

Projet Health North – BTS SIO SISR E6**Objectif**

L'objectif de cette documentation est d'expliquer la mise en place des services vitaux de l'infrastructure HEALTH NORTH. Seront donc décrites la configuration du domaine Active Directory, du service DNS, du service DHCP, des partages de fichiers, ainsi que la configuration de l'annuaire et des stratégies de groupe.

Serveurs utilisés

Les serveurs qui seront utilisés sont les suivants :

HN-GDLP-AD01	10.160.0.10	Windows Serveur 2022	Contrôleur de domaine principal
HN-GDLP-AD02	10.160.0.11	Windows Serveur 2022	Contrôleur de domaine secondaire
HN-GDLP-FS01	10.160.0.20	Windows Serveur 2022	Fichier / DFS / FSRM
HN-GDLP-FS02	10.160.0.21	Windows Serveur 2022	Fichier / DFS / réplication

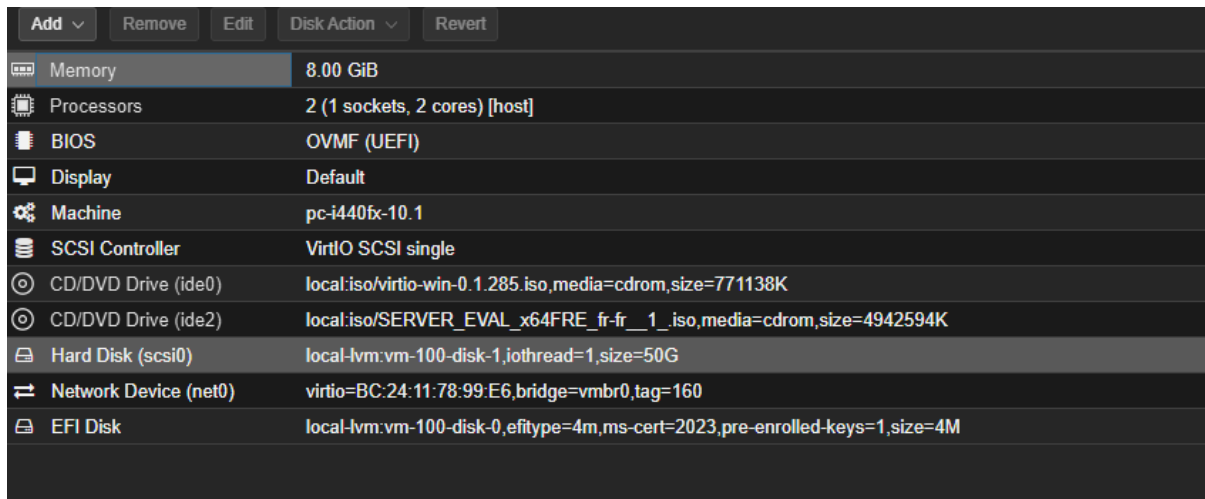
Mise en place :

Création des machines virtuelles

Dans notre cas, ce sont des machines virtuelles sur Proxmox, donc il est d'abord nécessaire de créer ces dernières.

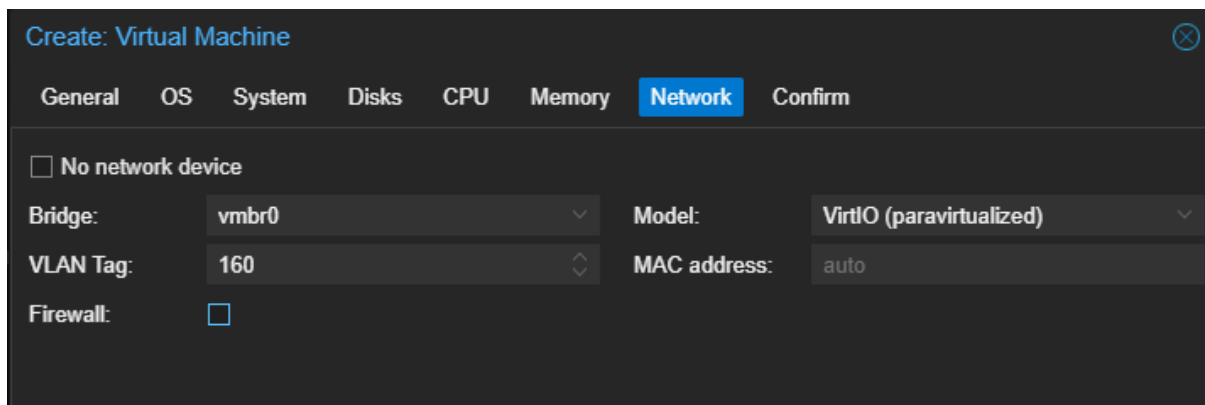
Pour cela, une fois connecté sur Proxmox, il suffit d'appuyer sur le bouton « Create VM ».

Puis, pour HN-GDLP-AD01, voici la configuration requise :



Component	Configuration
Memory	8.00 GiB
Processors	2 (1 sockets, 2 cores) [host]
BIOS	OVMF (UEFI)
Display	Default
Machine	pc-i440fx-10.1
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide0)	local:iso/virtio-win-0.1.285.iso,media=cdrom,size=771138K
CD/DVD Drive (ide2)	local:iso/SERVER_EVAL_x64FRE_fr-fr__1_.iso,media=cdrom,size=4942594K
Hard Disk (scsi0)	local-lvm:vm-100-disk-1,iosthread=1,size=50G
Network Device (net0)	virtio=BC:24:11:78:99:E6,bridge=vibr0,tag=160
EFI Disk	local-lvm:vm-100-disk-0,efitype=4m,ms-cert=2023,pre-enrolled-keys=1,size=4M

Il ne faut surtout pas oublier, dans la partie « Network », de décocher la partie « firewall », car nous n'utilisons pas celui de Proxmox. Également, il faut mettre dans le « VLAN TAG » le VLAN 160, car c'est le VLAN dans lequel les machines doivent être.



Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

No network device

Bridge: vibr0 Model: VirtIO (paravirtualized)

VLAN Tag: 160 MAC address: auto

Firewall:

Voici les configurations pour les autres machines :

HN-GDLP-AD02, qui est créé sur un autre hyperviseur afin d'assurer la redondance en cas de panne de l'un des hyperviseurs. Il a volontairement moins de RAM, car mon deuxième hyperviseur est moins puissant.

Virtual Machine 101 (HN-GDLP-AD02) on node 'HN-GDLP-H2' No Tags

Category	Component	Value
Summary	Memory	5.20 GiB
Hardware	Processors	2 (1 sockets, 2 cores) [host]
Cloud-Init	BIOS	OVMF (UEFI)
Options	Display	Default
Task History	Machine	pc-q35-10.1
Monitor	SCSI Controller	VirtIO SCSI single
Backup	CD/DVD Drive (ide0)	local:iso/virtio-win-0.1.285.iso,media=cdrom,size=771138K
Replication	CD/DVD Drive (ide2)	local:iso/SERVER_EVAL_x64FRE_fr-fr__1_.iso,media=cdrom,size=4942594K
Snapshots	Hard Disk (scsi0)	local-lvm:vm-101-disk-1,iotthread=1,size=50G
Firewall	Network Device (net0)	virtio=BC:24:11:FB:DE:FE,bridge=vibr0,firewall=1,tag=160
Permissions	EFI Disk	local-lvm:vm-101-disk-0,efitype=4m,ms-cert=2023,pre-enrolled-keys=1,size=4M

HN-GDLP-FS01, qui lui possède deux stockages : un premier pour le système d'exploitation et un second pour le stockage des fichiers.

Virtual Machine 102 (HN-GDLP-FS01) on node 'HN-GDLP-H1' No Tags

Category	Component	Value
Summary	Memory	8.19 GiB
Hardware	Processors	2 (1 sockets, 2 cores) [x86-64-v2-AES]
Cloud-Init	BIOS	OVMF (UEFI)
Options	Display	Default
Task History	Machine	pc-q35-10.1
Monitor	SCSI Controller	VirtIO SCSI single
Backup	CD/DVD Drive (ide0)	local:iso/virtio-win-0.1.285.iso,media=cdrom,size=771138K
Replication	CD/DVD Drive (ide2)	local:iso/SERVER_EVAL_x64FRE_fr-fr__1_.iso,media=cdrom,size=4942594K
Snapshots	Hard Disk (scsi0)	local-lvm:vm-102-disk-1,iotthread=1,size=50G
Firewall	Hard Disk (scsi1)	local-lvm:vm-102-disk-2,iotthread=1,size=150G
Permissions	Network Device (net0)	virtio=BC:24:11:7F:16:56,bridge=vibr0,firewall=1,tag=160
	EFI Disk	local-lvm:vm-102-disk-0,efitype=4m,ms-cert=2023,pre-enrolled-keys=1,size=4M
	TPM State	local-lvm:vm-102-disk-3,size=4M,version=v2.0

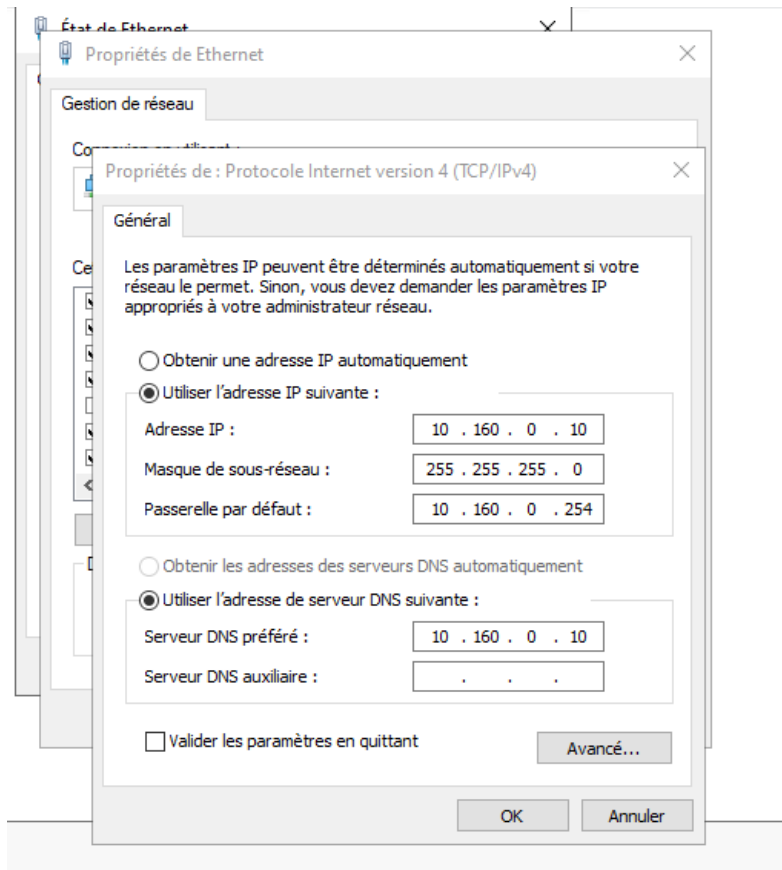
HN-GDLP-FS02, qui, comme HN-GDLP-AD02, n'est pas situé sur le même hyperviseur que HN-GDLP-FS01, possède lui aussi deux stockages et un peu moins de RAM, car l'hyperviseur est moins puissant.

Memory	6.04 GiB
Processors	2 (1 sockets, 2 cores) [host]
BIOS	OVMF (UEFI)
Display	Default
Machine	pc-q35-10.1
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide0)	local:iso/virtio-win-0.1.285.iso,media=cdrom,size=771138K
CD/DVD Drive (ide2)	local:iso/SERVER_EVAL_x64FRE_fr-fr__1_iso,media=cdrom,size=4942594K
Hard Disk (scsi0)	local-lvm:vm-103-disk-0,iotthread=1,size=50G
Hard Disk (scsi1)	ServeurFichier:vm-103-disk-1,iotthread=1,size=150G
Network Device (net0)	virtio=BC:24:11:E3:36:D2,bridge=vibr0,tag=160
EFI Disk	ServeurFichier:vm-103-disk-0,efitype=4m,ms-cert=2023,pre-enrolled-keys=1,size=1M
TPM State	local-lvm:vm-103-disk-1,size=4M,version=v2.0

Une fois les machines virtuelles créées, nous pouvons donc installer Windows Server 2022 et commencer par la configuration d'AD01.

