OU=_ADMINISTRATION,DC=oasis,DC=local
```

LAPS est fonctionnel sur le Tier 1, le mot de passe du compte SrvNTx est géré automatiquement et stocké chiffré dans Active Directory, accessible uniquement aux groupes habilités du tier.

10.1. Conclusion

Le déploiement de LAPS est fonctionnel sur les Tiers 1 et 2. Les attributs LAPS sont bien présents dans le schéma Active Directory suite à la mise à jour du schéma, visibles dans l'onglet « Éditeur d'attributs » de chaque objet ordinateur concerné.

Les permissions ont été correctement appliquées sur les OUs cibles, les machines disposent du droit de mettre à jour leur propre mot de passe dans l'annuaire, et seuls les groupes habilités **GDL-T2-LAPS-PWD-READ** et **GDL-T1-LAPS-PWD-READ** peuvent lire et réinitialiser les mots de passe de leur tier respectif.

Les GPO **O_T2_LAPS** et **O_T1_LAPS** sont appliquées correctement. Sur le poste 25GOA-V001 (T2), l'onglet LAPS dans ADUC affiche bien le compte géré TechNTx avec une date d'expiration et un mot de passe chiffré visible uniquement par les membres autorisés. Sur le serveur SRV-G-DFS01 (T1), le compte géré SrvNTx est également fonctionnel avec une rotation automatique confirmée.

Les GPO **O_T2_Administrateur_Disable** et **O_T1_Administrateur_Disable** désactivent bien le compte Administrateur intégré sur les machines concernées, forçant l'utilisation exclusive du compte personnalisé géré par LAPS.

11.Axes d'améliorations

Séparation des partitions NTDS et SYSVOL sur les DC principaux

Lors de l'installation des contrôleurs de domaine secondaires en mode Server Core, certaines bonnes pratiques de l'ANSSI ont été appliquées en plaçant les dossiers NTDS et SYSVOL sur une partition dédiée distincte du système (lecteur F:). Cette configuration n'a pas été appliquée aux DC principaux qui ont été installés en amont du projet, avant l'intégration de ces recommandations. Une migration des fichiers NTDS et SYSVOL vers une partition dédiée sur ces serveurs constitue un axe d'amélioration prioritaire.

PAW pour l'administration T0

Les postes RSAT T0 sont des machines Windows 11 standards. Un poste PAW (Privileged Access Workstation) dédié à l'administration T0 devrait être durci : pas de navigation internet, pas de messagerie, pas d'accès aux ressources T1/T2, chiffrement BitLocker. Sans PAW, un administrateur T0 qui utilise son poste RSAT pour d'autres usages expose ses informations d'identification à des vols en mémoire.

Retrait de GG-T0-Managers des Admins du domaine

Actuellement, le groupe GG-T0-Managers est membre permanent du groupe Admins du domaine, ce qui a été mis en place dans le cadre de ce projet à des fins fonctionnelles et de démonstration. Cette configuration va à l'encontre du principe du moindre privilège : un compte T0 compromis donne un accès permanent et immédiat aux droits les plus élevés du domaine.
La bonne pratique consiste à maintenir le groupe Admins du domaine vide en permanence. Lorsqu'une opération nécessite ces droits, un compte est ajouté manuellement au groupe, l'opération est effectuée, puis le compte est immédiatement retiré. Cette approche JIT (Just-In-Time) réduit drastiquement la fenêtre d'exposition en cas de compromission.

Silos d'authentification

Le tiering repose uniquement sur des GPO de restriction de connexion, qui sont appliquées côté client et peuvent être contournées par un attaquant ayant déjà compromis un poste. Les silos d'authentification appliquent le cloisonnement directement au niveau des contrôleurs de domaine lors de l'émission des tickets d'authentification : un compte T0 ne peut physiquement pas obtenir un ticket pour une machine T2, quelle que soit la configuration du poste. C'est le complément indispensable du tiering déjà en place, car la protection ne repose plus sur une règle contournable mais sur une décision prise par le DC lui-même.

12. Conclusion

Ce projet avait pour objectif de concevoir et déployer une infrastructure Active Directory complète et sécurisée pour l'entreprise Oasis, dans le cadre d'une prestation assurée par NTxSystem. L'ensemble des services demandés ont été mis en place et validés : Active Directory multi-sites avec réplication, DNS, DHCP avec load balancing, serveur de fichiers distribué DFS/DFSR, modèle de tiering T0/T1/T2, RSAT par tier et gestion des mots de passe locaux via LAPS.

L'infrastructure déployée répond aux exigences de disponibilité grâce à la redondance mise en place à plusieurs niveaux, deux contrôleurs de domaine par site avec réplication inter-site, DHCP en load balancing et espace de noms DFS accessible localement depuis chaque site. En cas de défaillance d'un serveur, les services continuent de fonctionner sans interruption pour les utilisateurs.

