Réalisation Technique

Infrastructure Active Directory et Services Associés

Sommaire

SOMMAIRE

Présentation

Active Directory est un service annuaire LDAP mis en place par Microsoft pour les machines Windows Serveur. Il permet d'administrer des ressources telles que les ordinateurs, des dossiers de partages, mais aussi des comptes utilisateurs par l'intermédiaire d'un système d'Identification/Authentification. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

Contexte du projet Stadium

Le projet 'Stadium' vise à refondre totalement l'infrastructure réseau d'un grand complexe sportif. Ce site accueille des événements sportifs et culturels majeurs et s'étend sur plusieurs bâtiments et sites distants. Le réseau existant, devenu obsolète et désorganisé avec le temps, ne permet plus de garantir des services performants, ni de répondre aux exigences de sécurité ou de modernisation. D'après le cahier des charges, la société NetworkingCompany a été mandatée pour concevoir, mettre en œuvre et sécuriser un réseau complet et évolutif réparti sur 3 sites (stade, billetterie, boutique), avec segmentation VLAN, haute disponibilité et administration centralisée via Active Directory.

Installation d'Active Directory, du DNS et du DHCP

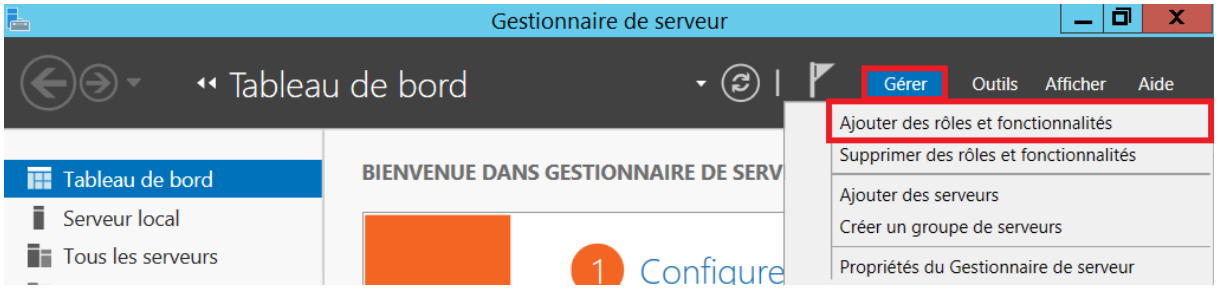
Prérequis

- Changer le nom de la machine en « Hermes »
- Mettre une adresse IP statique

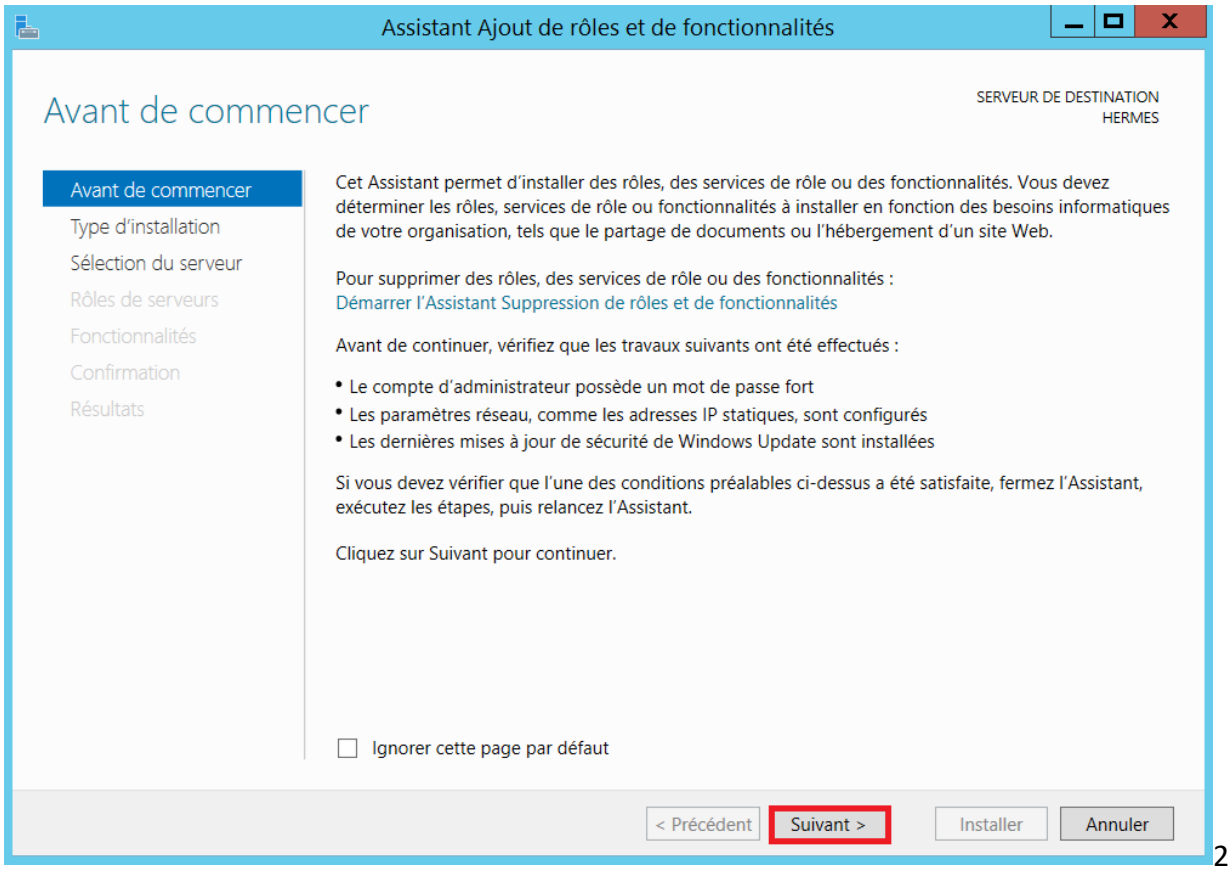
Nom M2achine : Hermes
Rôles : Active Directory
Adresse IP : 172.20.1.2
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 172.20.1.1
Serveur DNS préféré : 172.20.1.10

Installation des rôles AD, DNS, DHCP

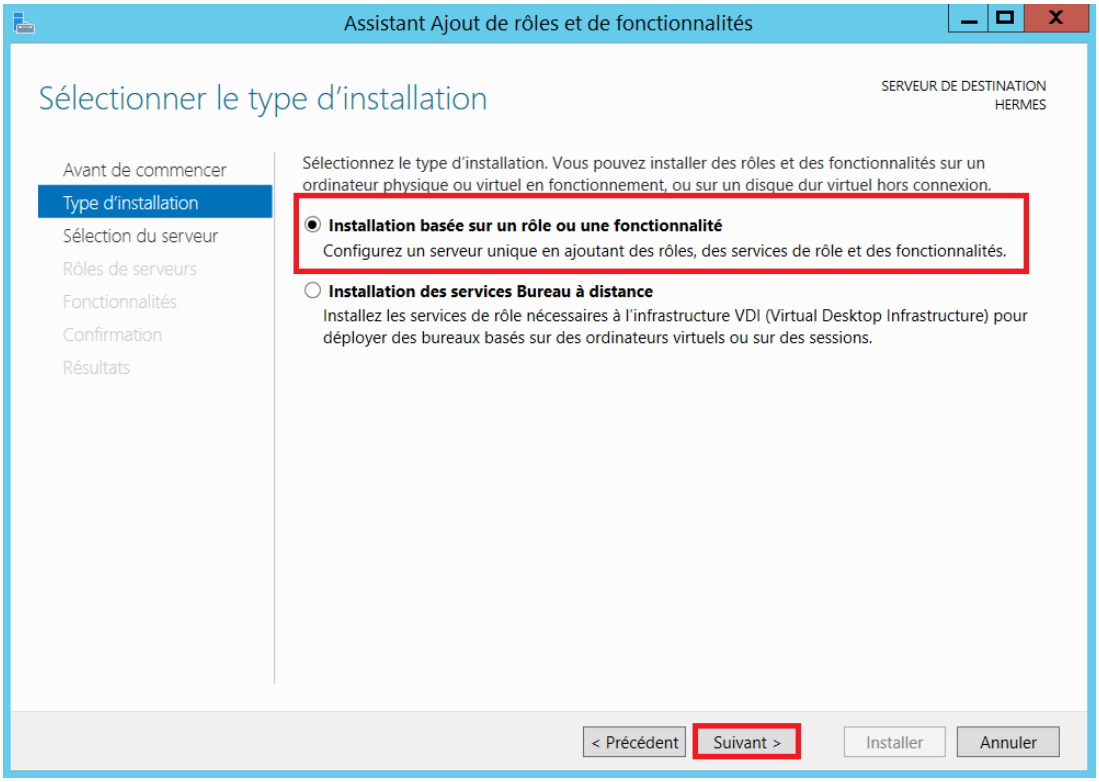
- Depuis le Gestionnaire de serveur, cliquer sur **gérer** puis «**Ajouter des rôles et des fonctionnalités**»