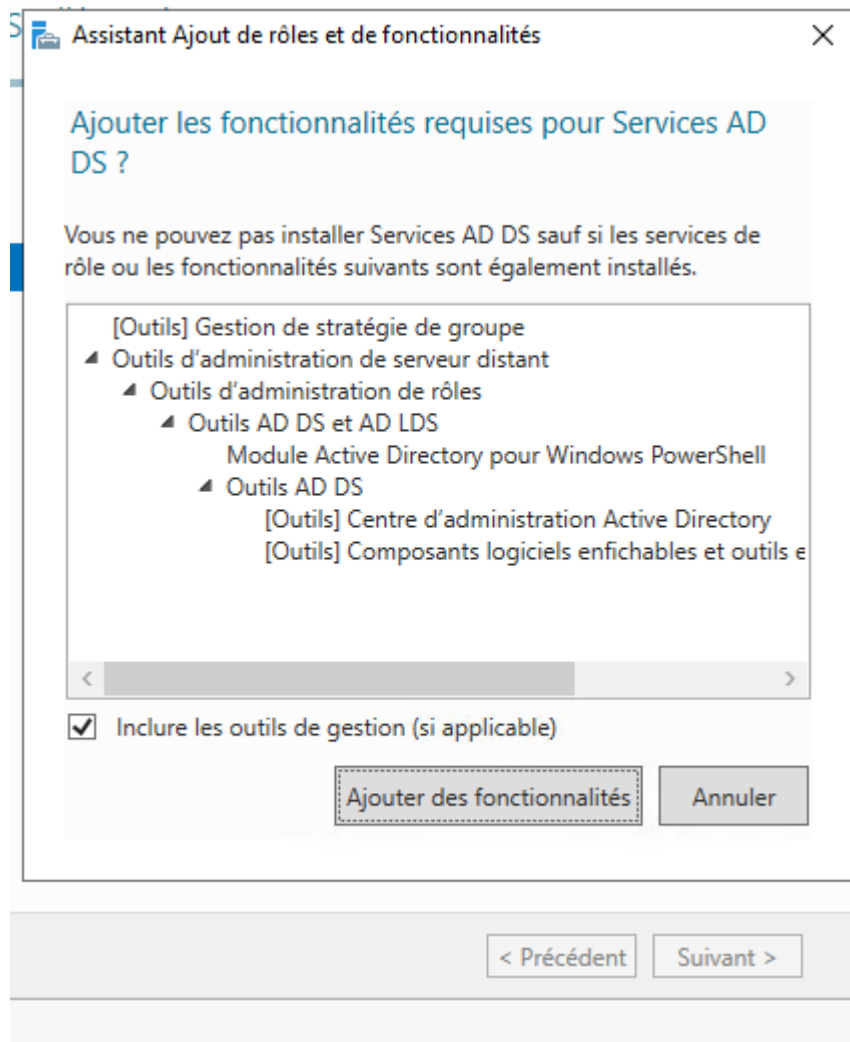
Configuration de HN-GDLP-AD01

La première étape est donc de lui attribuer l'adresse IP souhaitée, en IP fixe dans notre cas pour HN-GDLP-AD01 : 10.160.0.10.



Ensuite, la prochaine étape est de renommer l'ordinateur afin qu'il s'appelle : HN-GDLP-AD01. Pour cela, il suffit de cliquer sur le nom du serveur dans le gestionnaire de celui-ci. Une fois le nom entré, l'ordinateur va demander à redémarrer, laissez-le faire.

Une fois redémarré, il faut maintenant installer le service AD DS dans le gestionnaire de serveur, puis aller dans « Gérer » et « Ajouter des rôles ou fonctionnalités ». Par la suite, il suffit de cocher le rôle « Service AD DS », ce qui aura pour effet d'ajouter tous les rôles dont le serveur a besoin.



Une fois l'installation réalisée, il faut promouvoir le serveur en contrôleur de domaine, à l'aide de la notification se trouvant dans le drapeau jaune du gestionnaire de serveur.



Cette promotion il faut bien :

- Ajouter une nouvelle forêt
- Nom de domaine racine : health-north.fr

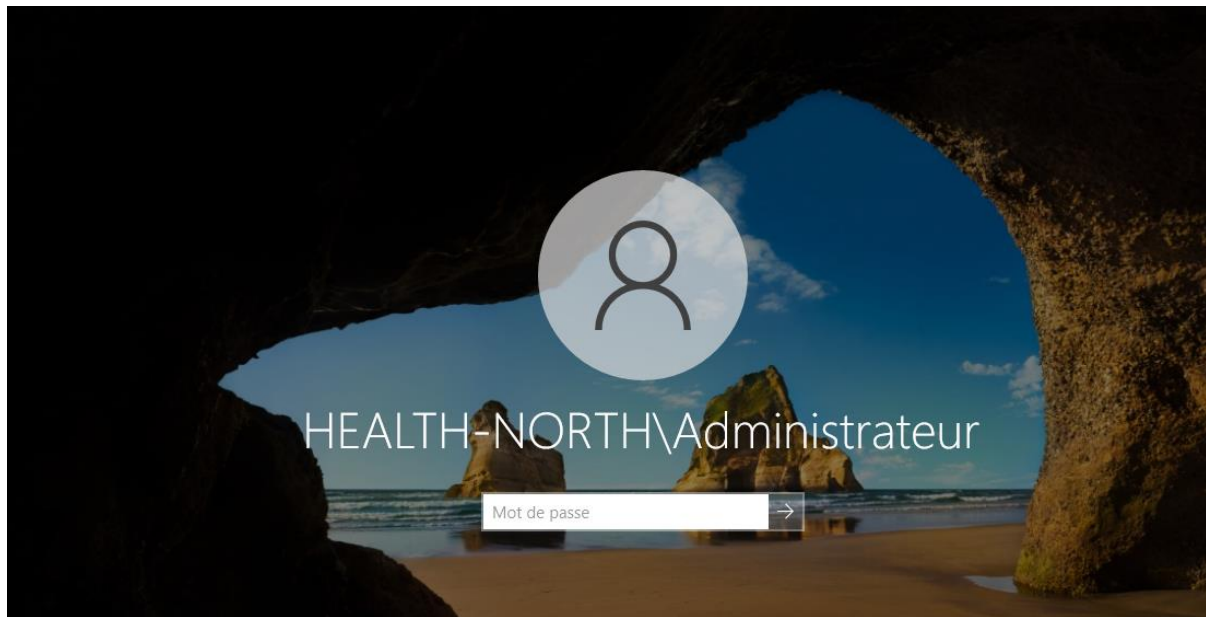
Créer un mot de passe fort pour le compte administrateur du domaine.

Le nom de domaine NetBIOS : Health-north

Après, on laisse tous les paramètres de base et on clique sur « installer ».

Cela peut prendre plusieurs minutes. Dès que le serveur est redémarré, il faut se connecter avec le compte administrateur du domaine en entrant le nom «NetBIOS», un antislash puis administrateur.

Comme ceci :



Dans le gestionnaire de serveur, nous devons voir que l'ordinateur est bien dans health-north.fr et qu'il s'appelle bien HN-GDLP-AD01, comme ceci :

onnaire de serveur ▸ Serveur local

PROPRIÉTÉS
Pour HN-GDLP-AD01

Nom de l'ordinateur	HN-GDLP-AD01	Dernières mises à jour installées	30/03/2026 01:29
Domaine	health-north.fr	Windows Update	Télécharger les mises à jour unique
		Dernière recherche de mises à jour :	Aujourd'hui à 11:07
Pare-feu Microsoft Defender	Domaine : Actif	Antivirus Microsoft Defender	Protection en temps réel : activée
Gestion à distance	Activé	Commentaires et diagnostics	Paramètres
Bureau à distance	Activé	Configuration de sécurité renforcée d'Internet Explorer	Actif
Association de cartes réseau	Désactivé	Fuseau horaire	(UTC+01:00) Bruxelles, Copenhagu
Ethernet	10.160.0.10, Compatible IPv6	ID de produit (Product ID)	00454-40000-00001-AA829 (activé
Gestion Azure Arc	Désactivé		
Version du système d'exploitation	Microsoft Windows Server 2022 Standard Evaluation	Processeurs	Intel(R) Xeon(R) Silver 4110 CPU @
Informations sur le matériel	QEMU Standard PC (i440FX + PIIX, 1996)	Mémoire installée (RAM)	7,99 Go
		Espace disque total	10 23 Go

ÉVÉNEMENTS
Tous les événements | 3 au total

Filtrer

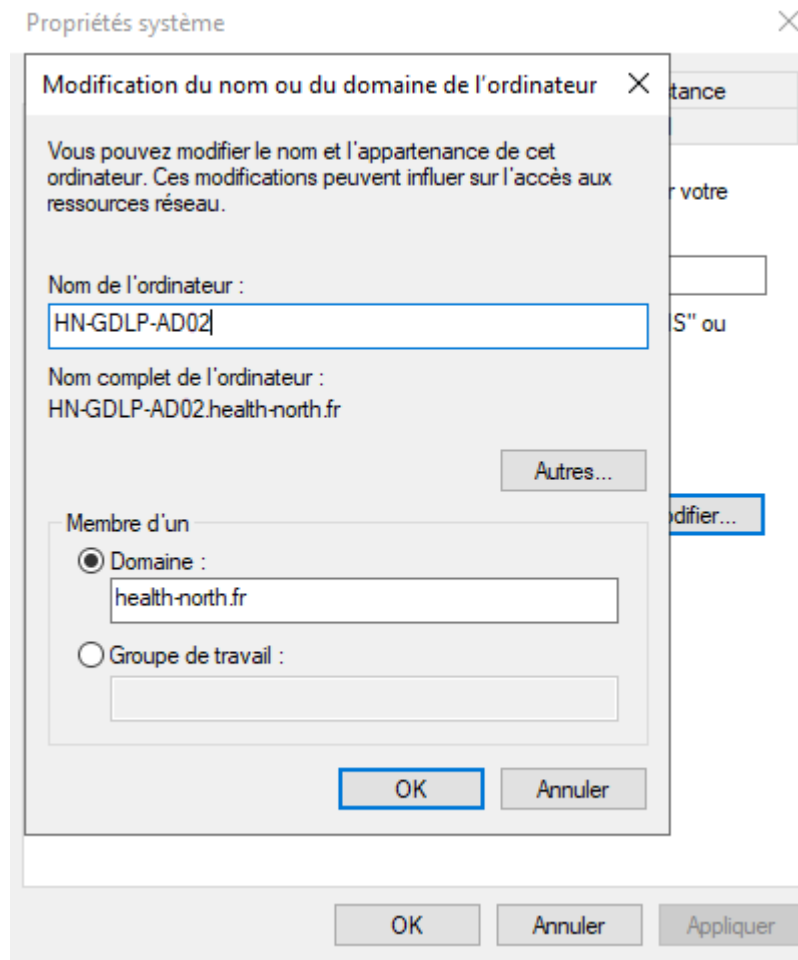
Une fois cela fait, nous pouvons passer à HN-GDLP-AD02.

Configuration HN-GDLP-AD02 et ajout à la forêt existante

Pour la configuration de HN-GDLP-AD02, il faut simplement suivre les mêmes étapes que pour HN-GDLP-AD01, à quelques détails près.

Le premier changement est l'adresse IP. Pour cette fois-ci, elle doit être différente, donc : 10.160.0.11

Ensuite, lors du renommage du serveur, il faut également cocher la case domaine et entrer le nom de domaine, donc health-north.fr.



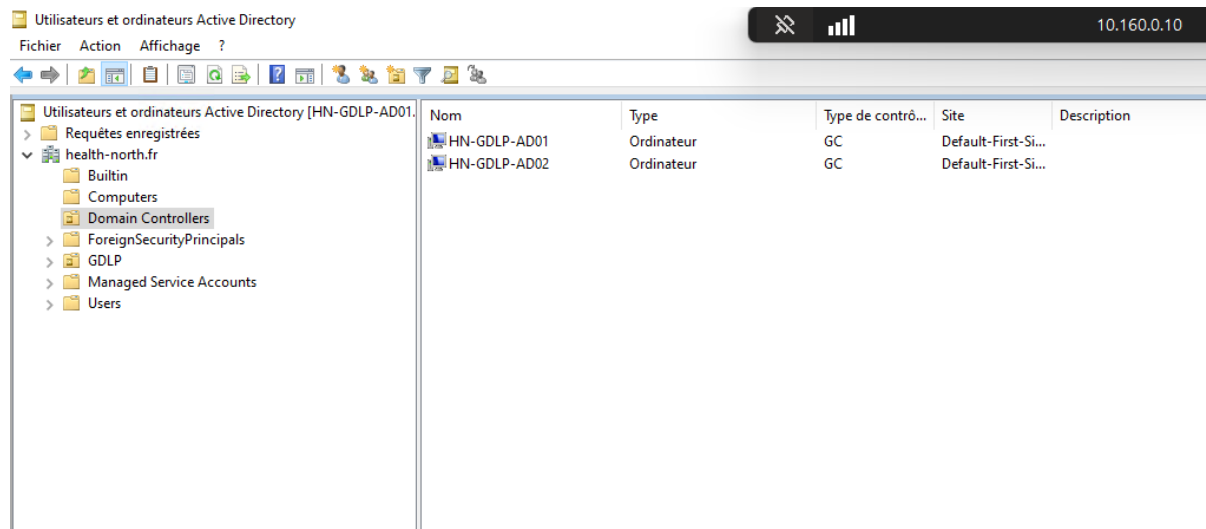
Une fois que le PC est ajouté dans le domaine et que le service Active Directory est également installé, il est possible d'ajouter ce serveur en tant que contrôleur de domaine (second contrôleur de domaine). Pour cela, dans la configuration de déploiement, il faut :

- Cocher « Contrôleur de domaine dans un domaine existant »
- Dans le champ domaine, entrer health-north.fr

Ensuite, dans la suite de la configuration, il est possible de laisser les options de base et de modifier uniquement :

Répliquer depuis « HN-GDLP-AD01 »

Une fois HN-GDLP-AD02 redémarré, il est possible de vérifier dans la console « Utilisateurs et ordinateurs Active Directory » si les deux contrôleurs de domaine sont bien présents.

