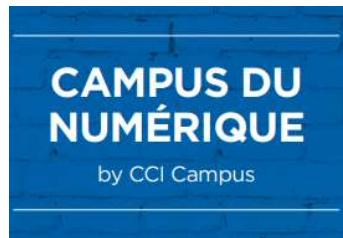


PROJET M2i



AP3

LIVRABLE 2

RAPPORT DE CLÔTURE DU PROJET

Date limite de remise : 31 décembre 2022

Les résultats, opinions et recommandations exprimés dans ce rapport émanent de l'auteur ou des auteurs et n'engagent aucunement CCI Campus

SOMMAIRE

Date limite de remise : 31 décembre 2022	1
1) RESUME DU PROJET	3
1.1) Définitions des rôles et responsabilités.....	3
1.2) Rappel des objectifs fixés	3
2) CONDUITE DU PROJET	4
2.1) Planning prévisionnel VS Planning réel	4
2.2) Ressources utilisées	6
2.3) Problèmes rencontrés et solutions apportées ou envisagées	8
2.4) Ancien schéma réseau VS nouveau	8
2.5) Tableau de synthèse	9
3) RESULTATS	10
3.1) Résultats attendus VS Résultats obtenus.....	10
4) ANALYSE FINALE	10
4.1) Analyse et état finale du projet.....	10
5) CONCLUSION	10
6) DOCUMENTATION TECHNIQUE	11
6.1) Création du serveur STG-SRV01.....	11
a) Information du serveur	11
b) Installation de l'Active directory	11
c) l'Arborescence	19
d) DNS	28
e) DHCP	36
f) Mise en place DFS DFS-R.....	47
g) Ajout d'un serveur d'espace de nom	55
h) Ajout de dossiers partagé	56
i) DFS-R configuration de la réPLICATION.....	59
6.2) Création du Routeur / Firewall Opensense Strasbourg.....	62
a) Information du serveur	62
b) Création de la VM.....	63
c) Configuration réseau	66

d) Configuration général	68
e) Mise en place VPN IPSEC.....	71
f) Mise en place du portail captif.....	76
6.3) Création du Routeur / Firewall Opensense Mulhouse	92
a) Information du serveur.....	92
b) Configuration réseau	92
c) Configuration générale	94
d) Mise en place VPN IPSEC	96
6.4) Serveur de Sauvegarde SAN et cliché instantané Shadow copy	103
a) Installation du serveur TrueNas	103
b) Configuration de TrueNas	107
c) Activation des clichés instantanés.....	112
d) Utilisation des versions précédentes	116

1) RESUME DU PROJET

1.1) Définitions des rôles et responsabilités

	Tom HOERMANN	Matteo ADDARIO
Responsabilité	Chef de projet	Technicien
Rôles	Routeur /Firewall VPN IpSec Portail captif ADDS, DNS, DHCP	SAN Truenas Shadowcopy DFS réPLICATION GPO

1.2) Rappel des objectifs fixés

La nouvelle CCI Grand Est a remplacé depuis le 1er janvier 2017 les 3 anciennes CCI régionales d'Alsace. En 2022, CCI Campus inaugure un nouveau campus du numérique avec 9 formations de Bac+2 à Bac+5. Pour ces nouvelles formations, la DSI a décidé de lancer un appel d'offres pour la création d'un réseau informatique indépendant, la création et l'équipement de nouvelles salles informatiques.

Pour ce faire, nous allons devoir améliorer le service aux utilisateurs et faciliter d'administration par la DSI en faisant un système d'information indépendant, un système informatique uniformisé, des liaisons inter-sites entre les établissements et des redondances.

Un retour sur investissement par la réduction des coûts sera à réaliser (possession/exploitation). On réalisera une documentation complète et on facilitera l'administration.

Faciliter le travail collaboratif en termes de partage et d'accessibilité des données inter-sites

Et enfin, la dernière partie que nous traiterons se trouve au niveau de la sécurité des systèmes et des données. Il faudra mettre un accès internet légal à disposition mais aussi faciliter la mise en place d'un PCA (plan de continuité d'activité), la redondance des serveurs, service et données et faire des sauvegardes régulières des serveurs.

Pour ce qui concerne les objectifs attendus pour cet Atelier professionnel, trois règles très importantes sont à respecter :

- Respecter la date de début et de fin de projet
- La solution que nous proposons doit être à moindre coût et nous avons un budget à respecter de maximum 100 000€ HT
- Rendre les livrables et effectuer les soutenances aux dates prévues

Pour ce qui est de la mise en œuvre technique, nous créerons une nouvelle salle informatique à Strasbourg et à Mulhouse en mettant en place des serveurs, des postes de travail, etc.... et faire attention au coût des licences et de la main d'œuvre.

Nous mettrons en place une liaison WAN inter-sites chiffrée mais aussi une harmonisation du plan d'adressage et de nommage sur l'ensemble des sites.

Nous créerons des serveurs et des rôles/services en haute disponibilité (AD/DNS/DHCP/DFS/Partage SMB/etc. ..)

Un portail-captif avec authentification forte sera mise en œuvre et il faudra qu'il soit conforme à la législation Française et Européenne.

Une redondance, des droits et des permissions adaptés devront être possible lors de l'accès aux données stockant les dossiers personnels des enseignants et des élèves sur les deux sites.

Et enfin, il faudra qu'on prenne en considération les recommandations de l'ANSSI.

2) CONDUITE DU PROJET

2.1) Planning prévisionnel VS Planning réel

Planning prévisionnel :

Taches à réaliser	Date de début	date de fin	Durée	Réalisateur
Serveur AD, DNS, DHCP	Vendredi 21/10/22	Vendredi 04/11/22	8 Heures	Julien GOMES
DFS, RéPLICATION	Vendredi 18/11/22	Vendredi 02/12/22	8 Heures	Julien GOMES
Routeur OpenSense + Firewall + portail captif	Vendredi 21/10/22	Vendredi 04/11/22	8 Heures	Tom HOERMANN
VPN IpSec	Vendredi 18/11/22	Vendredi 02/12/22	8 Heures	Tom HOERMANN
Serveur de sauvegarde trueNas + Shadow copy	Vendredi 21/10/22	Vendredi 04/11/22	8 Heures	Matteo ADDARIO
GPO	Vendredi 18/11/22	Vendredi 02/12/22	8 Heures	Matteo ADDARIO
Mise en commun + correcteur erreur	Vendredi 16/12/22	Vendredi 16/12/22	4 Heures	Groupe 2

Le planning prévisionnel nous montre que l'on avait chacun 2 jours pour réaliser nos parties, plus 4 heures de mise en commun et de correction d'erreur.

Diagramme de Gantt prévisionnel :

Diagramme de Gantt	Vendredi 21/10/22	Vendredi 04/11/22	Vendredi 18/11/22	Vendredi 02/12/22
Serveur AD, DNS, DHCP				
DFS, RéPLICATION				
Routeur OpenSense + Firewall + portail captif				
VPN IpSec				
Serveur de sauvegarde trueNas + Shadow copy				
GPO				
Mise en commun + correcteur erreur				

Planning réel :

Taches à réaliser	Date de début	date de fin	Débug	Durée	Réalisateur
Serveur AD, DNS, DHCP	Mercredi 14/12/22	Jeudi 15/12/22	Rien	8 Heures	Tom HOERMANN
DFS, RéPLICATION	Mercredi 14/12/22	Jeudi 15/12/22	2 heures jeudi 15/12/2022	8 Heures	Matteo ADDARIO
Routeur OpenSense + Firewall + portail captif	Vendredi 21/10/22	Vendredi 04/11/22	Rien	8 Heures	Tom HOERMANN
VPN IpSec	Vendredi 18/11/22	Vendredi 02/12/22	2 heures mercredi 14/12/2022	7 Heures	Tom HOERMANN
Serveur de sauvegarde trueNas + Shadow copy	Vendredi 21/10/22	Vendredi 04/11/22	2 heures mercredi 14/12/2022	8 Heures	Matteo ADDARIO
GPO	Vendredi 18/11/22	Vendredi 02/12/22	Rien	8 Heures	Matteo ADDARIO
Mise en commun + correcteur erreur	Vendredi 16/12/22	Vendredi 16/12/22	6 heures mercredi 14/12/2022	6 Heures	Matteo ADDARIO Tom HOERMANN

Le planning réel montre la partie serveur AD et serveur Core à était réalisé très tard au vu de l'abandon du technicien Julien Gomes dans le projet. Cette partie a donc était repartie entre les 2 autres opérateurs ce qui à créer du retard. Des heures de mise en commun et debug ont aussi était ajouté.

Diagramme de Gantt réel :

Diagramme de Gantt	Vendredi 21/10/22	Vendredi 04/11/22	Vendredi 18/11/22	Vendredi 02/12/22	mercredi 14/12/2022	Jeudi 15/12/2022
Serveur AD, DNS, DHCP						
DFS, RéPLICATION						
Routeur OpenSense + Firewall + portail captif						
VPN IpSec						
Serveur de sauvegarde trueNas + Shadow copy						
GPO						
Mise en commun + correction erreur						

2.2) Ressources utilisées

Devis interne :

AP3
LIVRABLE 2

GROUPE 2
HOERMANN Tom et ADDARIO Matteo

Description	Quantité	Prix unitaire HT	Prix total HT
PC Office Intel i7 Business	60	399,00 €	23 940,00 €
kit clavier + souris	60	38,40 €	2 304,00 €
Dell SE2222H Écran	60	129,00 €	7 740,00 €
NAS 4baies Synology RackStation RS822RP+	2	1 238,00 €	2 476,00 €
DD NAS 1 To WD Red Plus	6	76,29 €	457,74 €
Switch Cisco SB CBS250-48P-4G	2	999,99 €	1 999,98 €
Serveurs HPE ProLiant DL20 Gen10 Plus	6	1 176,99 €	7 061,94 €
HPE Midline - Disque dur - 2 To	12	201,60 €	2 419,20 €
Routeur industriel compact	2	219,00 €	438,00 €
License Windows servers 2016	6	882,00 €	5 292,00 €
License Windows 10 family	60	129,00 €	7 740,00 €

Total HT	61 868,86 €
TVA (20,00 %)	12 373,77 €
Total TTC	74 242,63 €

Devis externe :

Description	Quantité	Prix unitaire HT	Prix total HT
INFRASTRUCTURE - chef de projet	8	699,00 €	5592,00 €
INFRASTRUCTURE - Techniciens	8	399,00 €	3192,00 €
		Total HT	8784,00 €
		TVA (20,00 %)	1756,80 €
		Total TTC	10540,80 €

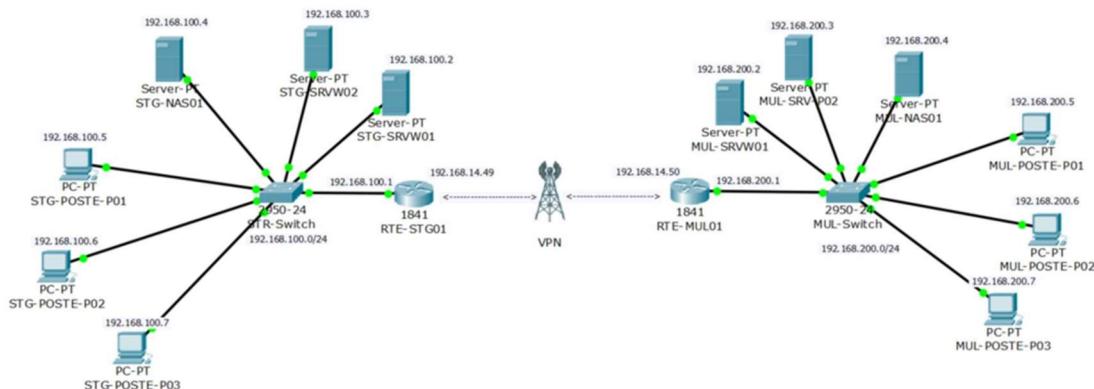
2.3) Problèmes rencontrés et solutions apportées ou envisagées

Technicien en moins → répartitions des tâches et augmentation du temps de travail

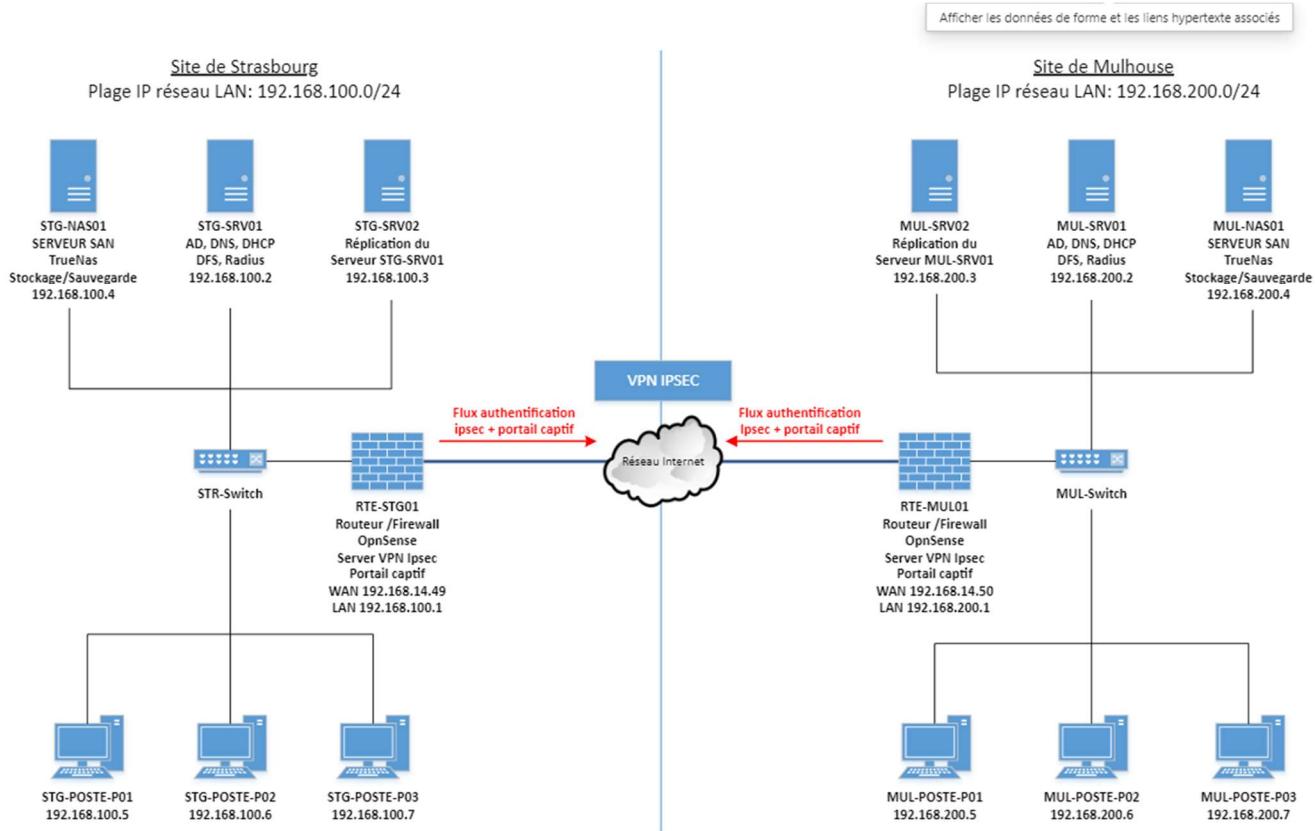
VPN IPSec qui n'arrive plus à faire la connexion tunnel → problème lié aux IP données par l'opérateur internet → résolue avec un changement de réseau et de configuration VirtualBox

2.4) Ancien schéma réseau VS nouveau

Ancien schéma réseau :



Nouveau schéma réseau :



2.5) Tableau de synthèse

Name	Ip address	Netmask	Passerelle	DNS
STRASBOURG				
RTE-STG01 LAN	192.168.100.1	255.255.255.0		192.168.100.2
RTE-STG01 WAN	172.20.10.4	255.255.255.0		192.168.100.2
STG-SRVW01	192.168.100.2	255.255.255.0	192.168.100.1	192.168.100.2
STG-SRVW02	192.168.100.3	255.255.255.0	192.168.100.1	192.168.100.2
STG-NAS01	192.168.100.4	255.255.255.0	192.168.100.1	192.168.100.2
STG-POSTE-P01	192.168.100.5	255.255.255.0	192.168.100.1	192.168.100.2
STG-POSTE-P02	192.168.100.6	255.255.255.0	192.168.100.1	192.168.100.2
STG-POSTE-P03	192.168.100.7	255.255.255.0	192.168.100.1	192.168.100.2
MULHOUSE				
RTE-MUL01 LAN	192.168.200.1	255.255.255.0		192.168.200.2
RTE-MUL01 WAN	172.20.10.3	255.255.255.0		192.168.200.2
MUL-SRVW01	192.168.200.2	255.255.255.0	192.168.200.1	192.168.200.2
MUL-SRVW02	192.168.200.3	255.255.255.0	192.168.200.1	192.168.200.2
MUL-NAS01	192.168.200.4	255.255.255.0	192.168.200.1	192.168.200.2
MUL-POSTE-P01	192.168.200.5	255.255.255.0	192.168.200.1	192.168.200.2
MUL-POSTE-P02	192.168.200.6	255.255.255.0	192.168.200.1	192.168.200.2
MUL-POSTE-P03	192.168.200.7	255.255.255.0	192.168.200.1	192.168.200.2

3) RESULTATS

3.1) Résultats attendus VS Résultats obtenus

Résultat Attendu	Résultat obtenus
Serveur ADDS, DNS, DHCP	Mis en place et opérationnel
DFS, réPLICATION	Mis en place et opérationnel
Routeur/Firewall	Mis en place et opérationnel
VPN IPsec	Mis en place et opérationnel
Portail Captif	Mis en place et opérationnel
Serveur de sauvegarde + Shadow copy	Mis en place et opérationnel

4) ANALYSE FINALE

4.1) Analyse et état finale du projet

Le service a donc été amélioré pour les utilisateurs et il permet de faciliter l'administration par la DSI avec ce nouveau système d'information indépendant. Le système informatique est maintenant uniformisé et des liaisons inter-sites entre les établissements sont possibles. La sécurité de pertes des données est amélioré grâce au système de redondances.

Le budget de 100 000€ HT établie par le client a été respecté. Le budget total du projet est donc de 84 783.40€ HT.

Le projet a été finaliser dans les temps et à respecté les demandes du cahier des charges.

5) CONCLUSION

Pour conclure, malgré les difficultés rencontrées avec le VPN IPSEC et la mise en place du DFS, les objectifs imposés dans le cahier des charges ont était remplies dans le temps et avec le budget imposé.

6) DOCUMENTATION TECHNIQUE

6.1) Création du serveur STG-SRV01

a) Information du serveur

Nom du serveur : STG-SRV01

Interfaces IP :

- LAN : 192.168.100.2

Taille disque dur : 60 GB

RAM : 2 GO

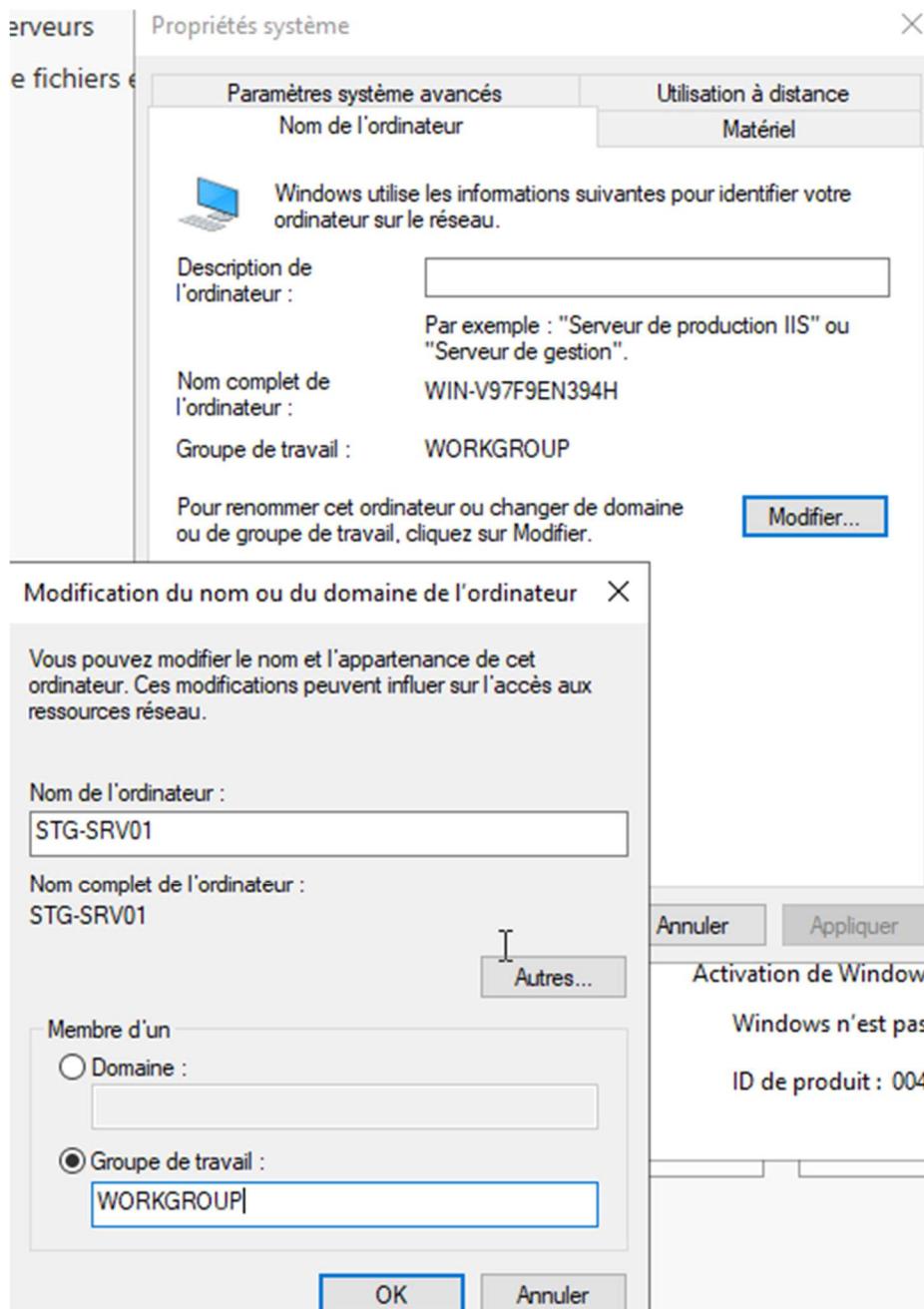
Version: Microsoft Windows 2019 Standard

b) Installation de l'Active directory

On tout d'abord changer le nom du serveur en se rendant dans le panneau de configuration :

Panneau de configuration > Système et sécurité > Système

Puis modifier les paramètres,



Et on redémarre.

On se rend maintenant dans le Gestionnaire de serveur et on va ajouter le rôle active directory « AD DS »

On clique sur ajouter des rôles et des fonctionnalités :

BIENVENUE DANS GESTIONNAIRE DE SERVEUR



1 Configurer ce serveur local

- 2 Ajouter des rôles et des fonctionnalités
- 3 Ajouter d'autres serveurs à gérer
- 4 Créer un groupe de serveurs
- 5 Connecter ce serveur aux services cloud

Puis on clique sur suivant,

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
STG-SRV01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

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

Sélectionner un serveur du pool de serveurs

Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :		
Nom	Adresse IP	Système d'exploitation
STG-SRV01	172.20.10.6, 19...	Microsoft Windows Server 2019 Standard

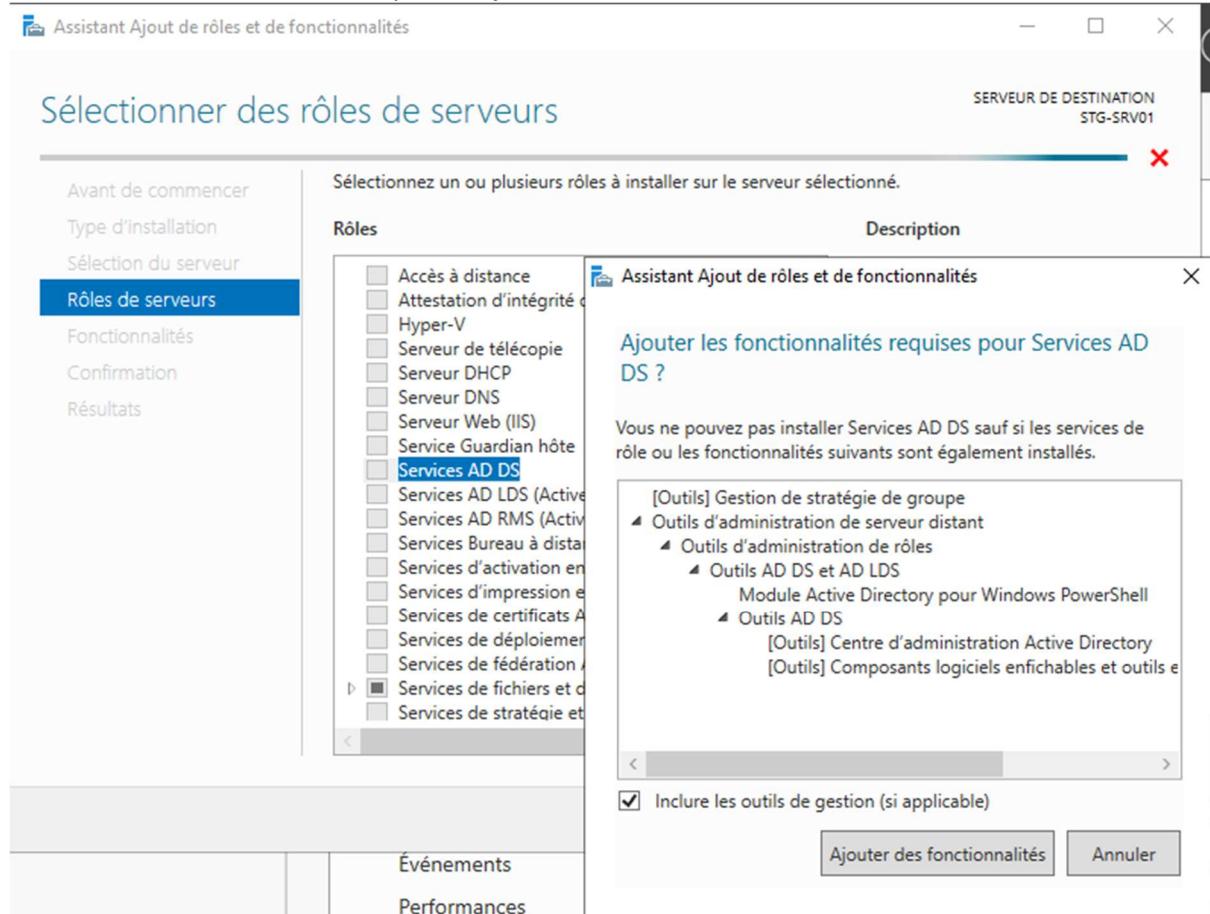
1 ordinateur(s) trouvé(s)

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

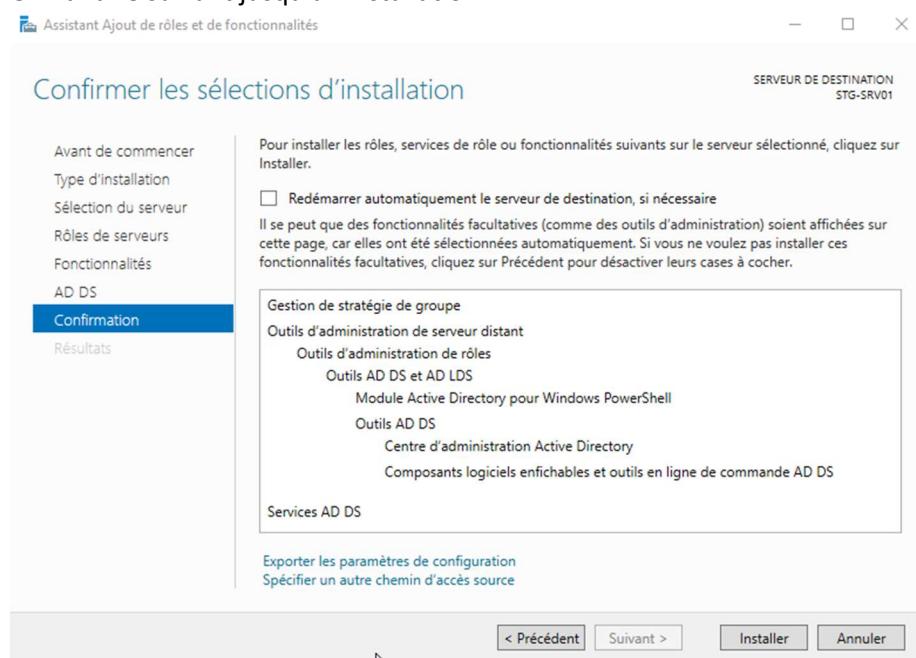
< Précédent Suivant > Installer Annuler

On sélectionne notre serveur, puis suivant,

On coche le rôle AD DS et on clique sur ajouter des fonctionnalités :



On va faire suivant jusqu'à l'installation :



Progression de l'installation

SERVEUR DE DESTINATION
STG-SRV01

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- AD DS
- Confirmation
- Résultats**

Afficher la progression de l'installation

1 Démarrage de l'installation

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

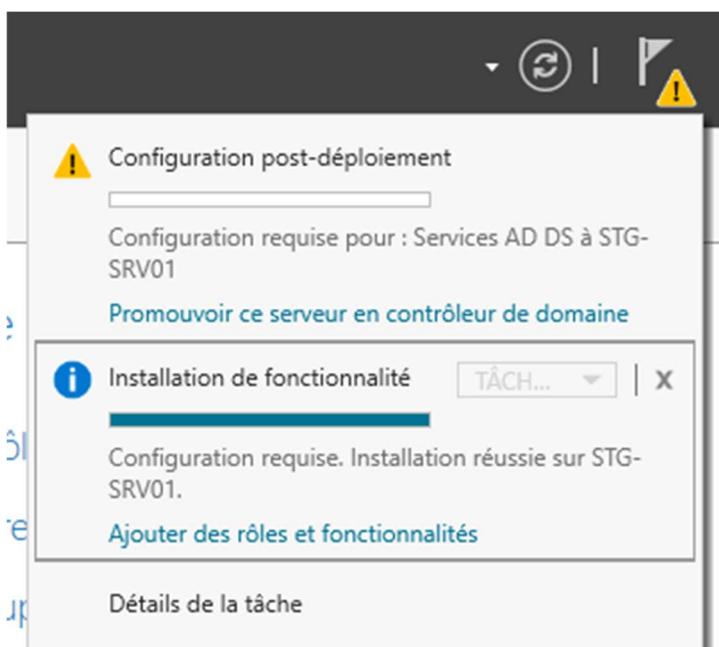
Composants logiciels enfichables et outils en ligne de commande AD DS

Services AD DS

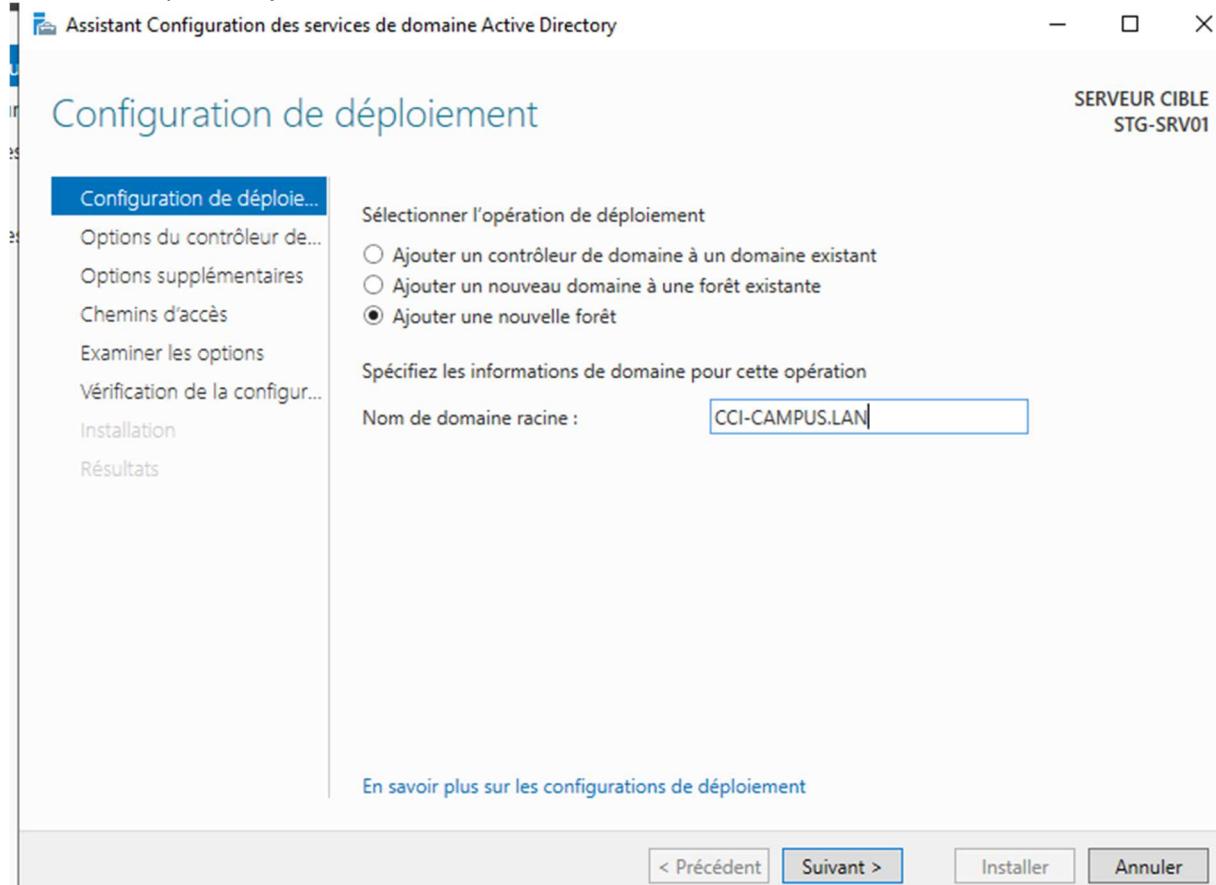
! Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

[Exporter les paramètres de configuration](#)

Une fois installé, on va cliquez sur le drapeau et ensuite sur « promouvoir cde serveur en contrôleur de domaine »

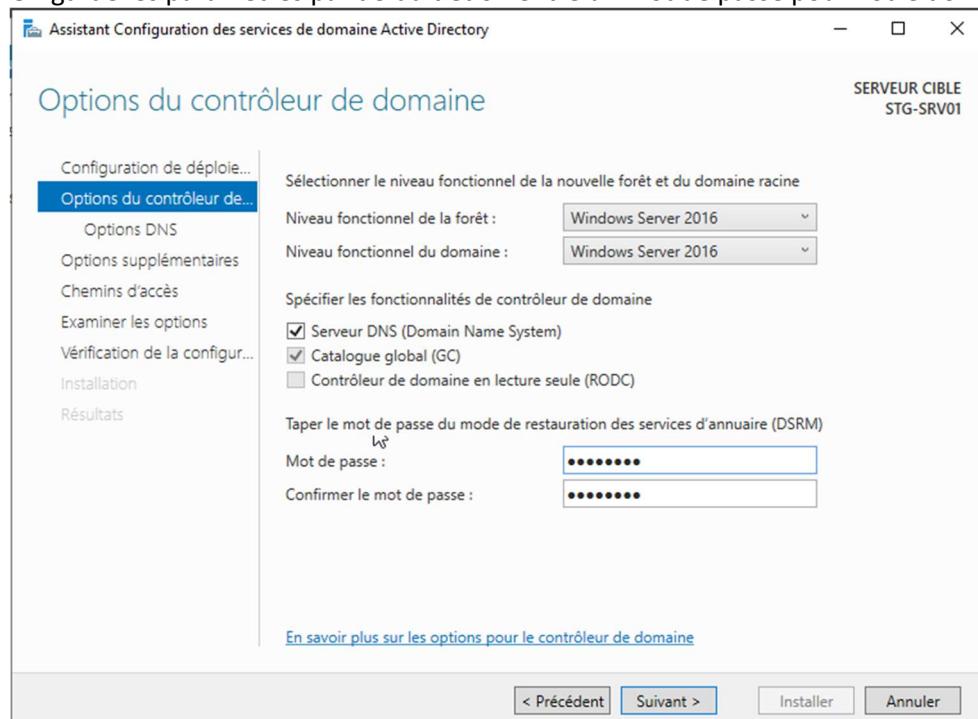


On choisit l'option « ajouter une nouvelle forêt » et on rentre notre nom de domaine :



Suivant,

On garde les paramètres par default et on entre un mot de passe pour notre domaine :



Suivant,

Options DNS

SERVEUR CIBLE
STG-SRV01

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#) X

[Configuration de déploie...](#)
[Options du contrôleur de...](#)
Options DNS
[Options supplémentaires](#)
[Chemins d'accès](#)
[Examiner les options](#)
[Vérification de la config...](#)
[Installation](#)
[Résultats](#)

Spécifier les options de délégation DNS

Crée une délégation DNS

[En savoir plus sur la délégation DNS](#)

< Précédent
Suivant >
Installer
Annuler

Suivant,

Options supplémentaires

SERVEUR CIBLE
STG-SRV01

[Configuration de déploie...](#)
[Options du contrôleur de...](#)
[Options DNS](#)
Options supplémentaires
[Chemins d'accès](#)
[Examiner les options](#)
[Vérification de la config...](#)
[Installation](#)
[Résultats](#)

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

On laisse et suivant,

Chemins d'accès

SERVEUR CIBLE
STG-SRV01

[Configuration de déploie...](#)
[Options du contrôleur de...](#)
[Options DNS](#)
[Options supplémentaires](#)
Chemins d'accès
[Examiner les options](#)
[Vérification de la config...](#)
[Installation](#)
[Résultats](#)

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :	<input type="text" value="C:\Windows\NTDS"/>	<input type="button" value="..."/>
Dossier des fichiers journaux :	<input type="text" value="C:\Windows\NTDS"/>	<input type="button" value="..."/>
Dossier SYSVOL :	<input type="text" value="C:\Windows\SYSVOL"/>	<input type="button" value="..."/>

Suivant,

Vérification de la configuration requise

SERVEUR CIBLE
STG-SRV01

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer... [Afficher plus](#) ×

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

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

! [Voir les résultats](#)

! Les contrôleurs de domaine Windows Server 2019 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

! Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer des adresses IP statiques IPv4 et IPv6.

! Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur les conditions préalables](#)

< Précédent Suivant > Installer Annuler

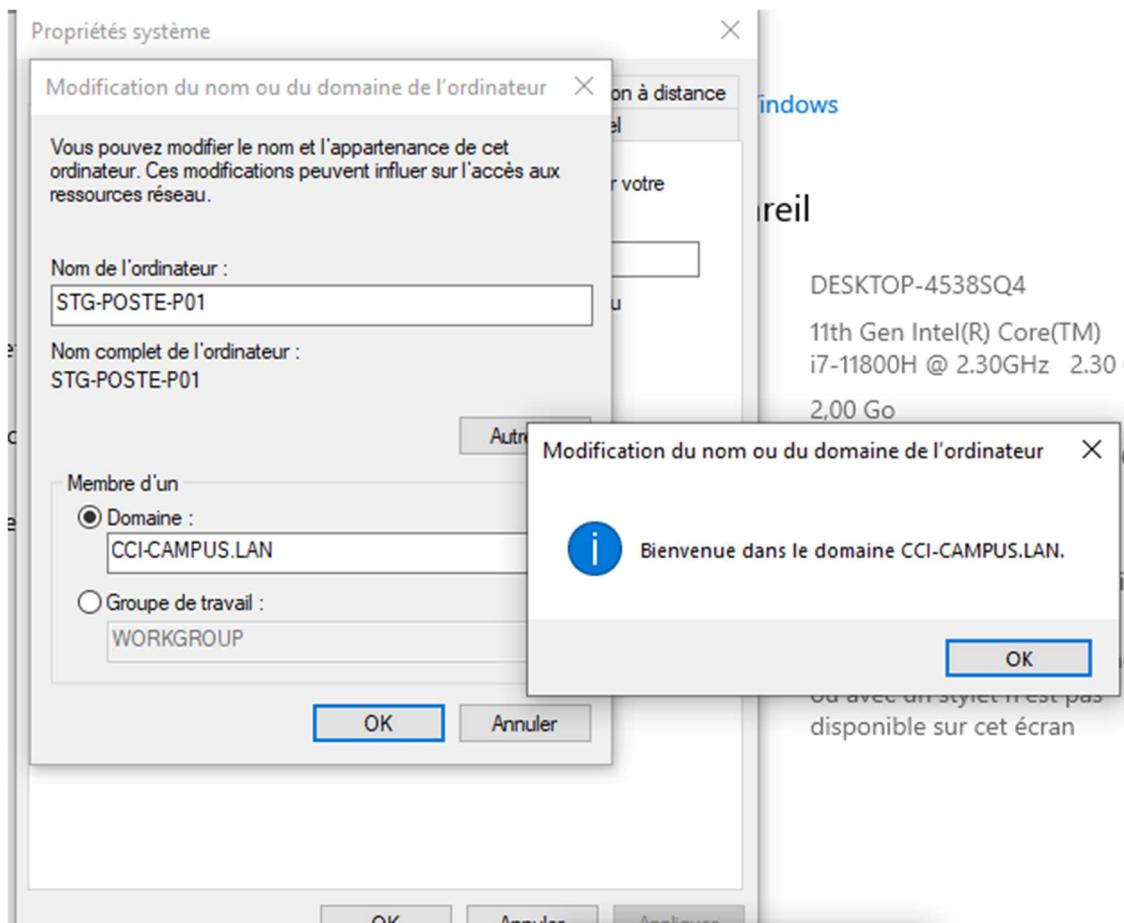
On clique sur installer,

On voit qu'on est bien dans le domaine :



On peut maintenant connecter nos équipements dans le domaine, par exemple pour les postes Windows 10, on se rend dans les paramètres Windows, changer le nom du pc, et on rentre le nom de domaine.

Après s'être identifier avec le mot de passe du domaine créé précédemment, on arrive à se connecter :



c) l'Arborescence

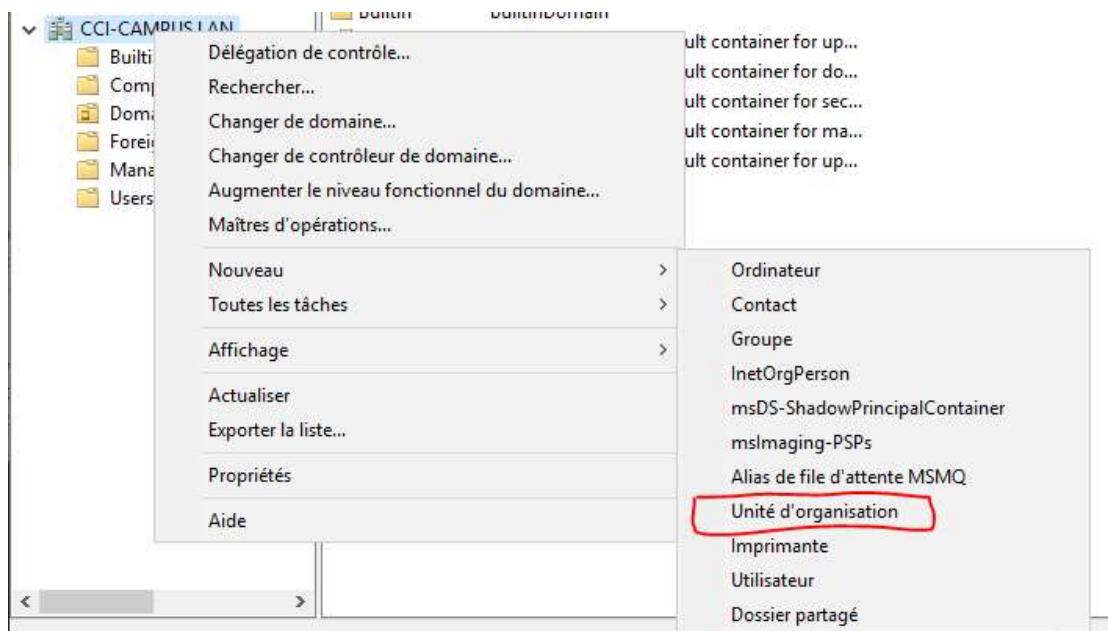
On va maintenant créer notre arborescence.

On se rend dans l'outils « Utilisateurs et ordinateurs Active directory »,

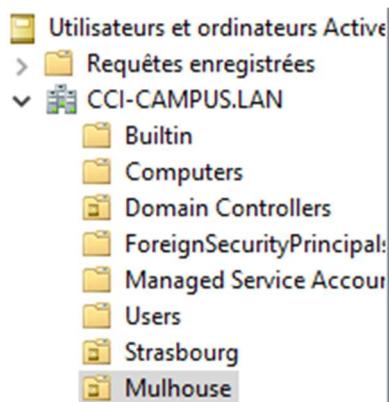
The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' (User and Computer Active Directory) management console. The left pane displays a tree view of the domain structure under 'CCI-CAMPUS.LAN', including 'Requêtes enregistrées', 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. The right pane lists objects with columns for 'Nom' (Name), 'Type' (Type), and 'Description'. The 'Computers' object is highlighted.

Nom	Type	Description
Builtin	builtinDomain	
Computers	Conteneur	Default container for up...
Domain Con...	Unité d'organisati...	Default container for do...
ForeignSecu...	Conteneur	Default container for sec...
Managed Se...	Conteneur	Default container for ma...
Users	Conteneur	Default container for up...

On va faire une clique droite sur notre nom de domaine et créer une Unité organisationnelle pour Strasbourg et une pour Mulhouse :



The image contains two separate windows of the 'Nouvel objet - Unité d'organisation' dialog box. Both windows have a title bar 'Utilisateurs et ordinateurs Active Directory' and a close button 'X'.
 Top window: The 'Créer dans' field is set to 'CCI-CAMPUS.LAN/'. The 'Nom:' field contains 'Strasbourg'. A checked checkbox 'Protéger le conteneur contre une suppression accidentelle' is present.
 Bottom window: The 'Créer dans' field is set to 'CCI-CAMPUS.LAN/'. The 'Nom:' field contains 'Mulhouse'. A checked checkbox 'Protéger le conteneur contre une suppression accidentelle' is present.



On va ensuite créer des UO « Groupes » et « users » dans strasbourg et mulhouse, dans l'uo groupes de strasbourg on va créer le groupe « GRP1 » et dans groupes de Mulhous on créer le groupe « GRP2 » :

The screenshot shows the 'Nouvel objet - Groupe' (New Object - Group) dialog box. The 'Créer dans' field is set to 'CCI-CAMPUS.LAN/Strasbourg'. The 'Nom du groupe' field contains 'GRP1'. The 'Nom de groupe (antérieur à Windows 2000)' field also contains 'GRP1'. Under 'Étendue du groupe', the 'Globale' option is selected. Under 'Type de groupe', the 'Sécurité' (Security) option is selected. At the bottom, the 'OK' button is highlighted with a blue border.

Nom	Type	Description
Users	Unité d'organisati...	
Groupes	Unité d'organisati...	

Nouvel objet - Groupe

Créer dans : CCI-CAMPUS.LAN/Mulhouse

Nom du groupe : **GRP2**

Nom de groupe (antérieur à Windows 2000) : **GRP2**

Étendue du groupe

- Domaine local
- Globale
- Universelle

Type de groupe

- Sécurité
- Distribution

On va créer les users « Paul » et « Pierre » dans le GRP1 de l'UO Strasbourg et créer les users « Isabelle » et « Nathalie » dans GRP2 de l'UO Mulhouse :

Paul :

Nouvel objet - Utilisateur

Créer dans : CCI-CAMPUS.LAN/Strasbourg

Prénom : **Paul** Initiales : **A**

Nom : **A**

Nom complet : **Paul A**

Nom d'ouverture de session de l'utilisateur :
Paul A @CCI-CAMPUS.LAN

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
CCI-CAMPUS **Paul A**



Nouvel objet - Utilisateur X

Créer dans : CCI-CAMPUS.LAN/Strasbourg

Mot de passe :

Confirmer le mot de passe :

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur X

Créer dans : CCI-CAMPUS.LAN/Strasbourg

Quand vous cliquerez sur Terminer, l'objet suivant sera créé :

Nom complet : Paul A

Nom de connexion de l'utilisateur : Paul A@CCI-CAMPUS.LAN

L'utilisateur ne peut pas changer de mot de passe.
Le mot de passe n'expire jamais.

Pierre :

Nouvel objet - Utilisateur X

 Créer dans : CCI-CAMPUS.LAN/Strasbourg

Prénom :	<input type="text" value="Pierre"/>	Initiales :	<input type="text"/>
Nom :	<input type="text" value="B"/>		
Nom complet :	<input type="text" value="Pierre B"/>		

Nom d'ouverture de session de l'utilisateur :
 ▾

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

	Nom	Type	Description
 Paul A	Paul A	Utilisateur	
 Pierre B	Pierre B	Utilisateur	

Utilisateurs et ordinateurs Active Directory

- > Requêtes enregistrées
- ▼ CCI-CAMPUS.LAN
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipal
 - Managed Service Account
 - Users
- ▼ Strasbourg
 - Users
 - Groupes
- Mulhouse

Isabelle :

Nouvel objet - Utilisateur

Créer dans : CCI-CAMPUS.LAN/Mulhouse

Prénom : Isabelle Initiales :
Nom : A
Nom complet : Isabelle A

Nom d'ouverture de session de l'utilisateur :
Isabelle A @CCI-CAMPUS.LAN

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
CCI-CAMPUS\ Isabelle A

< Précédent Suivant > Annuler

Nathalie :

Nouvel objet - Utilisateur

Créer dans : CCI-CAMPUS.LAN/Mulhouse

Prénom : Nathalie Initiales :
Nom : B
Nom complet : Nathalie B

Nom d'ouverture de session de l'utilisateur :
Nathalie B @CCI-CAMPUS.LAN

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
CCI-CAMPUS\ Nathalie B

Nom	Type	Description
Isabelle A	Utilisateur	
Nathalie B	Utilisateur	

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view displays the domain structure: 'Utilisateurs et ordinateurs Active' > 'Requêtes enregistrées' > 'CCI-CAMPUS.LAN' (which is expanded) > 'BuiltIn' > 'Computers' > 'Domain Controllers' > 'ForeignSecurityPrincipal' > 'Managed Service Account' > 'Users'. Below 'Users', two containers are expanded: 'Strasbourg' (containing 'Users' and 'Groupes') and 'Mulhouse' (containing 'Users' and 'Groupes'). The 'Users' folder under 'Strasbourg' is highlighted with a blue selection bar.

On ajoute maintenant les users dans leurs groupes respectifs :

GRP1 :

Propriétés de : GRP1

Général Membres Membre de Géré par

Membres :

Nom	Dossier Services de domaine Active Directory
Paul A	CCI-CAMPUS.LAN/Strasbourg/Users
Pierre B	CCI-CAMPUS.LAN/Strasbourg/Users

Ajouter... Supprimer

The screenshot shows the 'Properties of GRP1' dialog box. The 'Membres' tab is active, displaying a list of users assigned to the group. The list includes 'Paul A' and 'Pierre B', both listed under the path 'CCI-CAMPUS.LAN/Strasbourg/Users'. At the bottom of the dialog, there are 'Ajouter...' and 'Supprimer' buttons.

GRP2 :

Propriétés de : GRP2

Général Membres Membre de Géré par

Membres :

Nom	Dossier Services de domaine Active Directory
Isabelle A	CCI-CAMPUS.LAN/Mulhouse/Users
Nathalie B	CCI-CAMPUS.LAN/Mulhouse/Users

Ajouter... Supprimer

On crée aussi un compte Admin de secours :

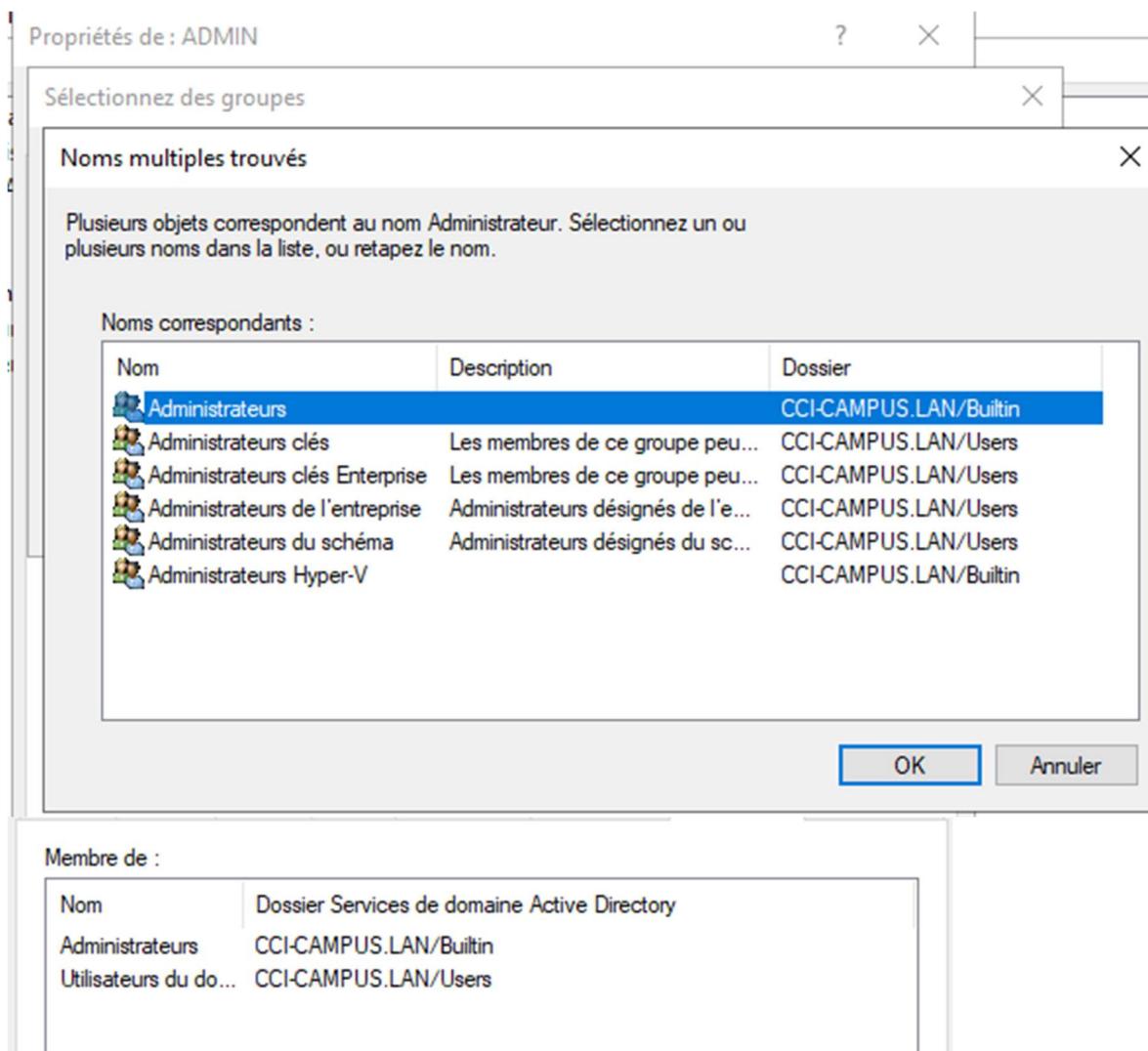
Nouvel objet - Utilisateur

Créer dans : CCI-CAMPUS.LAN/Strasbourg/Users

Prénom :	<input type="text" value="ADMIN"/>	Initiales :	<input type="text"/>
Nom :	<input type="text"/>		
Nom complet :	<input type="text" value="ADMIN"/>		
Nom d'ouverture de session de l'utilisateur :			
<input type="text" value="ADMIN"/>		@CCI-CAMPUS.LAN	
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
<input type="text" value="CCI-CAMPUS\"/>		<input type="text" value="ADMIN"/>	

< Précédent Suivant > Annuler

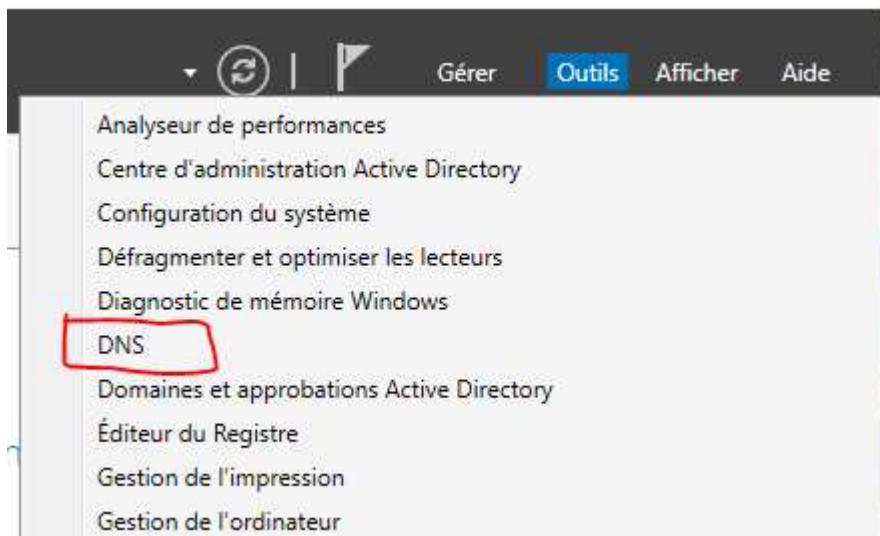
On l'ajoute dans le groupe Administrateur :



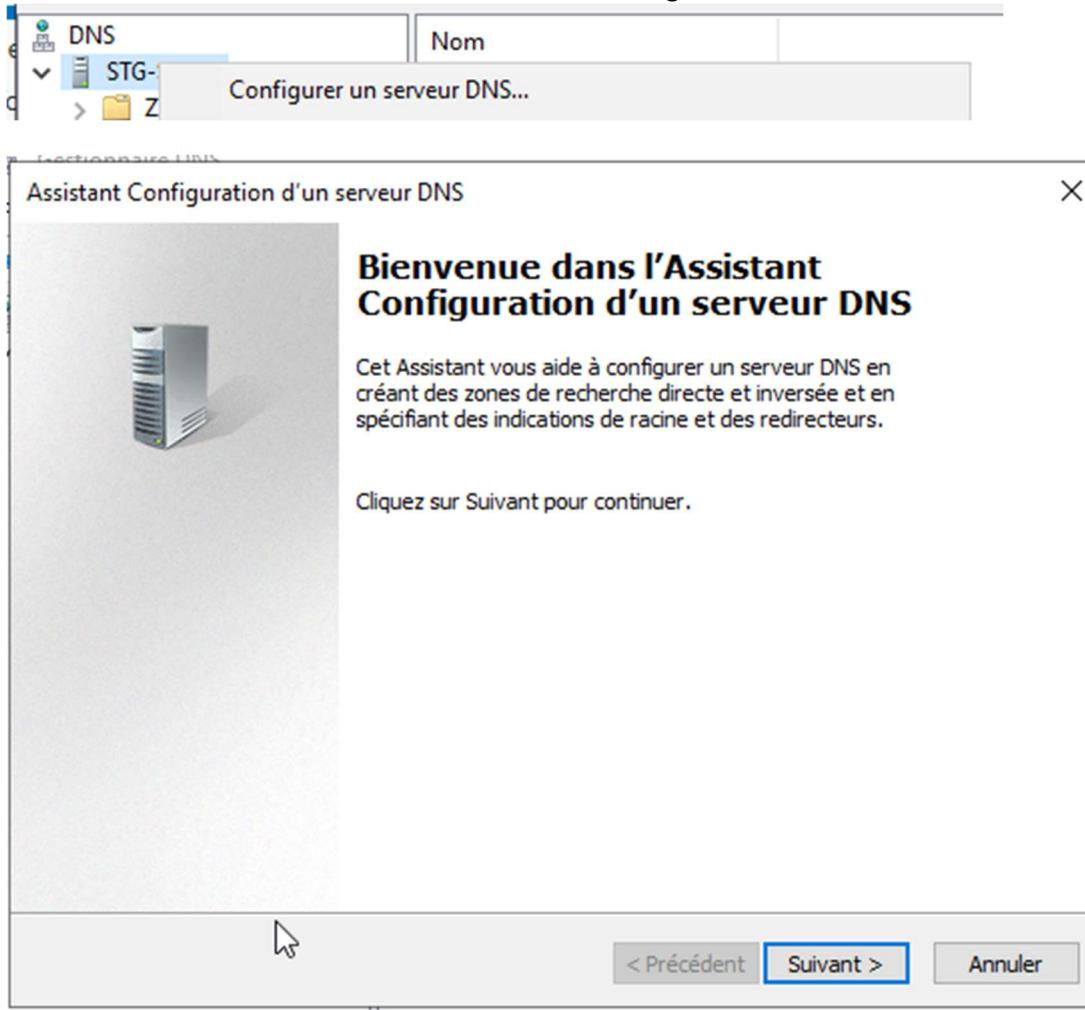
d) DNS

On va maintenant configurer notre DNS :

On se rend dans l'onglet « outils » et « DNS » :

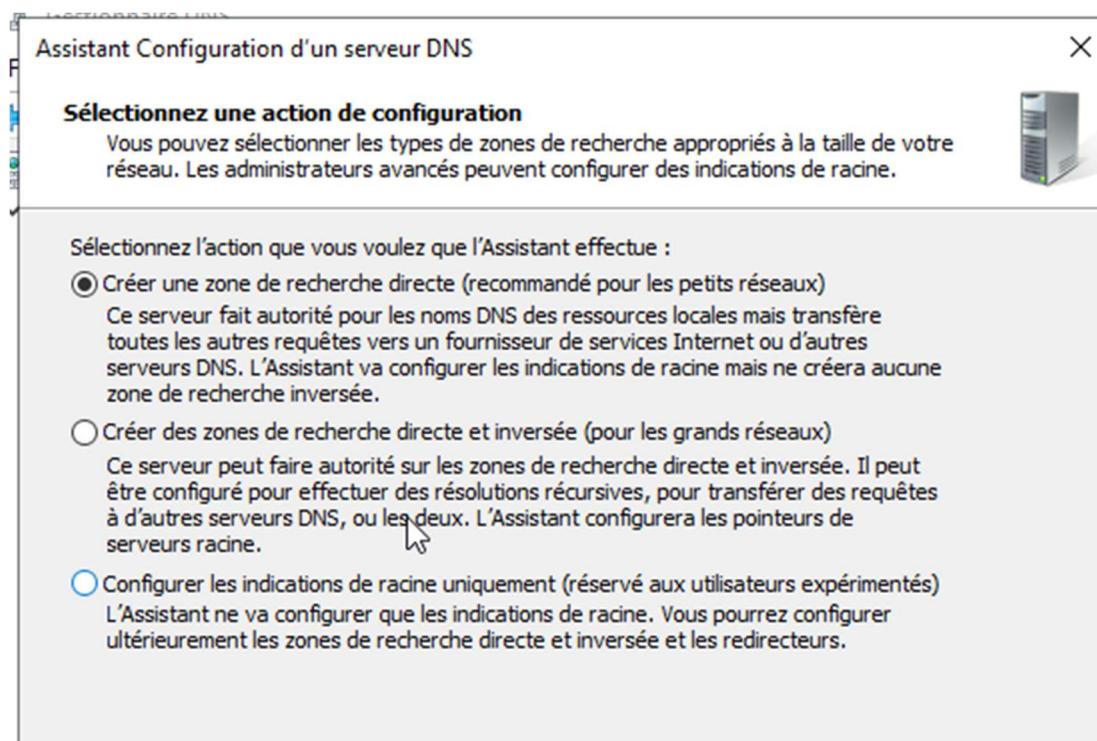


On fait un clic droit sur notre serveur et on choisit configurer un serveur Dns :

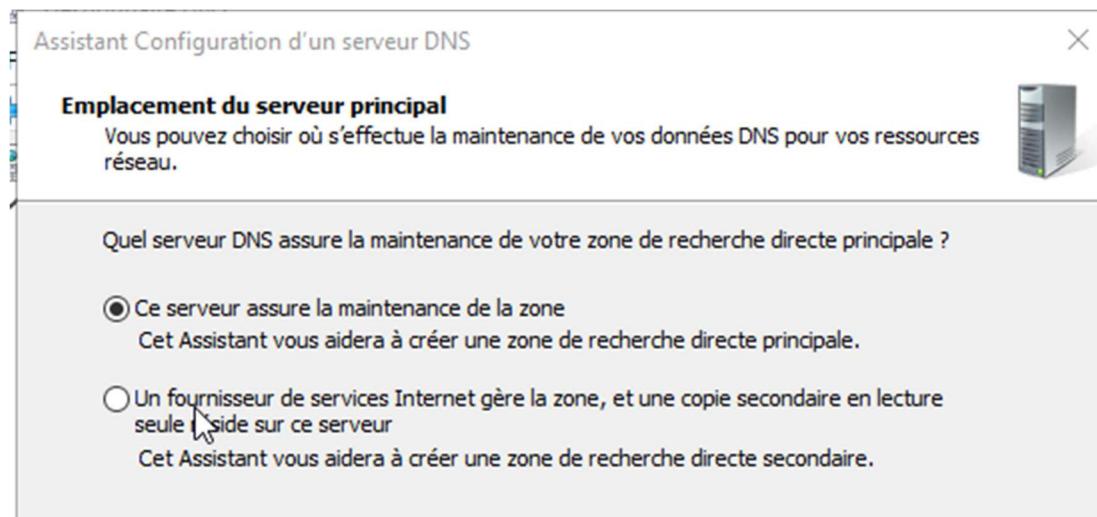


Suivant,

On choisit la zone directe :



Suivant,



Suivant,

On rentre le nom de la zone :

Assistant Nouvelle zone X**Nom de la zone**

Quel est le nom de la nouvelle zone ?



Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

CCI-CAMPUS.LAN

Suivant,

Assistant Nouvelle zone X**Mise à niveau dynamique**

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



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

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

N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)

Cette option n'est disponible que pour les zones intégrées à Active Directory.

Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées

Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.

 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

Ne pas autoriser les mises à jour dynamiques

Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent

Suivant >

Annuler

Suivant,

On rentre l'ip de notre serveur DNS :

Assistant Configuration d'un serveur DNS

Redirecteurs

Les redirecteurs sont des serveurs DNS vers lesquels ce serveur envoie les requêtes auxquelles il ne peut pas répondre.

Ce serveur DNS doit-il rediriger des requêtes ?

Oui, il doit rediriger les requêtes vers les serveurs DNS ayant les adresses IP suivantes :

Adresse IP	Nom de domaine co...	Validé
<Cliquez ici pour ...		
192.168.100.2	STG-SRV01.CCI-CA...	OK

Non, il ne doit pas rediriger les requêtes

Si ce serveur n'est pas configuré pour utiliser des redirecteurs, il peut toujours résoudre des noms en utilisant des serveurs de noms racines.

< Précédent Suivant > Annuler

Suivant,

Assistant Configuration d'un serveur DNS

Fin de l'Assistant Configuration d'un serveur DNS

Vous avez terminé l'Assistant Configuration d'un serveur DNS avec succès. Lorsque vous cliquerez sur Terminer, les paramètres suivants seront sauvegardés.

Paramètres :

Serveur DNS à configurer : STG-SRV01
Zone de recherche directe à créer : CCI-CAMPUS.LAN
Adresse IP du redirecteur : 192.168.100.2

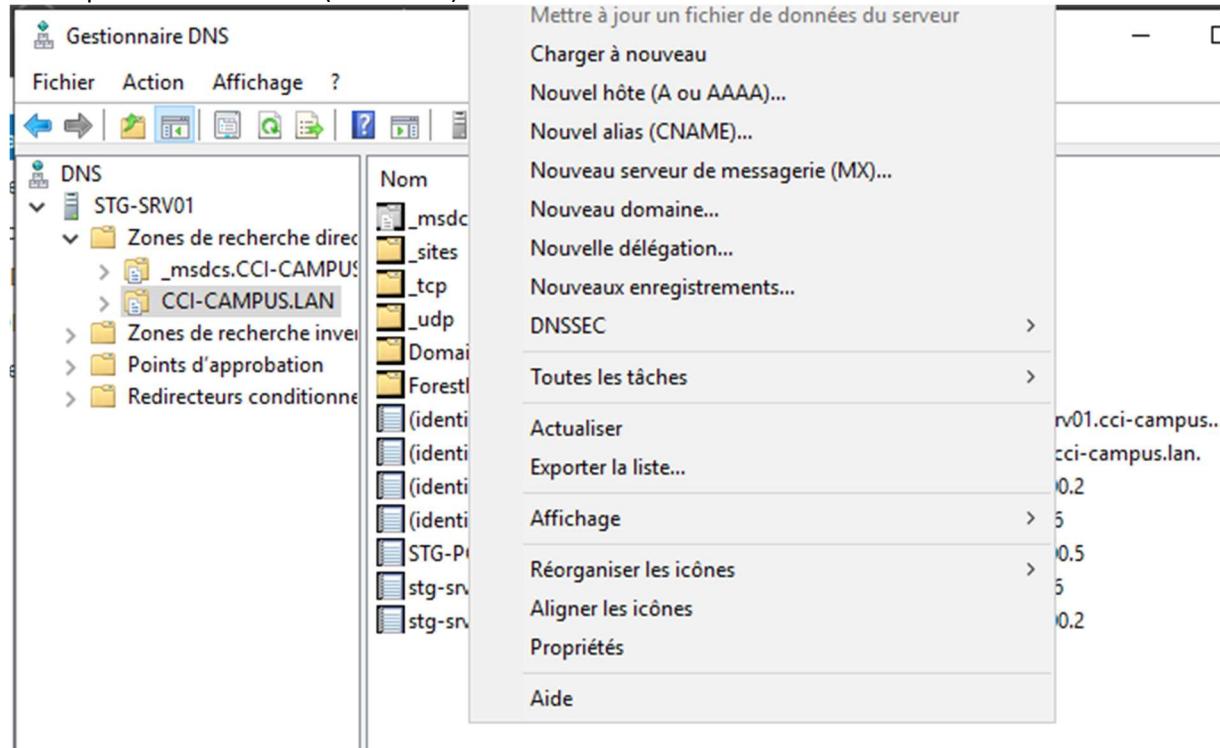
Configurez les hôtes qui utiliseront ce serveur DNS pour pointer vers ce serveur DNS pour la résolution des noms, puis vérifiez la résolution des noms à l'aide de nslookup. Si vous avez ajouté une nouvelle zone principale, ajoutez-lui des enregistrements de ressources pour les hôtes dont les noms doivent être résolus par ce serveur DNS.

Pour fermer cet Assistant, cliquez sur Terminer.