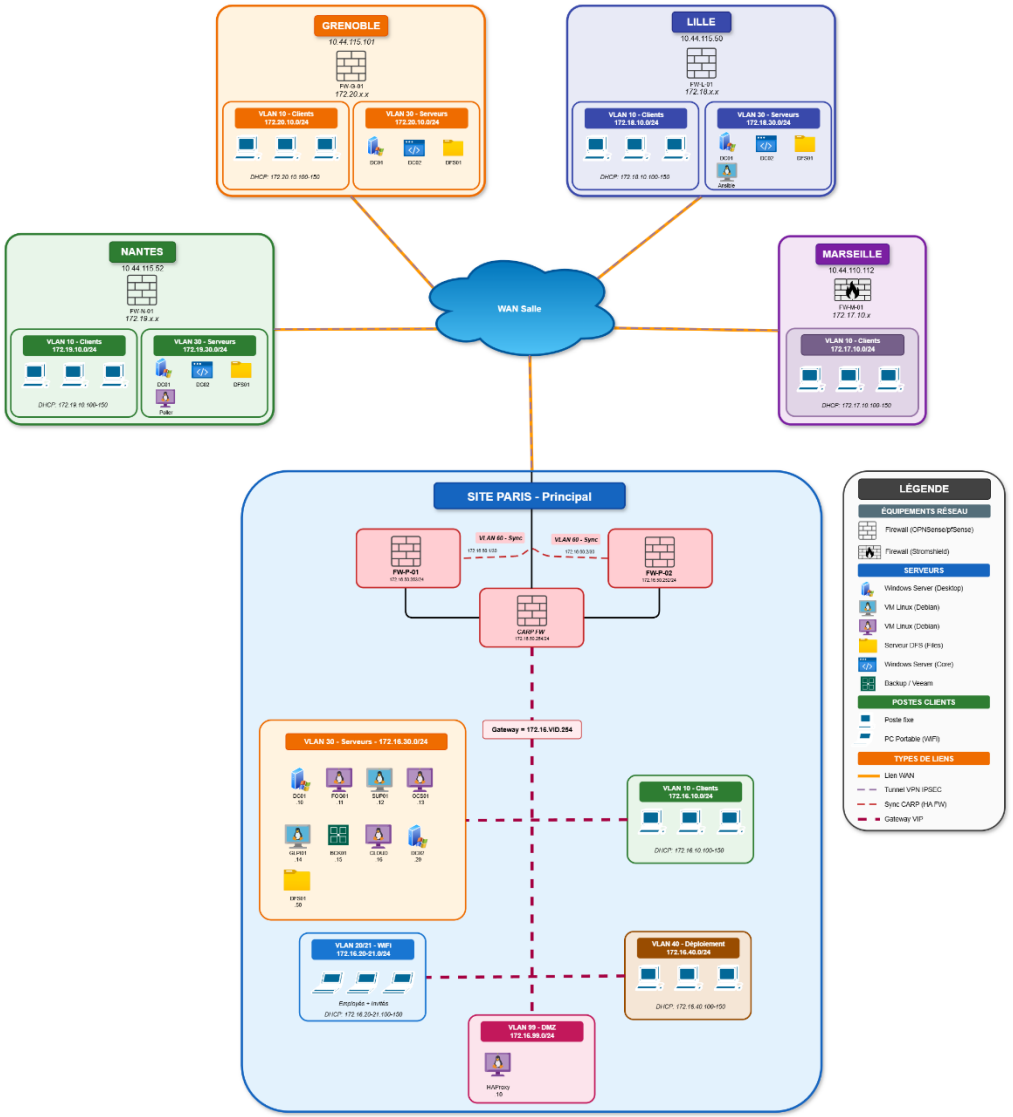
La sécurité de l'annuaire a été renforcée par la mise en place du modèle de tiering, qui segmente les droits d'administration et empêche les mouvements latéraux en cas de compromission d'un compte. Les délégations granulaires, les GPO de restriction de connexion et le déploiement de LAPS constituent un ensemble cohérent de mesures de protection alignées avec les recommandations de l'ANSSI.

Plusieurs difficultés ont été rencontrées au cours du projet. Le déploiement de LAPS sur certains postes a nécessité une mise à jour préalable des systèmes dont le niveau de mise à jour Windows était insuffisant pour supporter Windows LAPS natif. La mise en place du modèle de tiering a également été plus complexe que prévu. Ce projet a mis en évidence l'écart entre la théorie et la pratique. Si les concepts sont bien documentés, leur application concrète a demandé plusieurs remises en question, des retours en arrière et des ajustements sur l'organisation des OUs, des délégations et des GPO. C'est une leçon importante acquise au cours de ce projet : une bonne analyse en amont des ressources et des interactions entre les composants est indispensable pour éviter des itérations coûteuses en temps.