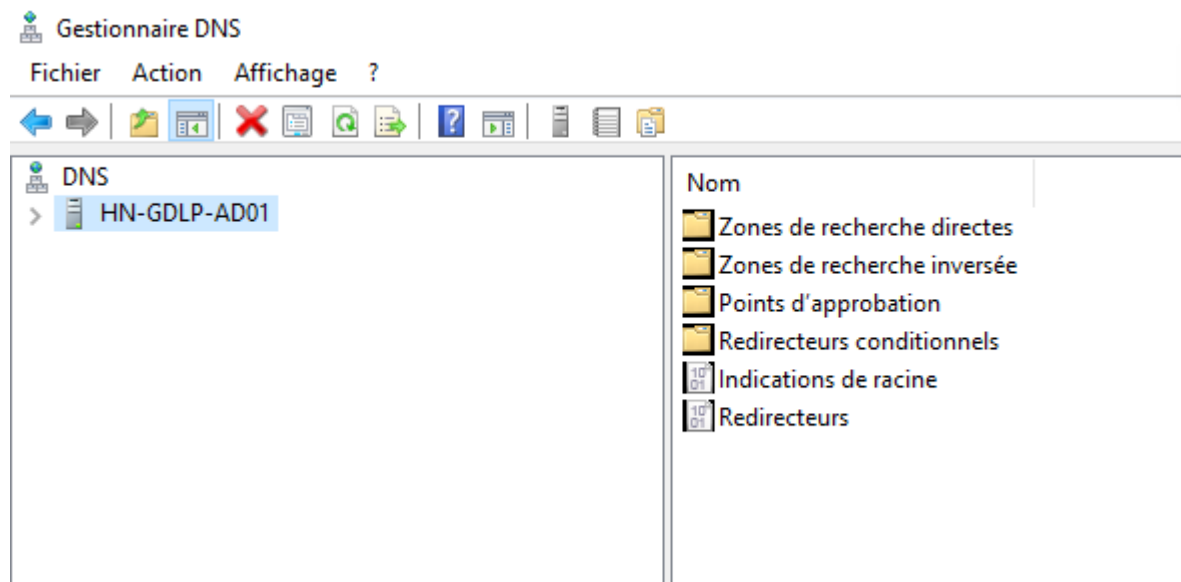


Une fois cela fait, nous allons pouvoir passer à la configuration du DNS.

Mise en place du DNS sur HN-GDLP-AD01 - HN-GDLP-AD02

Le rôle DNS est installé automatiquement lors de la mise en place d'Active Directory, il n'est donc pas nécessaire de l'installer. De plus, il est également préconfiguré automatiquement. En revanche, nous pouvons ajouter HN-GDLP-AD02, soit 10.160.0.11, en tant que DNS secondaire.

Ensuite, nous pouvons vérifier que les zones DNS sont bien créées sur les deux machines. Pour ce faire, il faut aller dans le Gestionnaire de serveur, puis dans « Outils » et « DNS », et nous arrivons ici :



Il faut après vérifier que l'on voit bien la zone directe :

On doit normalement voir : health-north.fr

Ensuite, dans la zone inverse, on doit normalement voir :

160.10in-addr.arpa

DNS		Nom	Type	État
▼	HN-GDLP-AD01	160.10.in-addr.arpa	Serveur principal intégré à Act...	En cour
>	Zones de recherche directes			
>	Zones de recherche inversée			
	Points d'approbation			
	Redirecteurs conditionnels			

Ainsi que nos deux contrôleurs de domaine.

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[11], hn-gdlp-ad01.health-north.fr., hostmaster....	statique
(identique au dossier parent)	Serveur de noms (NS)	hn-gdlp-ad02.	statique
(identique au dossier parent)	Serveur de noms (NS)	hn-gdlp-ad01.health-north.fr.	statique
(identique au dossier parent)	Serveur de noms (NS)	hn-gdlp-ad02.health-north.fr.	statique
10.160.0.10	Pointeur (PTR)	HN-GDLP-AD01.health-north.fr.	18/04/2026 10:00:00
10.160.0.11	Pointeur (PTR)	hn-gdlp-ad02.health-north.fr.	statique
10.160.0.11	Pointeur (PTR)	HN-GDLP-AD02.health-north.fr.	01/04/2026 11:00:00

Et si cela apparaît bien, nous pouvons effectuer des tests de ping depuis HN-GDLP-AD01.

Nous pouvons effectuer un « ping HN-GDLP-AD02 ».

Et inversement depuis HN-GDLP-AD02.

```
C:\Users\Administrateur>ping HN-GDLP-AD02

Envoi d'une requête 'ping' sur HN-GDLP-AD02.health-north.fr [10.160.0.11] avec 32 octets de données :
Réponse de 10.160.0.11 : octets=32 temps<1ms TTL=128
Réponse de 10.160.0.11 : octets=32 temps=1 ms TTL=128
Réponse de 10.160.0.11 : octets=32 temps=1 ms TTL=128
Réponse de 10.160.0.11 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.160.0.11:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Administrateur>
```

Si le ping fonctionne, nous pouvons passer à la mise en place du DHCP.

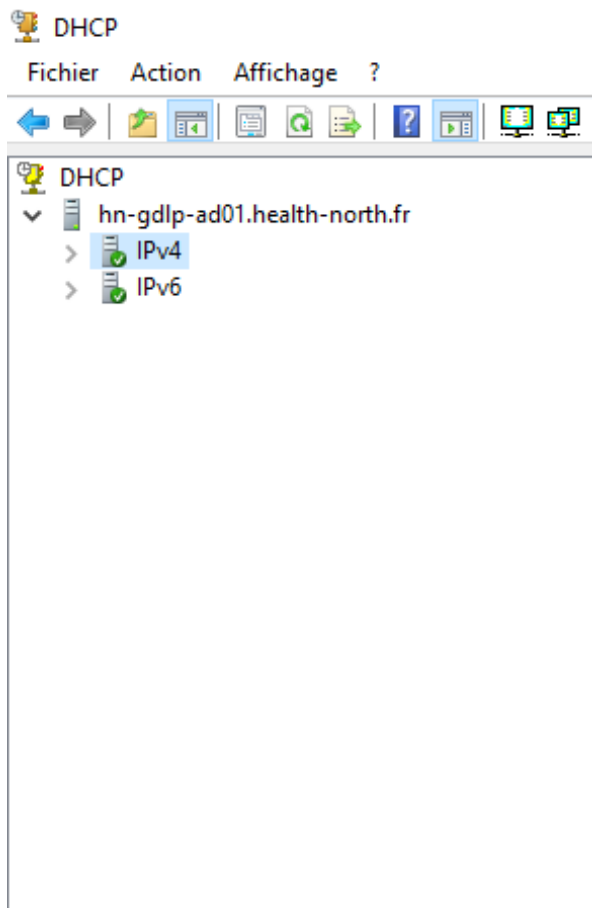
Mise en place du DHCP

Dans un premier temps, il faut installer le rôle DHCP sur nos deux serveurs. Pour ce faire, il faut aller dans « Gérer » puis « Ajouter des rôles et fonctionnalités », puis cocher DHCP. Ensuite, il faut terminer l'installation. Une fois cela fait, dans le drapeau jaune, nous pouvons cliquer sur « Terminer la configuration DHCP ».



Ici, nous pouvons laisser les informations de connexion préremplies, car nous sommes connectés avec le compte administrateur du domaine.

Une fois cela fait, nous pouvons ouvrir la console de gestion du DHCP en allant dans « Gestionnaire de serveur », puis dans « Outils » et enfin « DHCP ».



Ici, nous pouvons faire un clic droit sur IPv4 puis sélectionner « Nouvelle étendue ». Cela va ouvrir l'assistant de création d'une nouvelle étendue.

Avant tout, pour le projet, nous allons devoir créer plusieurs étendues. Voici un tableau les résumant toutes.

VLAN	Nom du réseau	Réseau	Passerelle	Réservé statique	Plage DHCP à créer	Durée du bail
300	Service informatique	10.3.0.0/24	10.3.0.254	10.3.0.1 à 10.3.0.50	10.3.0.51 à 10.3.0.251	8 h
301	Service infirmier	10.3.10.0/24	10.3.10.254	10.3.10.1 à 10.3.10.50	10.3.10.51 à 10.3.10.251	8 h
302	Service chirurgie	10.3.20.0/24	10.3.20.254	10.3.20.1 à 10.3.20.50	10.3.20.51 à 10.3.20.251	8 h

303	Service laboratoire	10.3.30.0/24	10.3.30.254	10.3.30.1 à 10.3.30.50	10.3.30.51 à 10.3.30.251	8 h
304	Service direction	10.3.40.0/24	10.3.40.254	10.3.40.1 à 10.3.40.50	10.3.40.51 à 10.3.40.251	8 h
400	Wifi Service	10.4.0.0/23	10.4.1.254	10.4.0.1 à 10.4.0.50	10.4.0.51 à 10.4.1.251	2 h
401	Wifi Patient	10.4.10.0/23	10.4.11.254	10.4.10.1 à 10.4.10.50	10.4.10.51 à 10.4.11.251	2 h

Comme exemple nous allons commencer par l'étendue « Service informatique ».

La première étape est de créer le nom de l'étendue qui est informatique_VLAN300

Assistant Nouvelle étendue

Nom de l'étendue

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



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

Nom :

Description :

< Précédent

Suivant >

Annuler

Ensuite, nous devons sélectionner la plage d'adresses que l'on veut que le DHCP distribue. Dans notre cas : 10.3.0.51 à 10.3.0.251.

Assistant Nouvelle étendue

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

Paramètres de configuration pour serveur DHCP

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

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent **Suivant >** Annuler

Ensuite, nous pouvons exclure les adresses IP que nous ne voulons pas que le DHCP distribue. Dans notre cas, il s'agit de la plage de 10.3.0.1 à 10.3.0.50 et de 10.3.0.252 à 10.3.0.254.

Puis, nous pouvons configurer la durée du bail, que nous pouvons fixer à 8h.

Par la suite, nous pouvons configurer notre passerelle par défaut pour cette étendue, qui est 10.3.0.254. Puis nous pouvons ajouter nos serveurs DNS, donc en premier 10.160.0.10, suivi de 10.160.0.11, puis nous pouvons créer l'étendue et l'activer.

Il faut ensuite répéter cette étape pour toutes les étendues en veillant à respecter les paramètres du tableau à créer afin d'obtenir le résultat final.

Contenu du serveur DHCP	État	Description	Relation de basculement
Étendue [10.3.10.0] Infirmier_VLAN301	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Étendue [10.3.30.0] Laboratoire_VLAN303	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Étendue [10.4.0.0] Wifi_Service_VLAN400	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Étendue [10.4.10.0] Wifi_Patient_VLAN401	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Étendue [10.3.40.0] Direction_VLAN304	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Étendue [10.3.20.0] Chirurgie_VLAN302	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Étendue [10.3.0.0] Informatique_VLAN300	** Actif **		hn-gdlp-ad01.health-north.fr-hn...
Options de serveur			
Stratégies			
Filtres			

La prochaine étape est de créer la structure de l'Active Directory.

Structure logique de l'Active Directory

L'objectif ici est de créer les unités d'organisation afin de ranger les comptes utilisateurs, les machines ainsi que les groupes, dans le but de faciliter la gestion de l'Active Directory. Dans un premier temps, allez dans la console « Utilisateurs et ordinateurs Active Directory ». Une fois dedans, il suffit de faire un clic droit sur health-north.fr, puis sur « Nouveau » et « Unité d'organisation ». Nommez-la GDLP. Ensuite, à l'intérieur, nous pouvons créer notre structure pour qu'à la fin cela ressemble à ceci.