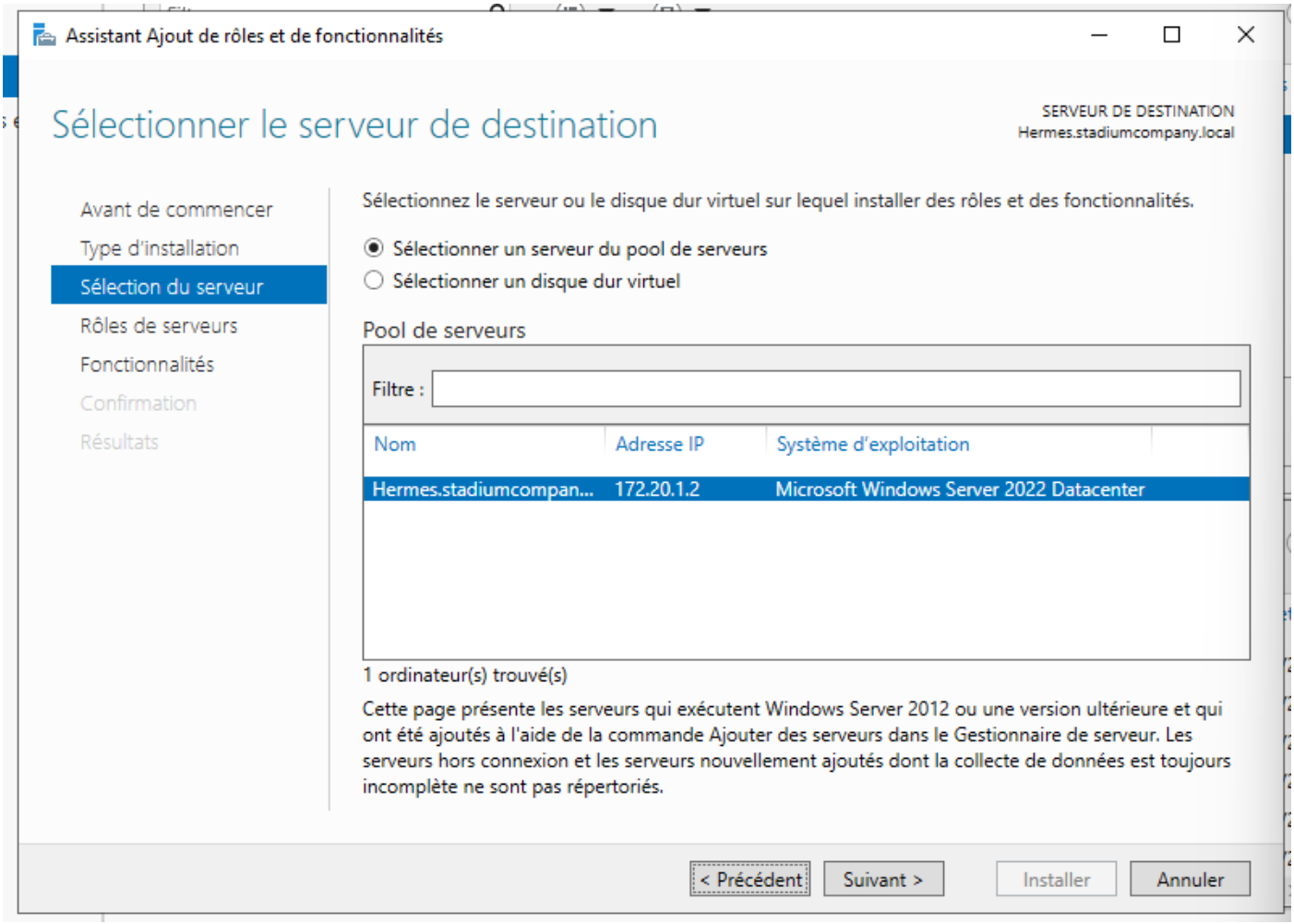
- Sur l'Assistant Ajout de rôles et de fonctionnalités, passer l'introduction avec **suivant**.


Assistant Ajout de rôles et de fonctionnalités
Avant de commencer
SERVEUR DE DESTINATION
HERMES
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 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
2

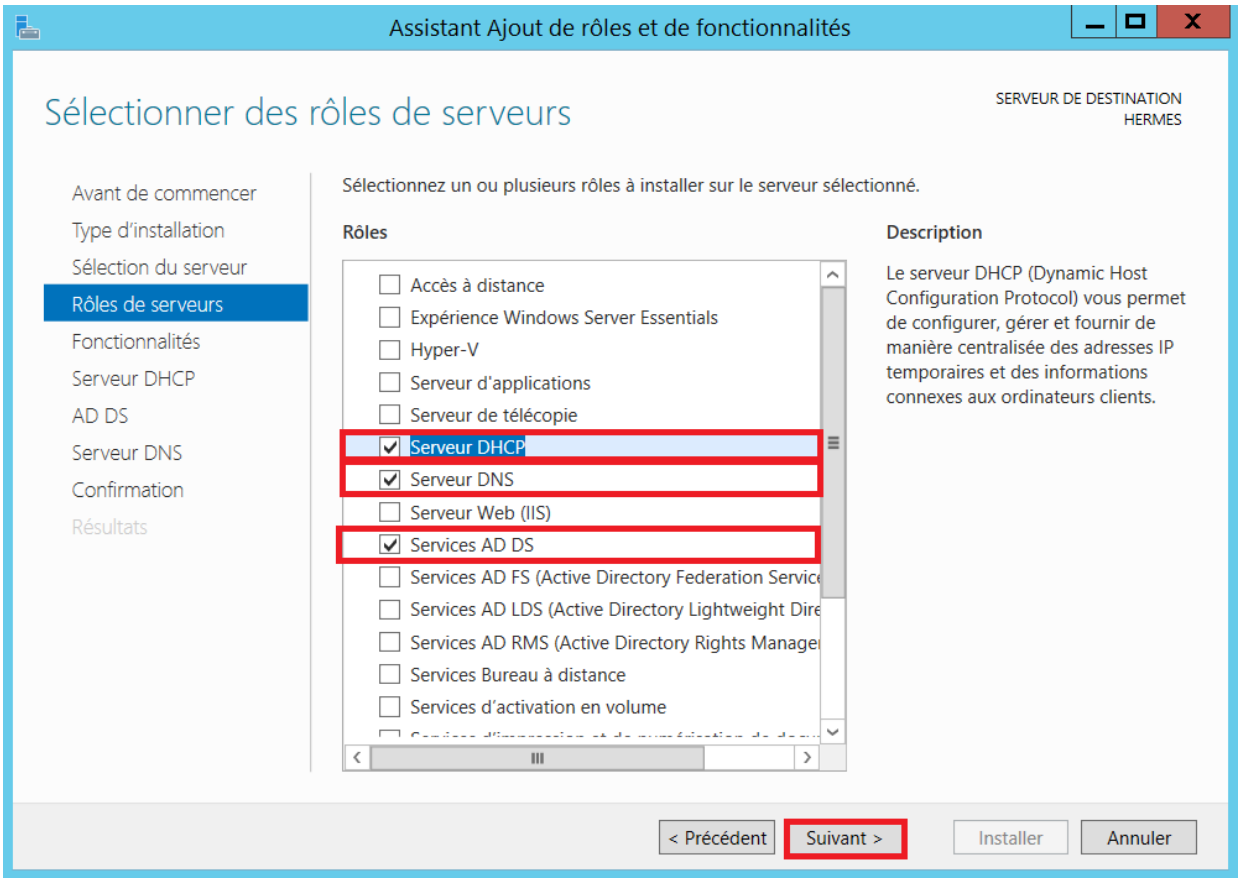
- Sélectionné le type **d'installation basée sur un rôle ou une fonctionnalité.**