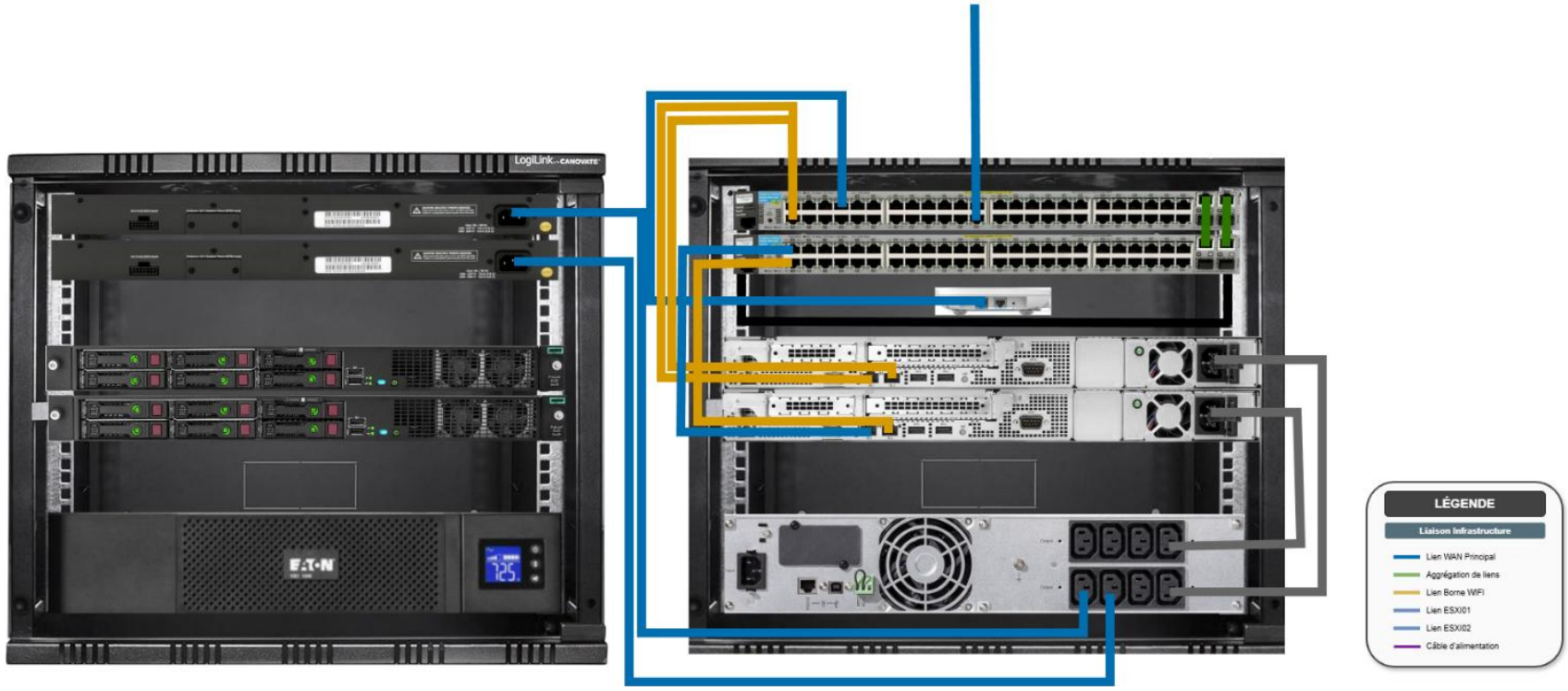
Les axes d'amélioration identifiés comme les silos d'authentification, PAW pour le Tier 0, retrait de GG-T0-Managers des Admins du domaine, séparation des partitions sur les DC principaux constituent des pistes concrètes pour renforcer davantage la sécurité de l'infrastructure dans le cadre d'une évolution future du projet.