	Nom	Type	Description
Utilisateurs et ordinateurs Active Directory [HN-GDLP-AD01.]			
> Requetes enregistrees			
▼ health-north.fr			
> Builtin			
> Computers			
> Domain Controllers			
> ForeignSecurityPrincipals			
▼ GDLP			
▼ Groupes			
> Chirurgie	Chirurgie	Unité d'organi...	
> Direction	Direction	Unité d'organi...	
> Infirmier	Infirmier	Unité d'organi...	
> Informatique	Informatique	Unité d'organi...	
> Laboratoire	Laboratoire	Unité d'organi...	
▼ Ordinateurs			
> Chirurgie			
> Direction			
> Infirmier			
> Informatique			
> Laboratoire			
▼ Serveurs			
> Bastion			
> BDD			
> Deploiement			
> Fichiers			
> Maintenance			
> WEB			
▼ Utilisateurs			
> Chirurgie			
> Direction			
> Infirmier			
> Informatique			
> Laboratoire			
> Managed Service Accounts			
> Users			

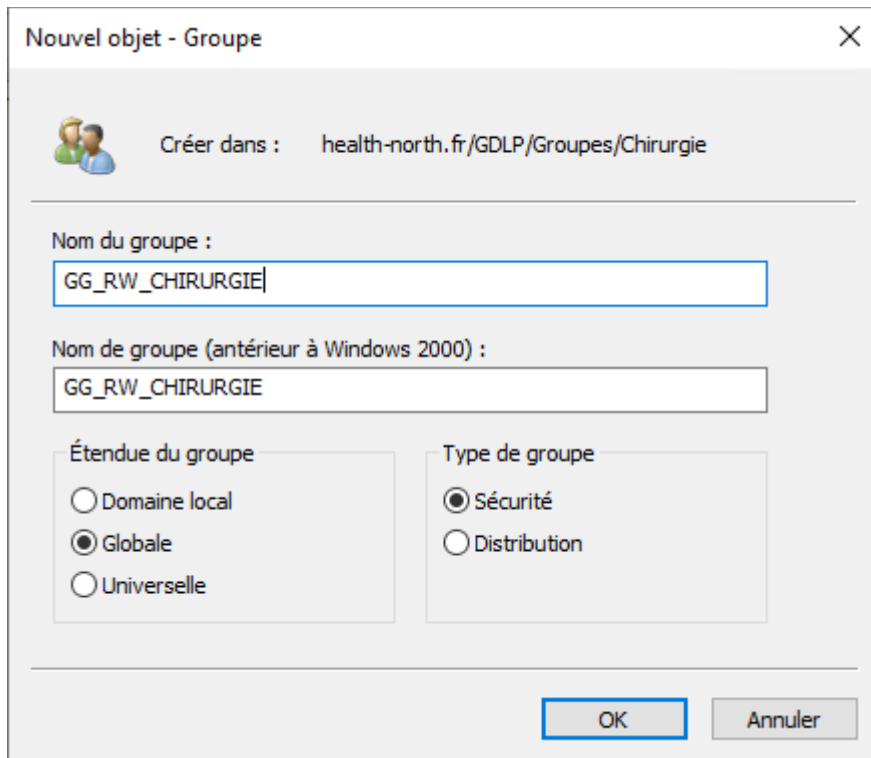
La prochaine étape est la création des groupes utilisateurs par service. Ces groupes vont nous être utiles pour gérer les droits d'accès aux partages de fichiers de chaque service. Il faut donc créer trois groupes par service.

GG_SERVICE : son but est de centraliser les groupes pour les utilisateurs d'un service, c'est-à-dire qu'il suffit de regrouper tous les groupes dans celui-ci et de l'appliquer uniquement aux utilisateurs d'un service.

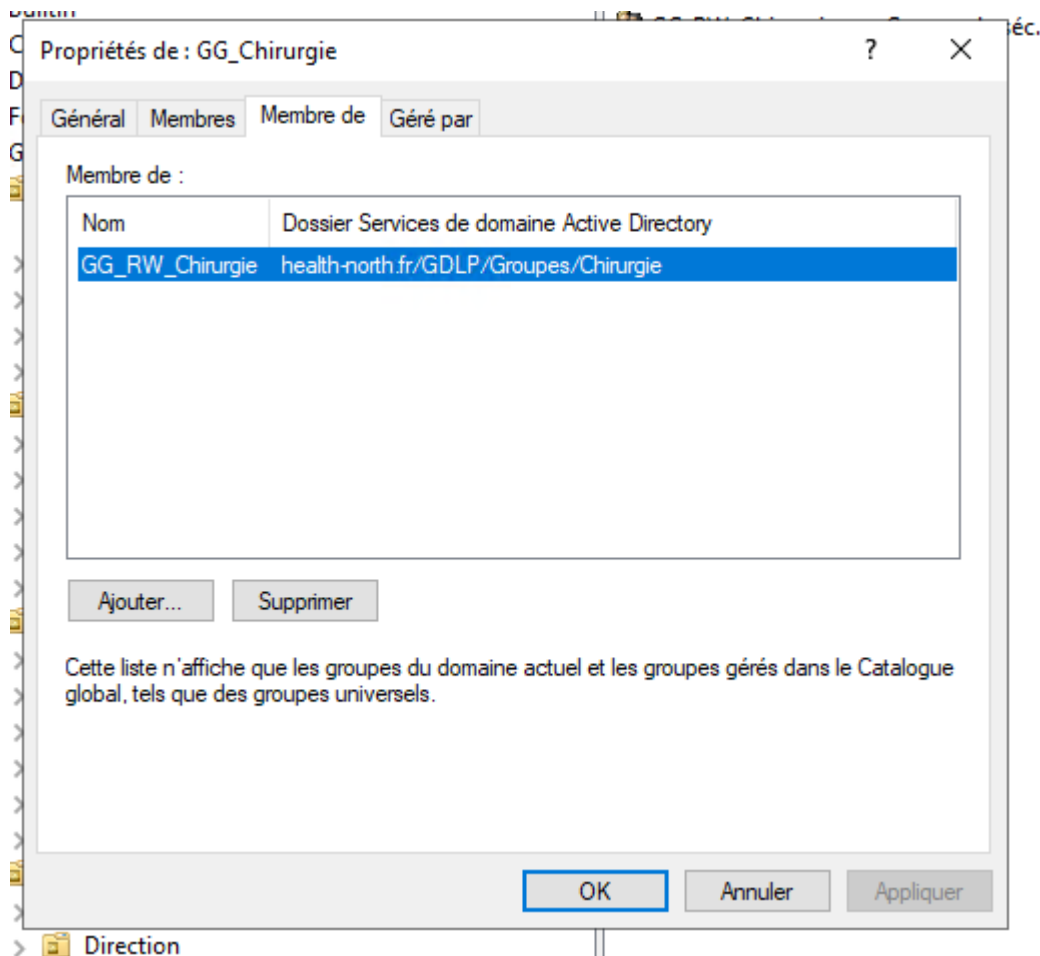
GG_RW_SERVICE : il donne l'accès en lecture et en écriture au partage du service.

GG_R_SERVICE : il donne l'accès en lecture seule au partage du service.

Afin de créer les groupes, il suffit de se placer dans la bonne unité d'organisation, puis de faire un clic droit sur « Nouveau », puis « Groupe », et d'entrer le nom du groupe.



Il faut donc répéter cela pour tous les groupes. Dès que cela est fait, nous pouvons imbriquer les groupes, ce qui signifie que nous pouvons ajouter le groupe « gg_service » au groupe « GG_RW_SERVICE ». Répétez cette opération pour tous les services.



L'étape suivante est la création d'utilisateurs, mais cela sera abordé dans une autre documentation.

Nous allons donc passer à l'étape de l'installation et de la mise en place des serveurs de fichiers et des partages.

Serveurs de fichiers et partages

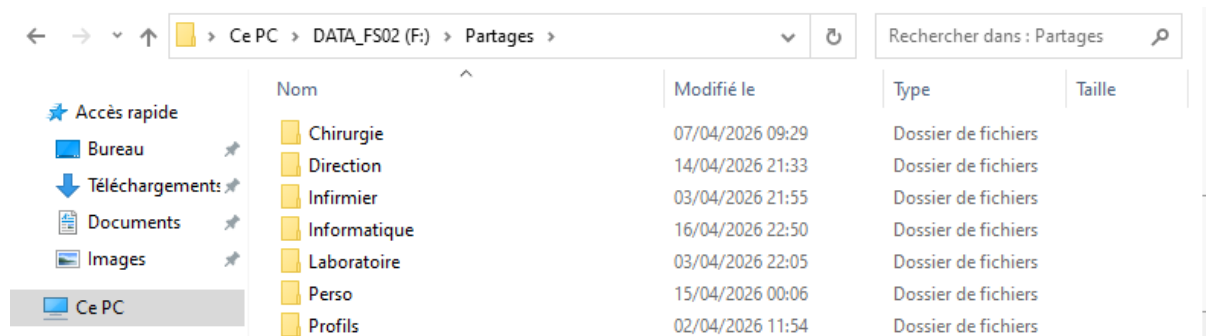
Dans un premier temps, nous pouvons installer les deux serveurs Windows comme vu précédemment, puis les faire rejoindre le domaine et leur attribuer les adresses IP et les noms suivants :

10.160.0.20 HN-GDLP-FS01

10.160.0.21 HN-GDLP-FS02

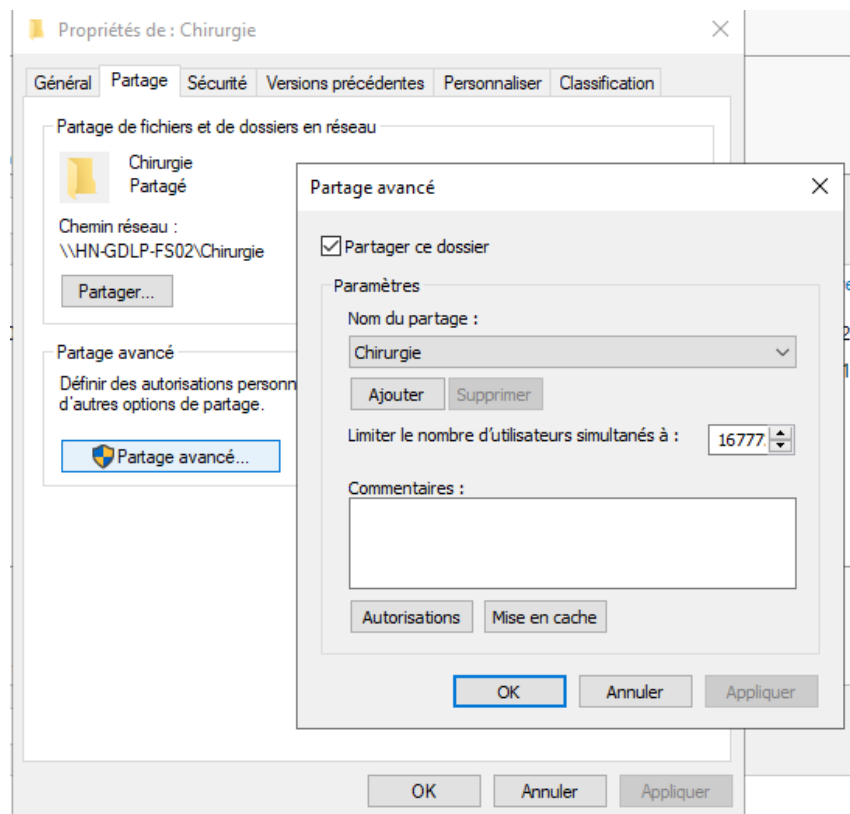
Ensuite, nous pouvons initialiser le second disque dans le gestionnaire de disques.

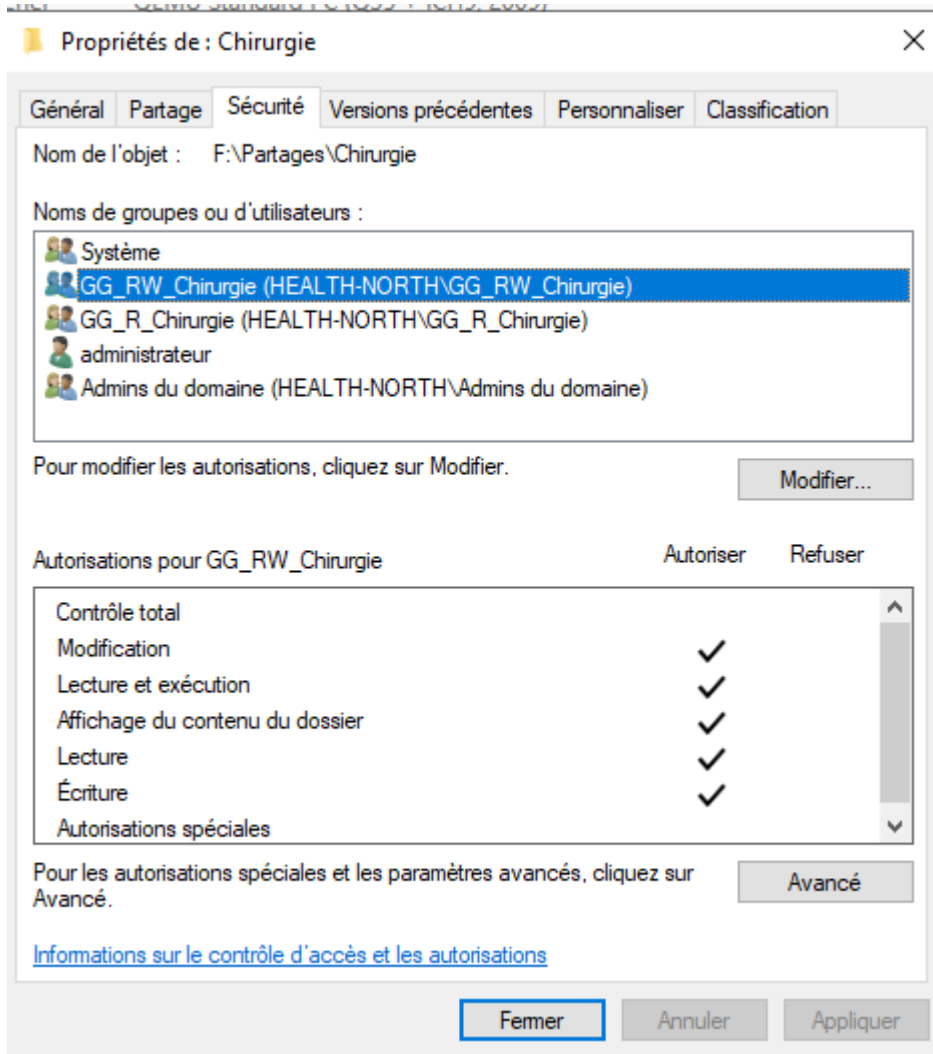
Une fois cela fait, nous pouvons créer l'arborescence des partages, dans le but de mettre en place un partage par service, ainsi qu'un dossier personnel qui stockera les dossiers de chaque utilisateur, ainsi qu'un dossier profil.