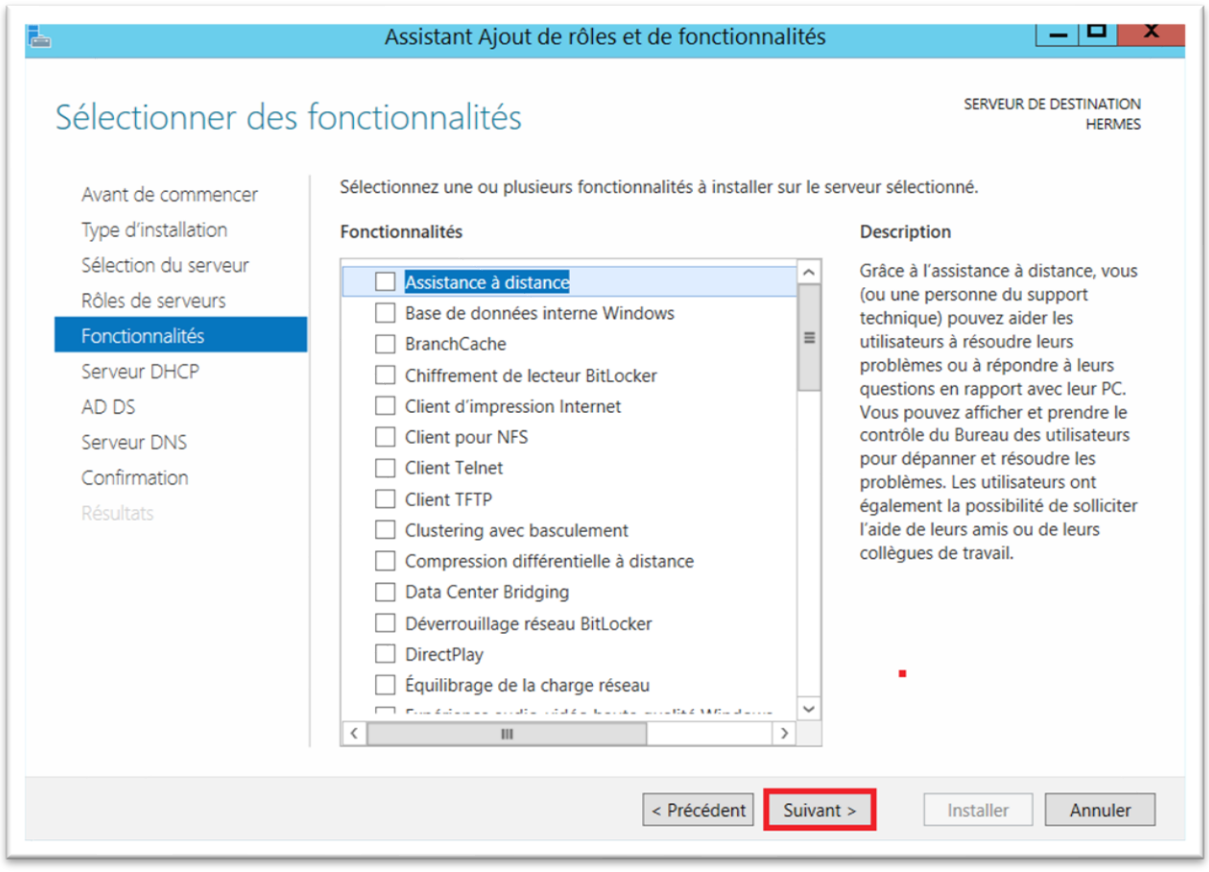
- **Sélectionner son serveur pool** pour installer les rôles et suivant.



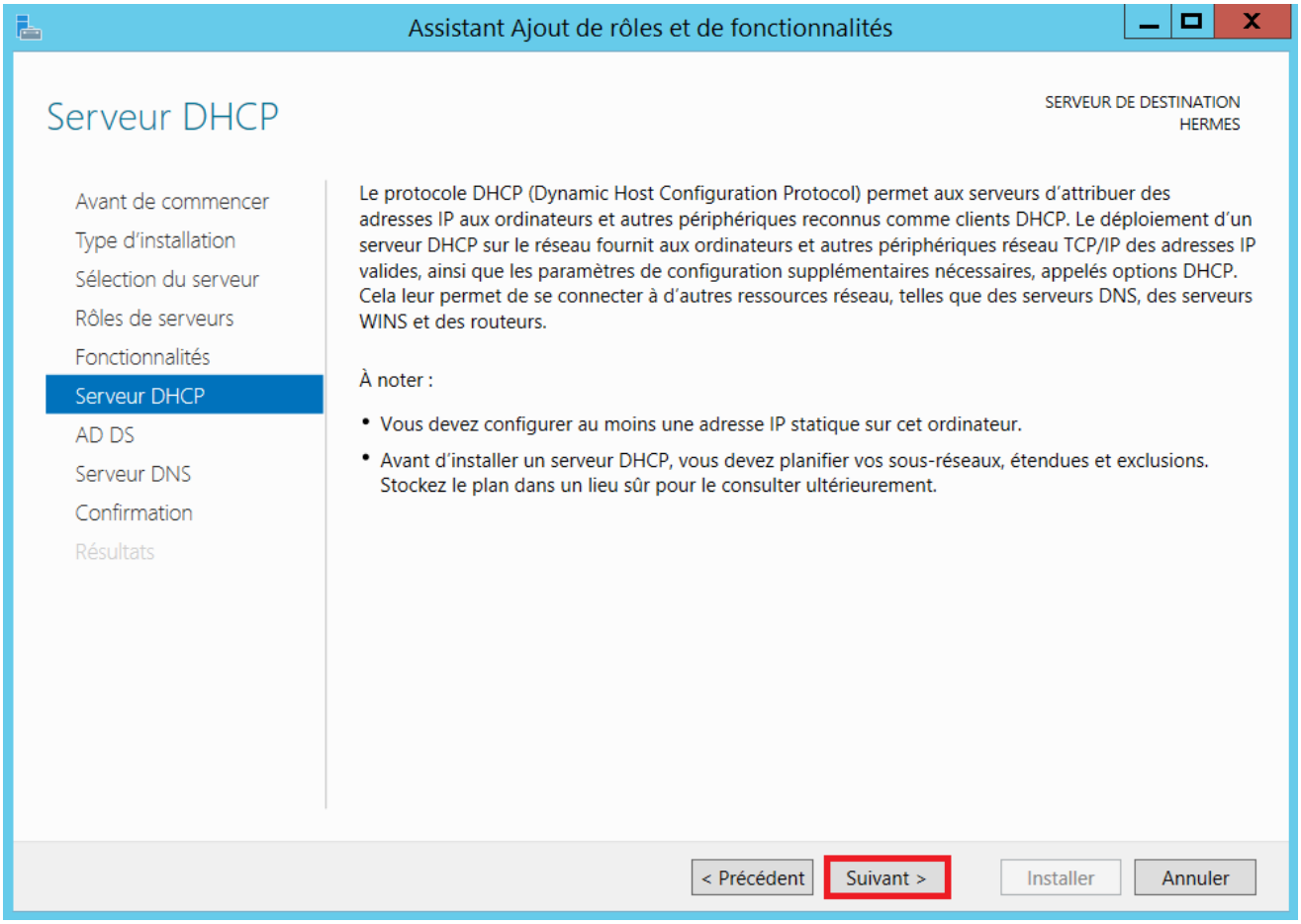
- Sélectionner les rôles **DHCP, DNS et AD DS**, puis suivant.