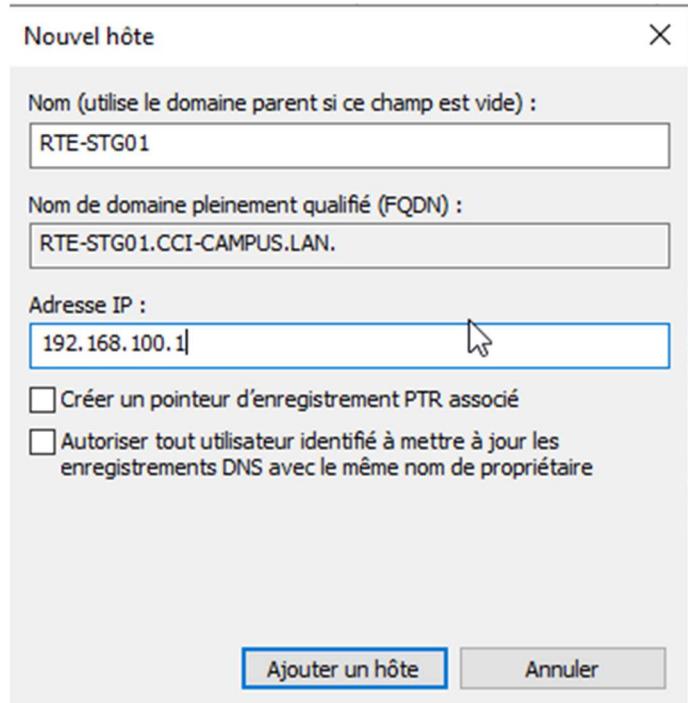
< Précédent Terminer Annuler

On peut créer les hôtes de nos serveur et routeurs :

On clique sur nouvel hôte (A ou AAA) :



Pour RTE-STG01 :



Pour SRV-STG02 :

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :
STG-SRV02

Nom de domaine pleinement qualifié (FQDN) :
STG-SRV02.CCI-CAMPUS.LAN.

Adresse IP :
192.168.100.3

Créer un pointeur d'enregistrement PTR associé
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Ajouter un hôte Terminé

Pour le STG-NAS01 :

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :
STG-NAS01

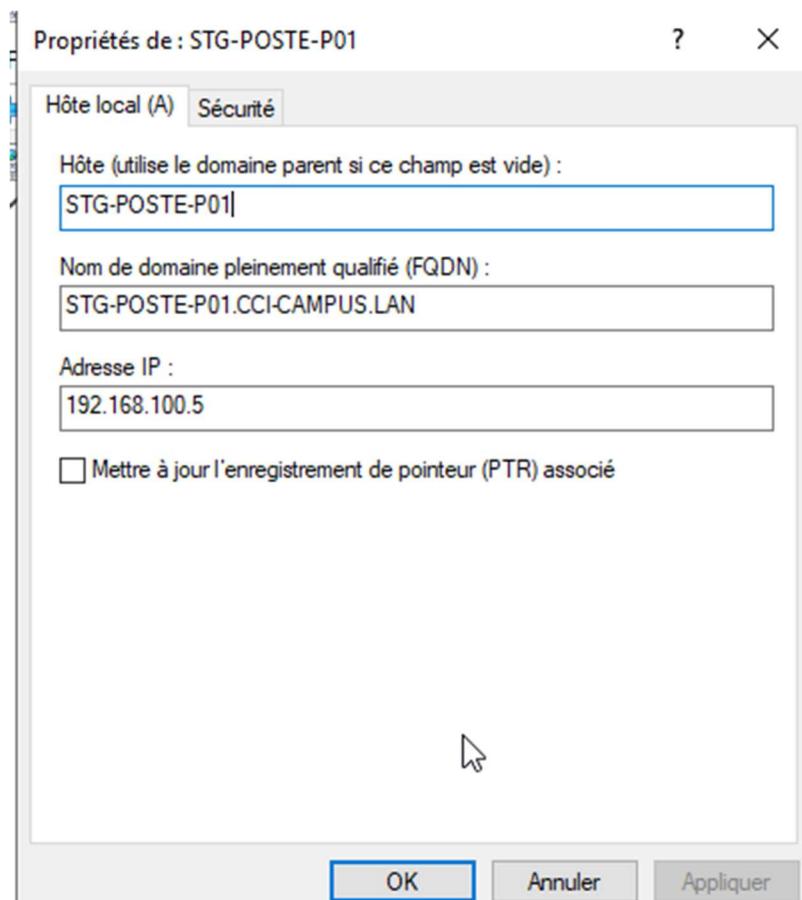
Nom de domaine pleinement qualifié (FQDN) :
STG-NAS01.CCI-CAMPUS.LAN.

Adresse IP :
192.168.100.4

Créer un pointeur d'enregistrement PTR associé
 Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Ajouter un hôte Terminé

Et pour les postes :



On peut retrouver nos hôtes via le cmd avec la commande nslookup :

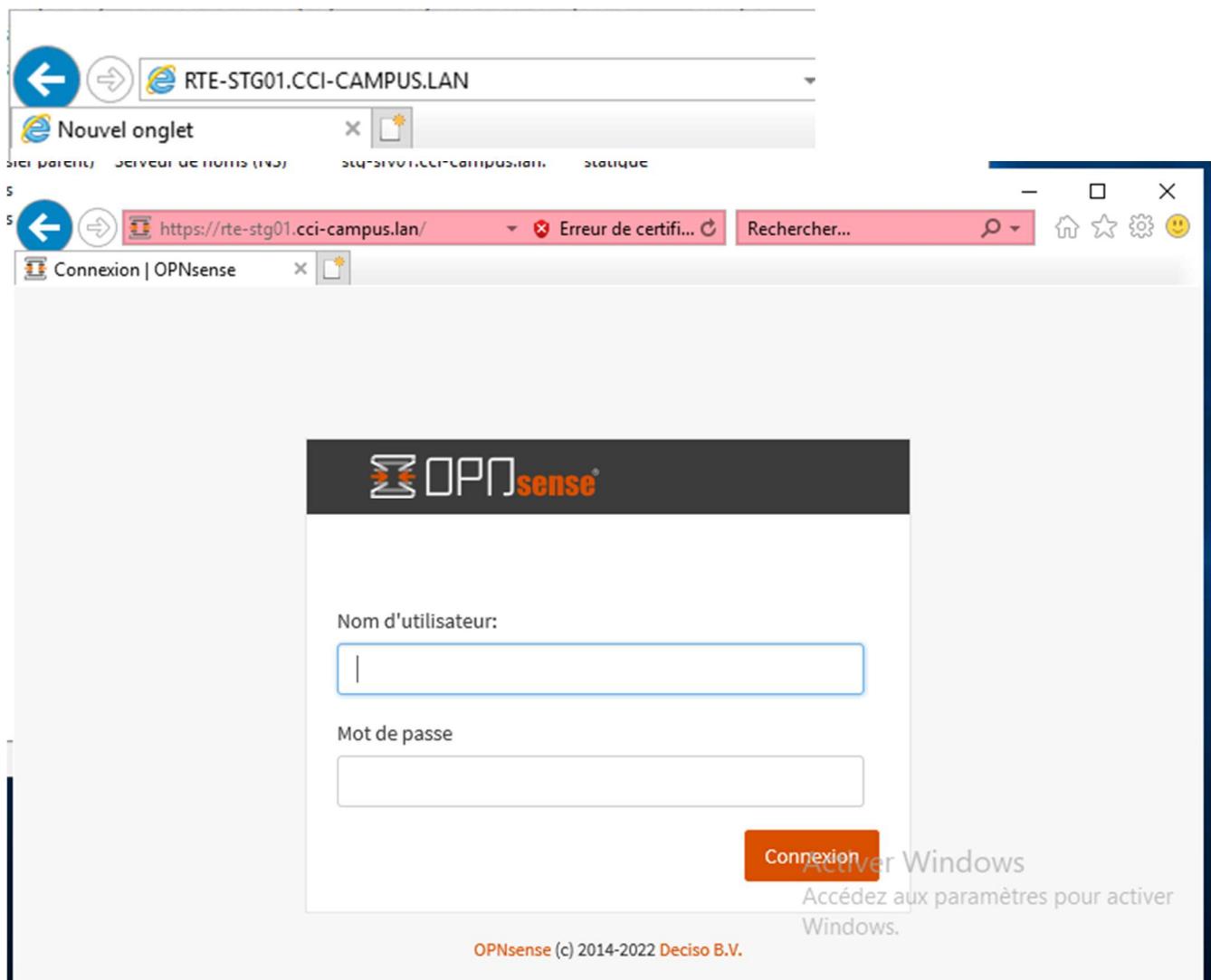
Exemple sur RTE-STG01 :

```
C:\Users\Administrateur>nslookup
DNS request timed out.
    timeout was 2 seconds.
Serveur par défaut : UnKnown
Address: ::1

> RTE-STG01
Serveur : UnKnown
Address: ::1

Nom : RTE-STG01.CCI-CAMPUS.LAN
Address: 192.168.100.1
```

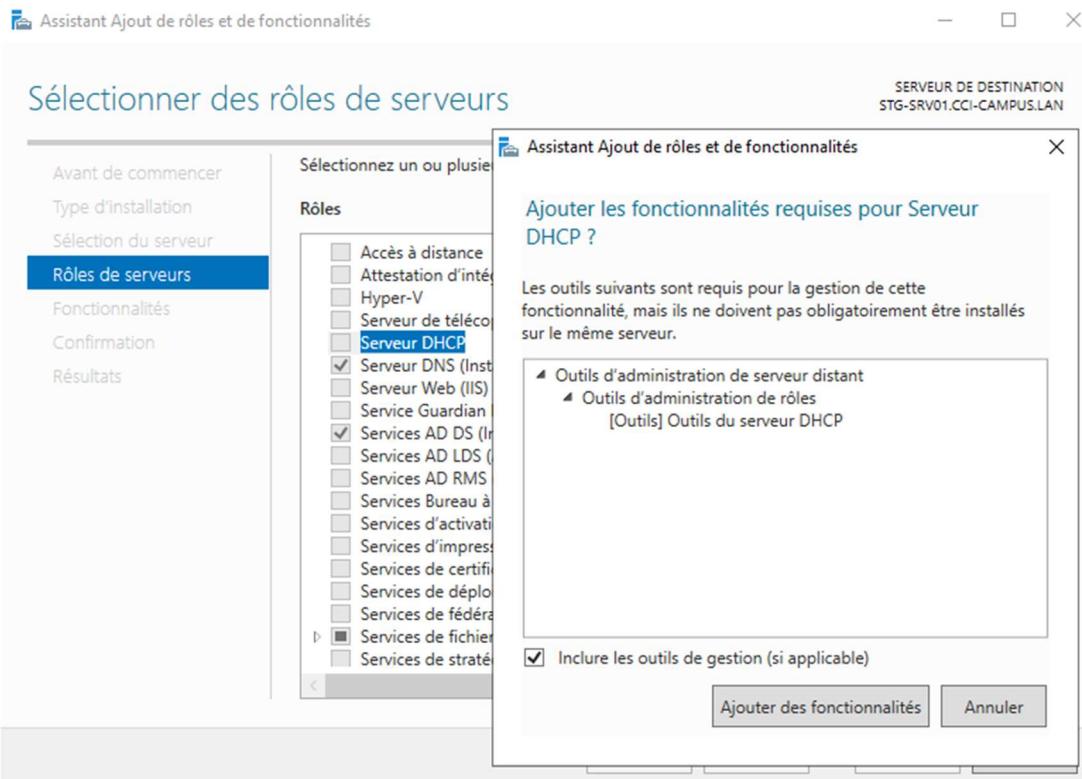
On peut maintenant essayer d'accéder en web à notre routeur RTE-STG01 grâce à son nom :



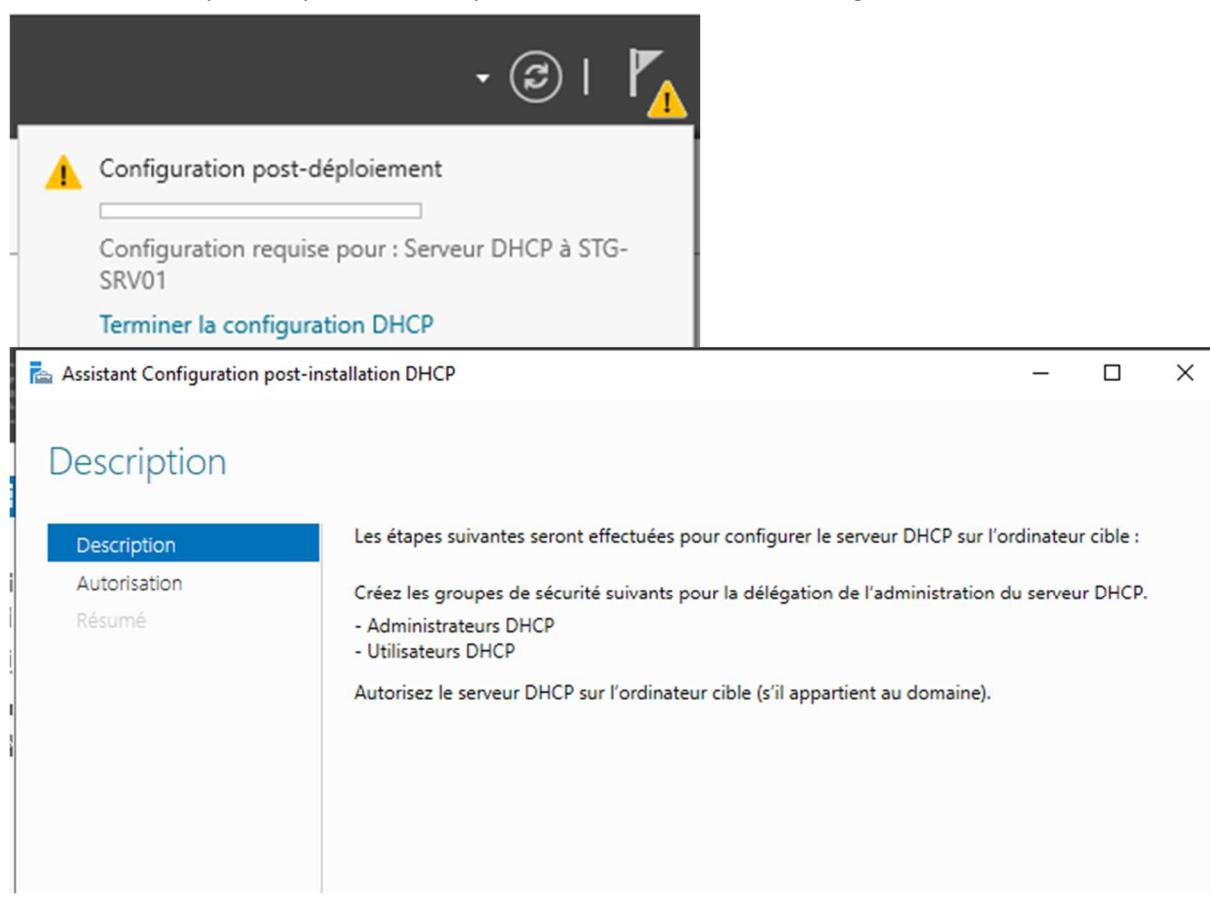
e) DHCP

On installe d'abord le rôles DHCP :

On se rend dans l'assistant ajout de rôles et fonctionnalités :

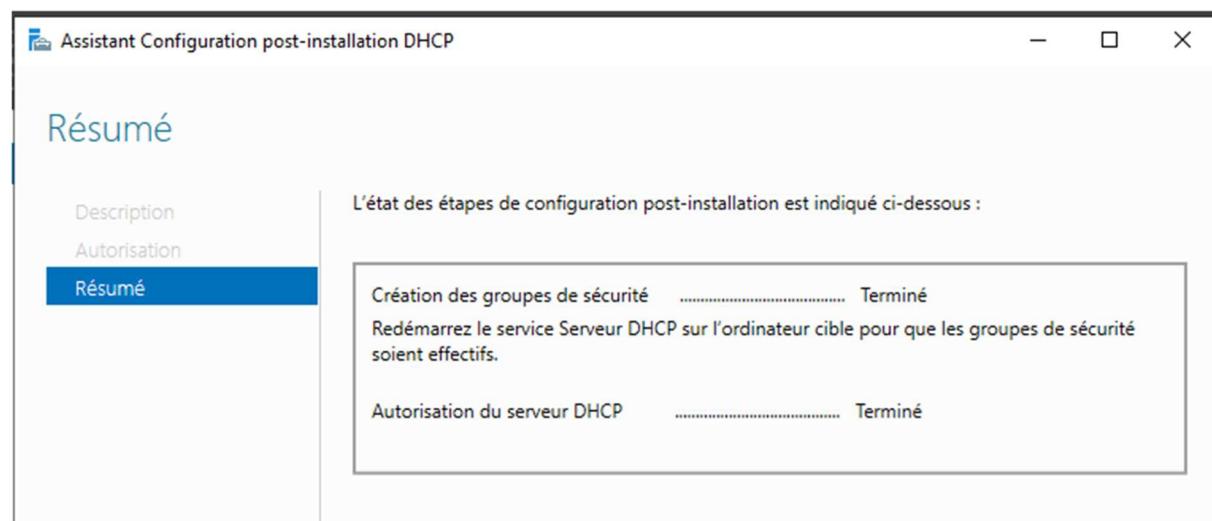
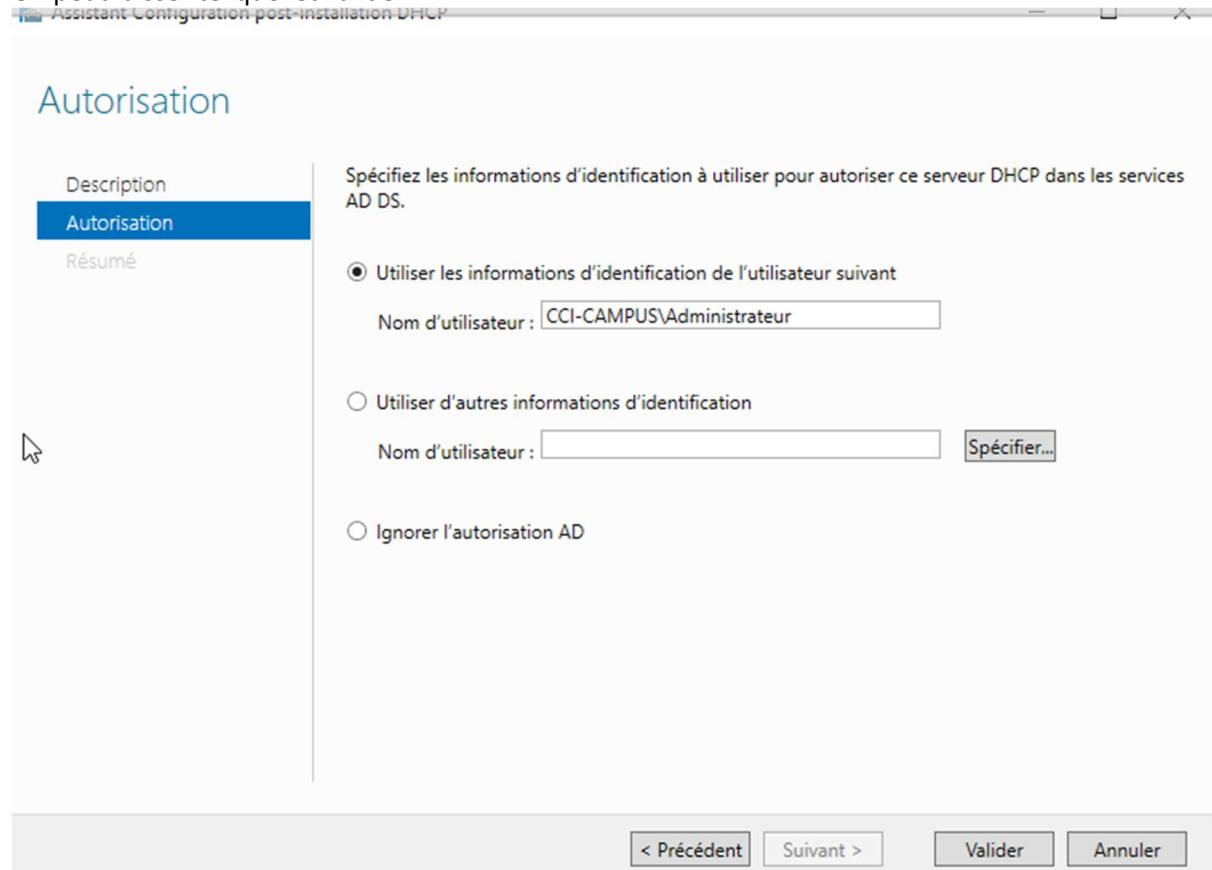


On clique sur ajouter des fonctionnalités, puis sur suivant jusqu'à l'installation.
Une fois fait, on peut cliquez sur le drapeau et faire « terminer la configuration DHCP » :



Suivant,

On peut laisser tel quel et valider :

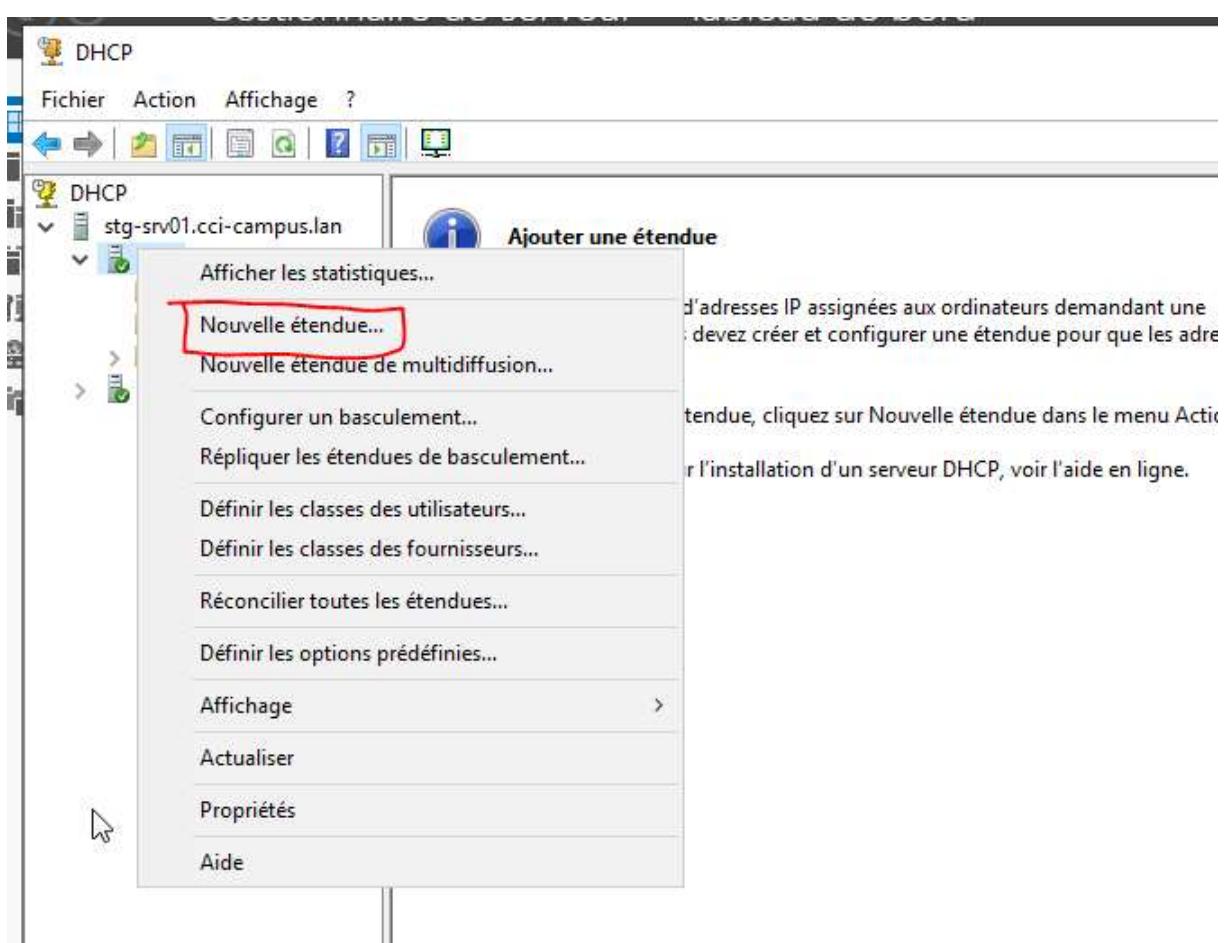


On ferme.

On a maintenant accès à l'outils DHCP que l'on peut ouvrir :



On fait un clic droit sur notre serveur puis sur ipv4 et on choisit l'option créer une nouvelle étendue :



On entre le nom de l'étendu :

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 :

On va définir l'étendu de la plage d'adresse IP :

Ici elle sera de 192.168.100.5 à 192.168.100.100 pour les postes clients

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

On ne va pas mettre d'adresse exclues :

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

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



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

Adresse IP de début :

Adresse IP de fin :

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

Suivant,

On met ensuite un bail d'une durée de 30 jours :

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

Suivant,

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.



Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

- Oui, je veux configurer ces options maintenant
 Non, je configurerai ces options ultérieurement

< Précédent **Suivant >** Annuler

Suivant,

On précise quel routeur doivent utiliser nos clients :

Assistant Nouvelle étendue

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP 

<input type="text" value="1"/>	Ajouter
192.168.100.1	Supprimer
	Monter
	Descendre

< Précédent Suivant > Annuler

Suivant,

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent : 

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :	Adresse IP :
<input type="text"/>	<input type="text" value="192.168.1.53"/>
Ré索oudre	Ajouter
	Supprimer
	Monter
	Descendre

< Précédent Suivant > Annuler

Suivant,

On laisse les paramètres WINS par default,

Assistant Nouvelle étendue

Serveurs WINS

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.



Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

Nom du serveur :

Résoudre

Adresse IP :

 . . .

Ajouter

Supprimer

Monter

Descendre

Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

< Précédent

Suivant >

Annuler

Suivant,

Assistant Nouvelle étendue

Activer l'étendue

Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.

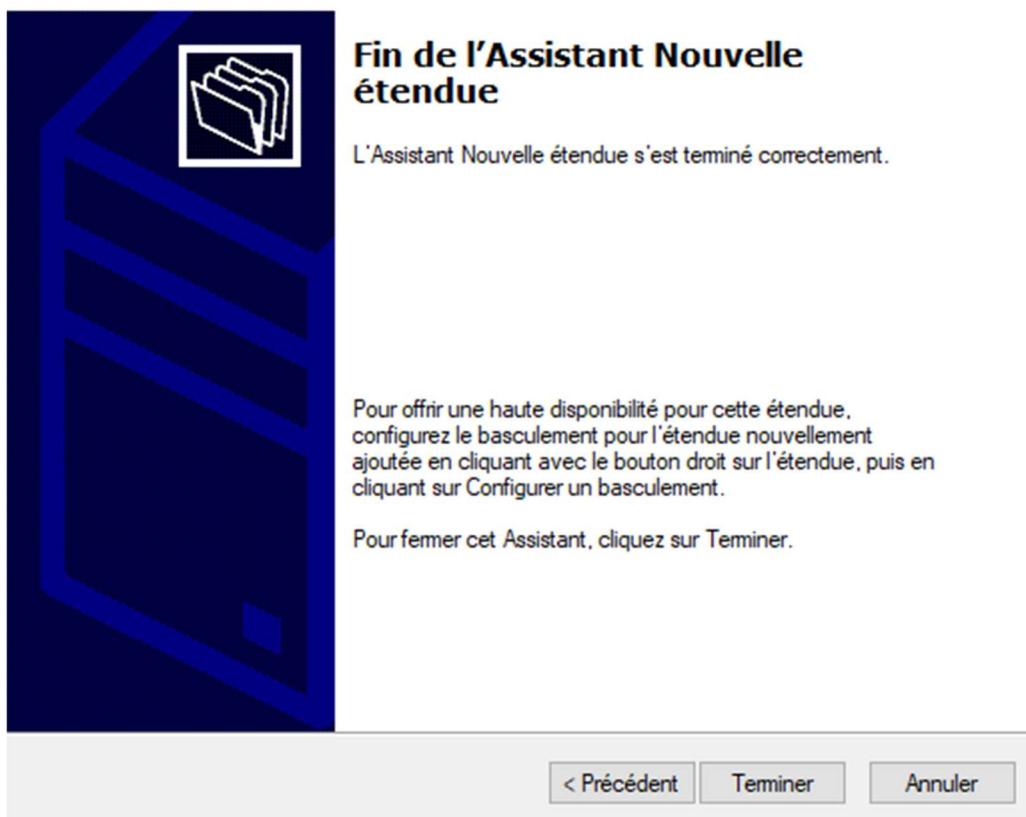


Voulez-vous activer cette étendue maintenant ?

- Oui, je veux activer cette étendue maintenant
- Non, j'activerai cette étendue ultérieurement

Suivant,

Assistant Nouvelle étendue

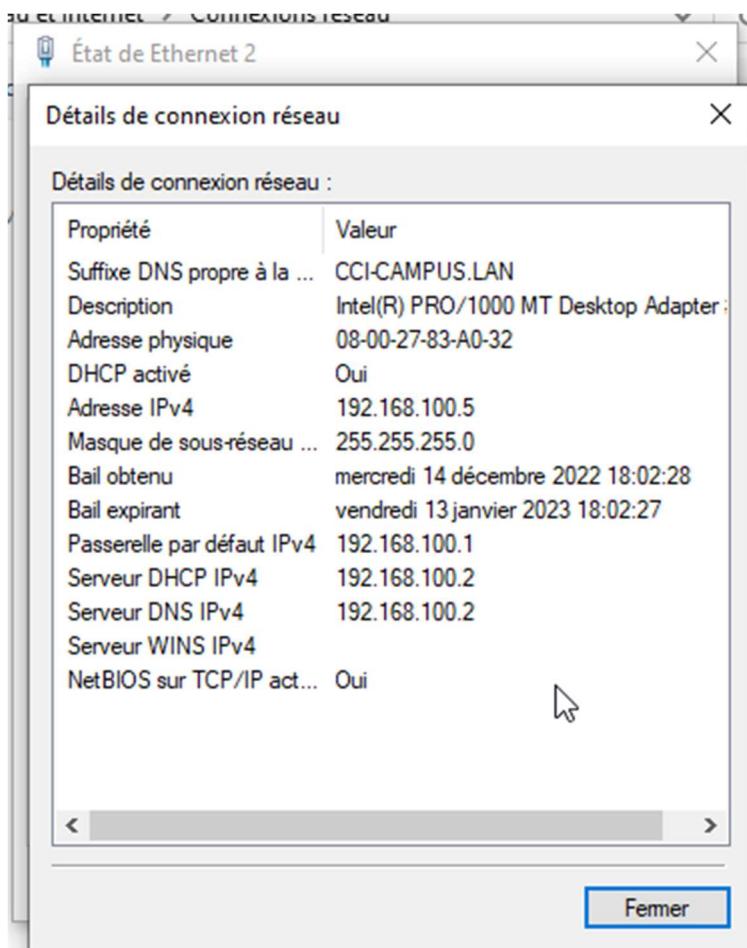


On constate que notre étendue est bien créée et actif :

Contenu du serveur DHCP	État	Description	Actions
Étendue [192.168.100.0] DCHPSTG	** Actif **	dhcp pour le site de St...	IPv4
Options de serveur			Autres actions
Stratégies			
Filtres			

On peut maintenant vérifier le bon fonctionnement du DHCP.

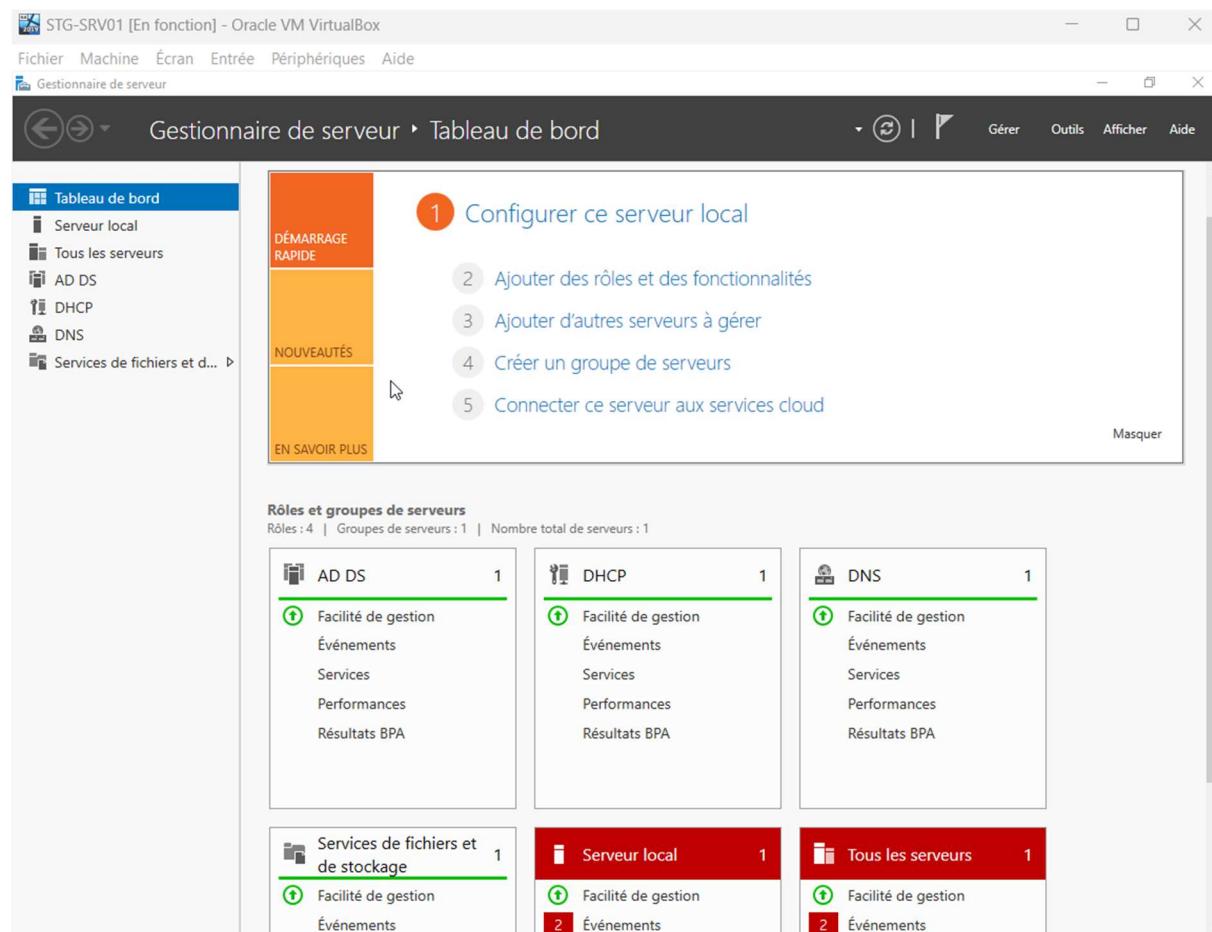
On se rend sur notre client Windows 10 STG-POSTE-P01 :



On voit que le DHCP est activé et qu'il a attribué l'IP 192.168.100.5 qui est la première adresse disponible de notre étendu.

f) Mise en place DFS DFS-R

1. Depuis le gestionnaire de serveur, cliquer sur Ajouter des rôles et des fonctionnalités.



2. Au lancement de l'assistant, cliquer sur le bouton Suivant

Assistant Ajout de rôles et de fonctionnalités

Avant de commencer

SERVEUR DE DESTINATION
STG-SRV01.CCI-CAMPUS.LAN

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
[Démarrer l'Assistant de Suppression de rôles et de fonctionnalités](#)

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur Suivant pour continuer.