Il est important de bien créer ces dossiers à l'identique sur les deux serveurs de fichiers. C'est cela qui va permettre de mettre en place la réplication entre les serveurs de fichiers.

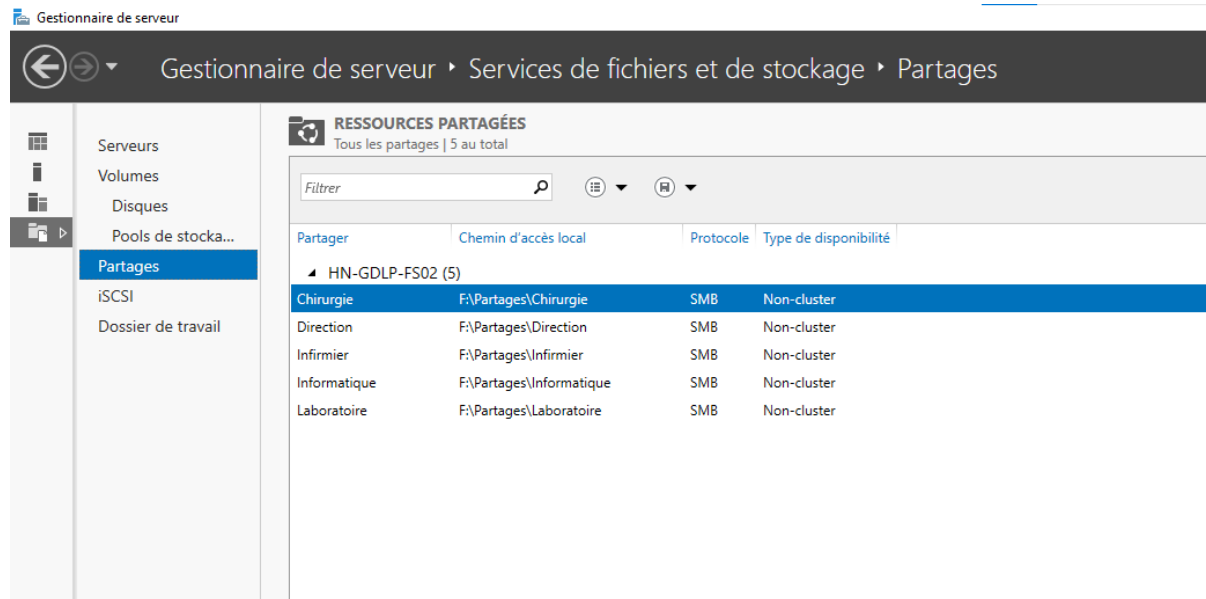
Une fois cela créé, il faut partager les dossiers en faisant un clic droit sur le dossier que l'on souhaite partager, puis en sélectionnant « Partage avancé ». Dans ce menu, il faut activer le partage, donner un nom au partage, puis configurer les autorisations dans l'onglet « Sécurité » de la page des propriétés.





Il faut donc donner le droit de modification au groupe « GG_RW_SERVICE » et le droit de lecture au groupe « GG_R_SERVICE » pour leur partage de service associé.

Afin de vérifier si les partages sont bien créés, nous pouvons aller vérifier cela dans le gestionnaire de serveur, dans « Services de fichiers et de stockage » puis « Partages ». Si cela a bien été réalisé, nous sommes censés voir les cinq partages.

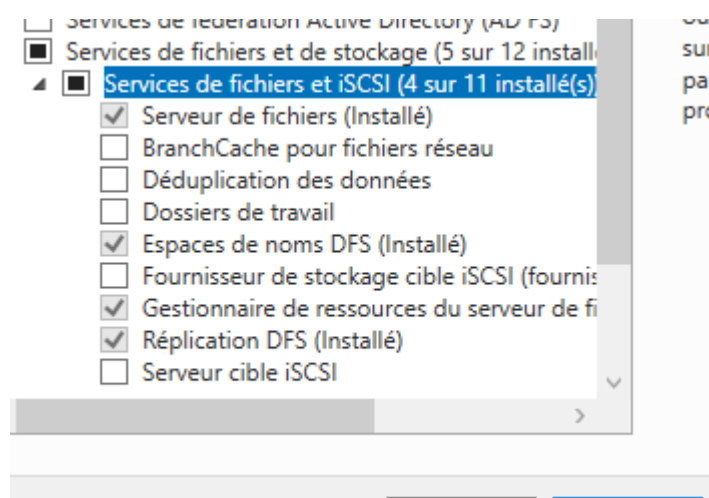


Après nous allons pouvoir configurer le DFS et FSRM (Distributed File System et File Server Resource Manager).

DFS et FSRM

Cette étape va nous permettre de créer un espace de noms pour héberger le partage de tous nos dossiers, ainsi que de mettre en place la réplication entre les deux serveurs de fichiers, et le filtrage des fichiers vidéo. Pour ce faire, il est nécessaire d'installer deux services supplémentaires sur les deux serveurs de fichiers :

Espace de noms DFS et réplication et Réplication DFS

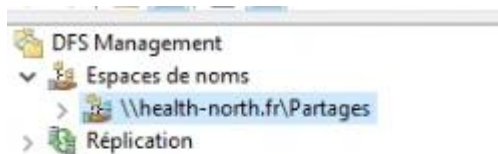


Une fois cela installé, nous allons pouvoir créer un espace de noms. Pour cela, il faut aller dans la gestion du système de fichiers DFS. Ensuite, il faut créer un nouvel espace de noms

en faisant clic droit sur « Espace de noms » puis sur « Assistant Nouvel espace de noms », où l'on choisit le serveur d'espace de noms, dans notre cas HN-GDLP-FS01.

Par la suite, nous devons choisir le nom et le chemin du partage, c'est-à-dire le nom du partage ainsi que le chemin vers le dossier que nous avons créé précédemment.

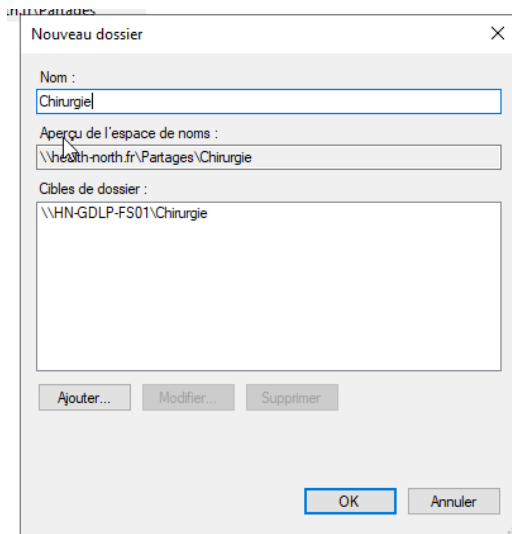
Après cela, nous pouvons cliquer sur « Suivant » et terminer la configuration.



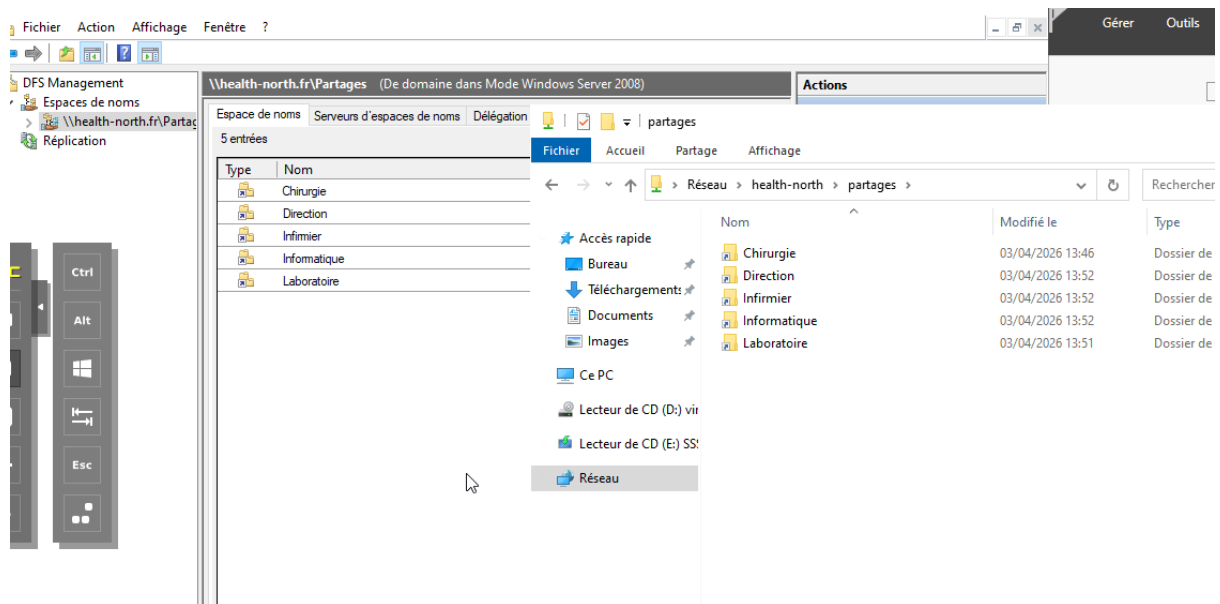
Il faut ensuite répéter l'opération sur HN-GDLP-FS02.

Puis, nous devons créer différents dossiers à l'intérieur de notre espace de noms. Pour cela, il faut faire un clic droit sur notre espace de noms, puis sur « Nouveau dossier ».

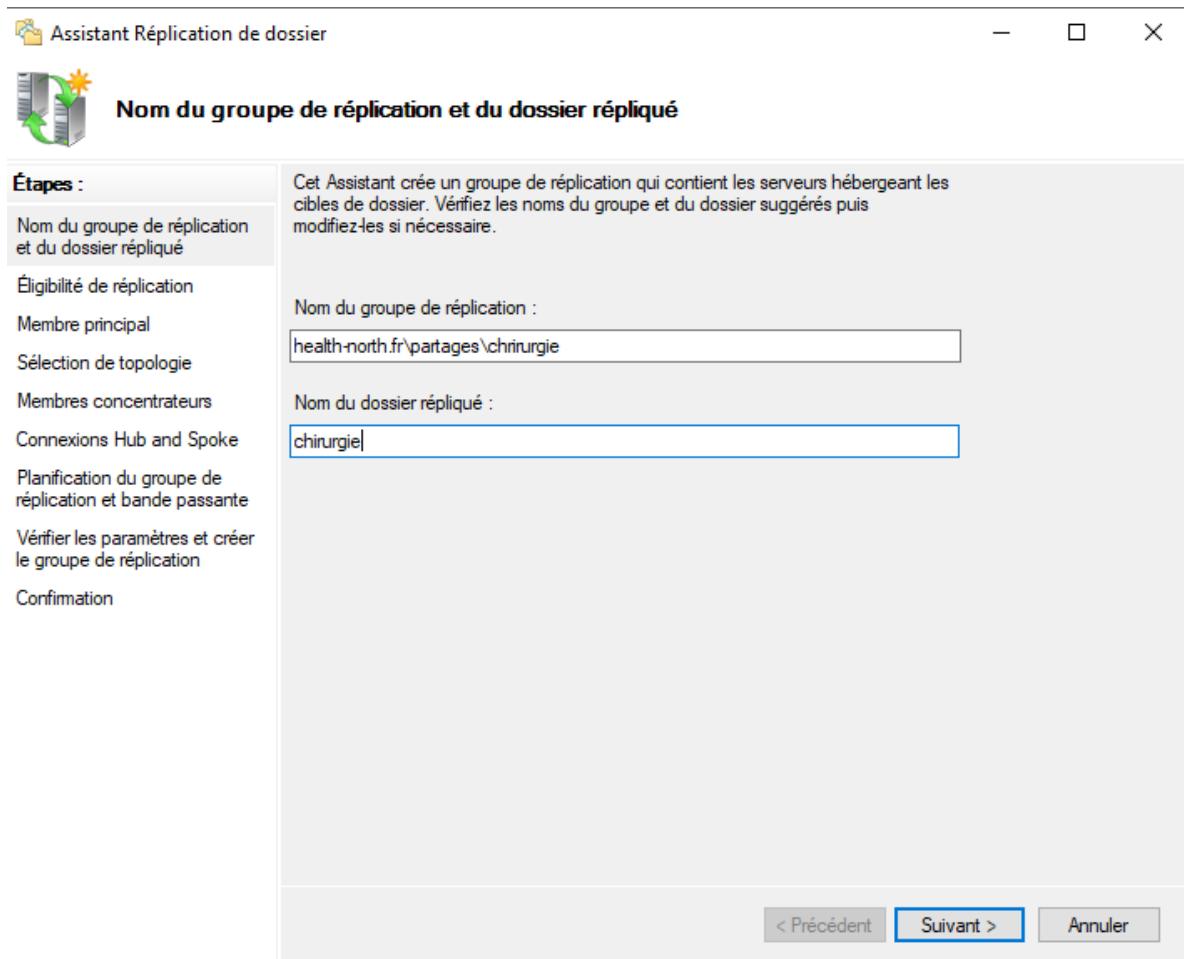
Ensuite, il faut choisir le nom du dossier et ajouter le chemin de partage. Par exemple, pour chirurgie c'est : \\hn-gdlp-fs01\chirurgie



Il faut ensuite reproduire cette étape pour tous les partages sur les deux serveurs de fichiers.