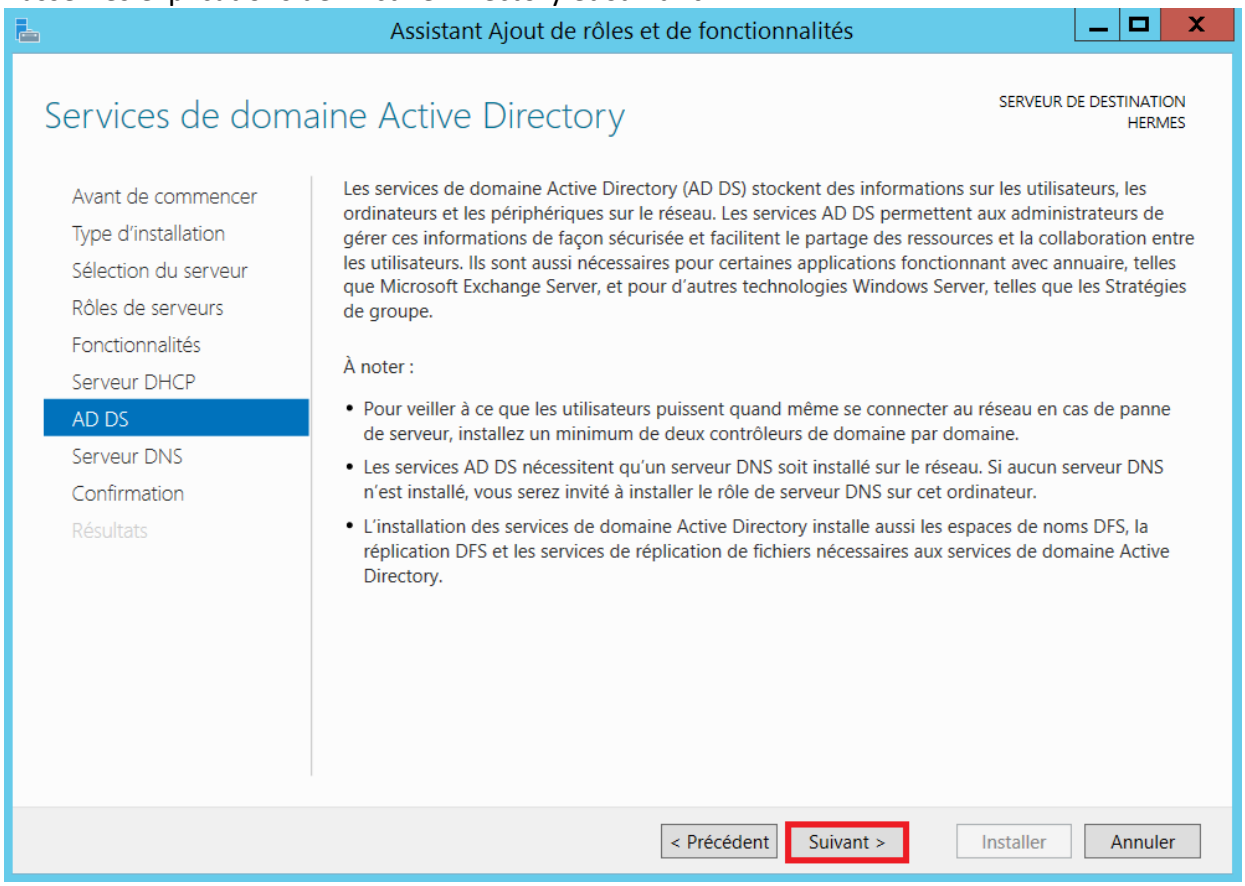
- Ne pas **sélectionner de fonctionnalités** et suivant.



Passer les explications du DHCP et **suivant**.

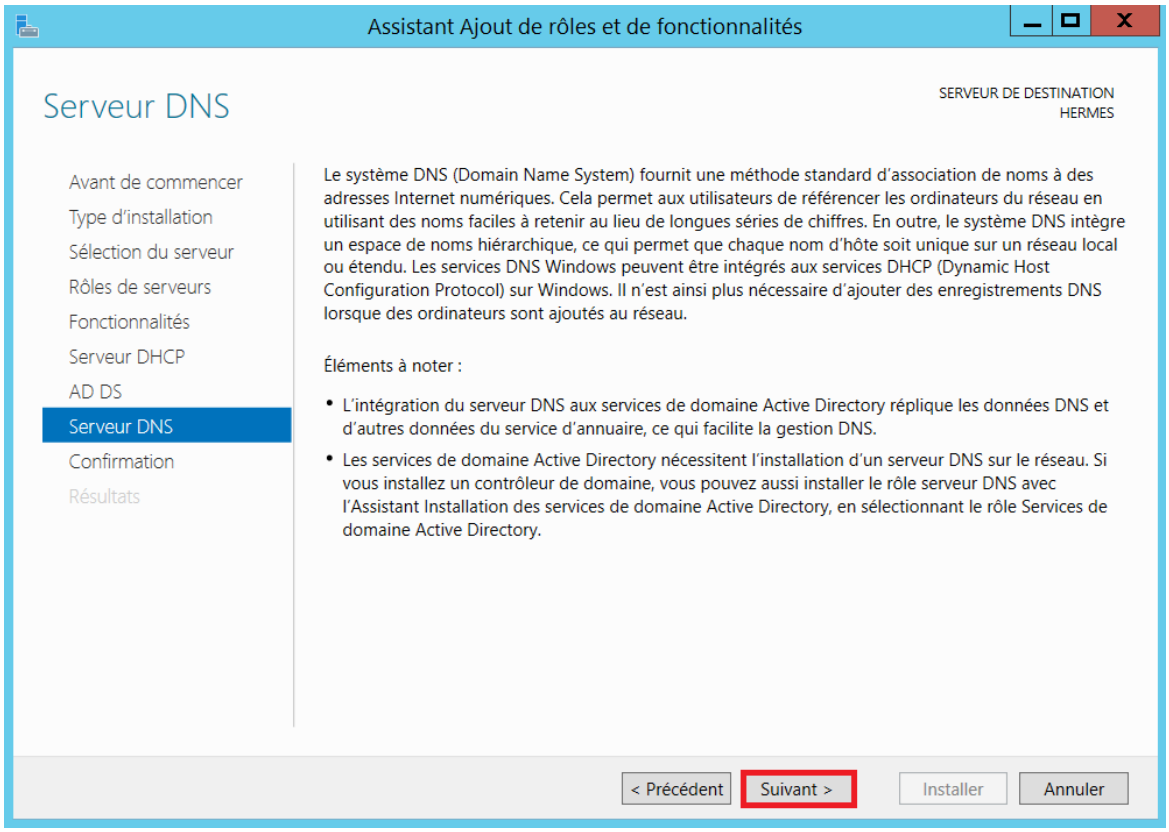


- Passer les explications de l'Active Directory et **suivant**.