Ignorer cette page par défaut

< Précédent Suivant > Installer Annuler

3. Choisir Installation basée sur un rôle ou une fonctionnalité et cliquer sur Suivant.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le type d'installation

SERVEUR DE DESTINATION
STG-SRV01.CCI-CAMPUS.LAN

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

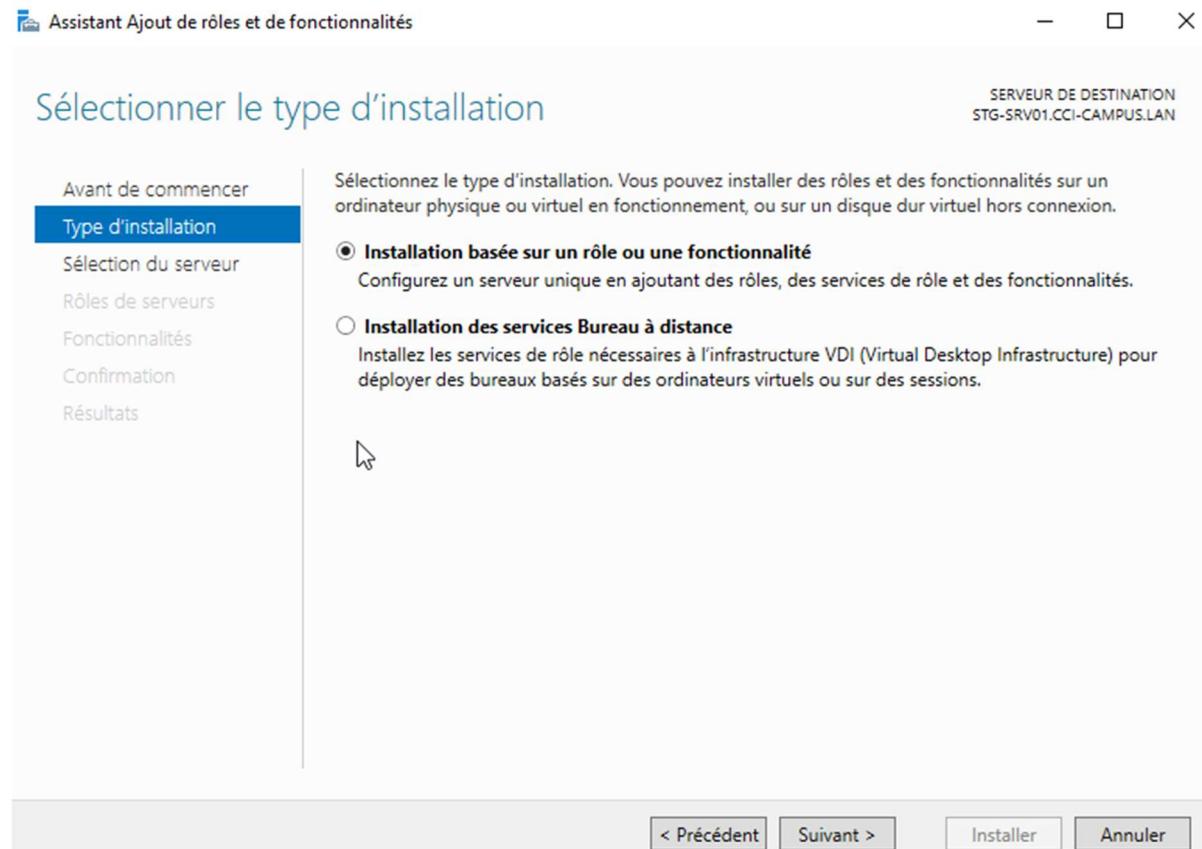
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

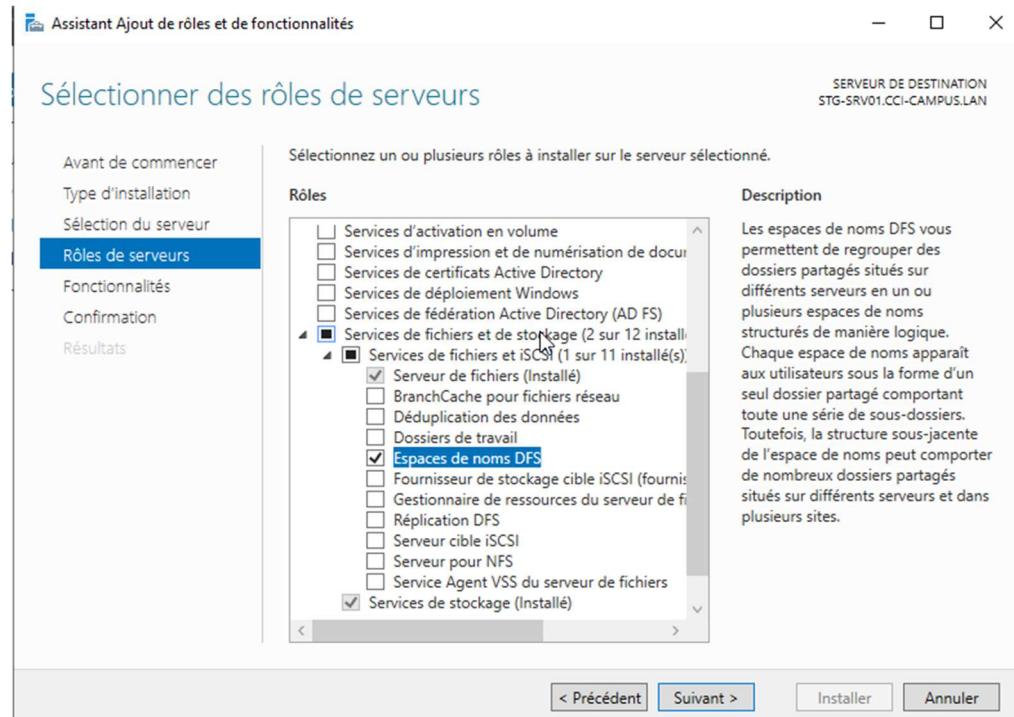
Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

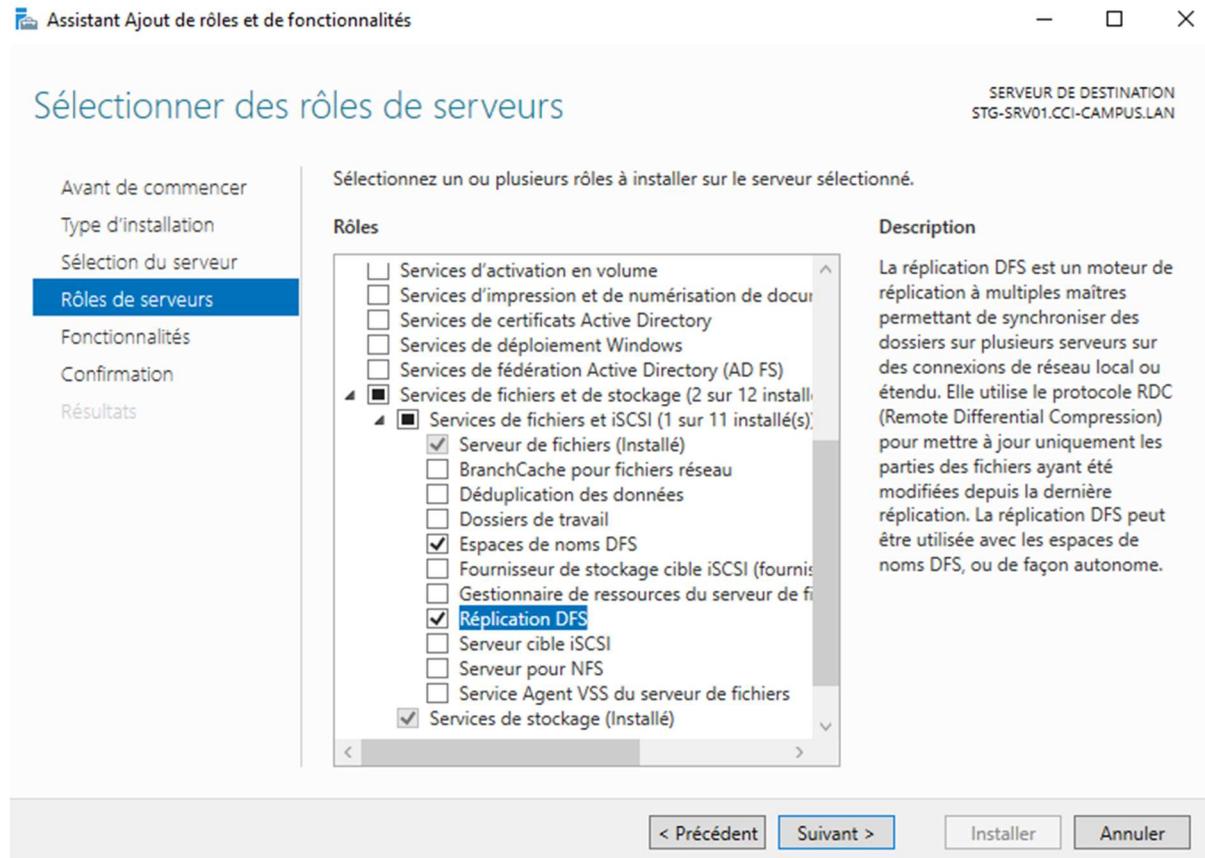
4. Sélectionner le serveur puis cliquer sur Suivant.



5. Cocher la case Espace de nom DFS qui se trouve dans Services de fichiers et de stockage / Services de fichiers et iSCSI.



6. Valider en cliquant des fonctionnalités en cliquant sur Ajouter des fonctionnalités.

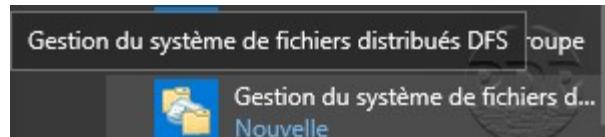


8. Cliquer sur Suivant

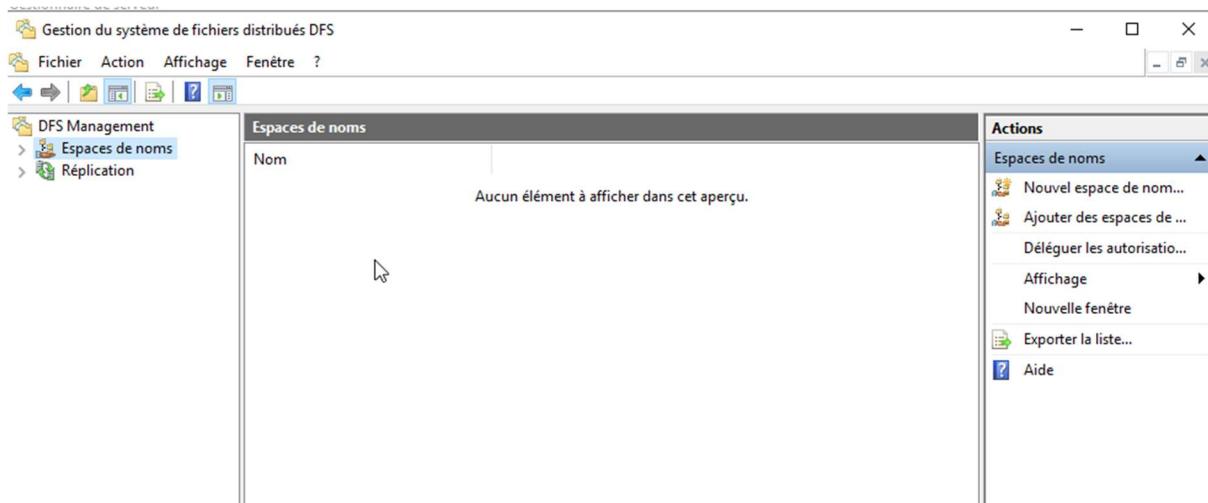
9. Passer la section Fonctionnalités en cliquant sur Suivant

10. Démarrer l'installation en cliquant sur le bouton Installer

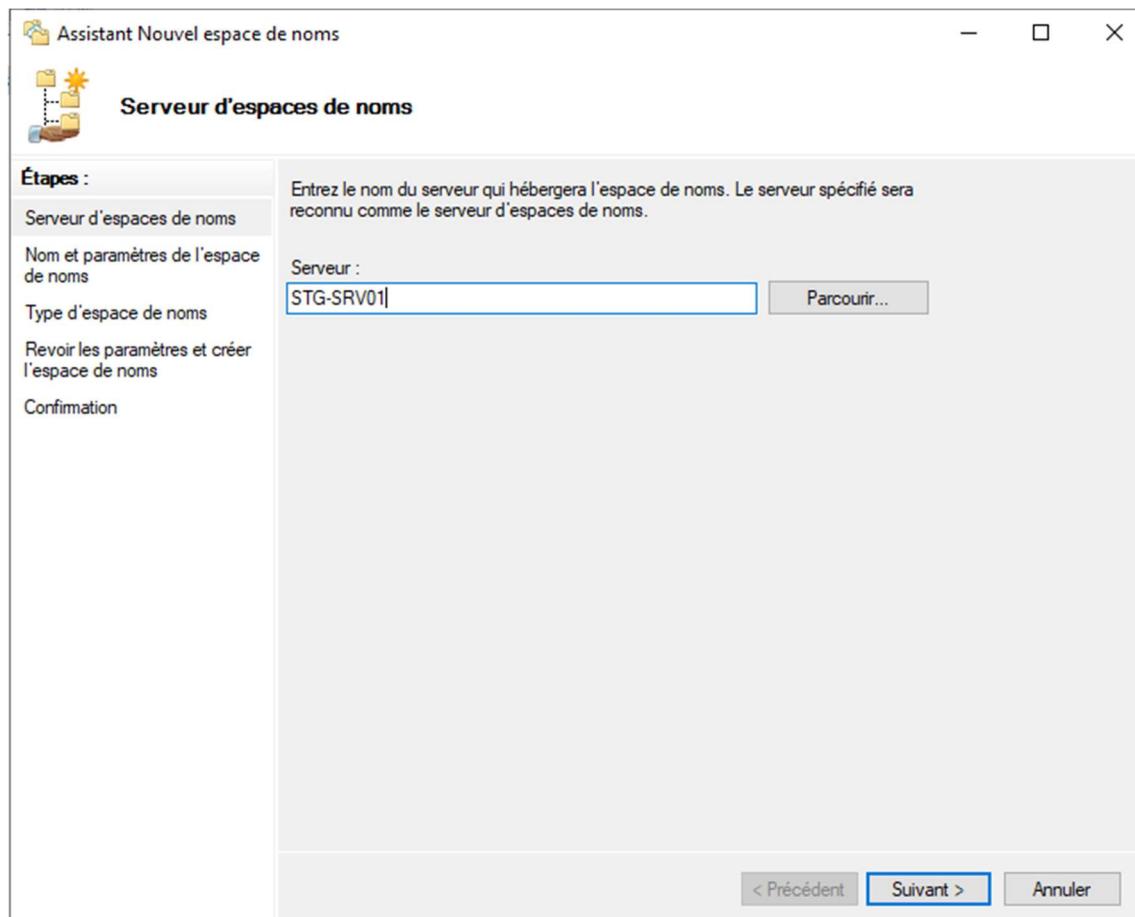
L'administration du rôle se fait à l'aide de la console Gestion du système de fichier distribués DFS.



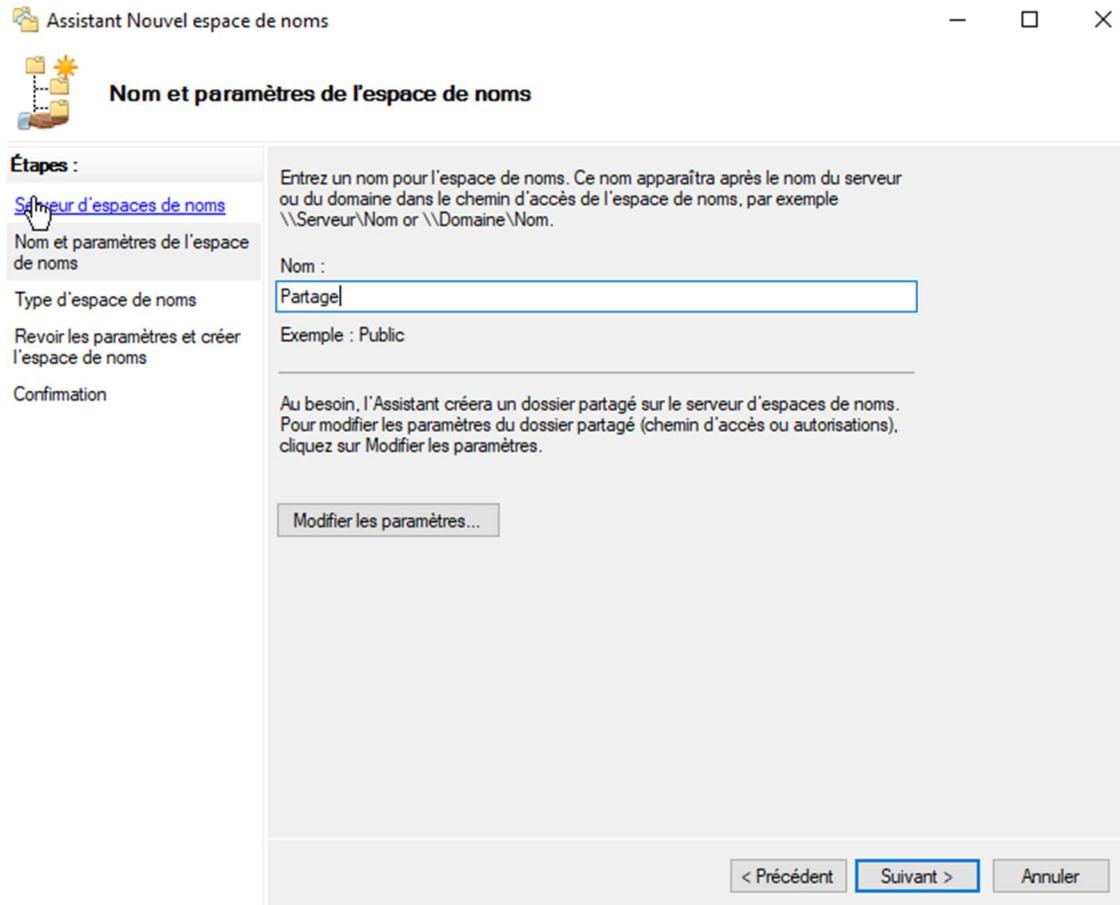
- Depuis la console « Gestion du système de fichier distribués DFS » cliquer sur Nouvel espace de nom ... qui se trouve dans la partie Actions.



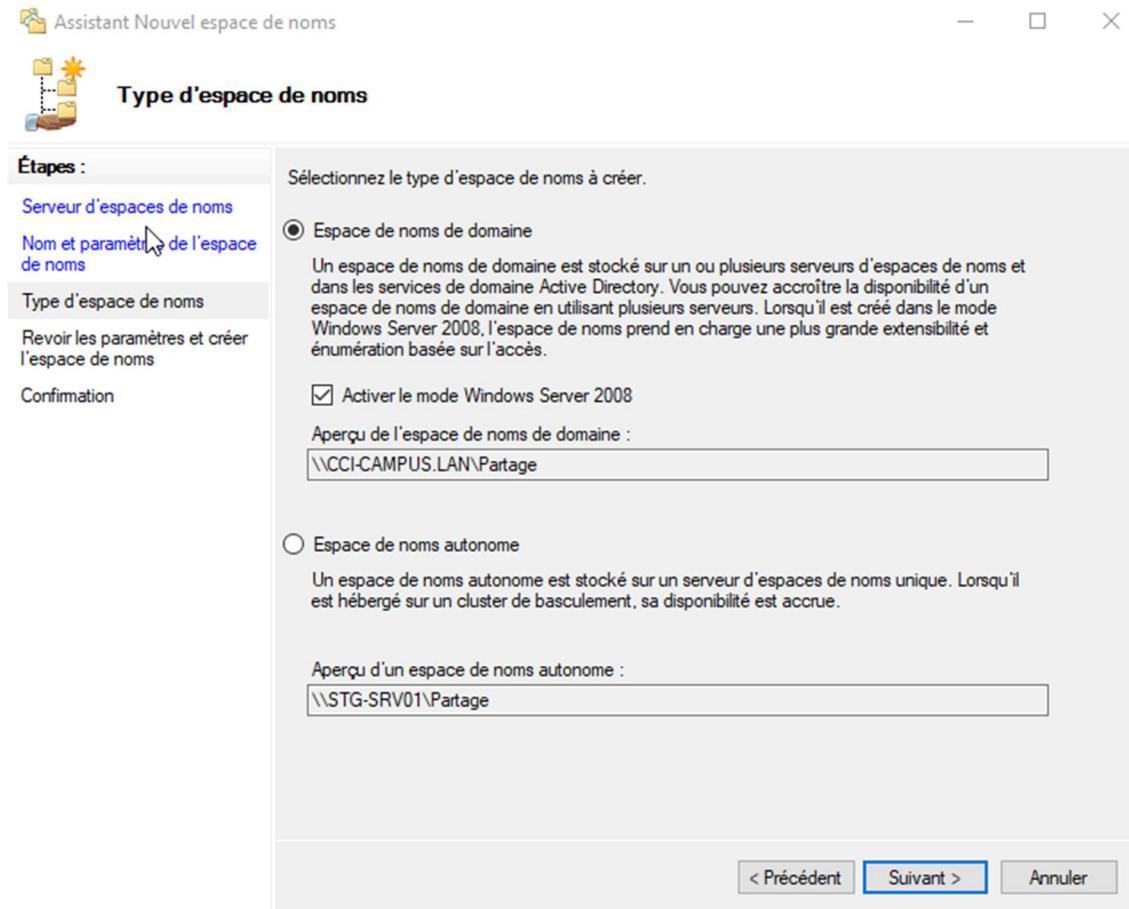
- Entrer le nom du serveur qui hébergera l'espace de nom puis cliquer sur Suivant.



3. Entrer le nom du partage racine puis cliquer sur Suivant.

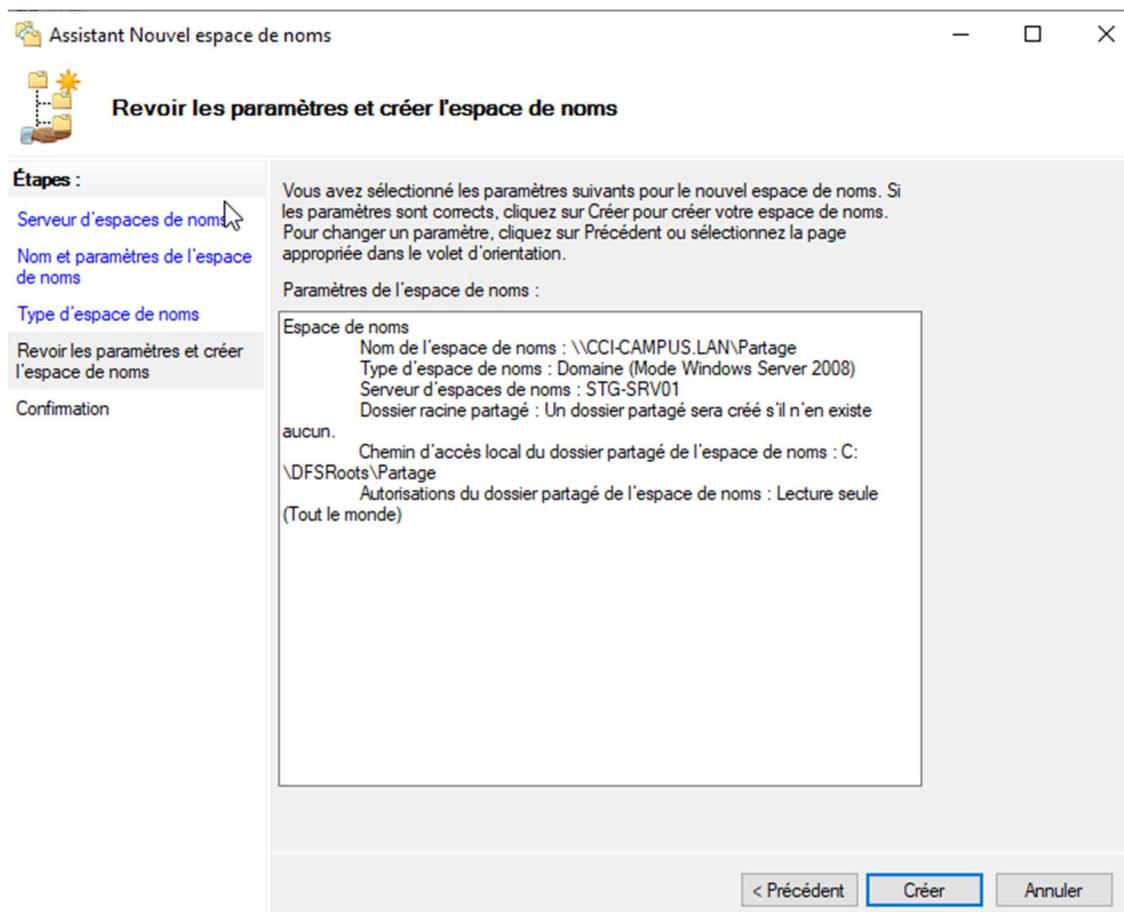


4. Choisir l'option Espace de nom de domaine puis cliquer sur Suivant.

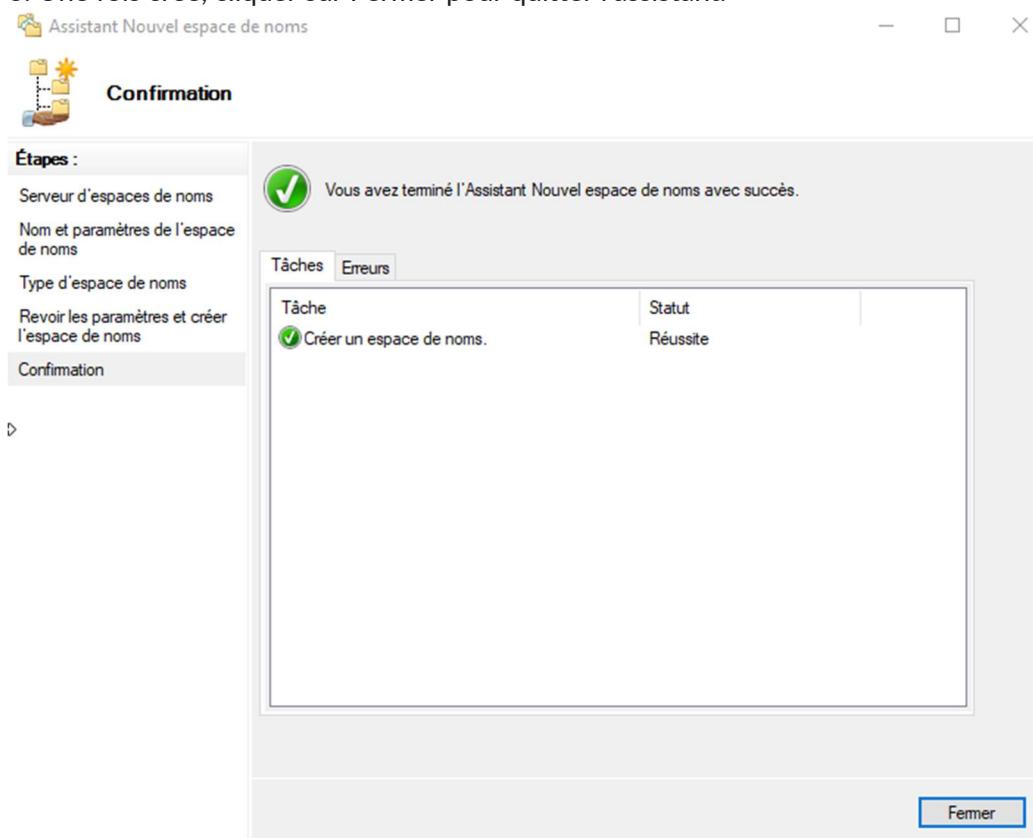


Un espace de nom de domaine permet l'accès au dossier par une adresse de type : \\nom-de-domaine\partage-racine\dossier-partagé.

5. Cliquer sur le bouton Créer



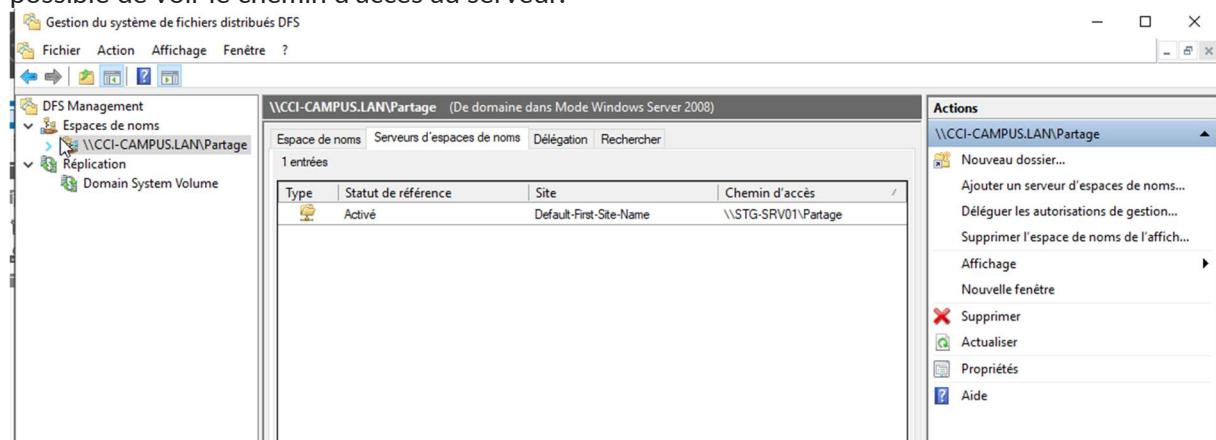
6. Une fois créé, cliquer sur Fermer pour quitter l'assistant.



7. Le namespace est disponible dans la console d'administration. Vous pouvez dès maintenant accéder au partage <\\domaine-ad\\partage>.

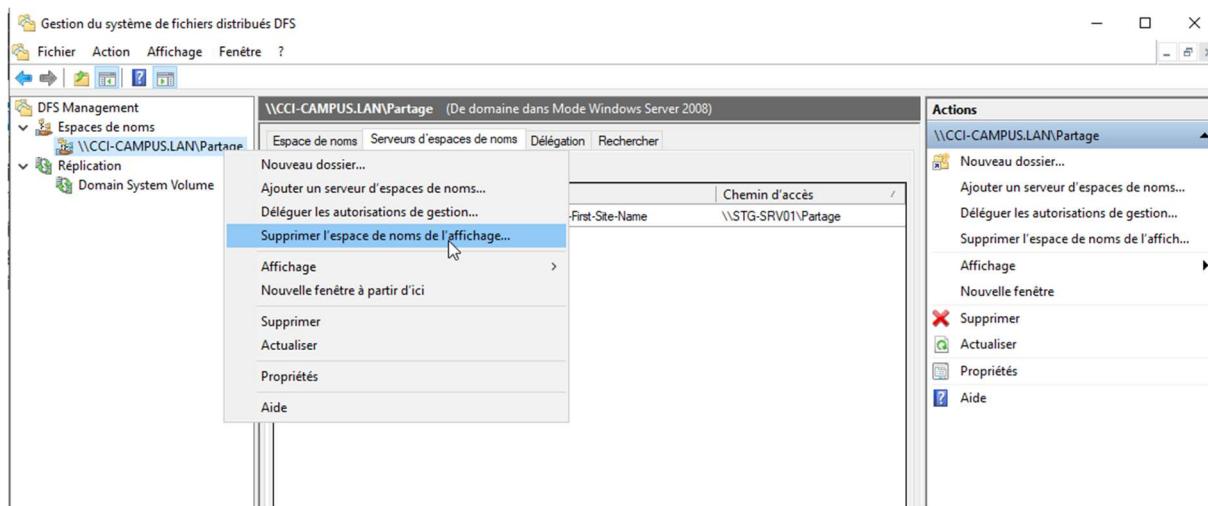


8. En cliquant sur l'espace de nom et en allant sur l'onglet Serveurs d'espace de noms, il est possible de voir le chemin d'accès au serveur.

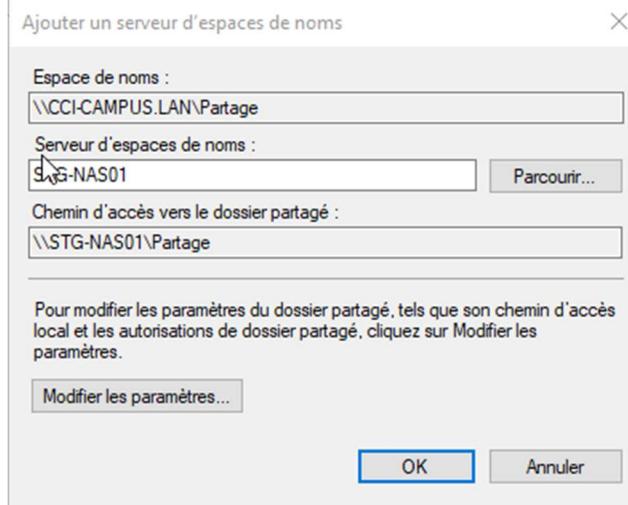


g) Ajout d'un serveur d'espace de nom

1. Depuis la console d'administration Gestion du système de fichier distribués, faire un clic droit sur l'espace de nom et cliquer sur Ajouter un serveur d'espace de nom ...



2. Entrer le nom du serveur puis cliquer sur OK



h) Ajout de dossiers partagé

Dans cette partie nous allons voir comment ajouter un dossier partagé.

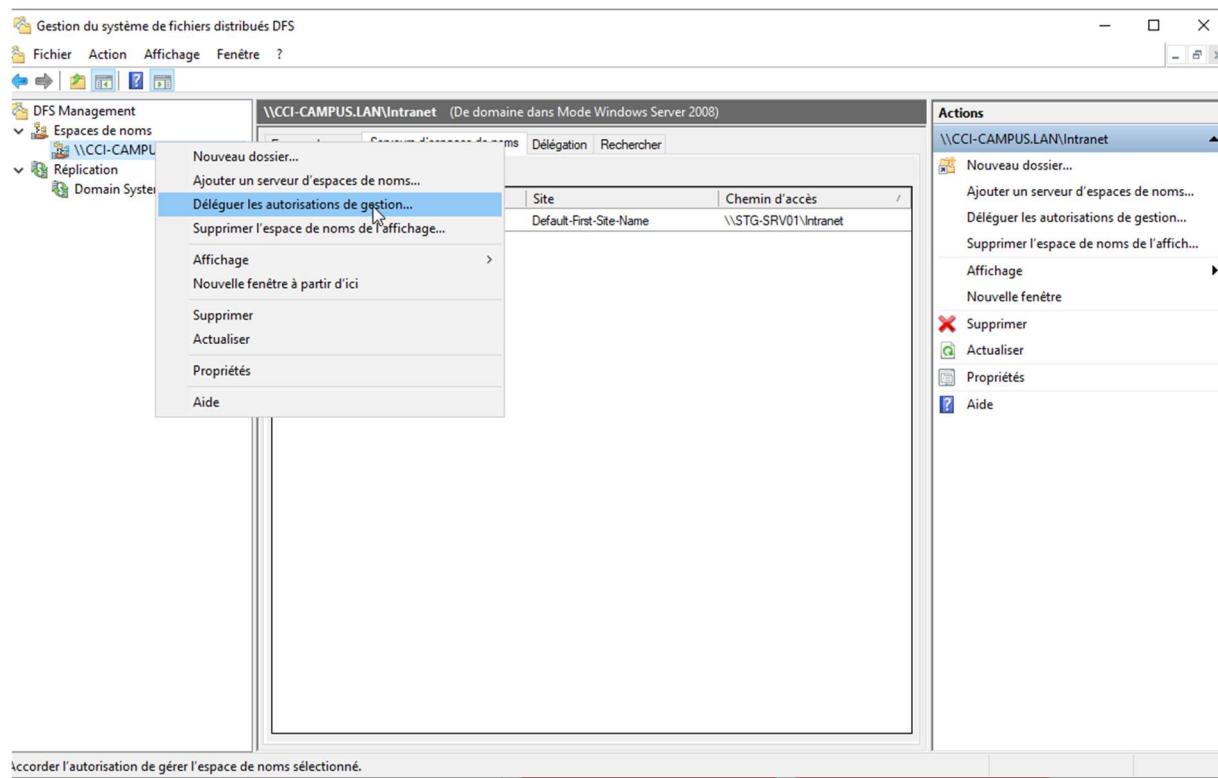
Le dossier sera accessible à l'adresse suivante : \\domaine-ad\namespace\dossier.