Par la suite, il faut ajouter FS02 en tant que serveur d'espace de noms secondaire dans FS01. Puis il faut ajouter FS02 comme cible pour chaque dossier partagé. En réalisant cette opération, il sera proposé de créer un groupe de réplication. Il faut accepter, puis un temps de chargement sera nécessaire. Après cela, nous arrivons sur l'assistant de réplication de dossier.

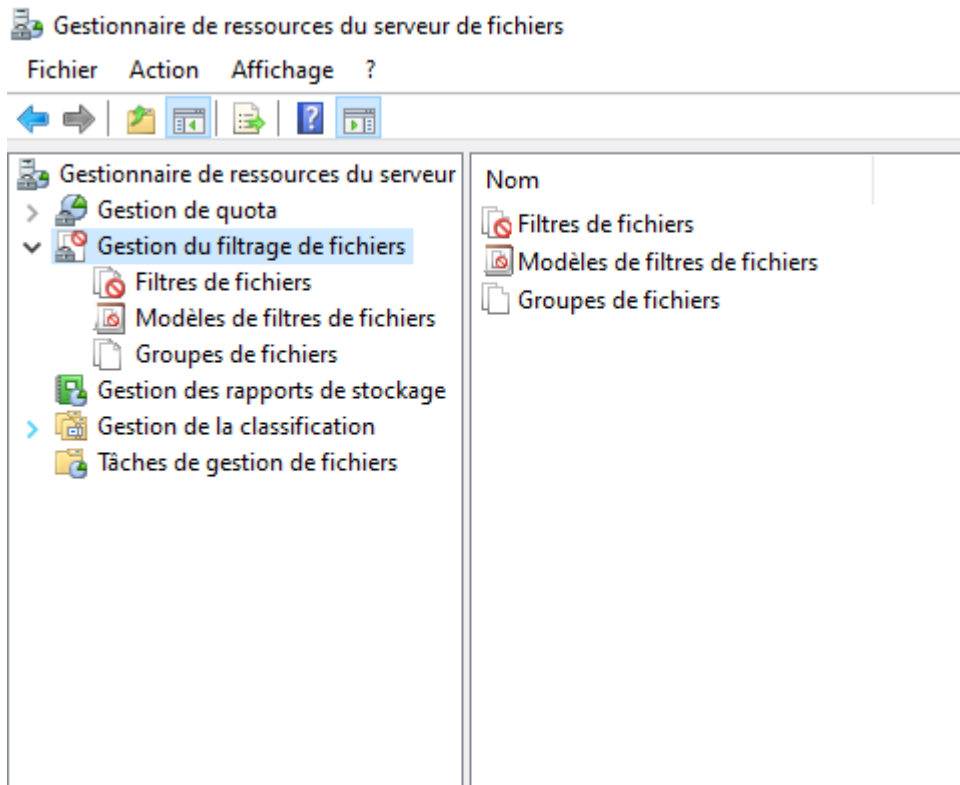


The screenshot shows a Windows application window titled 'Assistant Réplication de dossier'. The main title bar includes standard window controls (minimize, maximize, close). Below the title bar is a navigation pane on the left with the following steps listed: 'Nom du groupe de réplication et du dossier répliqué' (selected), 'Éligibilité de réplication', 'Membre principal', 'Sélection de topologie', 'Membres concentrateurs', 'Connexions Hub and Spoke', 'Planification du groupe de réplication et bande passante', 'Vérifier les paramètres et créer le groupe de réplication', and 'Confirmation'. The main area of the window contains a heading 'Nom du groupe de réplication et du dossier répliqué' with a small icon of a folder and a star. Below this heading is a descriptive text: 'Cet Assistant crée un groupe de réplication qui contient les serveurs hébergeant les cibles de dossier. Vérifiez les noms du groupe et du dossier suggérés puis modifiez-les si nécessaire.' There are two text input fields: 'Nom du groupe de réplication :' with the value 'health-north.fr\partages\chirurgie' and 'Nom du dossier répliqué :' with the value 'chirurgie'. At the bottom right of the window are three buttons: '< Précédent' (disabled), 'Suivant >' (active), and 'Annuler' (disabled).

Il faut donc bien renseigner le nom du dossier répliqué. Après, nous pouvons laisser toutes les configurations de base. Il faut simplement choisir le membre principal, dans notre cas FS01. Une fois cette étape terminée, le serveur va créer le groupe de réplication. Cette étape permet la synchronisation des fichiers entre FS01 et FS02. Pour le partage chirurgie, il faut donc répéter cette étape pour l'ensemble des partages.

Nous pouvons donc passer à l'étape suivante, qui est le filtrage des fichiers vidéo.

Pour cela, il faut aller dans le gestionnaire de ressources du serveur de fichiers.



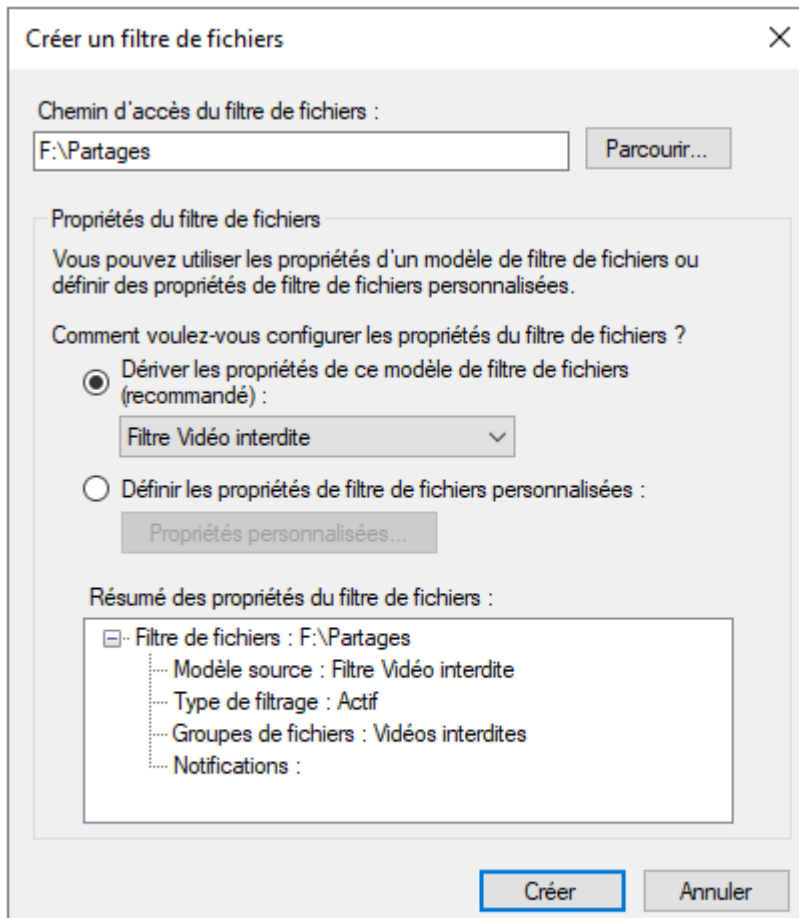
Il faut ensuite aller dans « Groupes de fichiers ».

Et créer un groupe de fichiers que l'on va appeler « Vidéo interdite » où l'on va ajouter l'ensemble des fichiers que l'on souhaite interdire dans les partages, comme ceci.



Ensuite, nous pouvons aller dans « Filtres de fichiers » et créer un filtre de fichiers.

Comme ceci, nous pouvons mettre directement le chemin du partage local sur le serveur, puis choisir le filtre « Vidéo interdite ».



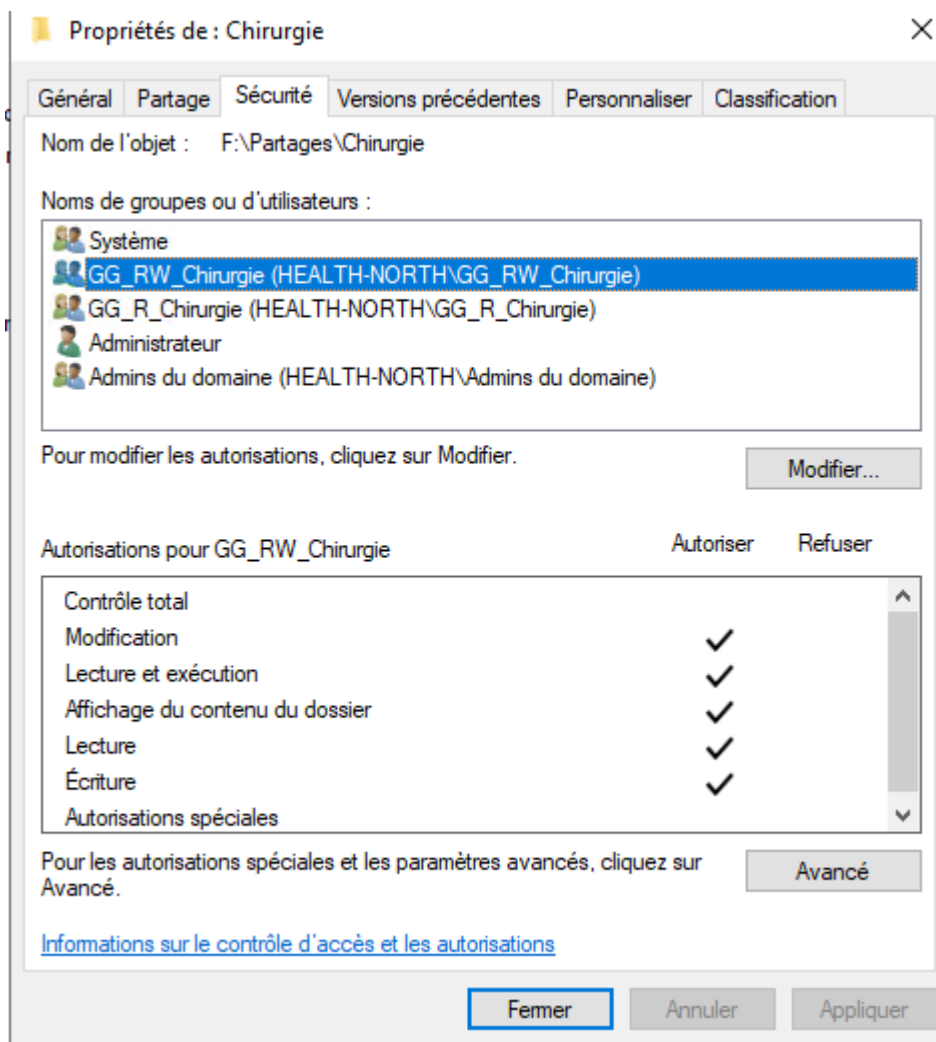
Cette étape est à répéter sur les deux serveurs.