13.Annexes

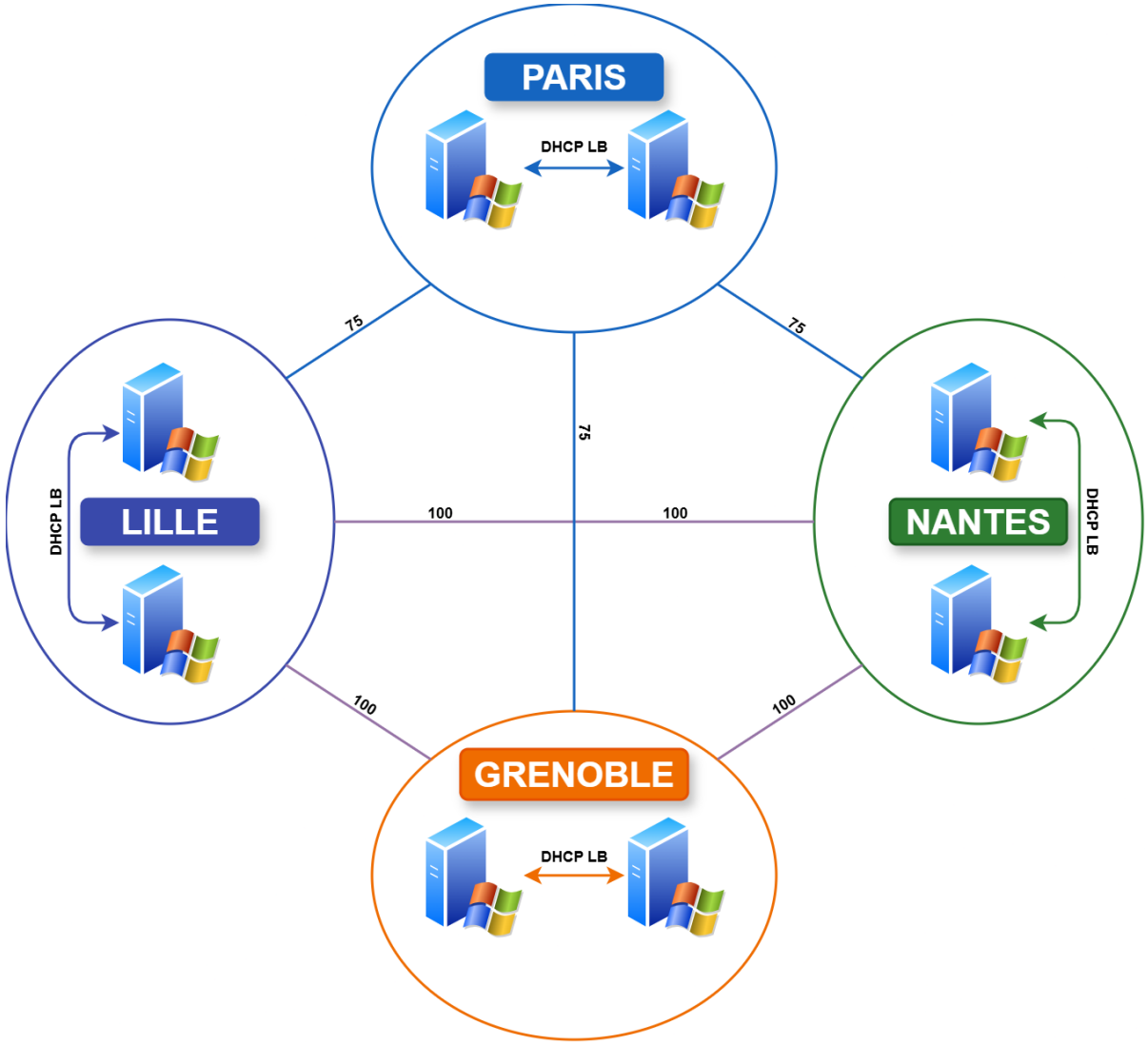
13.1. Annexe A – Schéma logique



13.2. Annexe B – Schéma physique



13.3. Annexe C – Schéma de réplication AD



13.4. Plan d'adressage

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

	Plage	Passerelle	DNS1	DNS2	Description
DHCP	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

	Plage	Passerelle	DNS1	DNS2	Description
DHCP	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

	Plage	Passerelle	DNS1	DNS2	Description
DHCP	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

Proxmox Grenoble

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-G-DC01	172.20.30.10	255.255.255.0	172.20.30.0	172.20.30.254	DC1 Grenoble
SRV-G-DC02	172.20.30.20	255.255.255.0	172.20.30.0	172.20.30.254	DC2 Core Grenoble
SRV-G-DFS01	172.20.30.50	255.255.255.0	172.20.30.0	172.20.30.254	DFS01 Grenoble
SRV-G-FOG01	172.20.30.30	255.255.255.0	172.20.30.0	172.20.30.254	FOG Grenoble
FW-G-01	172.20.10.254	255.255.255.0	172.20.10.0	172.20.10.254	IP FW-G-01 LAN Grenoble
FW-G-01	172.20.30.254	255.255.255.0	172.20.30.0	172.20.30.254	IP FW-G-01 SRV Grenoble
FW-G-01	172.20.99.254	255.255.255.0	172.20.99.0	172.20.99.254	IP FW-G-01 DMZ Grenoble
FW-G-01	10.44.115.101	255.255.255.0	10.44.115.0	10.44.115.254	IP WAN Grenoble

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.20.10.100-150	172.20.10.254	172.20.30.10	172.20.30.20	Plage DHCP Client Grenoble