Prérequis :

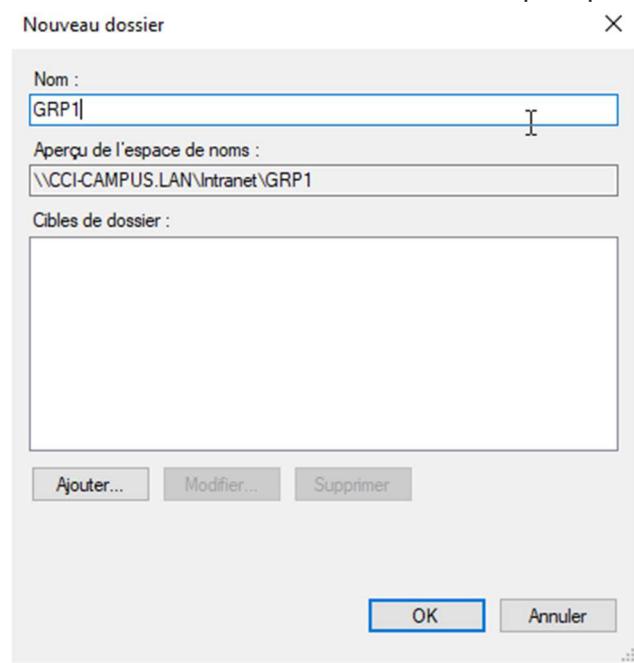
- Le dossier doit déjà être partagé.

Pour illustrer le tutoriel, nous allons ajouter dans un dossier Informatique qui est partagé sur le serveur LAB-FIC1.

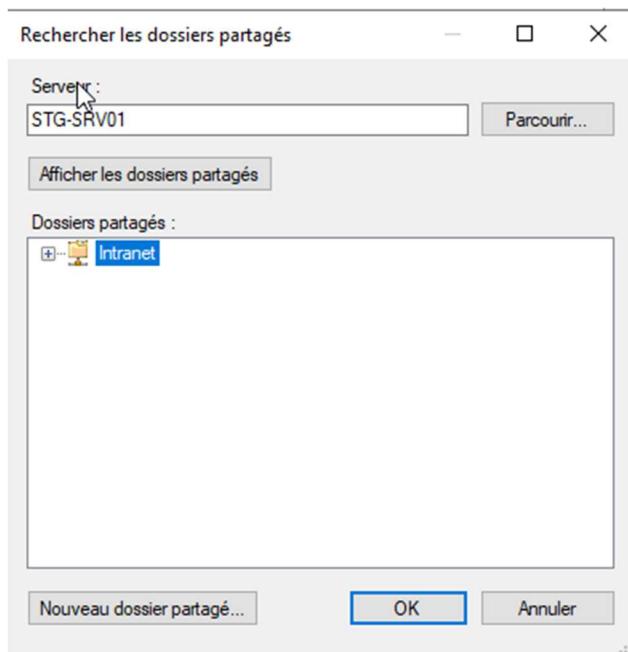
1. Depuis la console, faire un clic droit sur l'espace de nom et cliquer sur Nouveau dossier...



2. Entrer le nom du dossier dans le namespace puis cliquer sur Ajouter.



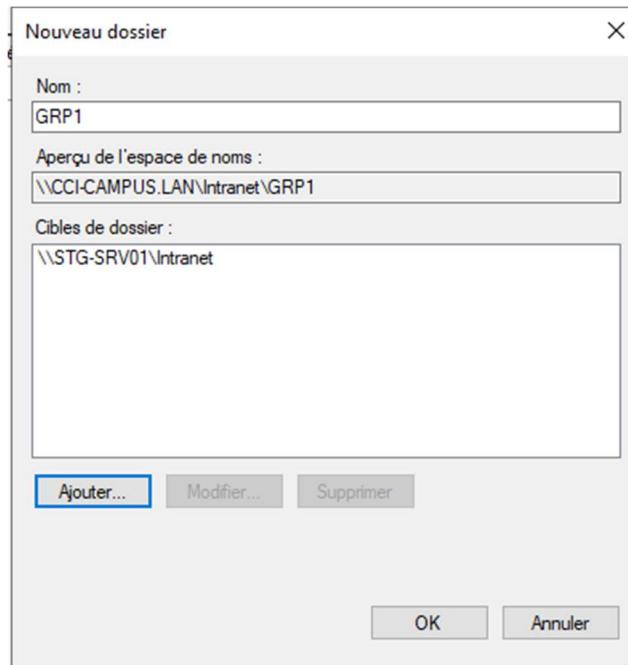
3. Saisir le nom du serveur, cliquer sur le bouton Afficher les dossiers partagés, sélectionner le dossier et appuyer sur OK.



4. Cliquer sur OK



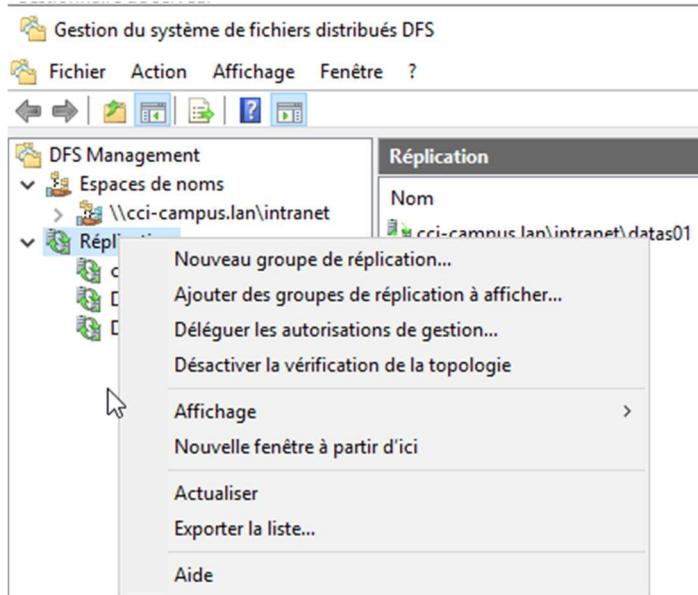
5. Cliquer sur OK



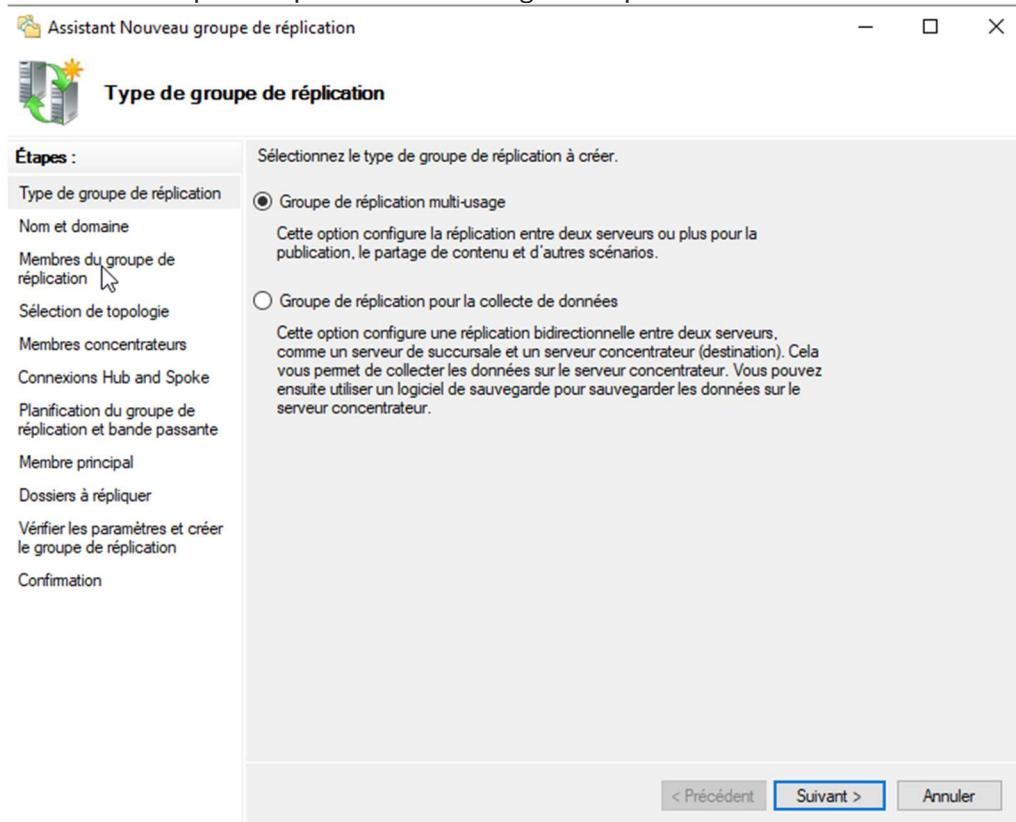
6. Le dossier est ajouté

i) DFS-R configuration de la réPLICATION

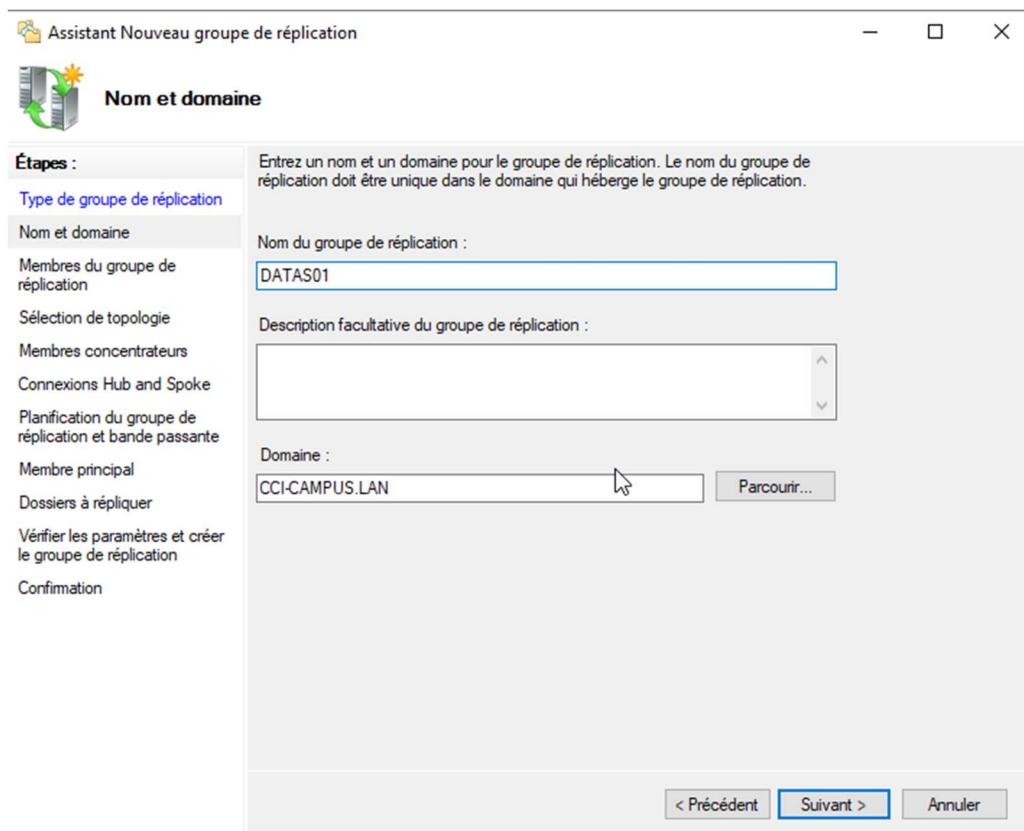
- Depuis la console, faire un clic droit sur RéPLICATION puis cliquer sur Nouveau groupe de réPLICATION



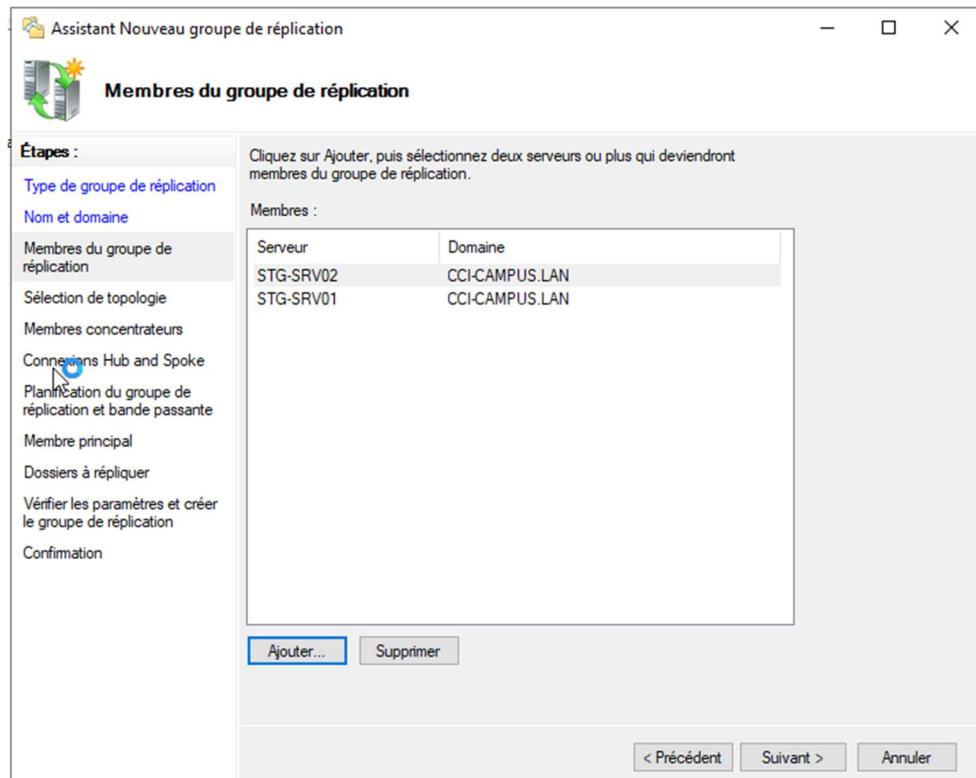
2. Choisir Groupe de réPLICATION multi-usage et cliquer sur Suivant.



3. Entrer le nom du groupe de réPLICATION, sélectionner le domaine puis cliquer sur Suivant.



4. Ajouter les serveurs membres du groupe de réPLICATION et cliquer sur Suivant.



5. Choisir la topologie en maille pleine et cliquer sur Suivant.

Assistant Nouveau groupe de réPLICATION

Sélection de topologie

Étapes :

- Type de groupe de réPLICATION
- Nom et domaine
- Membres du groupe de réPLICATION
- Sélection de topologie**
- Planification du groupe de réPLICATION et bande passante
- Membre principal
- Dossiers à réPLiquer
- Vérifier les paramètres et créer le groupe de réPLICATION
- Confirmation

Sélectionnez une topologie de connexions parmi les membres du groupe de réPLICATION.

Hub et Spoke

Cette topologie requiert au moins 3 membres dans le groupe de réPLICATION. Les membres spoke sont connectés à un ou deux hubs. Cette topologie est adaptée aux scénarios de publication où les données proviennent du membre hub et se répliquent sur les membres spoke.



Maille pleine

Dans cette topologie, chaque membre est répliqué avec tous les autres membres du groupe de réPLICATION. Cette topologie est surtout adaptée lorsqu'il existe au plus dix membres dans le groupe de réPLICATION.



Aucune topologie

Sélectionnez cette option si vous souhaitez créer une topologie personnalisée une fois l'Assistant terminé. Aucune réPLICATION ne peut s'effectuer tant que vous n'avez pas créé la topologie personnalisée.

< Précédent Suivant > Annuler

6. Sélectionner réPLICATION en continu et cliquer sur le bouton Suivant.

Assistant Nouveau groupe de réPLICATION

Planification du groupe de réPLICATION et bande passante

Étapes :

- Type de groupe de réPLICATION
- Nom et domaine
- Membres du groupe de réPLICATION
- Sélection de topologie
- Planification du groupe de réPLICATION et bande passante**
- Membre principal
- Dossiers à réPLiquer
- Vérifier les paramètres et créer le groupe de réPLICATION
- Confirmation

Sélectionnez la planification de réPLICATION et la bande passante à utiliser par défaut pour toutes les nouvelles connexions dans le groupe de réPLICATION.

Répliquer en continu à l'aide de la bande passante spécifiée

Utilisez cette option pour activer la réPLICATION 24 heures sur 24 et sept jours sur sept, avec la bande passante suivante :

Bande passante :

Complète

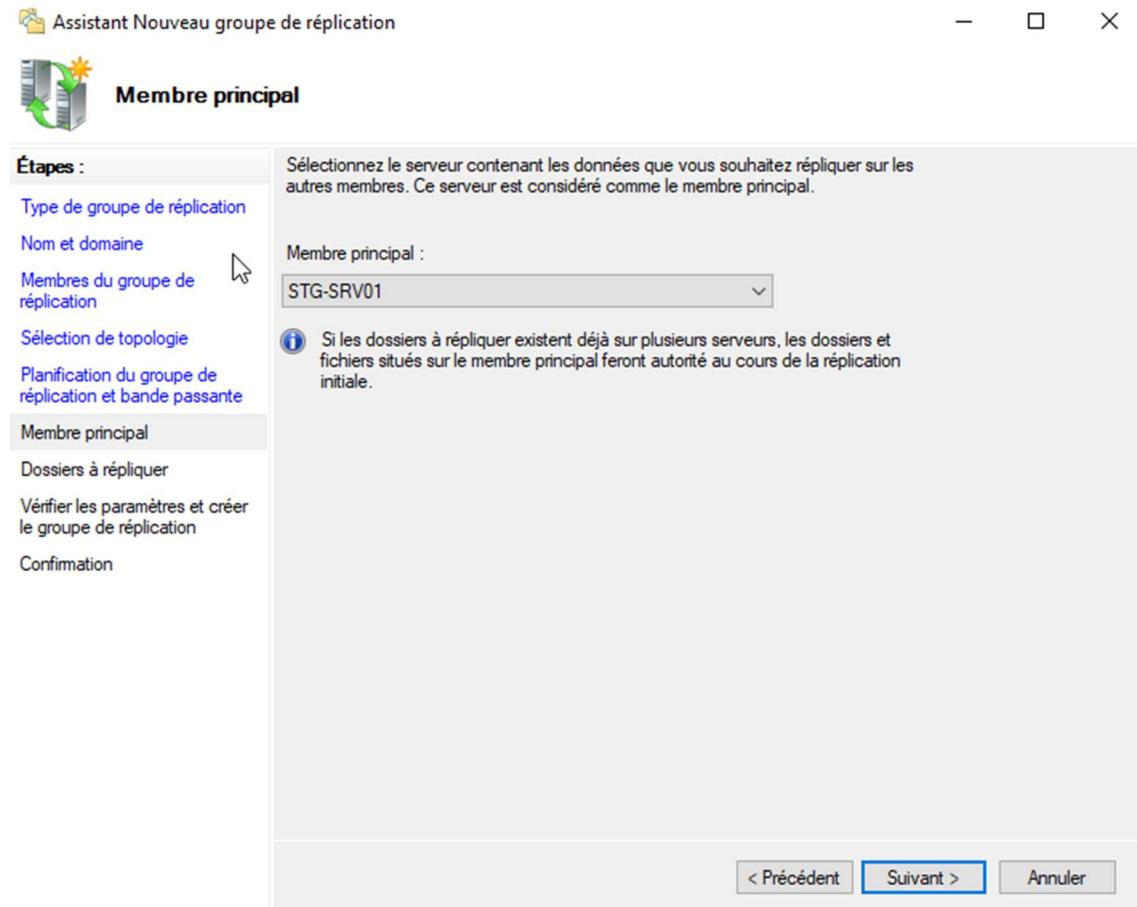
Répliquer aux jours et heures spécifiés

Utilisez cette option pour spécifier les jours et heures de réPLICATION par défaut. La planification de réPLICATION initiale n'a pas d'intervalle de réPLICATION. Vous devez en créer au moins un pour que la réPLICATION puisse avoir lieu.

Modifier la planification...

< Précédent Suivant > Annuler

7. Choisir le membre principal pour la réPLICATION puis cliquer sur Suivant.



6.2) Création du Routeur / Firewall OpenSense Strasbourg

a) Information du serveur

Nom du serveur : **RTE-STG01**

Interfaces IP :

- LAN : 192.168.100.1
- WAN : dhcp

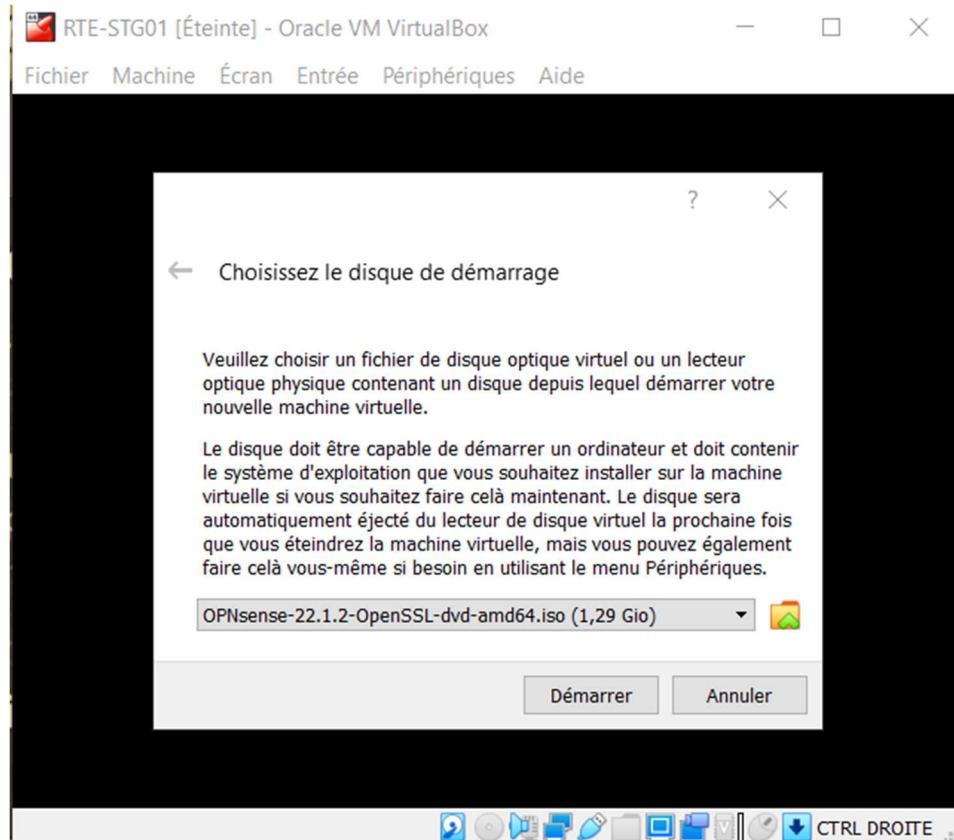
Taille disque dur : 20 GB

RAM : 512 MO

Version : OpenSense : 22.1.2

b) Création de la VM

On commence la création de la Vm :



Dès la phase de démarrage finis, on arrive sur cette interface :

```
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Fri Nov  4 14:57:05 UTC 2022

*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      -> v4/DHCP4: 0.0.0.0/8

HTTPS: SHA256 68 E5 73 38 05 12 F7 6E B0 8B 2A DD 46 7C 42 78
        45 4D D2 0D E0 88 86 42 0F C5 09 9C EE C8 B4 CE
SSH:   SHA256 OPOnIBb2PWSyHcB4Kx9b9i2LHb3iS7U6xGQLaWz5wuw (ECDSA)
SSH:   SHA256 x5P/CkQtFIUItDF4sB9x1TxUQJai8TkecSgoQOCqNSU (ED25519)
SSH:   SHA256 TKM23sp8NnavtWBCsbfscB7DtS1D74Bzy24DgGmfZKo (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login: 
```

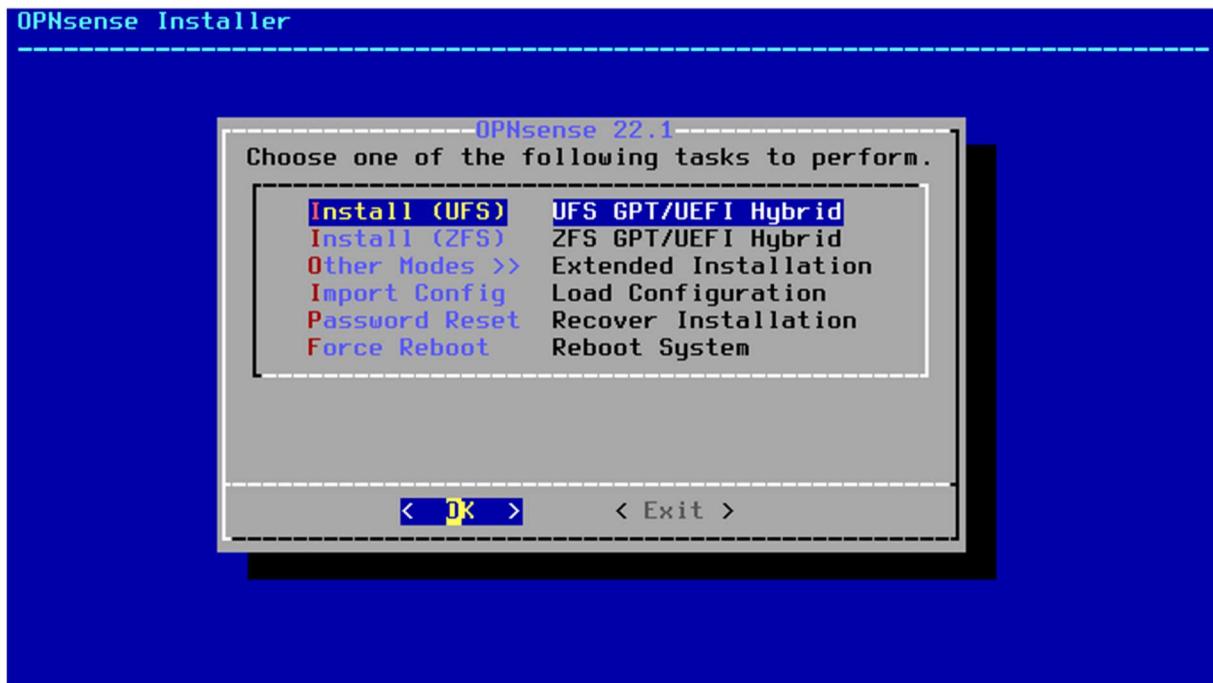
On se connecte avec le compte « installer » pour débuter l'installation.

Login : installer

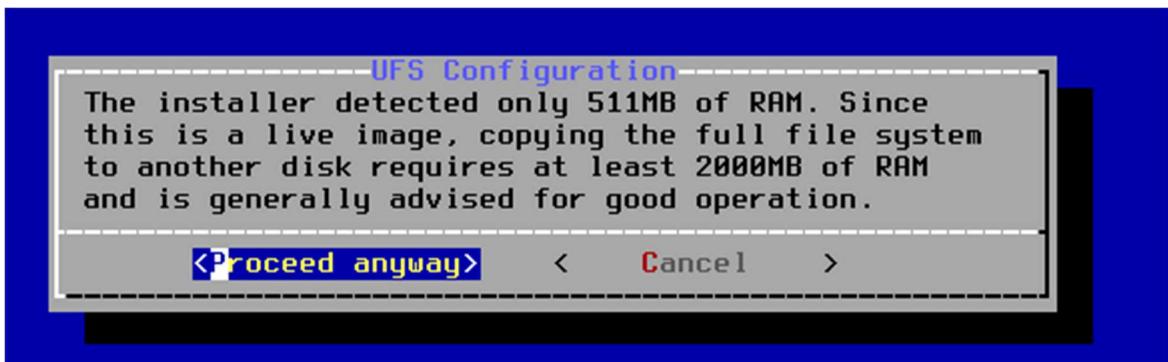
MDP : opnsense



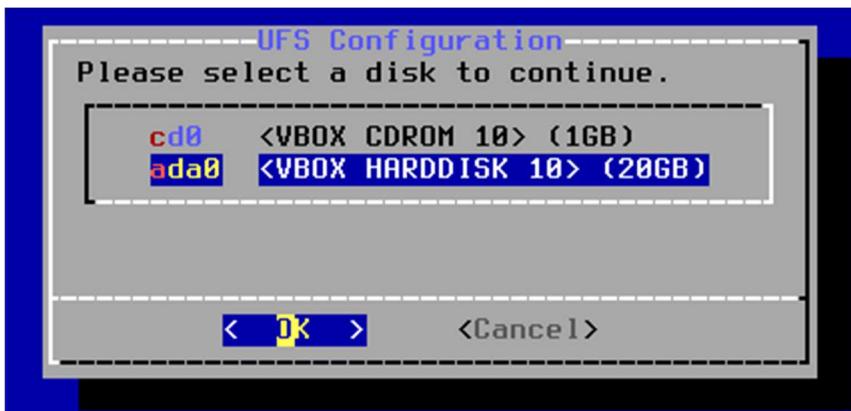
On va cliquer sur la barre espace à la ligne « France » et ensuite faire entrer pour continuer



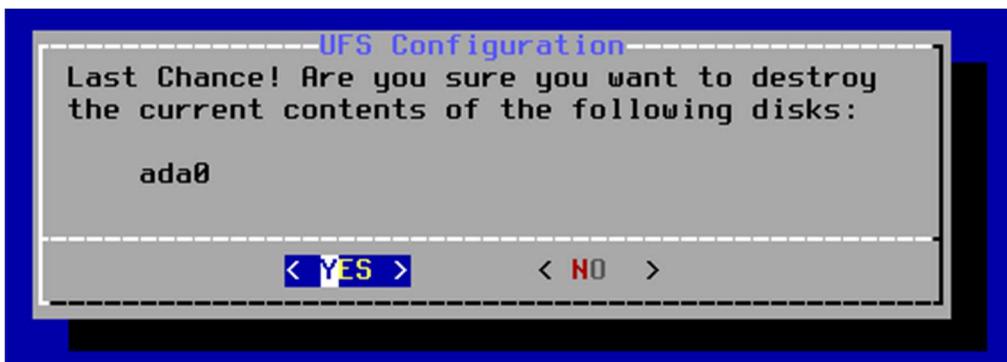
On fait entrée sur la ligne « install (UFS) »



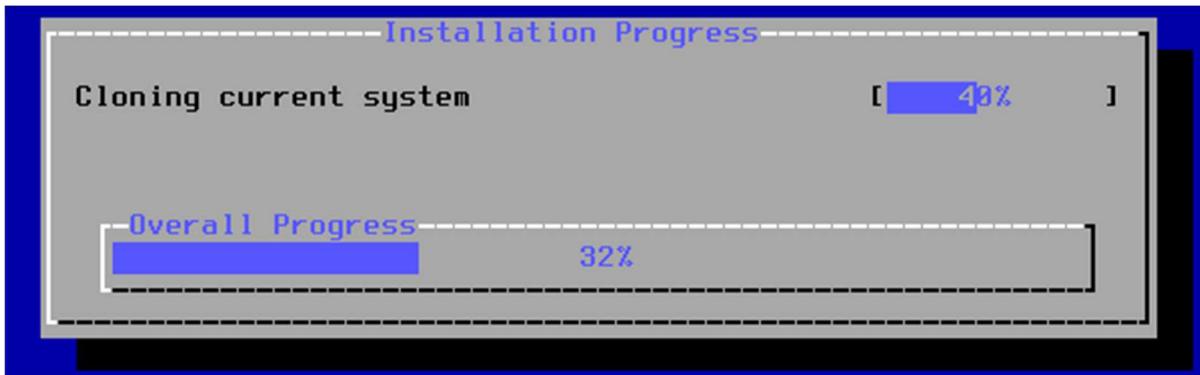
On choisit « proceed anyway »



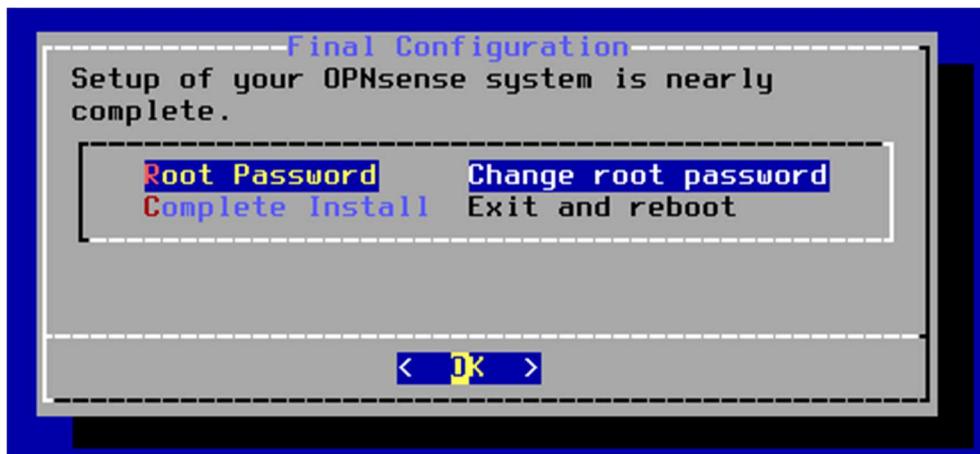
On choisit notre disque virtuel



Yes



Une fois l'installation terminé, on peut changer le mot de passe de root et ensuite choisir l'option « complete install » :



On arrive ensuite sur l'interface principale du serveur :

Et on se connecte avec le compte par default :

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      -> v4/DHCP4: 0.0.0.0/8

HTTPS: SHA256 67 10 C2 39 5F 1A BE E6 14 C0 D9 23 2E 6F 06 8C
        42 F6 5F 46 DD 5C 32 77 6E 9D 9E 90 34 E9 F5 86
SSH:   SHA256 toShFTJN0oREDPi0W7LFje5iu5mJoLa8ip4rtunHHM0 (ECDSA)
SSH:   SHA256 mywi60vxiu17xcNnSiPSoct5Ruqn9imHvF4vFrcAQUI (ED25519)
SSH:   SHA256 ug1G4nYNXHbLw0b85F4GNKQPY2B+I34CfqILP1vesR8 (RSA)

0) Logout          7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: [
```

Login : root

Mdp : opnsense

c) Configuration réseau

On va maintenant assigner les interfaces et changer l'ip de nos cartes réseaux.

Pour ce faire on va entrer l'option « 1 » :

```
Do you want to configure LAGGs now? [y/N]: n
```

```
Do you want to configure VLANs now? [y/N]: n
```

On va choisir la carte « em0 » pour l'interface WAN

```
Enter the WAN interface name or 'a' for auto-detection: em0
```

Et la carte « em1 » pour l'interface LAN

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1
```

Ensuite on confirme avec « y »

```
The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1

Do you want to proceed? [y/N]: y
```

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***
LAN (em1)      -> v4: 192.168.1.1/24
WAN (em0)      -> v4/DHCP4: 172.20.10.3/28
```

On change maintenant l'ip du LAN :

On choisit l'option « 2 »,

```
Enter an option: 2
```

Available interfaces:

```
1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)
```

```
Enter the number of the interface to configure: 1
```

On choisit le LAN,

On refuse le DHCP et on rentre l'ip statique et le masque :

```
Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

On refuse ensuite le reste :