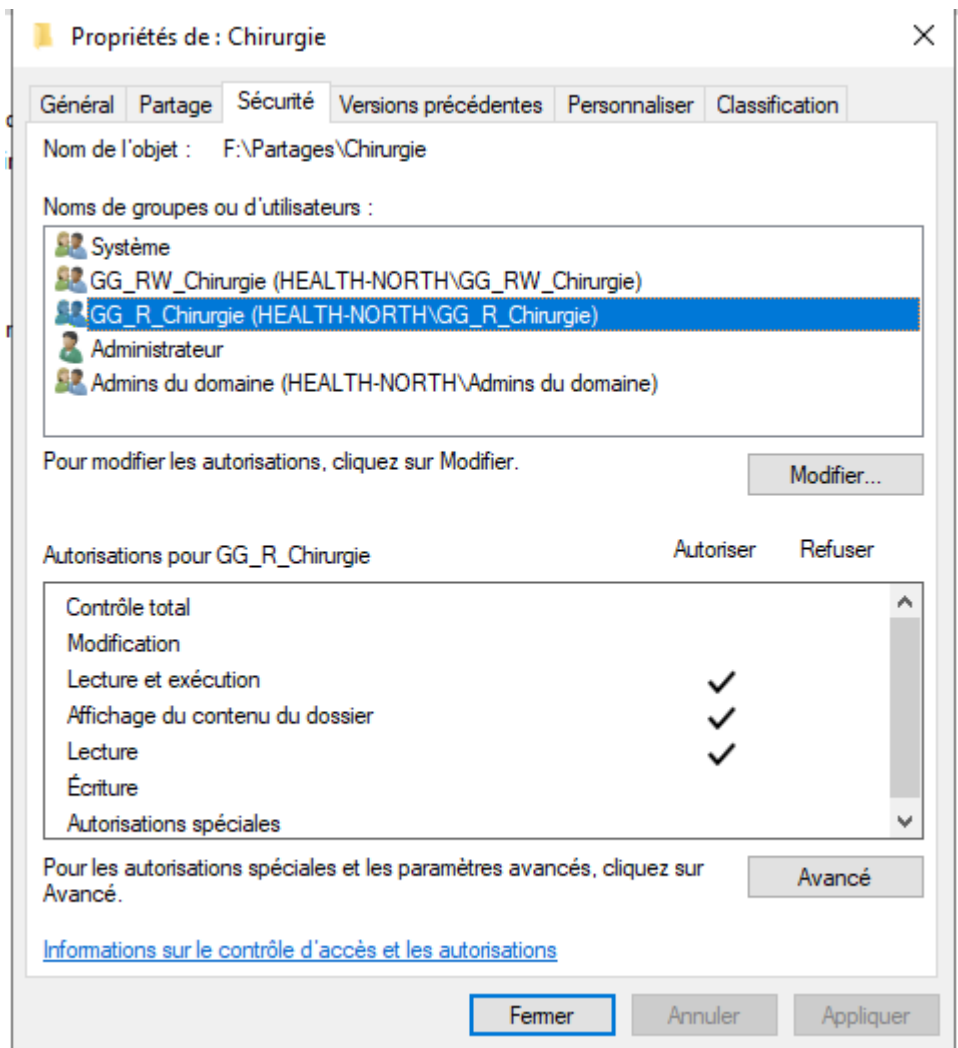
Pour finir, nous devons mettre en place les GPO pour les lecteurs réseau, la politique de mots de passe, et le blocage de l'accès au CMD, ainsi que la mise en place des fonds d'écran par utilisateur.

GPO et environnement utilisateur

Dans un premier temps, nous allons commencer par la mise en place des GPO pour les lecteurs réseau des utilisateurs.

Pour cela, sur les deux serveurs, dans le dossier partagé chirurgie, il faut aller dans les propriétés de sécurité et ajouter nos deux groupes, donc GG_RW_Chirurgie et GG_R_Chirurgie, puis attribuer les autorisations adéquates : pour GG_RW_Service, le droit de modification, et pour GG_R_Service, le droit de lecture, comme ceci.





Il faut donc répéter cette étape pour chaque dossier partagé sur les deux serveurs de fichiers. Puis, nous pouvons nous connecter sur AD01 afin de créer les GPO.

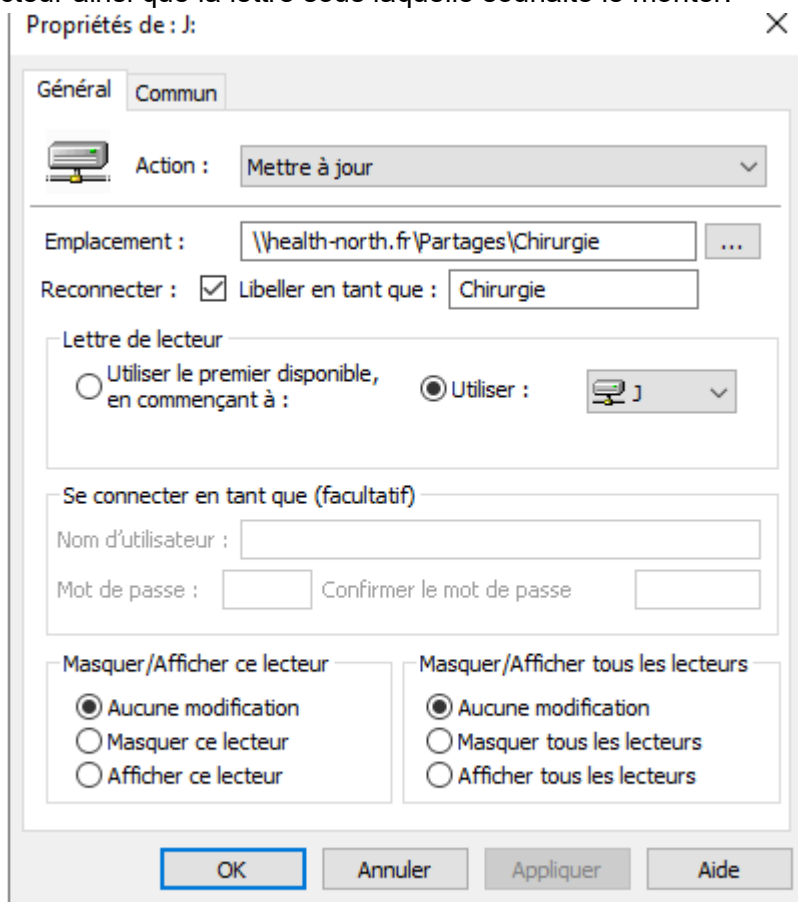
Pour ce faire, il faut aller sur la gestion des stratégies de groupe. Nous y retrouvons notre arborescence de l'Active Directory. Nous pouvons donc aller dans « Utilisateur » puis « Chirurgie » pour commencer à créer les GPO. Sur « Chirurgie », nous pouvons faire un clic droit et créer un objet GPO dans ce domaine, puis le lier ici.

Ensuite, nous pouvons donner un nom à notre GPO. Dans notre cas : GPO_Lecteur_J_Chirurgie.

Une fois créée, nous pouvons faire un clic droit et modifier la GPO. Ensuite, il faut aller dans :

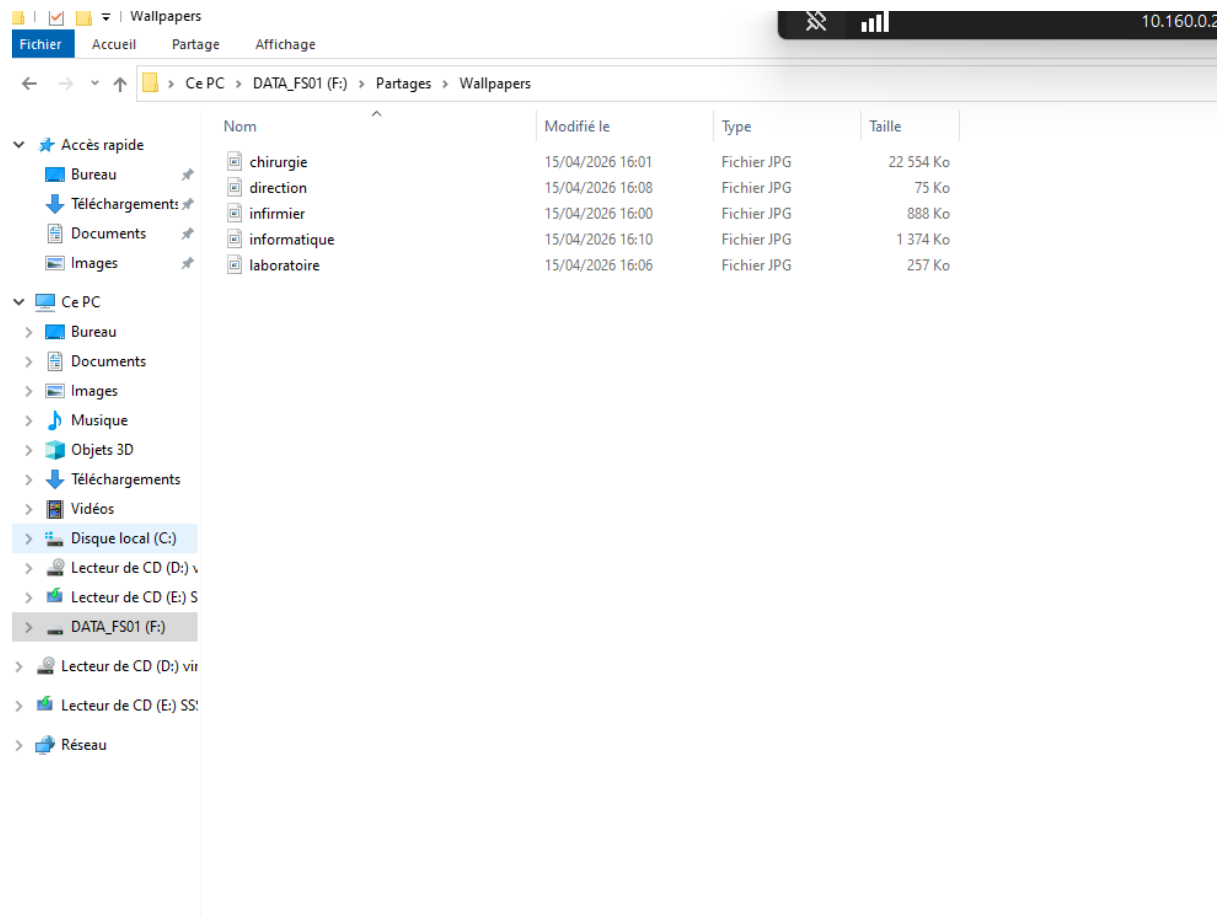
Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs.

Puis faire un clic droit, sélectionner « Nouveau lecteur », ajouter le chemin de partage du lecteur ainsi que la lettre sous laquelle souhaite le monter.



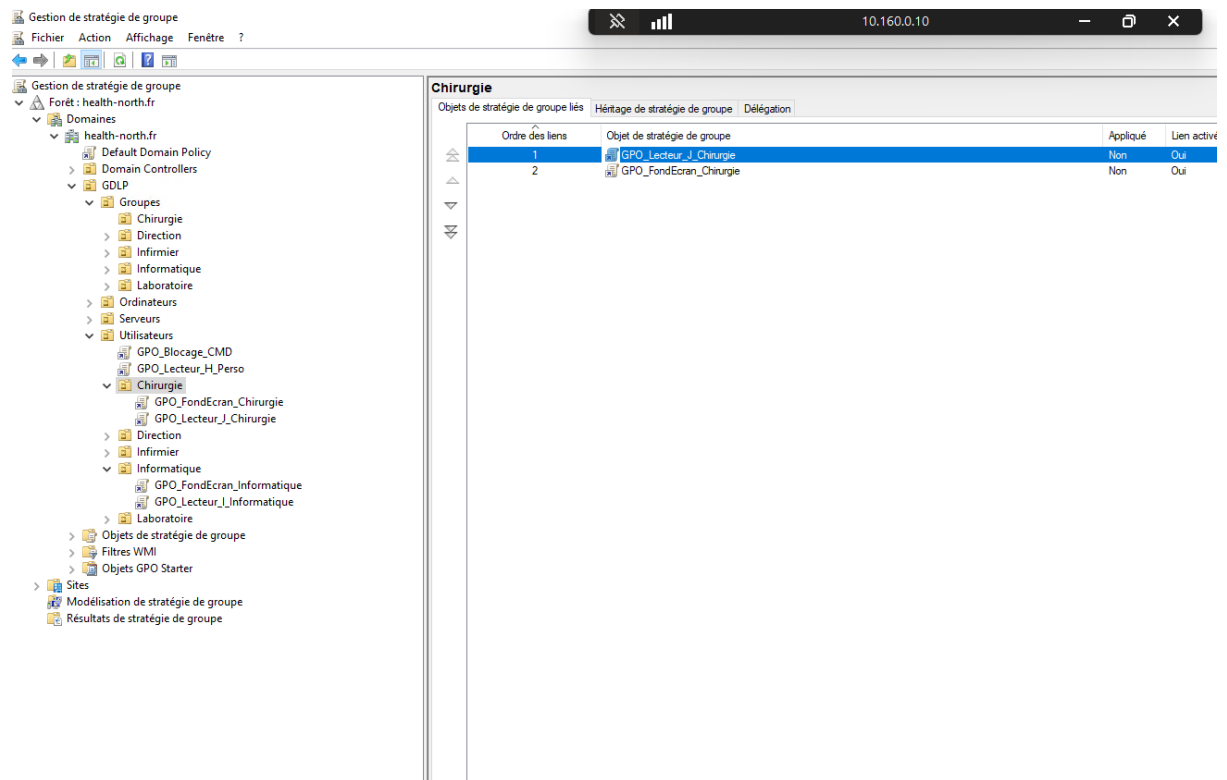
Il faut ensuite répéter cette opération pour tous les partages.