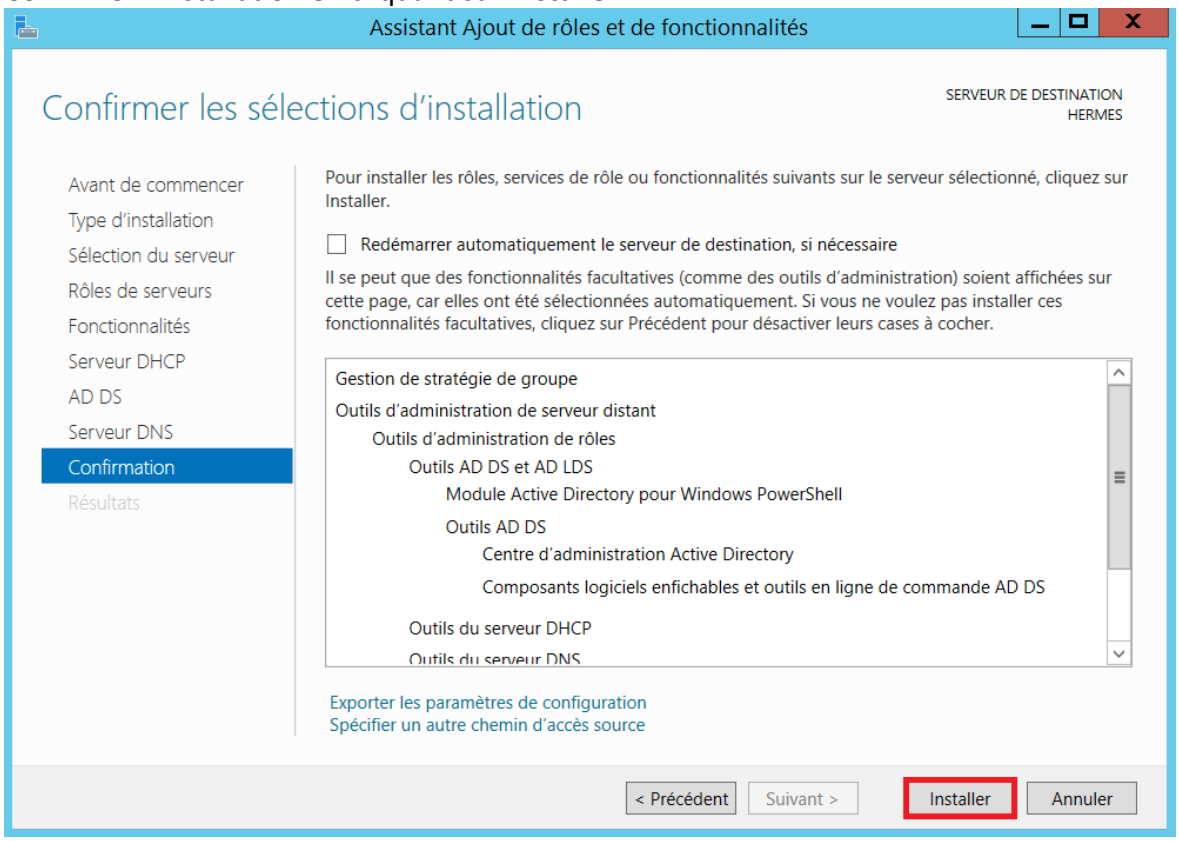


- Passer les explications du DNS et **suivant**.

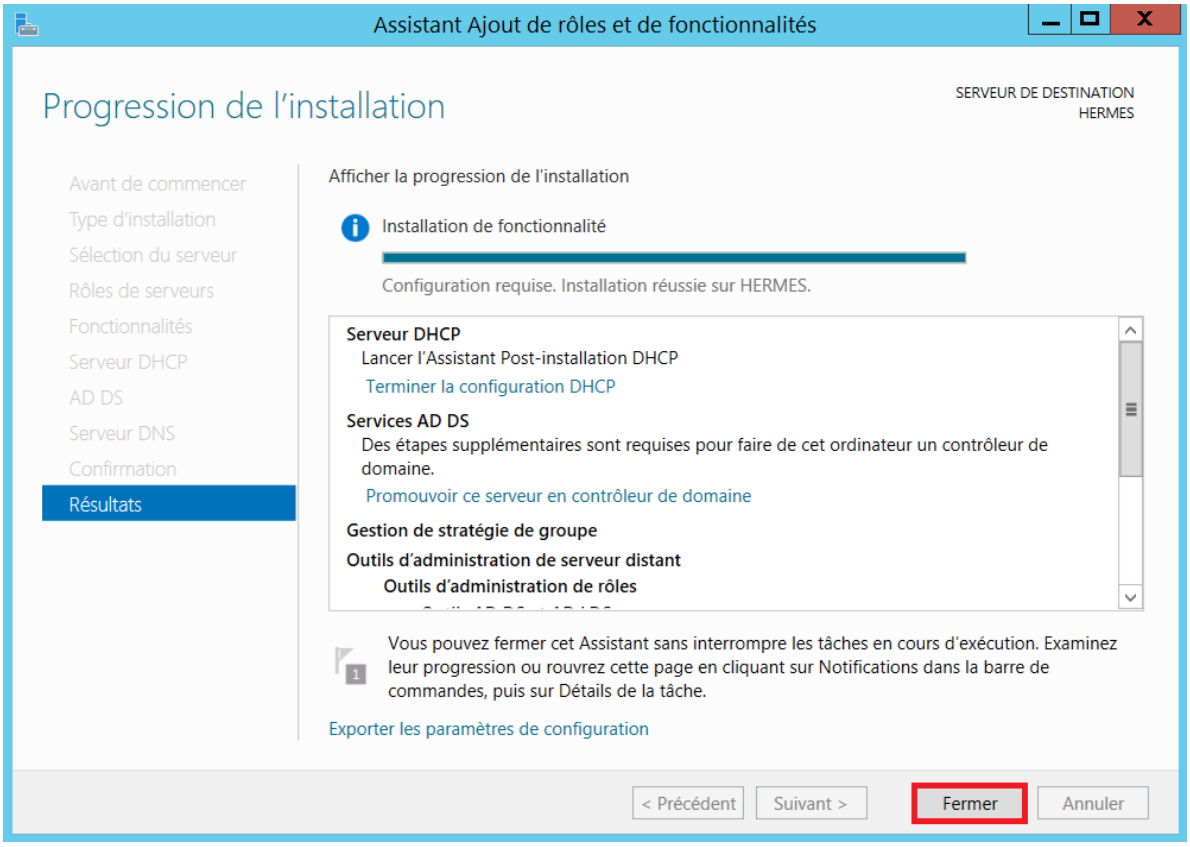
2



- Confirmer l'installation en cliquant sur **installer**.



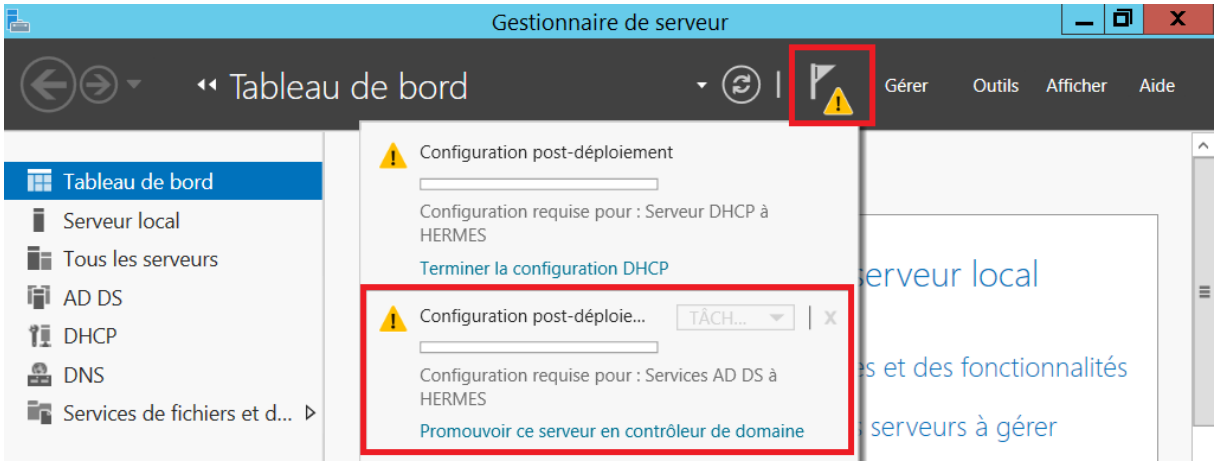
- **Fermer** la fenêtre d'Assistant Ajout de rôles et de fonctionnalités.