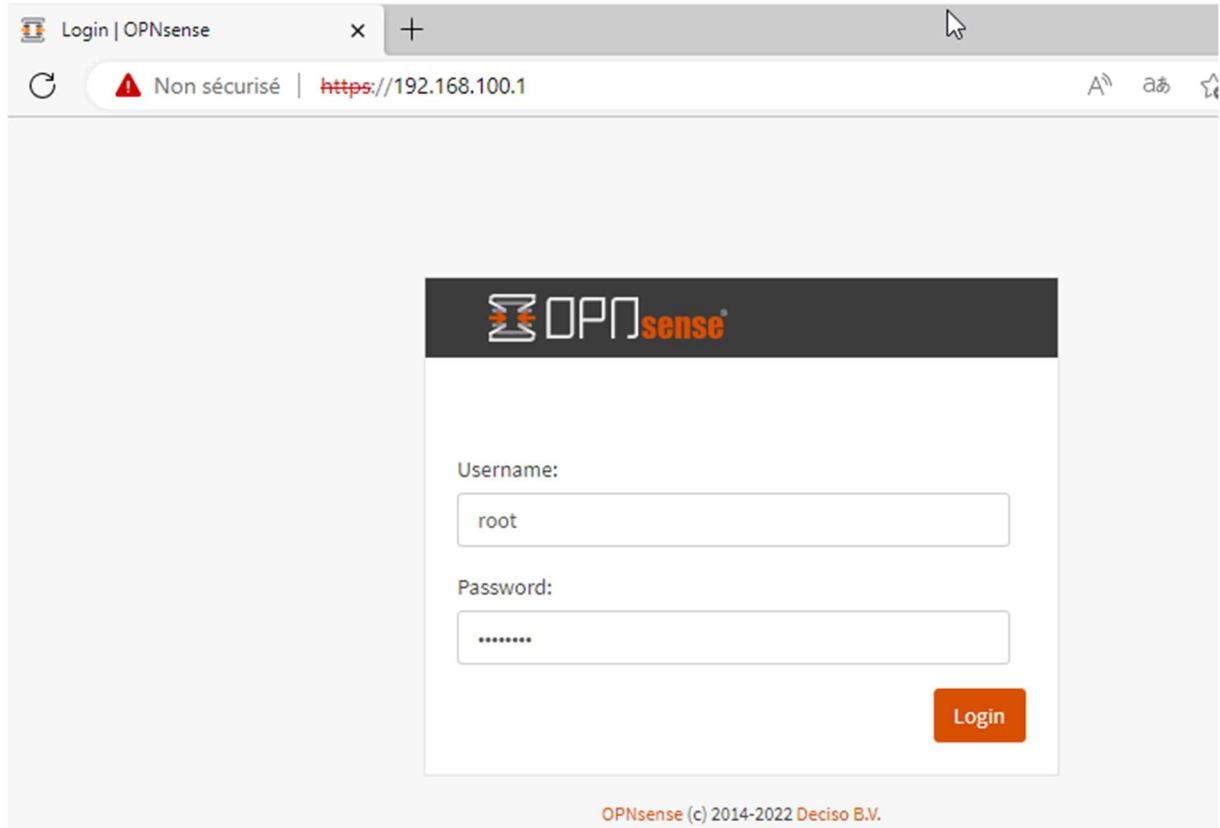
```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? [y/N] n
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
```

La configuration est maintenant terminée :

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***
LAN (em1)      -> v4: 192.168.100.1/24
WAN (em0)      -> v4/DHCP4: 172.20.10.3/28
*snapshot prise*
```

d) Configuration général

On peut maintenant accéder à notre routeur via un accès web avec notre client Windows



On peut commencer la configuration générale du serveur en cliquant sur le bouton « next » :

System: Wizard: General Setup

This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Next

On va rentrer les informations suivantes :

General Information	
Hostname:	RTE-STG01
Domain:	CCI-CAMPUS.LAN
Language:	French
Primary DNS Server:	192.168.100.2
Secondary DNS Server:	192.168.100.3
Override DNS:	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN
Unbound DNS	
Enable Resolver:	<input checked="" type="checkbox"/>
Enable DNSSEC Support:	<input type="checkbox"/>
Harden DNSSEC data:	<input type="checkbox"/>

Next,

Time server hostname: 0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2....
 Enter the hostname (FQDN) of the time server.

Timezone: Europe/Paris

Next

Next,

On laisse tout par default sauf le serveur dhcp :

Configuration du client DHCP

Nom d'hôte DHCP: 192.168.100.1

Adresse IP LAN: 192.168.100.1
 (Laisser vide pour aucun)

Masque de sous-réseau: 24

Suivant

On laisse par default et next

Mot de passe Root:

(Laisser vide pour garder l'actuel(le))

Confirmation Mot de passe Root:

.....



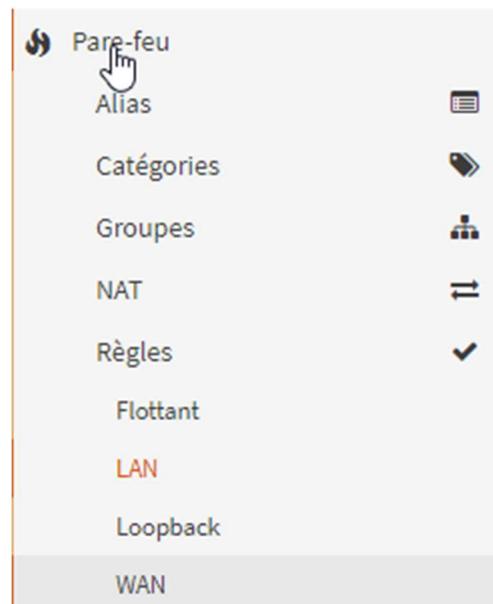
Suivant

On peut maintenant sauvegarder les changements et quitter.

snapshot prise

e) Mise en place VPN IPSEC

On va tout d'abord créer les règles firewall, pour ce faire, on va se rendre dans l'onglet « pare-feu → règles → WAN ».



On autorise le Protocol ESP, le port 500 et le port 4500 sur l'interface WAN :

The screenshot shows a table of firewall rules. A message at the top says "Les modifications ont été appliquées avec succès." (The changes have been applied successfully). The table has columns: Selectionnez une catégorie (Select a category), WAN, Protocole (Protocol), Source, Port, Destination, Port, Passerelle (Gateway), Planifier (Scheduler), Description (Description), and several edit and delete icons.

Selectionnez une catégorie	WAN	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description	
		IPv4 *	*	*	*	*	*	*	Automatically generated rules	
		IPv4 TCP/UDP	*	*	WAN adresse	500 (ISAKMP)	*	*		
		IPv4 TCP/UDP	*	*	LAN adresse	4500 (IPsec NAT-T)	*	*		
		IPv4 ESP	*	*	LAN adresse	*	*	*		

Ensuite, on se rend dans l'onglet « VPN → IPsec → Paramètre du Tunnel » :

The screenshot shows a navigation bar with VPN, IPsec (selected), and a lock icon. Below it is a link labeled "Paramètres du Tunnel".

Et on coche la case « activer IPsec » tout en bas :

VPN: IPsec: Paramètres du Tunnel

La configuration du tunnel IPsec a été modifiée.
Vous devez appliquer les modifications pour qu'elles prennent effet.

Phase 1

Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
Aucun résultat!					

Affichage des entrées 0 à 0 sur 0

Phase 2

Activé	Type	Sous-réseau local	Sous-réseau distant	Phase 2 Proposal	Commandes
Aucun résultat!					

Affichage des entrées 0 à 0 sur 0

Activer IPsec

On va maintenant configurer notre tunnel en cliquant sur le « + » à droite.

VPN: IPsec: Paramètres du Tunnel



Information générale

Désactivé Désactiver cette entrée phase1

Méthode de connexion : **défault**

Version Key Exchange : **V2**

Protocole Internet : **IPv4**

Interface : **WAN**

Passerelle distante : **172.20.10.3**

Passerelle dynamique Allow any remote gateway to connect

Description :

Proposition Phase 1 (Authentification)

Méthode d'authentification : **Mutual PSK**

Mon identifiant : **Mon adresse IP**

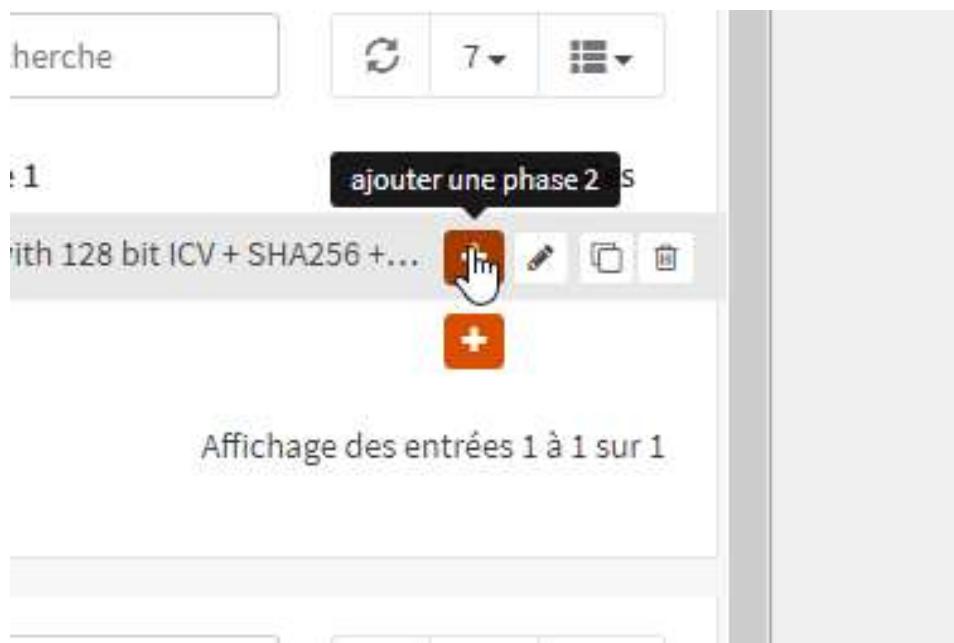
ID du correspondant : **Adresse IP du correspondant**

On rentre notre passerelle distante qui est le WAN du routeur de Mulhouse,

❶ ID du correspondant	Adresse IP du correspondant
❷ Clé Pré-Partagée (PSK)	12345
Proposition Phase 1 (Algorithmes)	
❸ Algorithme de chiffrement	256 bit AES-GCM with 128 bit ICV
❹ Algorithme de hachage	SHA256
❺ Groupe de clé DH	14 (2048 bits)
❻ Durée de vie	28800
Options avancées	
❼ Installe les politiques	<input checked="" type="checkbox"/>
⍽ Désactiver le Renouvellement de clé	<input type="checkbox"/>
⍾ Désactiver Réauthentification	<input type="checkbox"/>
⍲ Isolation de tunnel	<input type="checkbox"/>
⍳ SHA256 96 Bit Truncation	<input type="checkbox"/>
⍴ NAT Traversant	Activer
⍵ Désactiver MOBIKE	<input type="checkbox"/>

On rentre notre clé de cryptage qui est ici « 12345 », puis on Save.

Phase 1					
Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
<input checked="" type="checkbox"/>	IPv4 IKEV2	172.20.10.3		256 bit AES-GCM with 128 bit ICV + SHA256 + ...	
Affichage des entrées 1 à 1 sur 1					
<input type="button" value="<<"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value=">>"/>					



On clique sur « ajouter une phase 2 »,

On entre l'adresse réseau de l'interface LAN du site de Mulhouse :

The screenshot shows a configuration form for a VPN tunnel. At the top, the title is 'VPN: IPsec: Paramètres du Tunnel'. Below it is a section titled 'Information générale' with fields for 'Désactivé' (unchecked), 'Mode' (set to 'Tunnel IPv4'), and 'Description' (empty). The next section is 'Réseau Local' with 'Type' set to 'LAN sous-réseau' and 'Adresse:' set to '192.168.200.0' with a subnet mask of '32'. The following section is 'Réseau Distant' with 'Type' set to 'Réseau' and 'Adresse:' set to '192.168.200.0' with a subnet mask of '24'. The final section is 'Proposition Phase 2 (SA/Échange de Clés)' with 'Protocole' set to 'ESP', 'Algorithmes de chiffrement' set to 'aes256gcm16', and 'Algorithmes de hachage' set to 'SHA256'. The 'Adresse:' field for the distant network is highlighted with a blue border.

On change l'algorithme de chiffrement en AES256 et l'algorithme de hachage en SHA256 :

Proposition Phase 2 (SA/Échange de Clés)

● Protocole

ESP

● Algorithmes de chiffrement

AES256

● Algorithmes de hachage

SHA256

Note: For security reasons avoid the use of the SHA1 algorithm.

● Groupe de clés PFS

off

● Durée de vie

3600

secondes

Options avancées

● Ping automatiquement l'hôte

● Entrées SPD manuelles

Sauvegarder

On Save.

Ce qui nous donne ça :

VPN: IPsec: Paramètres du Tunnel

Phase 1					
Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 IKEv2	172.20.10.3	256 bit AES-GCM with 128 bit ICV + SHA256 +...	
1 Affichage des entrées 1 à 1 sur 1					

Phase 2					
Activé	Type	Sous-réseau local	Sous-réseau distant	Phase 2 Proposal	Commandes
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ESP IPv4 tunnel	LAN	192.168.200.0/24	AES256 + SHA256
1 Affichage des entrées 1 à 1 sur 1					

Activer IPsec

On va maintenant se rendre dans l'onglet « vue globale des statuts » et cliquez sur le bouton « start » à droite sur les 2 serveurs :

VPN: IPsec: Vue globale des statuts

Connexion	Version	ID locale	Adresse IP locale	ID distant	Adresse IP distante	Auth locale	Auth distante	Statut
(con1)	IKEv2	172.20.10.4	172.20.10.4	172.20.10.3	172.20.10.3	pre-shared key	pre-shared key	

Une fois fait, on aperçoit que nos 2 serveurs sont bien reliés :

VPN: IPsec: Vue globale des statuts

Connexion	Version	ID locale	Adresse IP locale	ID distant	Adresse IP distante	Auth locale	Auth distante	Statut
(con1)	IKEv2	172.20.10.4	172.20.10.4	172.20.10.3	172.20.10.3	pre-shared key	pre-shared key	

Hôte Distant	Sous-réseaux locaux	SPI(s)	Sous-réseaux distants	État	Stats
172.20.10.3	192.168.100.0/24	entrant : c01f8755 sortant : c80cb37a	192.168.200.0/24	INSTALLED Routé	Heure : 10 Octets entrants : 0 Octets sortants : 0

f) Mise en place du portail captif

On va tout d'abord ajouter un interface réseau à notre sur notre serveur qui hébergera le portail captif (ici RTE-STG01) :

On se rend dans l'onglet : Interface → assignations

Interfaces: Assignations

Interface	Port réseau
LAN	em1 (08:00:27:08:10:e4)
WAN	em0 (08:00:27:ff:3c:66)
Nouvelle interface:	em2 (08:00:27:e3:5a:30)

Sauvegarder

On clique sur le + ce qui va nous créer l'interface OPT1 :

Interfaces: Assignations

Interface	Port réseau	
LAN	em1 (08:00:27:08:10:e4)	
OPT1	em2 (08:00:27:e3:5a:30)	
WAN	em0 (08:00:27:ff:3c:66)	

Sauvegarder

On save.

On clique sur « OPT1 », on arrive sur son interface :

Interfaces: [OPT1]

Basic configuration	
Activer	<input type="checkbox"/> Activer l'interface
Verrouiller	<input type="checkbox"/> Empêcher la suppression de l'interface
Device	em2
Description	GuestNet

Sauvegarder **Annuler**

On coche « activer l'interface ».

On choisit ensuite un type de configuration ipv4

Generic configuration	
 ⓘ Bloquer les réseaux privés	<input type="checkbox"/>
 ⓘ Bloquer les adresses bogon (non attribuées par l'IANA)	<input type="checkbox"/>
 ⓘ Type de configuration IPv4	Adresse IPv4 statique
 ⓘ Type de configuration IPv6	Aucun
 ⓘ Adresse MAC	<input type="text"/>
 ⓘ MTU (Maximum Transmission Unit)	<input type="text"/>
 ⓘ MSS	<input type="text"/>
 ⓘ Vitesse et duplex	Par défaut (sans préférence, souvent autoselect)
 ⓘ Mode promiscuité	<input type="checkbox"/>
 ⓘ Dynamic gateway policy	<input type="checkbox"/> Cette interface ne nécessite pas de système intermédiaire pour faire office de passerelle
Hardware settings	
 ⓘ Overwite global settings	<input type="checkbox"/>

Et on rentre l'adresse de la carte :

Configuration adresse IPv4 statique	
 ⓘ Adresse IPv4	192.168.100.142
 ⓘ Passerelle IPv4	Auto-déetecte
<input type="button" value="Sauvegarder"/> <input type="button" value="Annuler"/>	

On va ensuite activer le dhcp notre interface GuestNet. On se rend dans l'onglet Services → DHCPv4 → GuestNet :



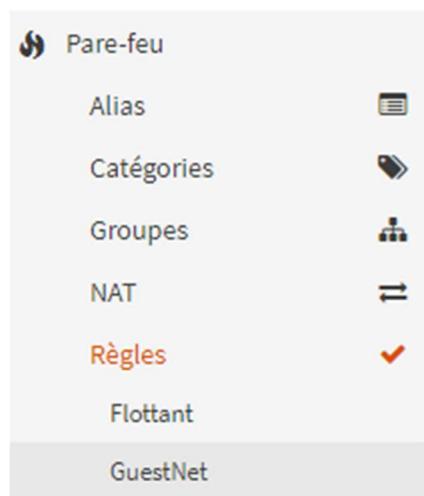
On rentre les informations suivantes :

Services: DHCPv4: [GuestNet]

		aide complète ⓘ		
ⓘ Activer	<input checked="" type="checkbox"/> Activer le serveur DHCP sur l'interface GuestNet			
ⓘ Refuser les clients inconnus	<input type="checkbox"/>			
ⓘ Ignore Client UIDs	<input type="checkbox"/>			
ⓘ Sous-réseau	192.168.100.0			
ⓘ Masque de sous-réseau	255.255.255.0			
ⓘ Plage disponible	192.168.100.1 - 192.168.100.254			
ⓘ Plage	de	à		
	<input type="text" value="192.168.100.5"/>	<input type="text" value="192.168.100.100"/>		
ⓘ Étendues supplémentaires	Début de l'étendue	Fin de l'étendue	Description	+
ⓘ Serveurs WINS	<input type="text"/> <input type="text"/>			
ⓘ Serveurs DNS	<input type="text"/> <input type="text"/>			
ⓘ Passerelle	<input type="text"/>			

Et on sauvegarde.

On peut maintenant configurer nos règles firewall sur notre interface :



On crée une règle qui laisse passer le DNS :

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description					
								Automatically generated rules					
<input type="checkbox"/>	IPv4 TCP/UDP	GuestNet net	*	GuestNet adresse	53 (DNS)	*	*	Allow DNS					

On ajoute une règle qui ouvre tous les ports de 8000 à 10000 pour l'authentification du portail captif :

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description					
								Automatically generated rules					
<input type="checkbox"/>	IPv4 TCP/UDP	GuestNet net	*	GuestNet adresse	53 (DNS)	*	*	Allow DNS					
<input type="checkbox"/>	IPv4 TCP	GuestNet net	*	GuestNet adresse	8000 - 10000	*	*	Allow Captive Portal Login					

On ajoute une règle qui bloque l'accès au réseau LAN depuis le GuestNet

<input type="checkbox"/>	IPv4 *	GuestNet net	*	LAN net	*	*	*	Block Local Networks					
--------------------------	--------	--------------	---	---------	---	---	---	----------------------	--	--	--	--	--

Ce qui nous donne les règles suivantes :

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description					
								Automatically generated rules					
<input type="checkbox"/>	IPv4 TCP/UDP	GuestNet net	*	GuestNet adresse	53 (DNS)	*	*	Allow DNS					
<input type="checkbox"/>	IPv4 TCP	GuestNet net	*	GuestNet adresse	8000 - 10000	*	*	Allow Captive Portal Login					
<input type="checkbox"/>	IPv4 *	GuestNet net	*	LAN net	*	*	*	Block Local Networks					
<input type="checkbox"/>	IPv4 *	GuestNet net	*	*	*	*	*						
autoriser		bloquer		rejeter		tracer		entrant	première correspondance				
passer (désactivé)		bloquer (désactivé)		rejeter (désactivé)		tracer (désactivé)		sortant	dernière correspondance				

Une fois les règles FW créée, on peut se rendre dans l'onglet : Services → Portail Captif → Administration



Services: Portail Captif: Administration

Zones Modèles

<input type="checkbox"/> Activé	Description	Commandes
Aucun résultat!		

+ Sauvegarder

« < 1 > » Affichage des entrées 0 à 0 sur 0

Appliquer

On clique sur le + pour créer notre portail captif,

Editer la zone

(i) mode avancé aide complète

(i) Activé <input checked="" type="checkbox"/>	
(i) Numéro de zone <input type="text" value="0"/>	
(i) Interfaces <input type="text" value="GuestNet"/>	<input type="button" value="Tout effacer"/>
(i) Authenticate using <input type="text" value="Nothing selected"/>	<input type="button" value="Tout effacer"/>
(i) Always send accounting requests <input type="checkbox"/>	
(i) Enforce local group <input type="text" value="aucun(e)"/>	<input type="button" value="Tout effacer"/>
(i) Délai d'inactivité (minutes) <input type="text" value="0"/>	
(i) Hard timeout (minutes) <input type="text" value="0"/>	
(i) Concurrent user logins <input type="checkbox"/>	
(i) Certificat SSL <input type="text" value="aucun(e)"/>	<input type="button" value="Tout effacer"/>
(i) Nom d'hôte <input type="text"/>	
(i) Adresses autorisées <input type="text"/>	<input type="button" value="Tout effacer"/> <input type="button" value="Copy"/> <input type="button" value="Paste"/>
(i) Proxy transparent (HTTP) <input type="checkbox"/>	
(i) Proxy transparent (HTTPS) <input type="checkbox"/>	
(i) Modèle personnalisé <input type="text" value="aucun(e)"/>	<input type="button" value="Tout effacer"/>
(i) Description <input type="text" value="Guest Network"/>	

Sauvegarder

On rentre les informations suivantes et on save.

On va maintenant créer un modèle pour l'interface d'authentification du portail captif, on se rend dans l'onglet « Modèles » :

Services: Portail Captif: Administration

Zones Modèles

Ouvrir un fichier

Recherche

Command...

Download default template

Aucun résultat!

Affichage des entrées 0 à 0 sur 0

Appliquer

On clique sur « download default template »

On import ensuite le modèle téléchargé en cliquant sur le +.

Envoyer un fichier

Nom du modèle

CCI Template

File input

Choisir un fichier template_default.zip

Envoyer

Services: Portail Captif: Administration

Zones Modèles

Recherche

Command...

Affichage des entrées 1 à 1 sur 1

Appliquer

On va maintenant limiter la bande passante utilisable par les potes clients.

On se rend dans l'onglet « pare-feu → Shaper → Tuyaux » :

Pare-feu: Shaper

Tuyaux Files d'attente Règles

Activé	Bandwidth Metric	Masque	Description	Command...
Aucun résultat!				

Affichage des entrées 0 à 0 sur 0

Appliquer Réinitialiser

On clique sur le +,

On crée un « Tuyau » de 10 Mbit/S pour la bande passante des téléchargements :

Éditer le tuyau (pipe)

mode avancé aide complète

Activé

Bandwidth Metric Mbit/s

Masque

Activer CoDel

Enable PIE

Description

Annuler Sauvegarder

Et un autre de 1 Mbit/S pour l'upload :

Éditer le tuyau (pipe)

mode avancé aide complète

<input checked="" type="checkbox"/> Activé	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Bande passante	<input type="text" value="1"/> Bande passante totale pour ce tuyau
<input checked="" type="checkbox"/> Bandwidth Metric	Mbit/s ▼
<input checked="" type="checkbox"/> Tout effacer	
<input checked="" type="checkbox"/> Masque	destination ▼
<input checked="" type="checkbox"/> Tout effacer	
<input checked="" type="checkbox"/> Activer CoDel	<input type="checkbox"/>
<input checked="" type="checkbox"/> Enable PIE	<input type="checkbox"/>
<input checked="" type="checkbox"/> Description	<input type="text" value="Upload"/>

[Annuler](#) [Sauvegarder](#)

On crée ensuite des règles :

Pare-feu: Shaper

<input type="checkbox"/> Activé	#	Interface	Protocole	Source	Destination	Cible	Description	Commandes
Aucun résultat!								
+ ■								
« < 1 > »								
Affichage des entrées 0 à 0 sur 0								
					Appliquer Réinitialiser			

On clique sur +.

Éditer la règle

mode avancé aide complète ⓘ

Activé

Sequence

Interface ▼
✖ Tout effacer

Interface 2 ▼
✖ Tout effacer

Protocole ▼
✖ Tout effacer

Max Packet Length

Source ✖ Tout effacer Copy Paste

Invert source

Src-port

Destination ✖ Tout effacer Copy Paste

Invert destination

Dst-port

DSCP ▼
✖ Tout effacer

Direction ▼
✖ Tout effacer

Cible ▼
✖ Tout effacer

Description

Description to identify this rule.

Annuler Sauvegarder

On a donc la règles pour la cible « Download »,

Éditer la règle

mode avancé [aide complète](#)

Activé

Sequence

Interface [Tout effacer](#)

Interface 2 [Tout effacer](#)

Protocole [Tout effacer](#)

Max Packet Length

Source [Tout effacer](#) [Copy](#) [Paste](#)

Invert source

Src-port

Destination [Tout effacer](#) [Copy](#) [Paste](#)

Invert destination

Dst-port

DSCP [Tout effacer](#)

Direction [Tout effacer](#)

Cible [Tout effacer](#)

Description

Description to identify this rule.

[Annuler](#) [Sauvegarder](#)

Et la règles pour la cible « upload ».

Pare-feu: Shaper

Tuyaux Files d'attente Règles

Activé	#	Interface	Protocole	Source	Destination	Cible	Description	Commandes
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	WAN	ip	any	any	Download	Limit Guest dow...  
<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	WAN	ip	any	any	Upload	Limit Guest Uplo...  

Affichage des entrées 1 à 2 sur 2

< < 1 > >>

Appliquer **Réinitialiser**

On save et on applique.

On crée maintenant le « Bon d'échange », on se rend dans « Système → Accès → Serveurs :

-  Accueil
-  Rapports
-  Système
 - Accès
 - Utilisateurs
 - Groupes
 - Serveurs

Système: Accès: Serveurs

Nom du serveur	Type	Nom d'hôte
Base de données locale 	Base de données locale	RTE-STG01 

On clique sur le +.

On rentre les informations suivantes :

Système: Accès: Serveurs

		aide complète
❶ Nom descriptif	Bon d'échange	
❷ Type	Bon d'échange	
❸ Utiliser des mots de passe simples (moins sécurisés)	<input checked="" type="checkbox"/>	
❹ Longueur du nom d'utilisateur	8	
❺ Longueur des mots de passe	8	
Sauvegarder		

On save.

Système: Accès: Serveurs

Nom du serveur	Type	Nom d'hôte	
Bon d'échange	Bon d'échange	RTE-STG01	
Base de données locale	Base de données locale	RTE-STG01	

Ensuite on se rend dans :



Services: Portail Captif: Bons d'échange

Bon d'échange	Nothing selected			
<input type="checkbox"/>				
	Recherche	10		
Bon d'échange	Valide à partir de	Valide jusqu'à	Expire le	État
Aucun résultat!				
Affichage des entrées 0 à 0 sur 0				
<input icon"="" trash="" type="button" value="Expirer les bons d'échange sélectionnés 		<input icon"="" trash="" type="button" value="Supprimer les bons d'échange expirés 		<input icon"="" plus="" type="button" value="Créer des bons d'échange

On clique sur « créer des bons d'échange »,

Générer des bons d'échange

×

Paramètres	Valeur
Validité	1 jour
Expire dans	jamais
Nombre de bon(s) d'échange	25
Groupname	20221230142437

Générer
Fermer

On crée un bon d'échange d'une validité de 1 jour qui n'expire jamais.

Une fois qu'on a cliqué sur générer, on arrive sur cette page et un fichier CSV se télécharge :

Services: Portail Captif: Bons d'échange

Bon d'échange				
			20221230142437	Delete
<input type="checkbox"/>	Bon d'échange	Valide à partir de	Valide jusqu'à	Expire le
<input type="checkbox"/>	mY2XXfQn	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	vgVqN4Zn	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	snMhWPCf	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	nF2nbDgY	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	AnK7fMGp	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	6nVGBJt8	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	FsW8NAbd	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	uQzLbtIU	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	mdgcTUhg	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused
<input type="checkbox"/>	QQQDCbGd	Dec 30, 2022 3:25 PM	Dec 31, 2022 3:25 PM	unused

Affichage des entrées 1 à 10 sur 25

Expirer les bons d'échange sélectionnés
Supprimer les bons d'échange expirés
Créer des bons d'échange

Téléchargements



20221230142437.csv
Ouvrir un fichier

On retrouve dans notre CSV les Informations des comptes :

```

20221230142437 - Bloc-notes
Fichier Edition Format Affichage Aide
username,password,vouchergroup,expirytime,validity
"mY2XXfQn","sZHhYVAu","20221230142437","0","86400"
"vgVqN4Zn","brbKqYkc","20221230142437","0","86400"
"snMhWPCf","JDAmbfJ3","20221230142437","0","86400"
"nF2nbDgY","HYWL4KWJ","20221230142437","0","86400"
"AnK7fMGp","waTLVAUV","20221230142437","0","86400"
"6nVGBJt8","ihM7nFdQ","20221230142437","0","86400"
"FsW8NAbd","BYmH2SYn","20221230142437","0","86400"
"uQzLbtIU","M6J3fjyG","20221230142437","0","86400"
"mdgcTUhg","Ym998JRn","20221230142437","0","86400"
"QJQDCbGd","RKwSRfCZ","20221230142437","0","86400"
"AXQQFX4R","4DJXLJnE","20221230142437","0","86400"
"H4LkfhsF","D2yB897V","20221230142437","0","86400"
"iUBFbeui","cuSQHm3j","20221230142437","0","86400"
"H24sfh3D","uCnnBDJY","20221230142437","0","86400"
"VmChW99k","hz2upQSw","20221230142437","0","86400"
"SnCLL7sK","G7BCJNnw","20221230142437","0","86400"
"vVfwIGmm","b8MTzDYb","20221230142437","0","86400"
"JxhbbAEi","AYMMJZMh","20221230142437","0","86400"
"6FrBMsic","frTHHm8r","20221230142437","0","86400"
"WUWedBMS","FQtctbi4","20221230142437","0","86400"
"2WBM4irL","9Qh2HTM2","20221230142437","0","86400"
"ViFG4mQq","qyJShmbQ","20221230142437","0","86400"
"JJ3bQLsb","pAsXAhm7","20221230142437","0","86400"
"4g2qtWnL","3inWTS7z","20221230142437","0","86400"
"tW7DWML","DhSSYB7f","20221230142437","0","86400"

```

On peut retourner dans l'onglet administration du portail captif et le modifier :

Services: Portail Captif: Administration

Activé	Description	Commandes
<input type="checkbox"/>	Guest Network	

Affichage des entrées 1 à 1 sur 1

Appliquer

On peut maintenant mettre notre bon d'échange comme méthode d'authentifications :

Editer la zone

mode avancé aide complète

Activé

Numéro de zone 0

Interfaces GuestNet ▾

Tout effacer

Authenticate using Bon d'échange ▾

Tout effacer

Always send accounting requests

Enforce local group aucun(e) ▾

Tout effacer

Délai d'inactivité (minutes) 0

Hard timeout (minutes) 0

Concurrent user logins

Certificat SSL aucun(e) ▾

Tout effacer

Nom d'hôte

Adresses autorisées

Tout effacer

et choisir notre modèle précédemment créer :

Proxy transparent (HTTP)

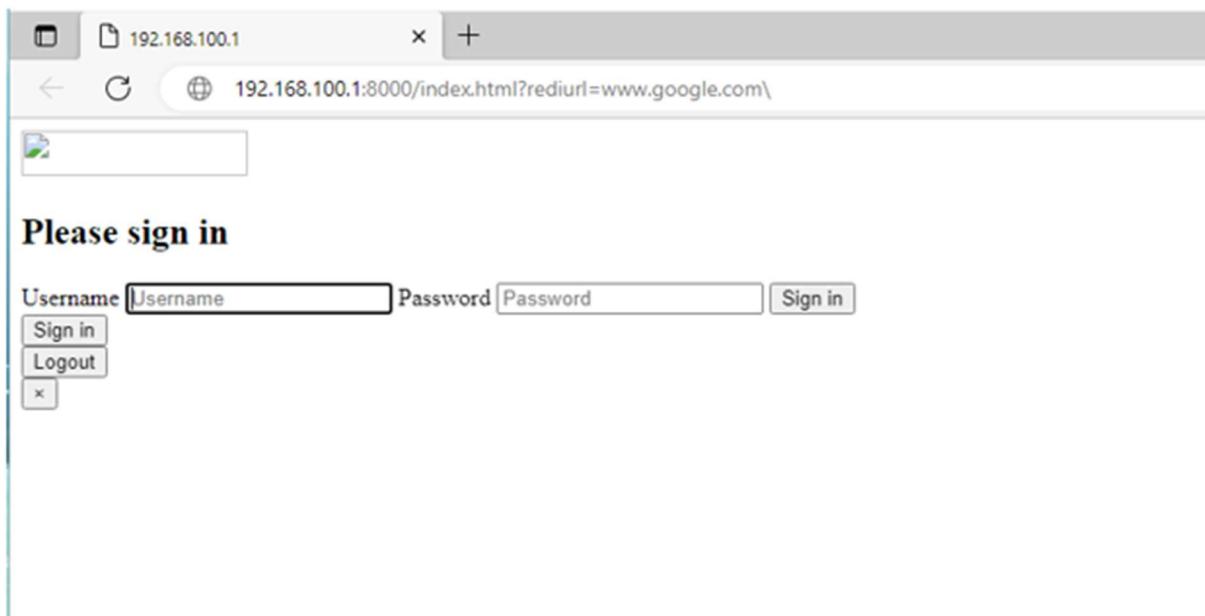
Proxy transparent (HTTPS)

Modèle personnalisé CCI Template ▾

Tout effacer

Description Guest Network

Nous pouvons à présent essayer d'ouvrir une page web avec notre client Windows :



L'accès au web nous demande bien une authentification.

Le portail captif est bien mis en place.

6.3) Création du Routeur / Firewall Opensense Mulhouse

a) Information du serveur

Nom du serveur : **RTE-MUL01**

Interfaces IP :

- LAN : 192.168.200.1
- WAN : dhcp

Taille disque dur : 20 GB

RAM : 512 MO

Version d'OpenSense : 22.1.2

b) Configuration réseau

On va maintenant assigner les interfaces et changer l'ip de nos cartes réseaux.

Pour ce faire on va entrer l'option « 1 » :

```
Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n
```

On va choisir la carte « em0 » pour l'interface WAN

```
Enter the WAN interface name or 'a' for auto-detection: em0
```

Et la carte « em1 » pour l'interface LAN

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1
```

Ensuite on confirme avec « y »

```
The interfaces will be assigned as follows:
```

```
WAN  -> em0
LAN  -> em1
```

```
Do you want to proceed? [y/N]: y
```

```
*** OPNsense.localdomain: OPNsense 22.1.2_2 (amd64/OpenSSL) ***

LAN (em1)      -> v4: 192.168.1.1/24
WAN (em0)      -> v4/DHCP4: 172.20.10.3/28
```

On change maintenant l'ip du LAN :

On choisit l'option « 2 »,

```
Enter an option: 2
```

```
Available interfaces:
```

```
1 - LAN (em1 - static, track6)
2 - WAN (em0 - dhcp, dhcp6)
```

```
Enter the number of the interface to configure: 1
```

On choisit le LAN,

On refuse le DHCP et on rentre l'ip statique et le masque :

```
1 - LAN (em1 - static)
2 - WAN (em0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
P> 192.168.200.1

e
Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
s    255.255.0.0    = 16
s    255.0.0.0    = 8
s

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

On refuse ensuite le reste :

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] n
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
```

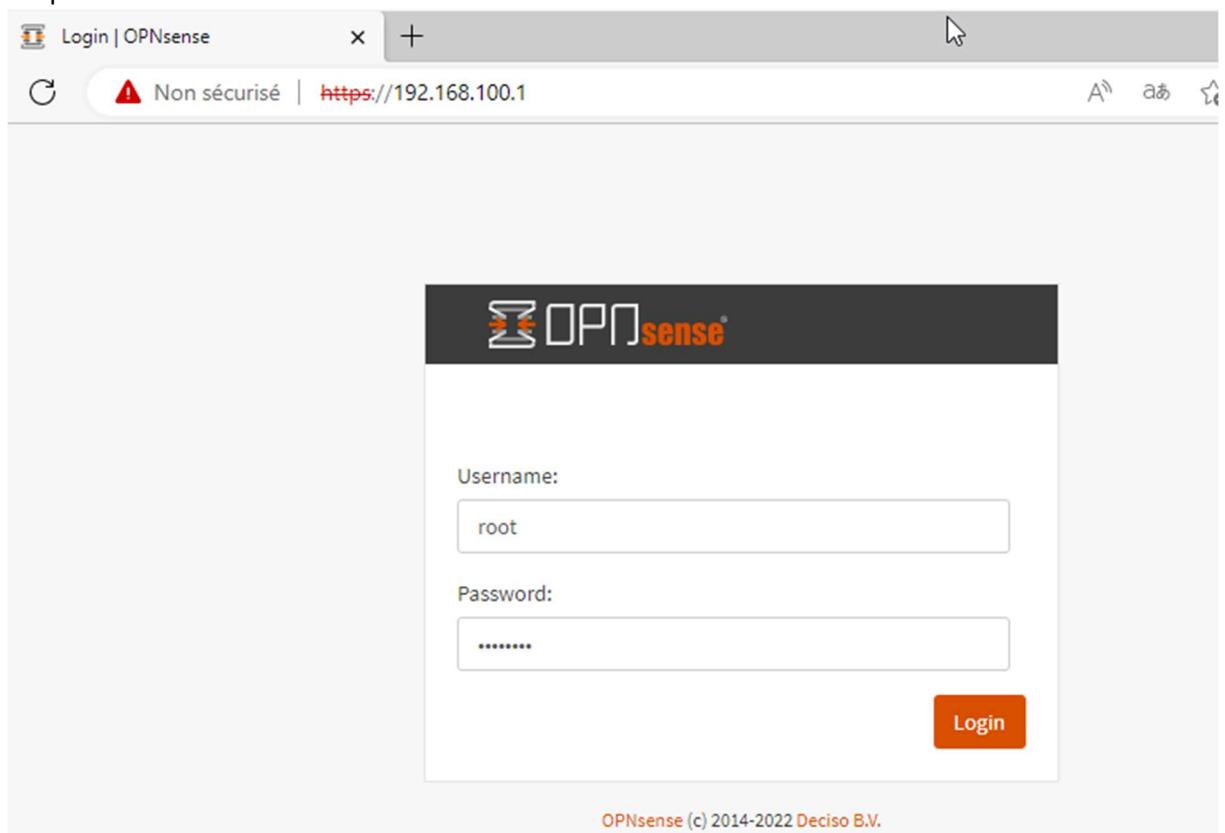
La configuration est maintenant terminée :

```
LAN (em1)      -> v4: 192.168.200.1/24
WAN (em0)      -> v4/DHCP4: 0.0.0.0/8
```

snapshot prise

c) Configuration générale

On peut maintenant accéder à notre routeur via un accès web avec notre client Windows



On peut commencer la configuration générale du serveur en cliquant sur le bouton « next » :

System: Wizard: General Setup

This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Next

On va rentrer les informations suivantes :

i Nom d'hôte	RTE-MUL01
i Domaine	CCI-CAMPUS.LAN
i Fuseau horaire	Europe/Paris
i Langue	Français
i Thème	opnsense

Next,

Time server hostname:	0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2....
Enter the hostname (FQDN) of the time server.	
Timezone:	Europe/Paris

Next

Next,

On rentre nos serveurs DNS :

i Serveurs DNS	Serveur DNS
	192.168.200.2
	192.168.200.3

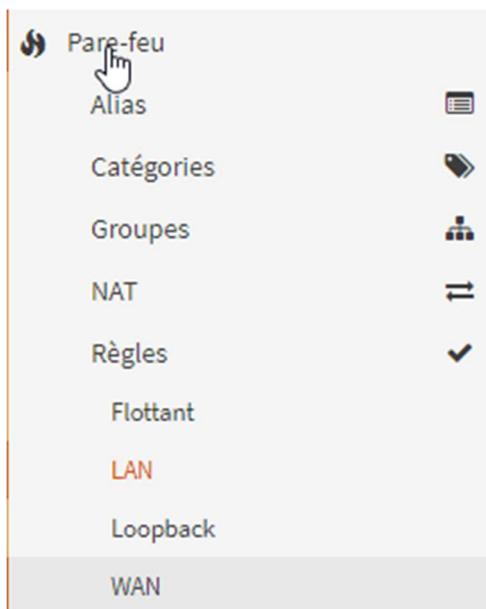
On change le mot de passe du compte root :

Mot de passe Root:
(Laisser vide pour garder l'actuel(le))	
Confirmation Mot de passe Root:
Suivant	

On peut maintenant sauvegarder les changements et quitter.
snapshot prise

d) Mise en place VPN IPSEC

On va tout d'abord créer les règles firewall, pour ce faire, on va se rendre dans l'onglet « pare-feu → règles → WAN ».