Une fois cela fait, nous pouvons mettre en place des fonds d'écran par service. Pour cela, il faut créer, sur les serveurs de fichiers, un partage exactement comme précédemment, nommé « Wallpaper ». À l'intérieur, il faut y placer les images que l'on souhaite utiliser comme fonds d'écran, avec un nom précis, comme ceci.



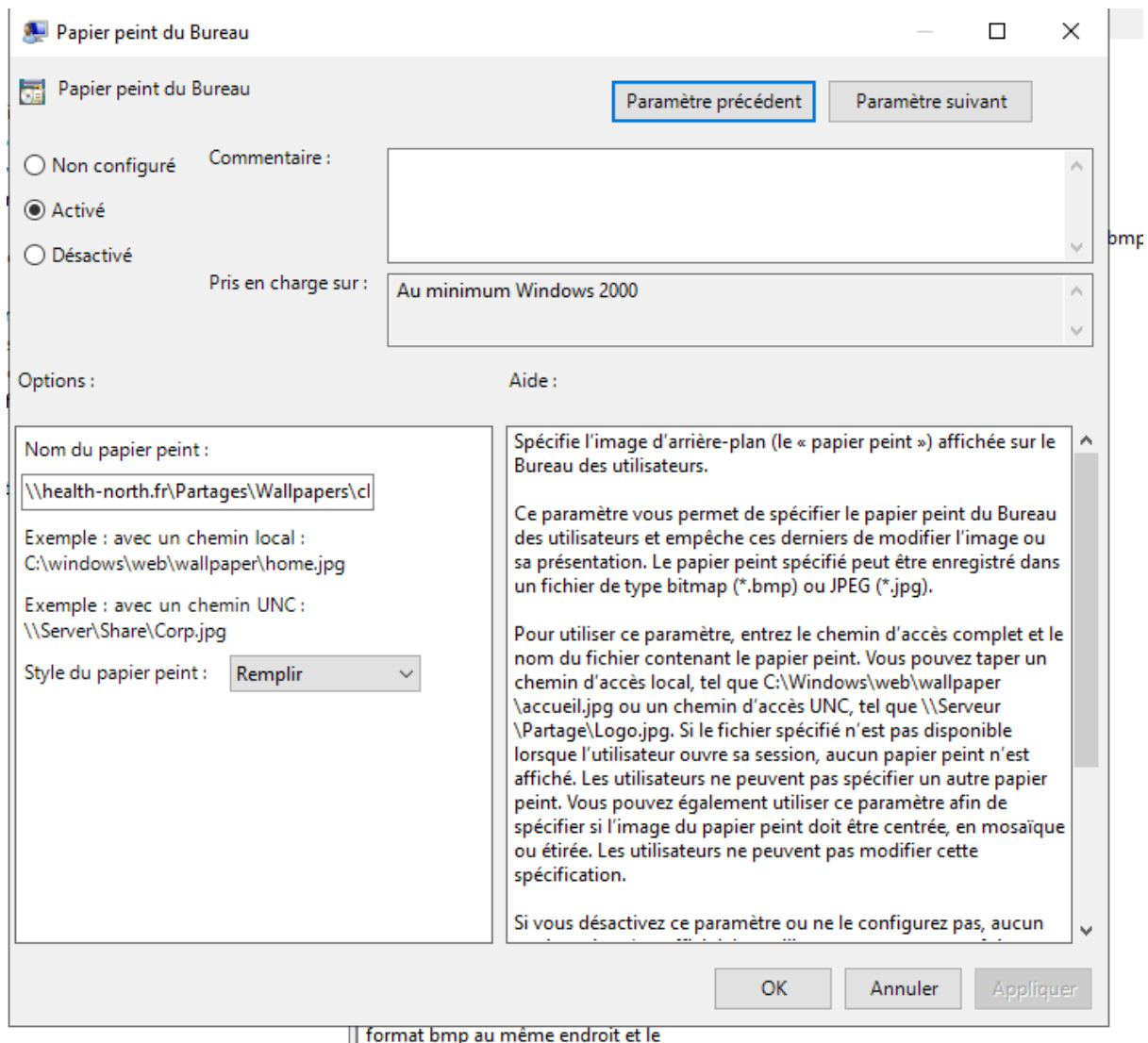
Une fois cela fait, nous pouvons mettre en place les GPO de fond d'écran. Pour ce faire, toujours dans « Chirurgie », nous pouvons créer une nouvelle GPO nommée :

GPO_FondEcran_Chirurgie.



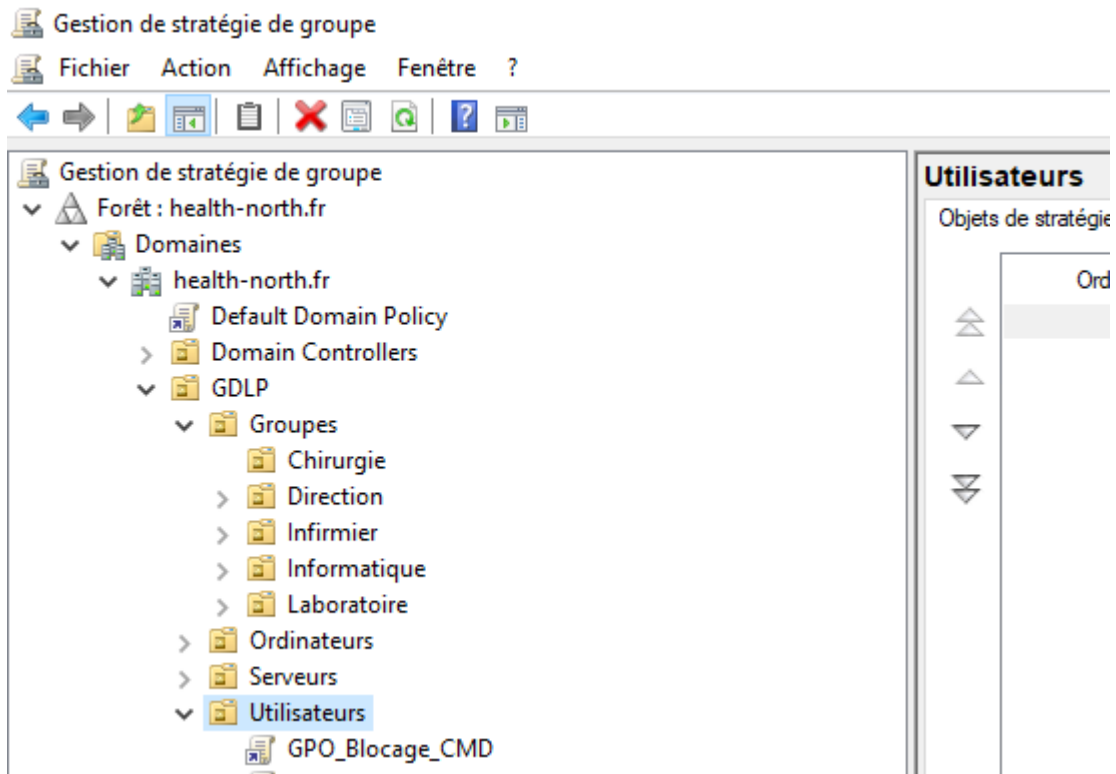
Il faut ensuite aller dans « Configuration utilisateur » > Stratégies > Modèles d'administration > Bureau > Bureau.

Ensuite, nous devons activer la règle et définir le chemin du papier peint en fonction du partage que nous avons créé.

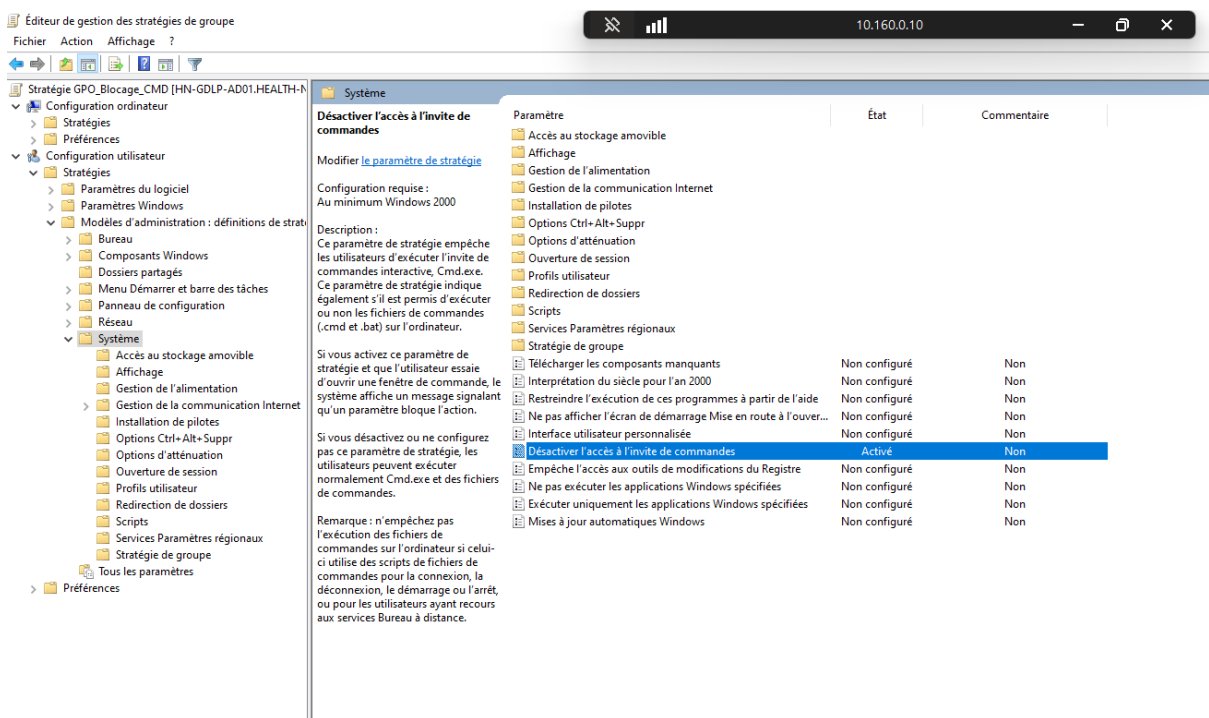


Par la suite, nous allons mettre en place la stratégie de mots de passe ainsi que celle de blocage du CMD.

Pour le blocage du CMD, nous allons la créer à la racine de notre unité organisationnelle « Utilisateurs ».

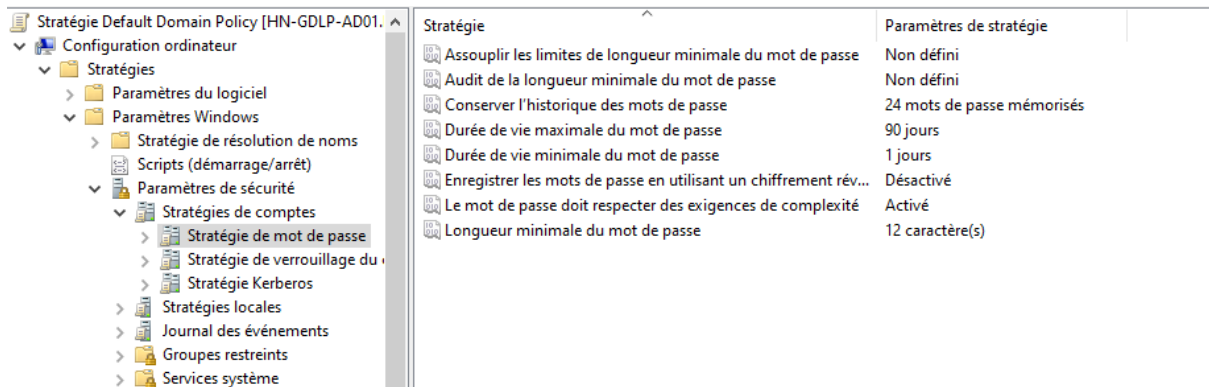


Ensuite, il faut aller ici pour activer cette règle.



Puis, il faut aller à la racine de health-north.fr et modifier la « Default Domain Policy ».

Ensuite, il faut se rendre à cet endroit afin d'appliquer les paramètres comme ceci.



Lorsque cette étape est terminée, nous pouvons procéder aux tests. Pour cela, il suffit de nous connecter avec un compte utilisateur, et de vérifier si le bon fond d'écran du service s'applique, ainsi que de vérifier si nous pouvons ouvrir le CMD.