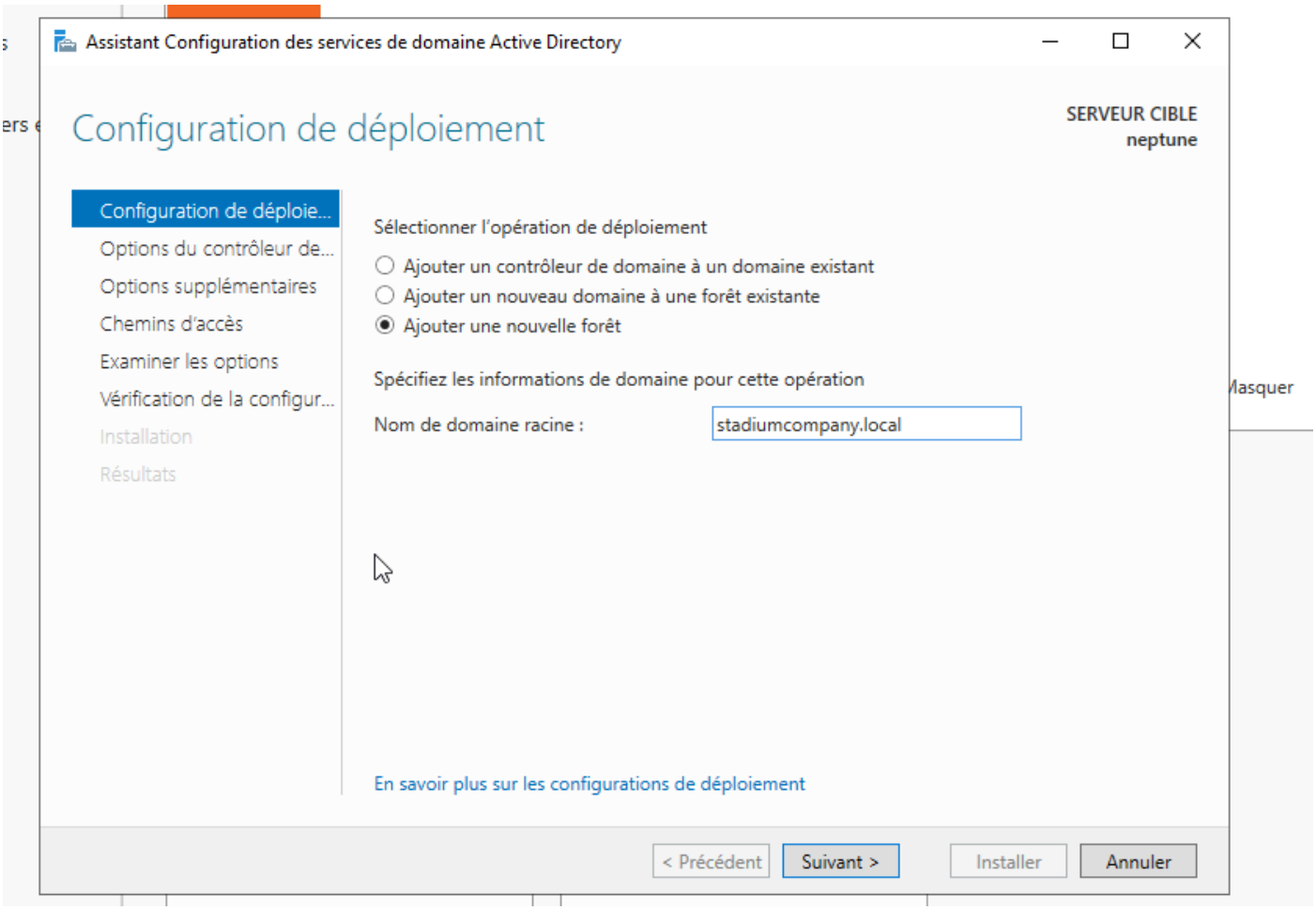
Configuration de l'Active Directory

Création du domaine

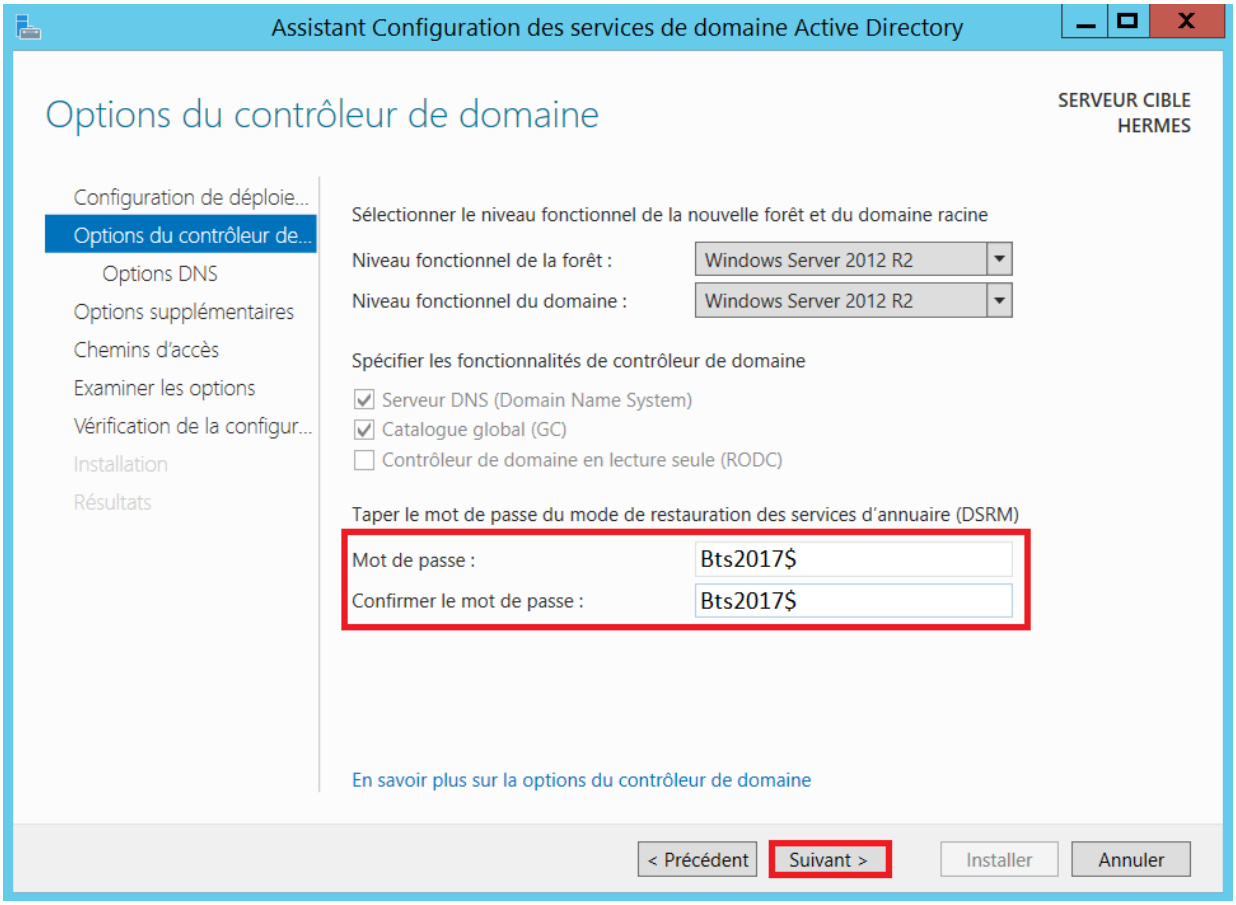
- Sur le gestionnaire de serveur, **Cliquer sur le drapeau**, puis **cliquer sur « Promouvoir ce serveur en contrôleur de domaine »**.



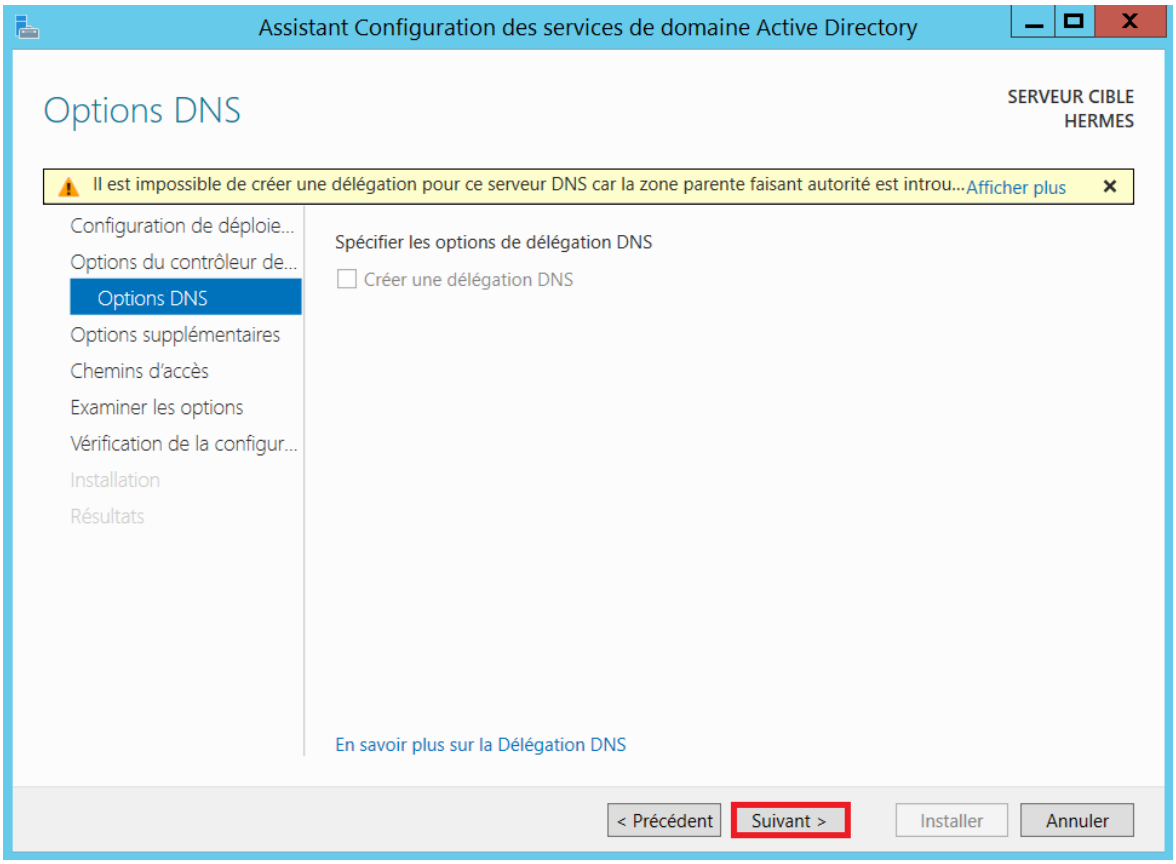
- **Ajouter une nouvelle forêt**, le nom de domaine est stadiumcompany.local.2