On va autoriser le Protocol ESP, le port 500 et le port 4500 sur l'interface WAN :

Pare-feu: Règles: WAN

Sélectionnez une catégorie

Inspect

Les modifications ont été appliquées avec succès.

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description	
								Automatically generated rules	
	IPv4 *	*	*	*	*	*	*		
	IPv4 TCP/UDP	*	*	WAN adresse	500 (ISAKMP)	*	*		
	IPv4 TCP/UDP	*	*	LAN adresse	4500 (IPsec NAT-T)	*	*		
	IPv4 ESP	*	*	LAN adresse	*	*	*		

Ensuite, on se rend dans l'onglet « VPN → IPsec → Paramètre du Tunnel » :

The screenshot shows the IPsec configuration interface. At the top, there are tabs for 'VPN' and 'IPsec'. Below them, a sub-tab 'Paramètres du Tunnel' is selected. The main area displays the 'Paramètres du Tunnel' configuration page. It includes sections for 'Phase 1' and 'Phase 2', each with tables for 'Activé', 'Type', and 'Proposition Phase 1' or 'Phase 2 Proposal'. A note at the top states: 'La configuration du tunnel IPsec a été modifiée. Vous devez appliquer les modifications pour qu'elles prennent effet.' An orange 'Appliquer les changements' button is visible. On the left side, a sidebar lists various network management options like Accueil, Rapports, Système, Interfaces, Pare-feu, VPN, and OpenVPN.

Et on coche la case « activer IPsec » tout en bas :

The screenshot shows the 'Paramètres du Tunnel' configuration page. The 'Phase 1' and 'Phase 2' sections are visible, each with their respective tables. At the bottom of the page, there is a checkbox labeled 'Activer IPsec'. This checkbox is checked, indicating that IPsec is enabled. The rest of the interface remains the same as the previous screenshot, showing the configuration tables and the note about applying changes.

On va maintenant configurer notre tunnel en cliquant sur le « + » à droite.

VPN: IPsec: Paramètres du Tunnel



Information générale

[aide complète](#)

Désactivé	<input type="checkbox"/> Désactiver cette entrée phase1
Méthode de connexion	défaut
Version Key Exchange	V2
Protocole Internet	IPv4
Interface	WAN
Passerelle distante	172.20.10.4
Passerelle dynamique	<input type="checkbox"/> Allow any remote gateway to connect
Description	

Proposition Phase 1 (Authentification)

Méthode d'authentification	Mutual PSK
Mon identifiant	Mon adresse IP
ID du correspondant	Adresse IP du correspondant

On rentre notre passerelle distante qui est le WAN du routeur de Strasbourg,

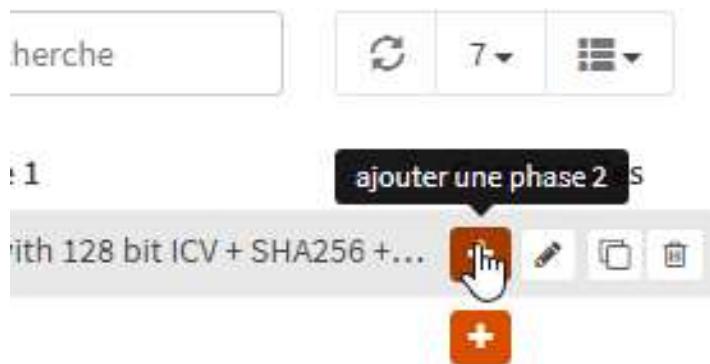
❶ ID du correspondant	Adresse IP du correspondant
❷ Clé Pré-Partagée (PSK)	12345
Proposition Phase 1 (Algorithmes)	
❸ Algorithme de chiffrement	256 bit AES-GCM with 128 bit ICV
❹ Algorithme de hachage	SHA256
❺ Groupe de clé DH	14 (2048 bits)
❻ Durée de vie	28800
Options avancées	
❼ Installe les politiques	<input checked="" type="checkbox"/>
⽩ Désactiver le Renouvellement de clé	<input type="checkbox"/>
⽪ Désactiver Réauthentification	<input type="checkbox"/>
⽫ Isolation de tunnel	<input type="checkbox"/>
⽬ SHA256 96 Bit Truncation	<input type="checkbox"/>
⽭ NAT Traversant	Activer
⽮ Désactiver MOBIKE	<input type="checkbox"/>

On rentre notre clé de cryptage qui est ici « 12345 », puis on Save.

VPN: IPsec: Paramètres du Tunnel

Phase 1					
Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	IPv4 IKEv2	172.20.10.4		256 bit AES-GCM with 128 bit ICV + SHA256 +...	

Affichage des entrées 1 à 1 sur 1



On clique sur « ajouter une phase 2 »,

On entre l'adresse réseau de l'interface LAN du site de Mulhouse :

VPN: IPsec: Paramètres du Tunnel

Information générale		aide complète 🔗
Désactivé	<input type="checkbox"/>	
Mode	Tunnel IPv4	
Description		
Réseau Local		
Type	LAN sous-réseau	
Adresse:	192.168.100.0	32
Réseau Distant		
Type:	Réseau	
Adresse:	192.168.100.0	24
Proposition Phase 2 (SA/Échange de Clés)		
Protocole	ESP	

On change l'algorithme de chiffrement en AES256 et l'algorithme de hachage en SHA256 :

i Protocole	ESP
i Algorithmes de chiffrement	AES256
i Algorithmes de hachage	SHA256
Note: For security reasons avoid the use of the SHA1 algorithm.	
i Groupe de clés PFS	off
i Durée de vie	3600
secondes	
Options avancées	
i Ping automatiquement l'hôte	
i Entrées SPD manuelles	
Sauvegarder	

On peut save.

Ce qui nous donne ça :

VPN: IPsec: Paramètres du Tunnel					
Phase 1 <div style="float: right;"> <input type="button" value="Recherche"/> <input type="button" value="Filtre"/> 7 <input type="button" value="Trier"/> </div>					
Activé	Type	Passerelle distante	Mode	Proposition Phase 1	Commandes
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 IKEv2	172.20.10.4	256 bit AES-GCM with 128 bit ICV + SHA256 + ...	<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Supprimer"/> <input style="background-color: #d9534f; color: white; border-radius: 5px; border: none; padding: 2px 5px; margin-left: 10px;" type="button" value="+"/>
Affichage des entrées 1 à 1 sur 1					
Phase 2 <div style="float: right;"> <input type="button" value="Recherche"/> <input type="button" value="Filtre"/> 7 <input type="button" value="Trier"/> </div>					
Activé	Type	Sous-réseau local	Sous-réseau distant	Phase 2 Proposal	Commandes
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ESP IPv4 tunnel	LAN	192.168.100.0/24	AES256 + SHA256
Affichage des entrées 1 à 1 sur 1					

On va maintenant se rendre dans l'onglet « vue globale des statuts » et cliquez sur le bouton « start » à droite sur les 2 serveurs :

Accueil

Rapports

Système

Interfaces

Pare-feu

VPN

- IPsec
- Paramètres du Tunnel
- Clients mobiles
- Clés pré-partagées
- RSA Key Pairs
- Paramètres avancés
- Vue globale des statuts**

VPN: IPsec: Vue globale des statuts

Connexion	Version	ID locale	Adresse IP locale	ID distant	Adresse IP distante	Auth locale	Auth distante	Statut
(con1)	IKEv2	172.20.10.3	172.20.10.3	172.20.10.4	172.20.10.4	pre-shared key	pre-shared key	

Une fois fait, on aperçoit que nos 2 serveurs sont bien reliés :

VPN: IPsec: Vue globale des statuts

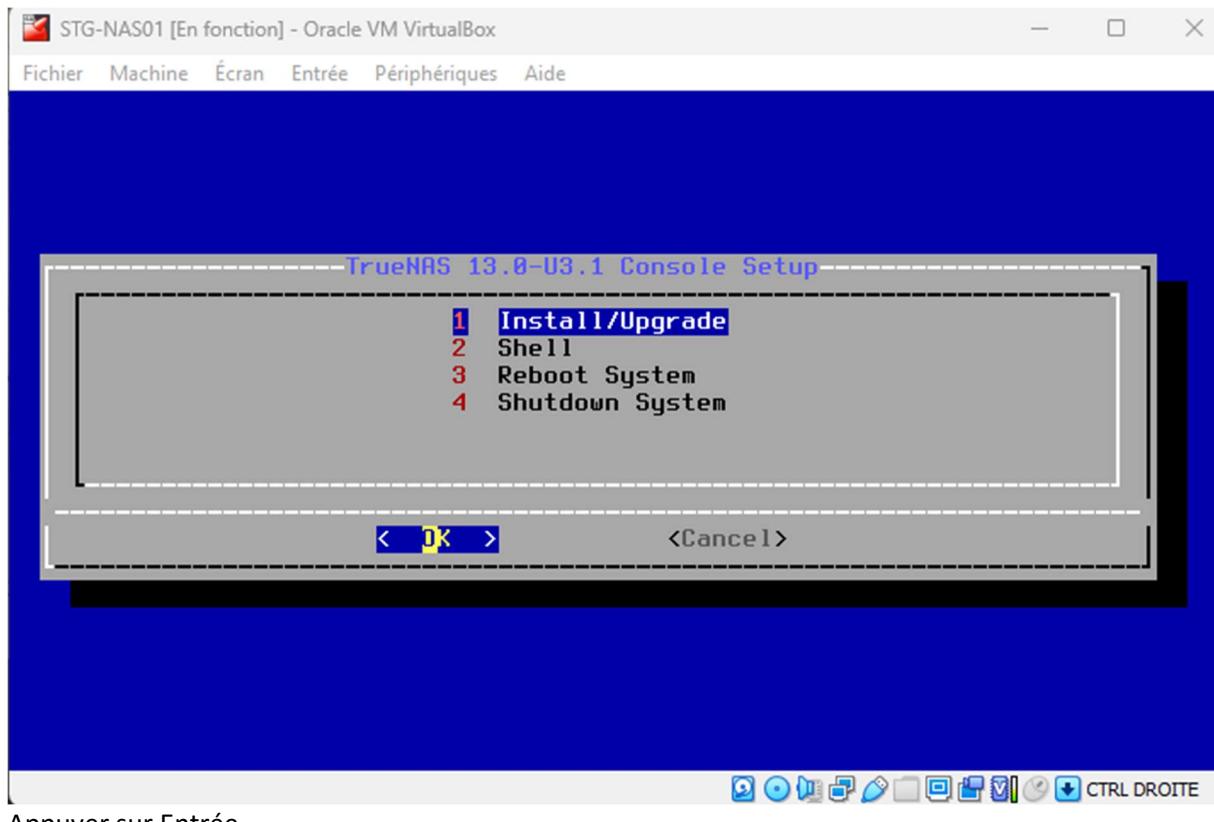
Connexion	Version	ID locale	Adresse IP locale	ID distant	Adresse IP distante	Auth locale	Auth distante	Statut
(con1)	IKEv2	172.20.10.3	172.20.10.3	172.20.10.4	172.20.10.4	pre-shared key	pre-shared key	

Hôte Distant	Sous-réseaux locaux	SPI(s)	Sous-réseaux distants	État	Stats
172.20.10.4	192.168.200.0/24	entrant : c80cb37a sortant : c01f8755	192.168.100.0/24	INSTALLED Routé	Heure : 1 Octets entrants : 0 Octets sortants : 0

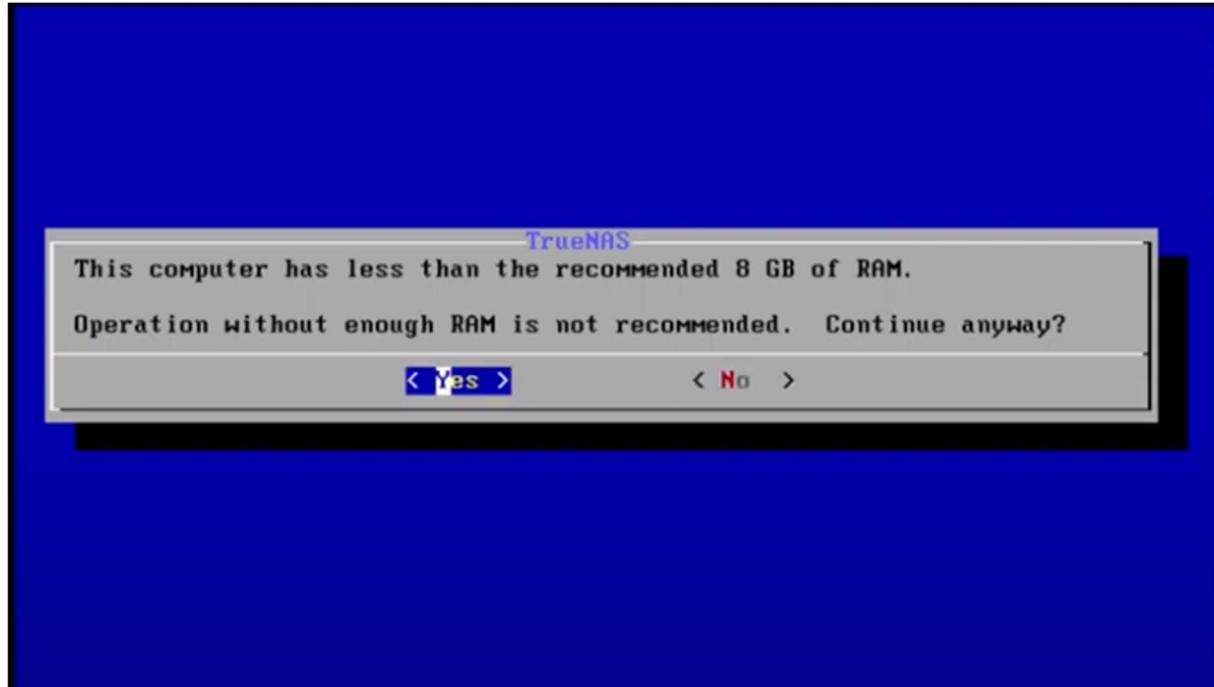
Notre VPN IPSec est maintenant opérationnel et en place.

6.4) Serveur de Sauvegarde SAN et cliché instantané Shadow copy

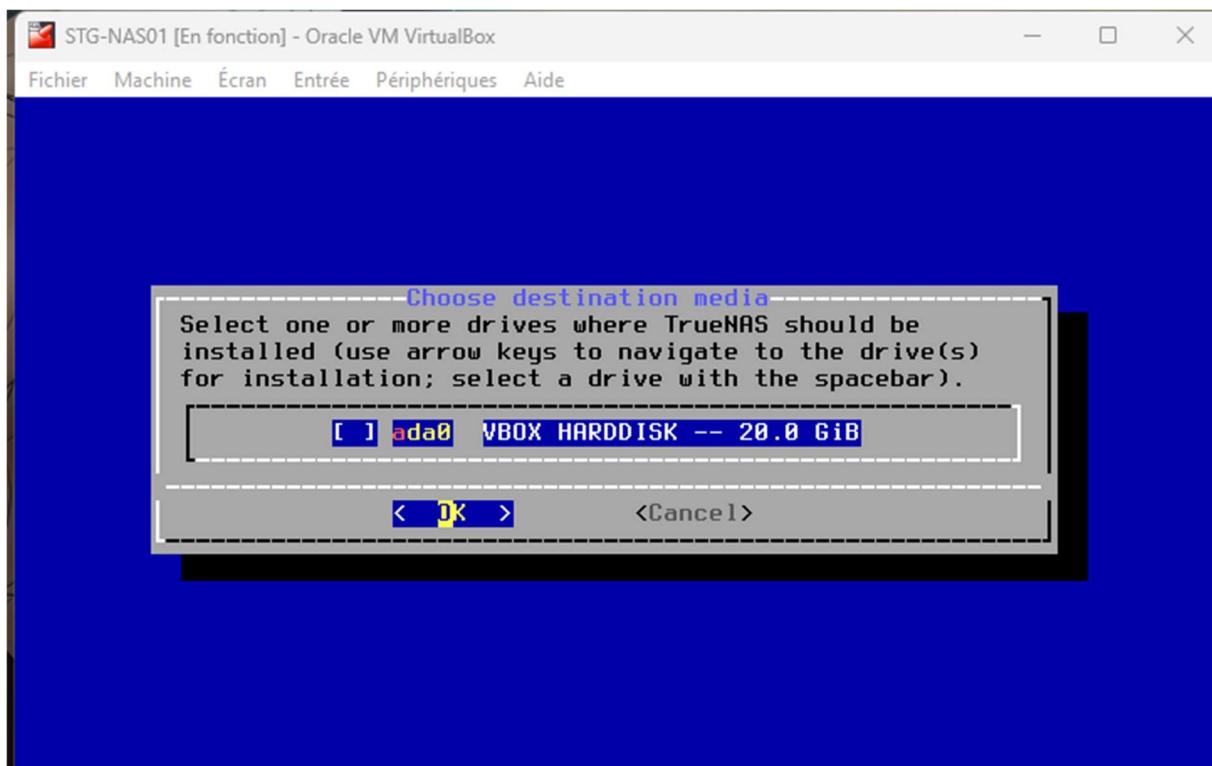
a) Installation du serveur TrueNas



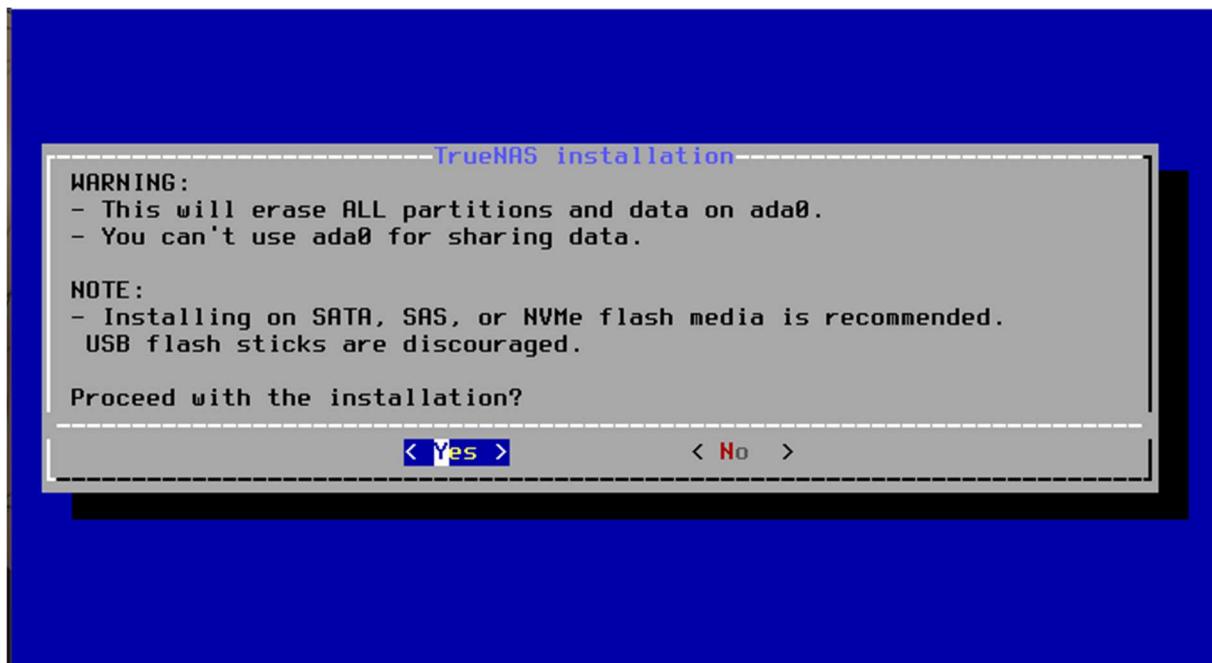
Appuyer sur Entrée



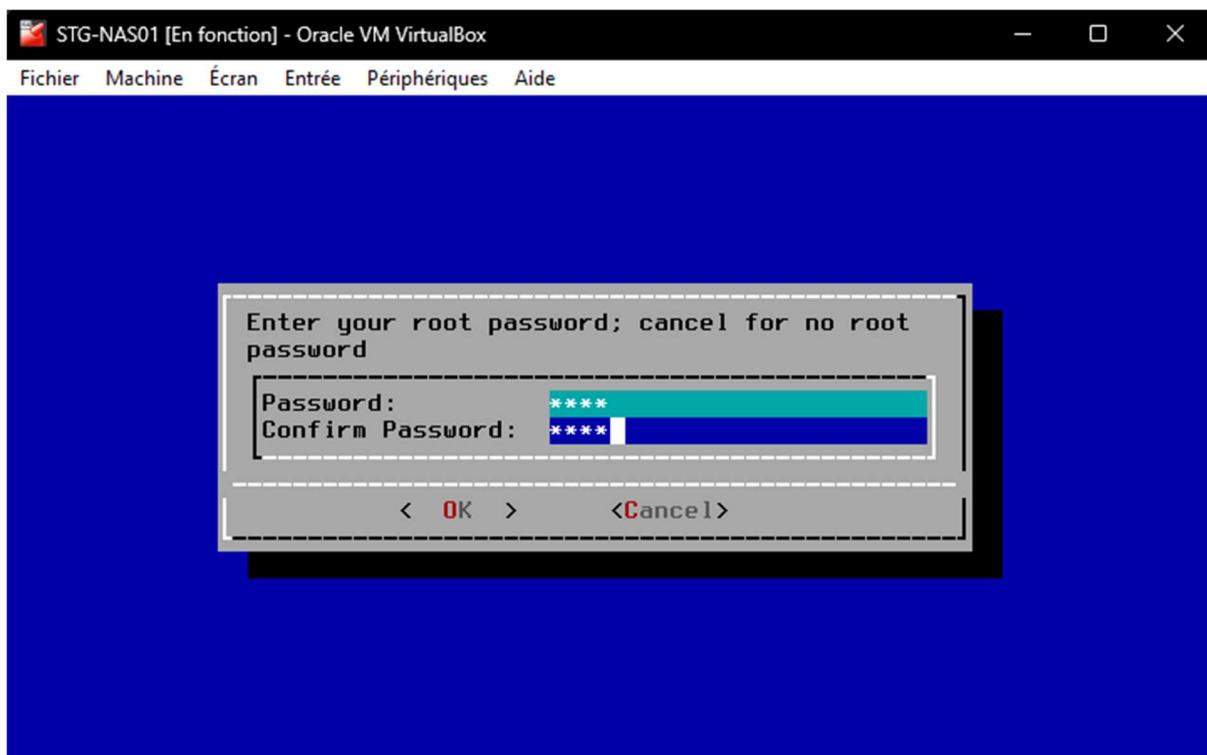
Appuyer sur tab pour sélectionner Yes et appuyer sur entrée



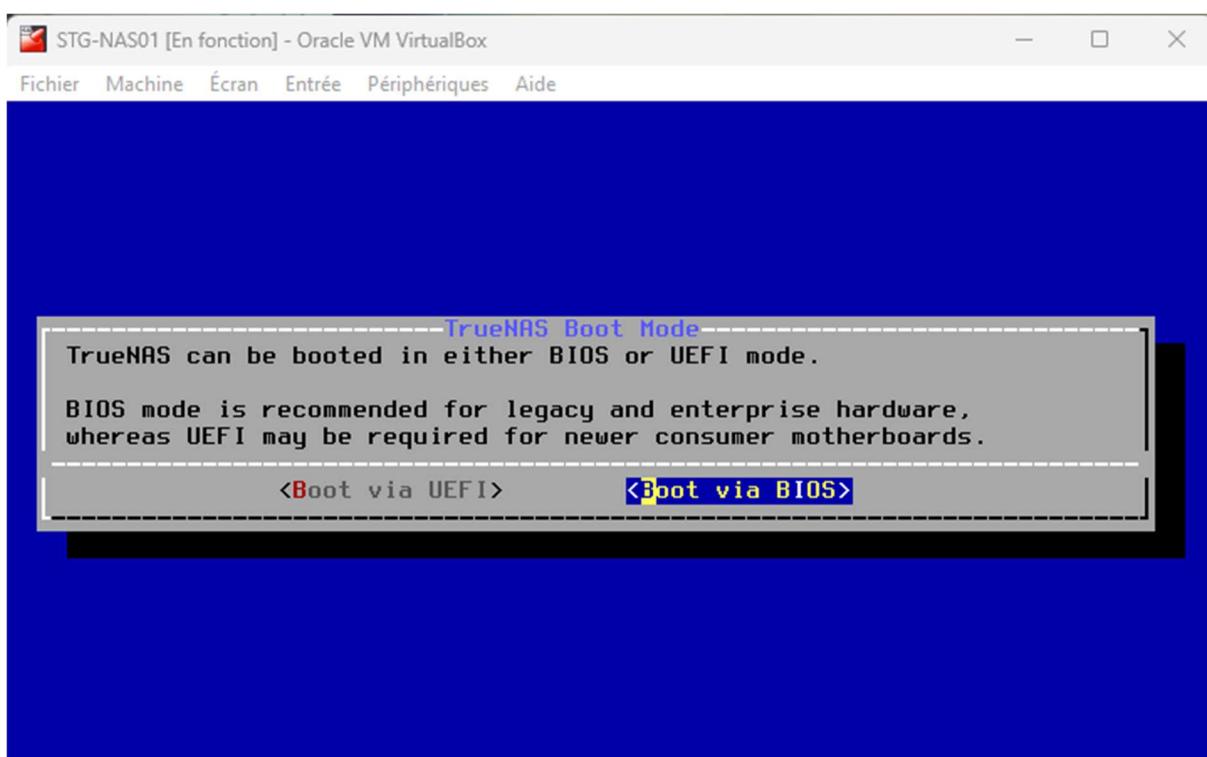
Appuyer sur espace pour sélectionner et appuyer sur Entrée



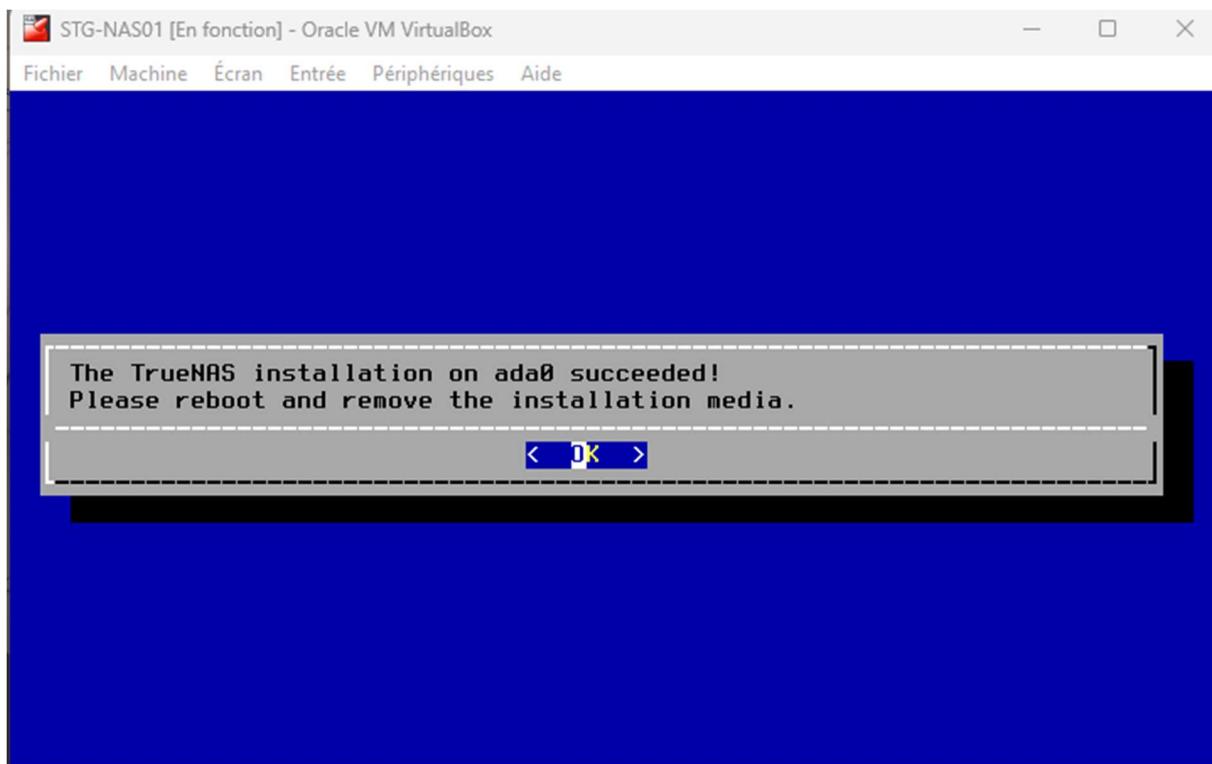
Appuyer sur Entrée et garder par défaut



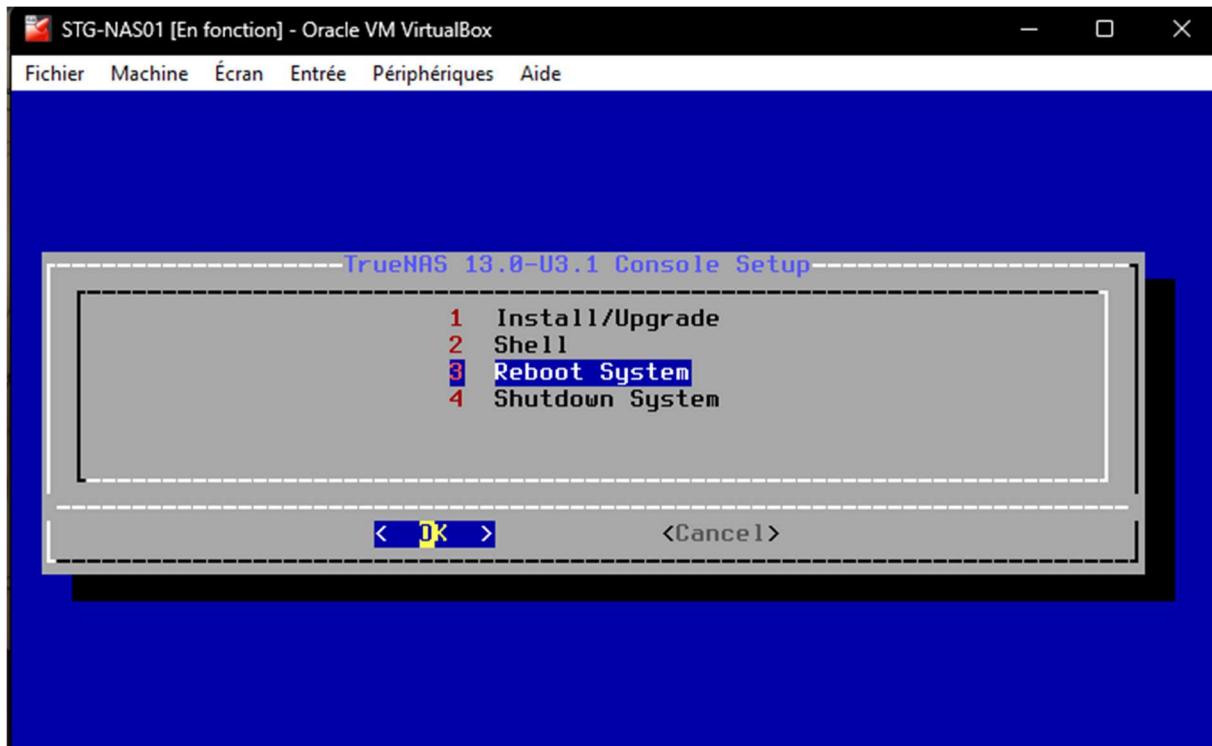
Entrer un mot de passe pour le root



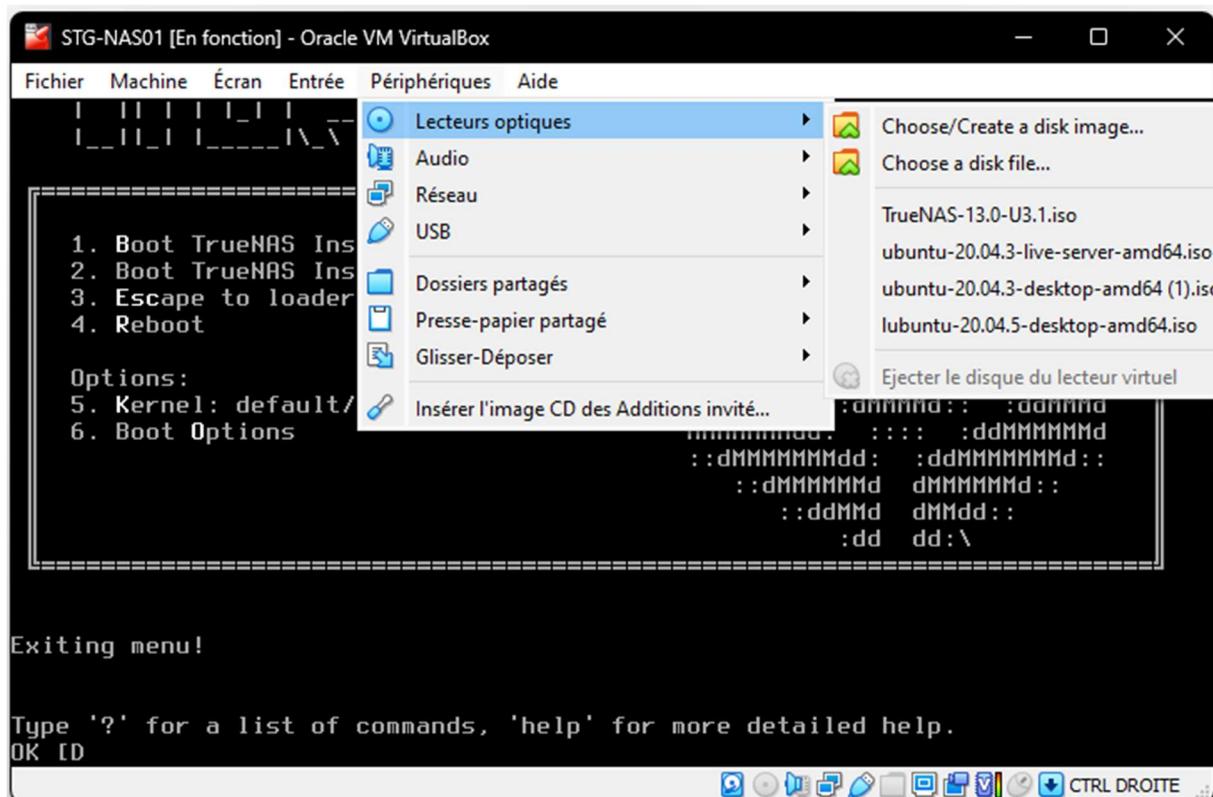
Garder par défaut et appuyer sur Entrée



Appuyer sur entrée



Sélectionner 3 et appuyer sur Entrée pour redémarrer le système.