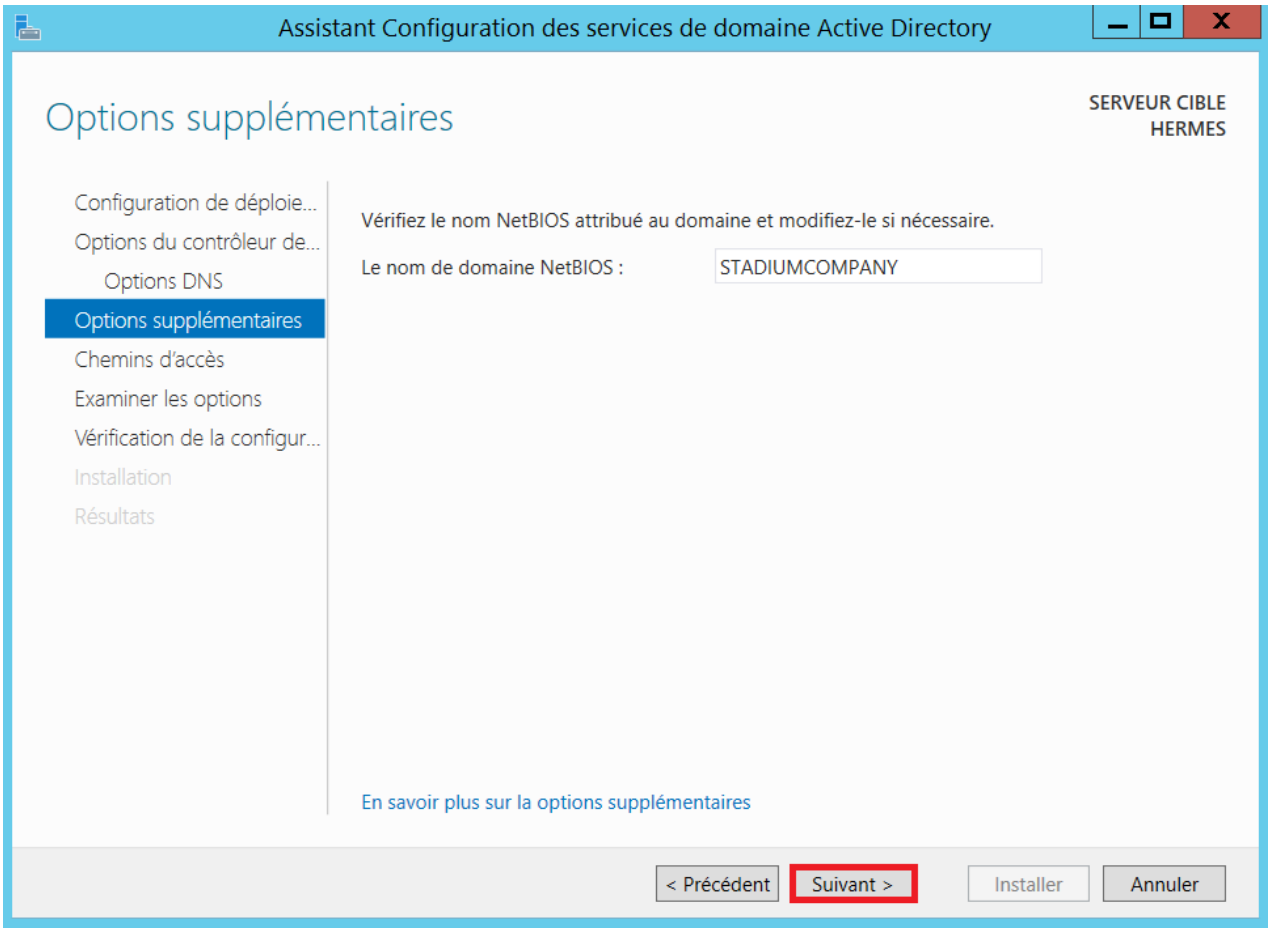
- Informer le mot de passe du domaine. Le mot de passe sera : **Bts2017$**



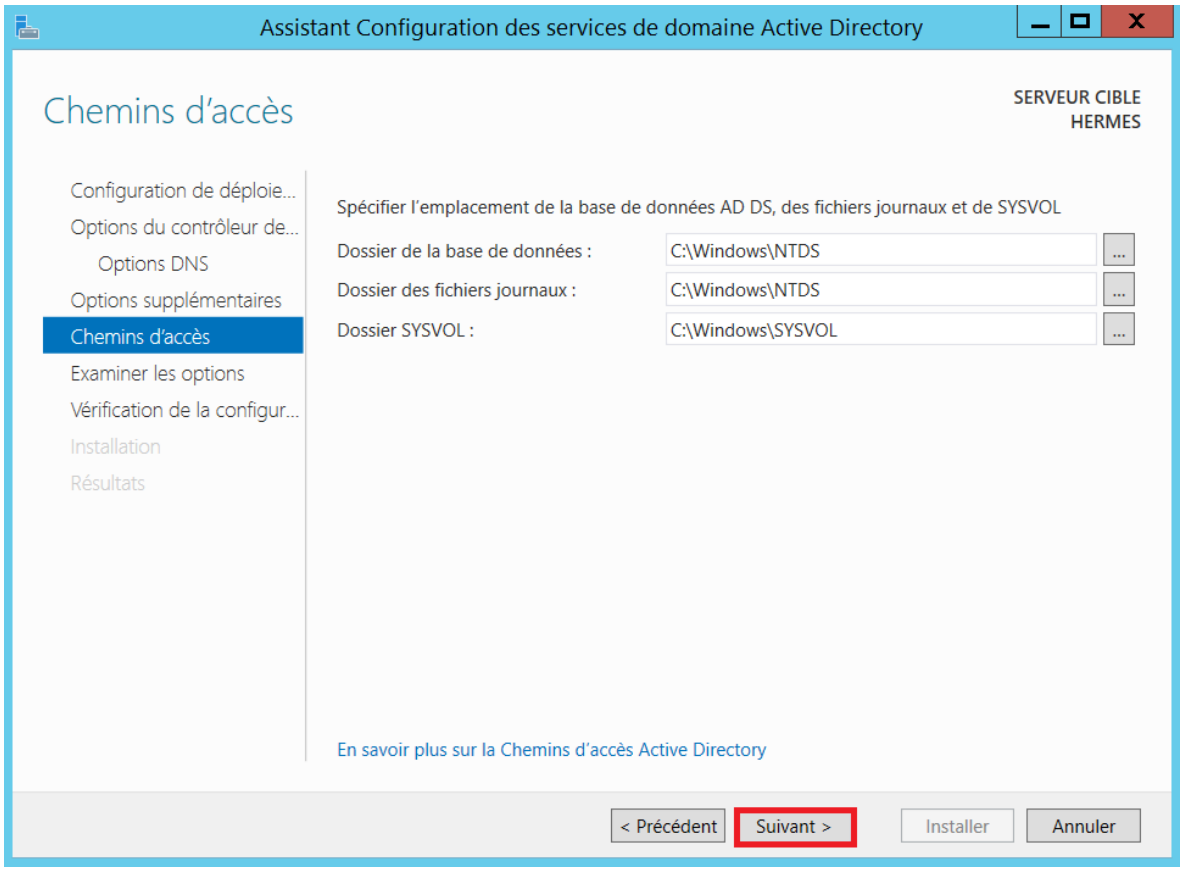
- Passer l'option DNS car le rôle a déjà été installer, faire **suivant**.