Exiting menu!

Type '?' for a list of commands, 'help' for more detailed help.
OK [D]

Cliquez sur Périphérique et aller dans lecteurs optiques pour éjecter le disque du lecteur
Ensuite reboot

b) Configuration de TrueNas

Pour créer une « POOL » aller dans « Storage » puis cliquer sur « ADD ».

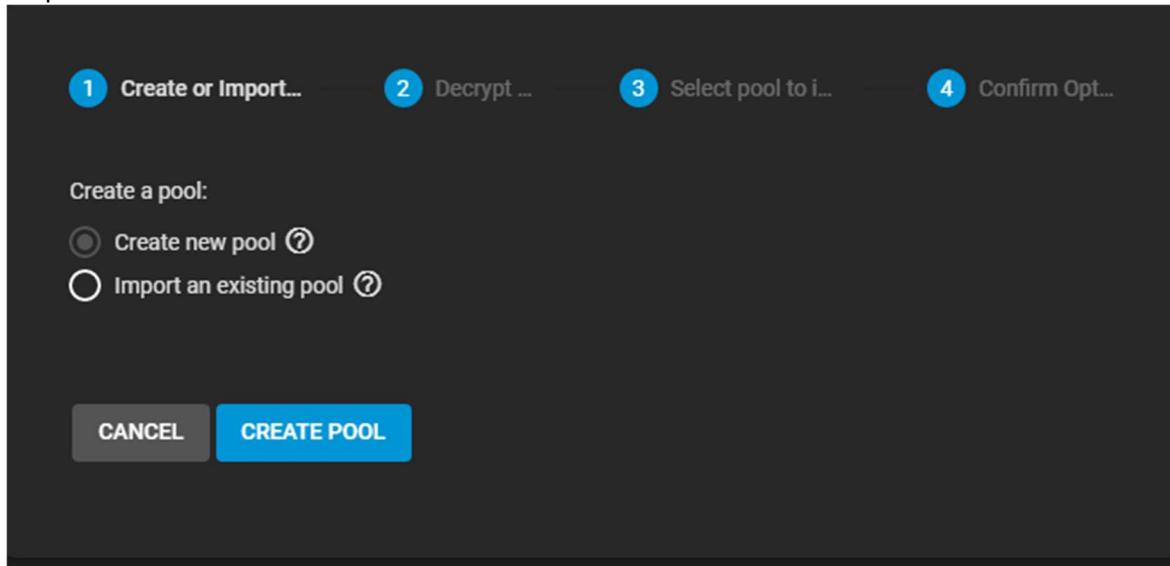
The screenshot shows the TrueNAS Core web interface. The left sidebar has the following navigation links:

- Dashboard
- Accounts
- System
- Tasks
- Network
- Storage (selected)
- Pools
- Snapshots
- VMware-Snapshots
- Disks
- Import Disk

The main content area is titled "Storage / Pools" and displays the message "No pools". In the top right corner, there is a blue "ADD" button.

Dans le panneau latéral, cliquer sur « Storage » puis « Pools ».

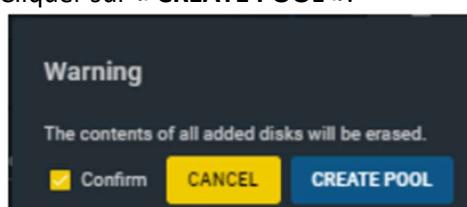
Cliquer ensuite sur le bouton « ADD » en haut à droite.



- 1- Renseigner le nom du Pool dans le champ « **Name** ».
- 2- Faire basculer le ou les disques de gauche **Available Disks** à droite **Data VDevs**.
- 3- TrueNAS vous propose un **type de vDev** en fonction du nombre de disques.
- 4- Une estimation de la taille finale (après construction du RAID) est également affichée.
- 5- Cliquer sur « **CREATE** ».

Cocher la case « **Confirm** ».

Cliquer sur « **CREATE POOL** ».



Création des Datasets dans TrueNAS

Pools										ADD		
Save (System Dataset Pool)		ONLINE	6.81 MiB (0%) Used	46.02 GiB Free								
Name	Type	Used	Available	Compression	Compression	Readonly	Dedup	Comments				
Save	FILESYSTEM	6.81 MiB	46.02 GiB	lz4	18.86	false	OFF					

Création du Dataset « PUBLIC » (Qui sera accessible par tous les utilisateurs) :

Cliquer sur les « ... » à droite du Dataset.

Cliquer sur « Add Dataset ».

The screenshot shows the ZFS Pool configuration interface. At the top, it displays "Save (System Dataset Pool) ONLINE ✓ | 6.86 MiB (0%) Used | 46.02 GiB Free". Below this, there's a table with columns: Ised, Available, Compression, Compression Ratio, Readonly, Dedup, and Comments. The values shown are 6.86 MiB, 46.02 GiB, lz4, 18.86, false, OFF, and a dropdown menu. To the right of the table is a sidebar titled "Dataset Actions" containing the following options: Add Dataset, Add Zvol, Edit Options, Edit Permissions, User Quotas, Group Quotas, and Create Snapshot.

Name : Renseigner le nom du Dataset.

Comments : Renseigner une description pour ce Dataset.

Share Type : Choisir le type de partage. Il faudra choisir « **SMB** » pour un partage **Windows**.

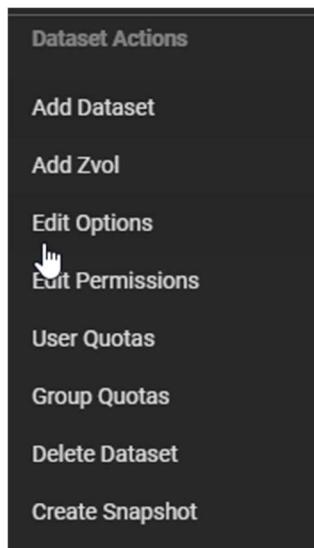
Cliquer sur « **SUBMIT** » pour valider.

The screenshot shows the "Other Options" configuration section. It includes fields for "ZFS Deduplication" (Inherit (off)), "Case Sensitivity" (Insensitive), and "Share Type" (SMB). Each field has a help icon (a question mark inside a circle) to its right.

Configuration des permissions :

Cliquer sur les « ... ».

Cliquer sur « **Edit ACL** ».



Cliquer sur « ADD ACL ITEM ».

Se rendre dans « Accounts », « Groups » et cliquer sur « ADD » :

Group	GID	Builtin	Permit Sudo
No data to display			

Name : ADMIN.

Cliquer sur « SAVE ».

Group Configuration

GID *
1000

Name *
ADMIN

Permit Sudo (?)

Samba Authentication (?)

Allow Duplicate GIDs (?)

SUBMIT **CANCEL**

Se rendre dans « Accounts », « Users » et cliquer sur « ADD » :

Auxiliary Groups : Sélectionner les groupes d'appartenances :

- **builtin_administrators** uniquement pour les **Administrateurs** (Paul).
- Les utilisateurs seront automatiquement ajoutés au groupe **builtin_users**.

Sélectionner le répertoire d'accueil de l'utilisateur.

Cocher la case « **Microsoft Account** » si l'utilisateur se connectera principalement depuis une machine Windows.

Cocher la case « **Permit Sudo** » uniquement pour les administrateurs.

Cocher la case « **Permit Sudo** » uniquement pour les administrateurs.

Un conseil : Ne pas toucher à la partie « **Home Directory Permissions** ».

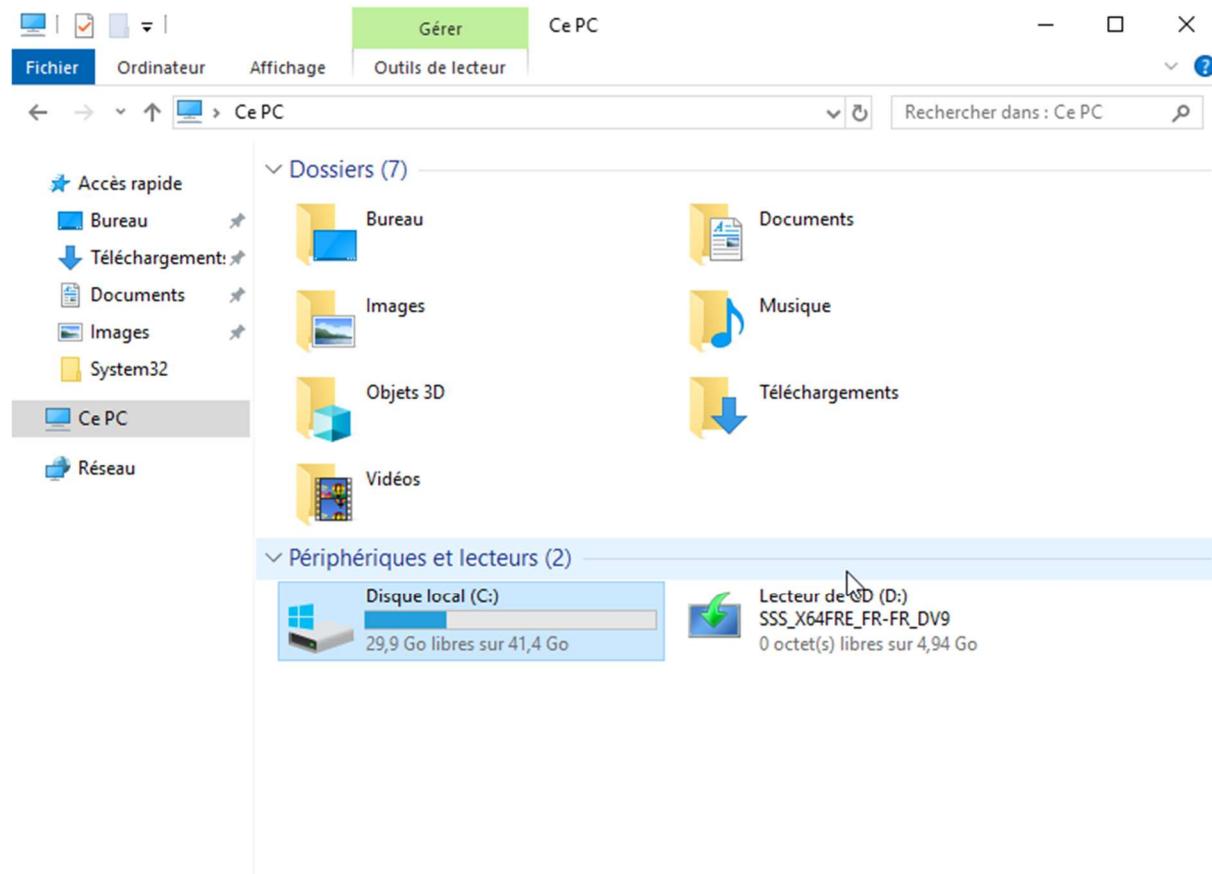
Répéter l'opération pour les autres utilisateurs.

Cliquer sur « **SUBMIT** »

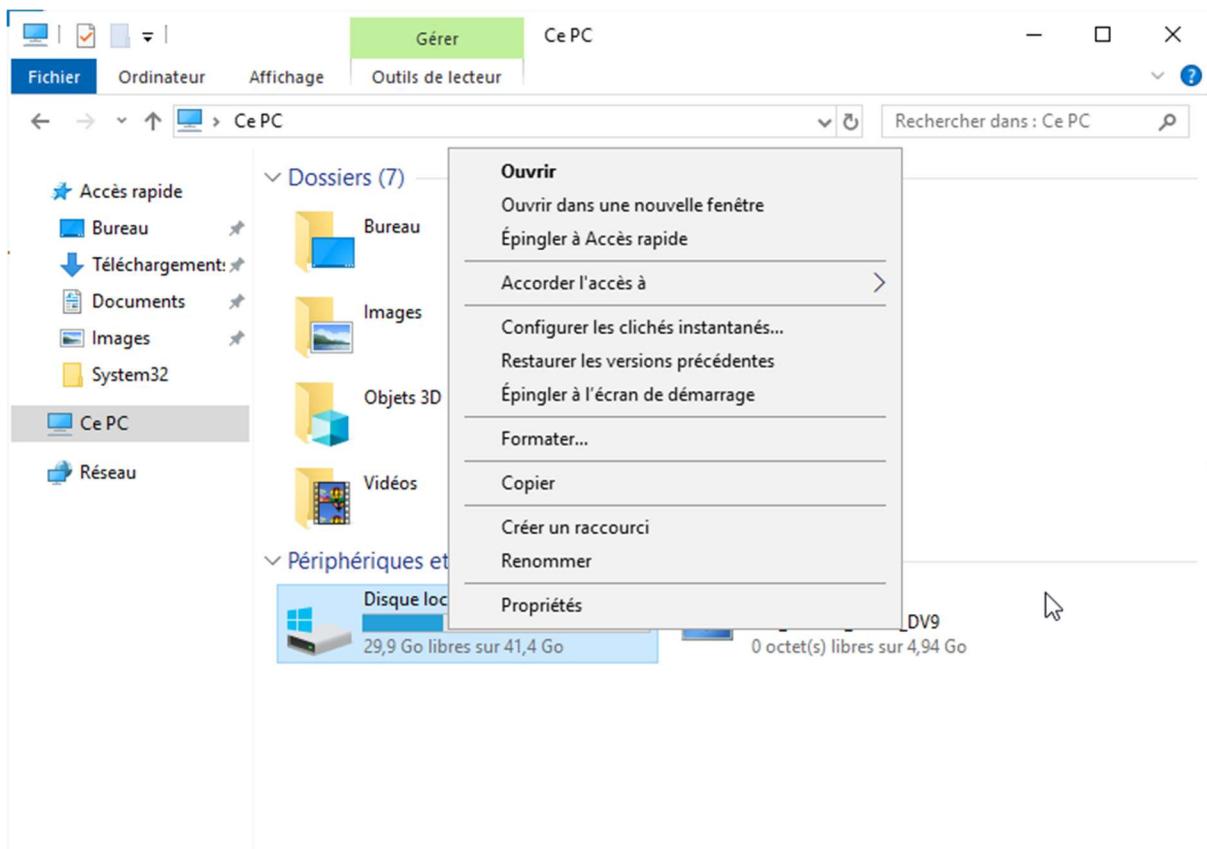
Users			
Username	UID	Builtin	Full Name
paul	1000	no	Paul
SID: 1002			
Home directory: /mnt/Save/USERS/paul			
Shell: /bin/sh			
Mail: N/A			
Password Disabled: false			
Lock User: false			
Permit Sudo: false			
Microsoft Account: false			
Samba Authentication: true			
Username	UID	Builtin	Full Name
paul	1000	no	Paul
pierre	1001	no	Pierre
root	0	yes	root

c) Activation des clichés instantanés

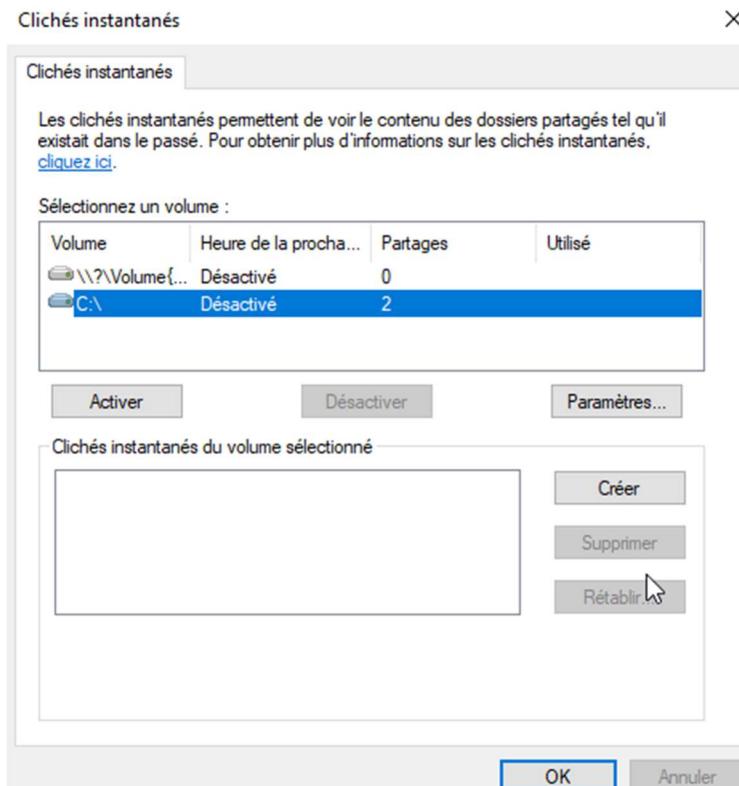
- Ouvrir l'explorateur Windows, faire un clic droit sur la partition où les clichés instantanés sont à activer



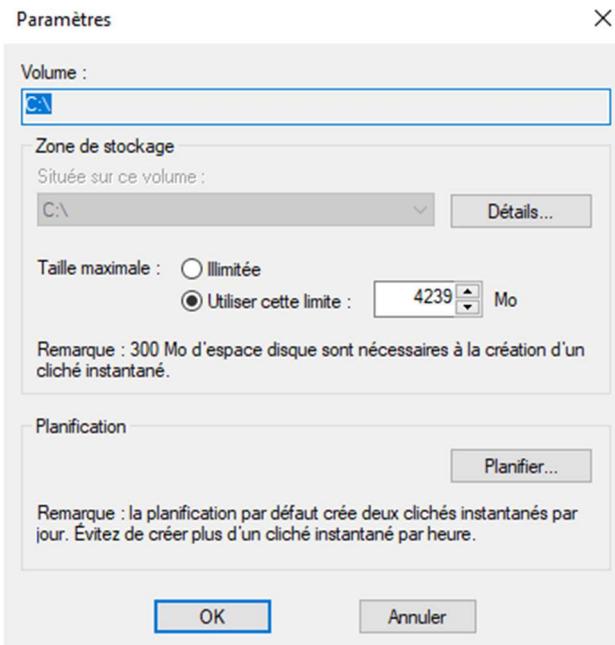
Et cliquer sur Configurer les clichés instantanés.



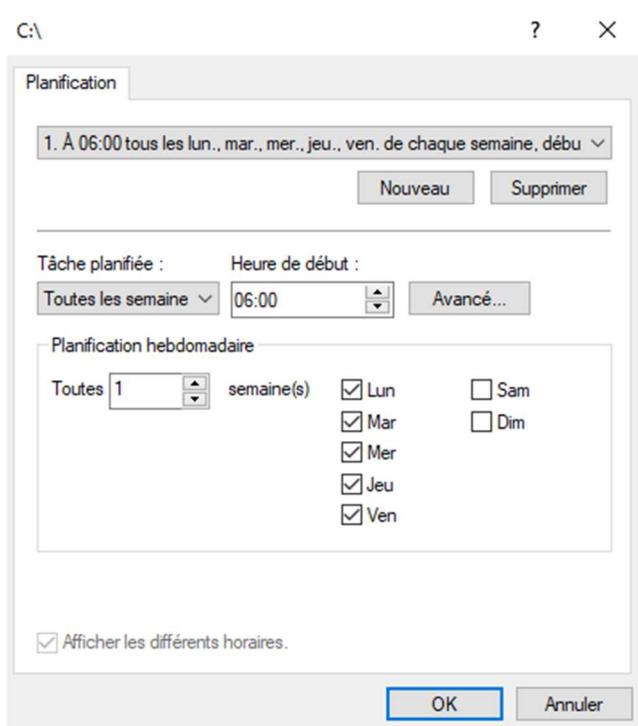
2. Avant d'activer les clichés instantanés, cliquer sur Paramètres



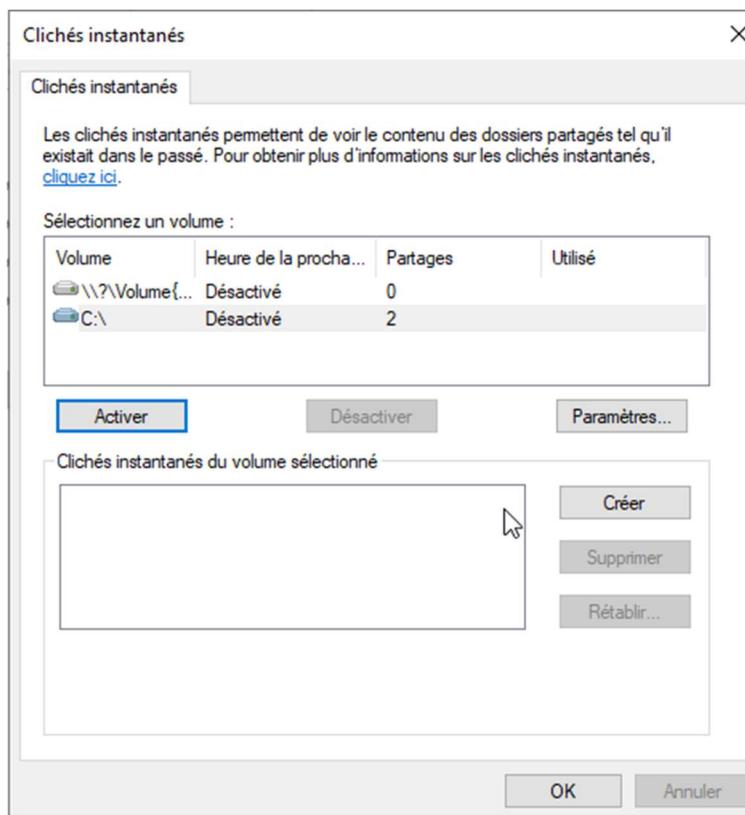
3. D'ici, il est possible de configurer l'espace alloué aux clichés instantanés (plus l'espace est grand, plus il y aura de point de restauration). Il est aussi possible de gérer la planification, cliquer sur le bouton Planifier



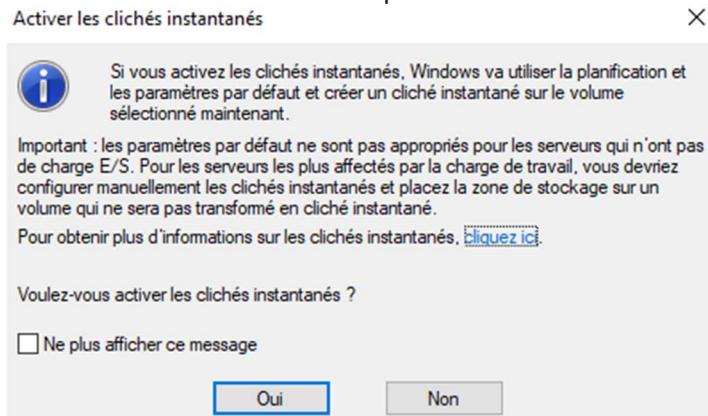
4. Par défaut, il y a deux clichés de configurer à 7H et 12H, le LMMJV



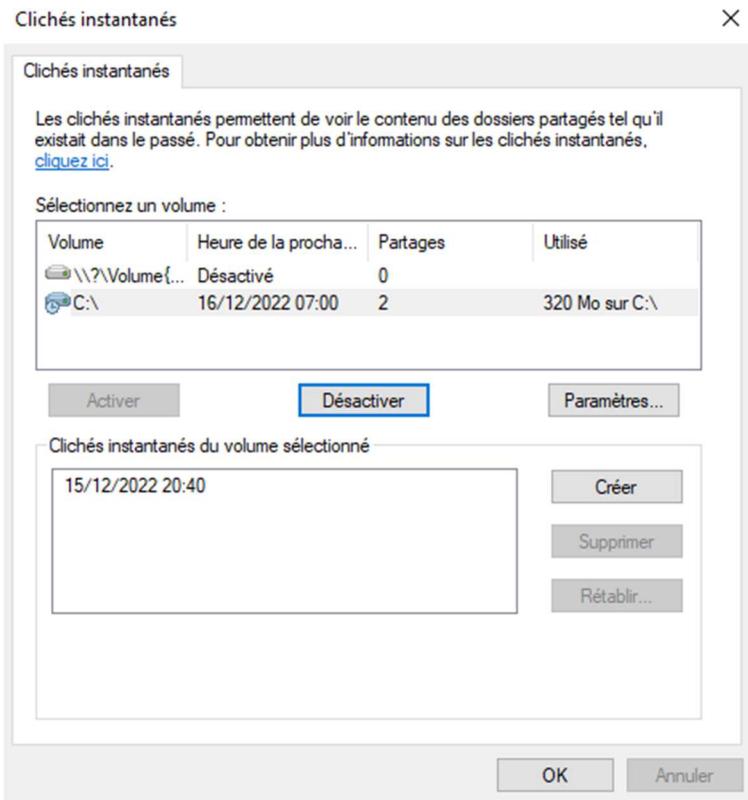
6. Maintenant que les clichés sont paramétrés, cliquer sur Activer



7. Confirmer l'activation en cliquant sur Oui



8. Les clichés instantanés sont maintenant activés, un premier cliché est fait lors de l'activation.

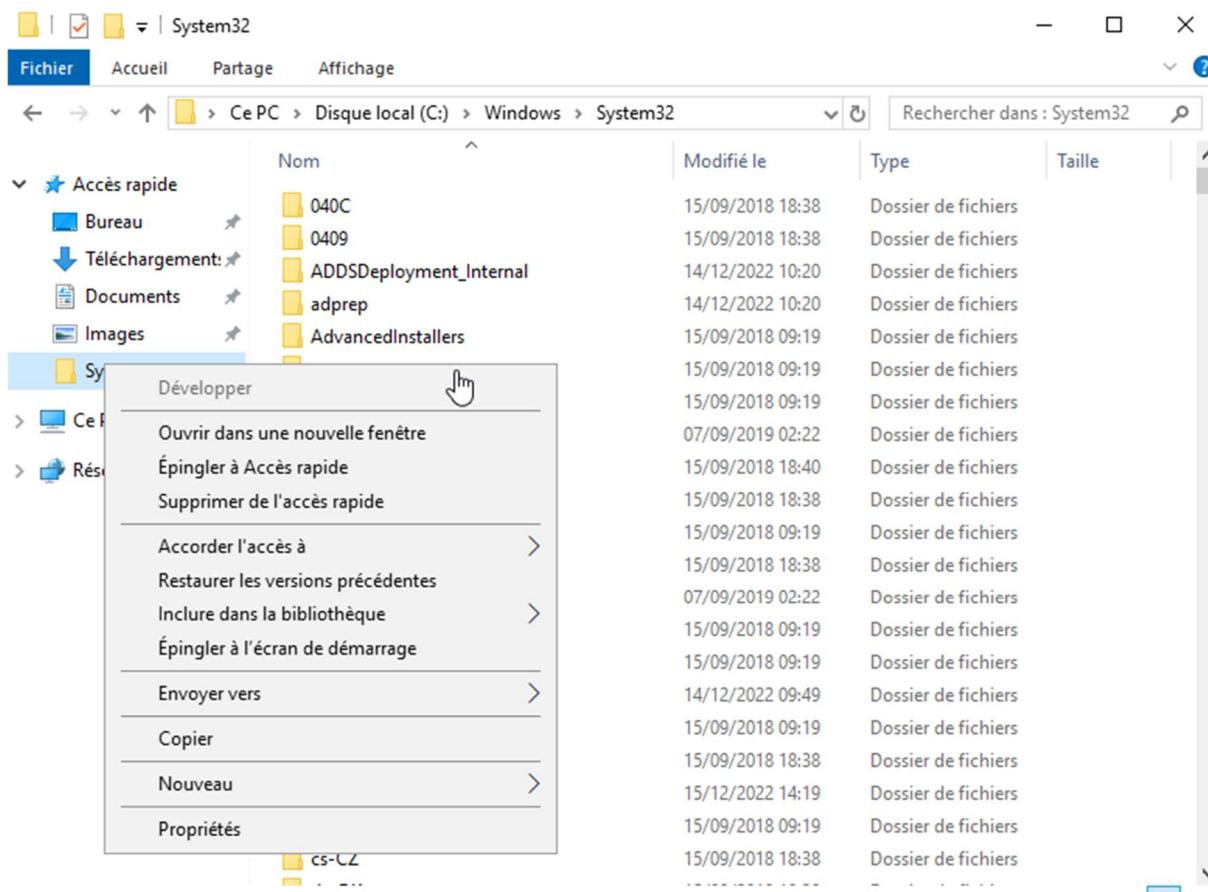


d) Utilisation des versions précédentes

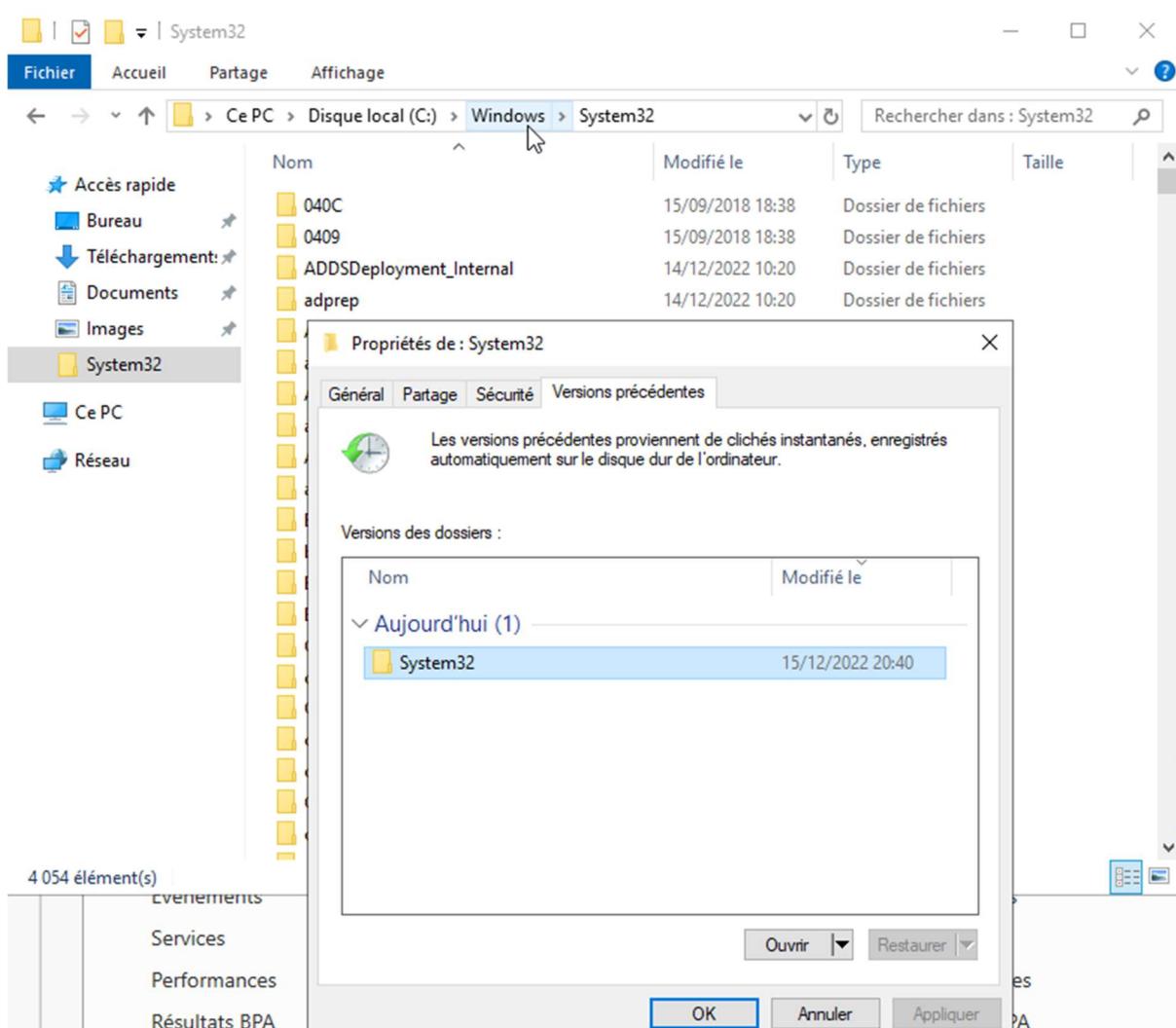
L'accès aux versions précédentes est disponible à l'aide de l'Explorateur Windows sur les clients (W7/8/10) et sur les Serveur (2008/2012/2016/2019...). Elles sont disponibles aussi bien locale que par les partages réseaux et par défaut sont accessibles à tout le monde.

1. Depuis l'explorateur Windows, aller sur le dossier où l'on souhaite restaurer le fichier et faire un clic droit dessus. En fonction de l'emplacement et du système deux options sont disponibles, cliquer sur :

- Restaurer les versions précédentes
- Propriétés



2. Si l'on passe par Propriétés, aller sur l'onglet Versions précédentes. Choisir le point de restauration à explorer et cliquer sur Ouvrir.



Nos clichés instantanés sont maintenant en place et opérationnelle.

Fin de Procédure