Assistant Configuration des services de domaine Active Directory
Options DNS
SERVEUR CIBLE
HERMES
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introu...
Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier les options de délégation DNS
Créer une délégation DNS
En savoir plus sur la Délégation DNS
< Précédent
Suivant >
Installer
Annuler

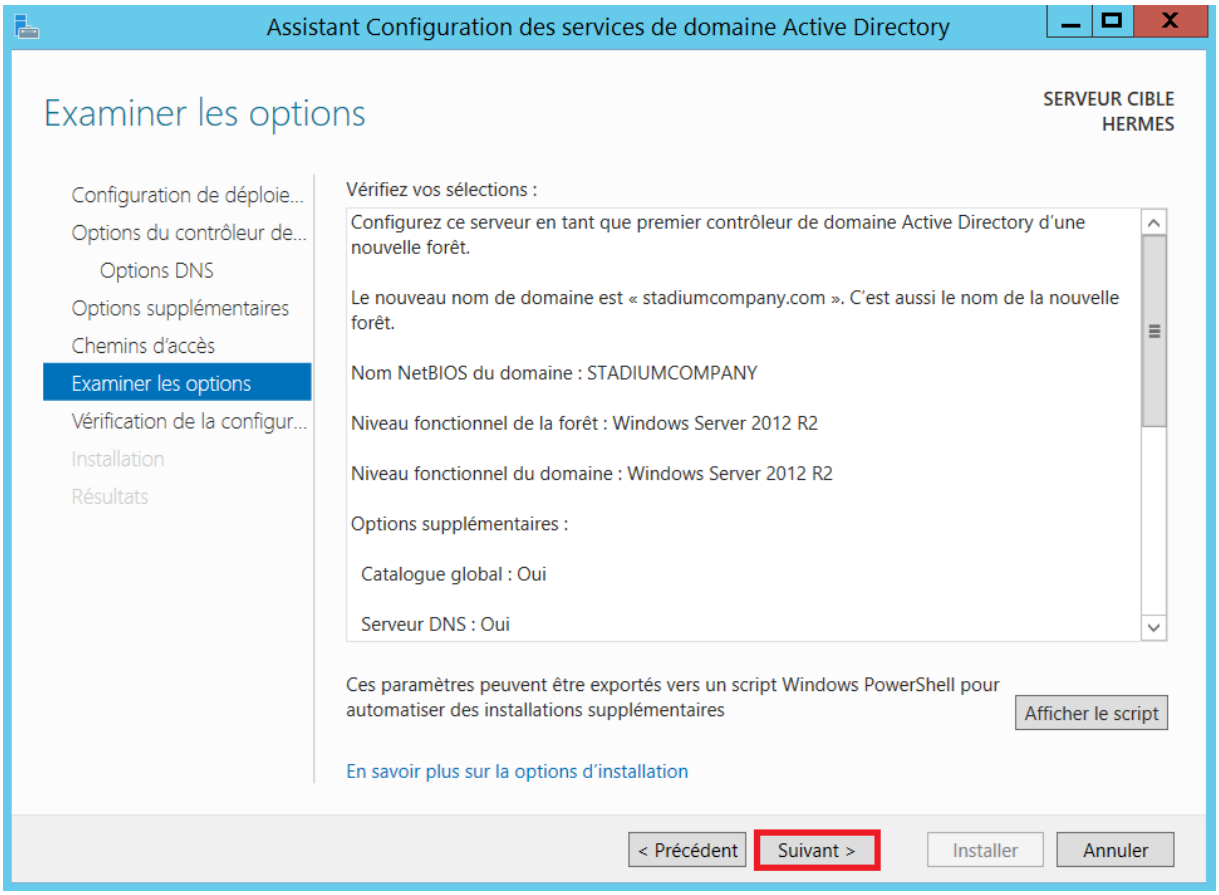
- Confirmer le nom NetBIOS, faire **suivant**.



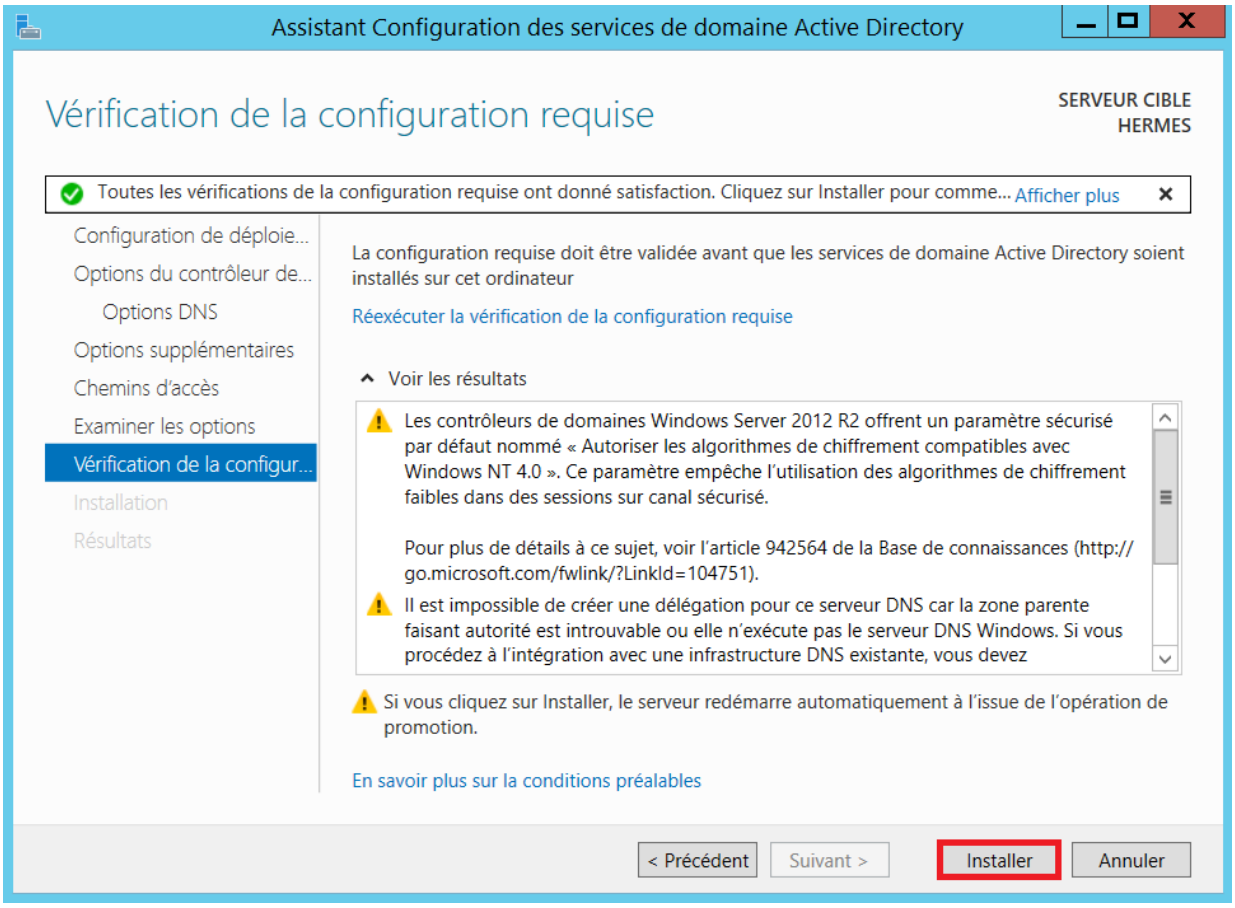
- Garder le chemin d'accès par défauts, faire **suivant**.



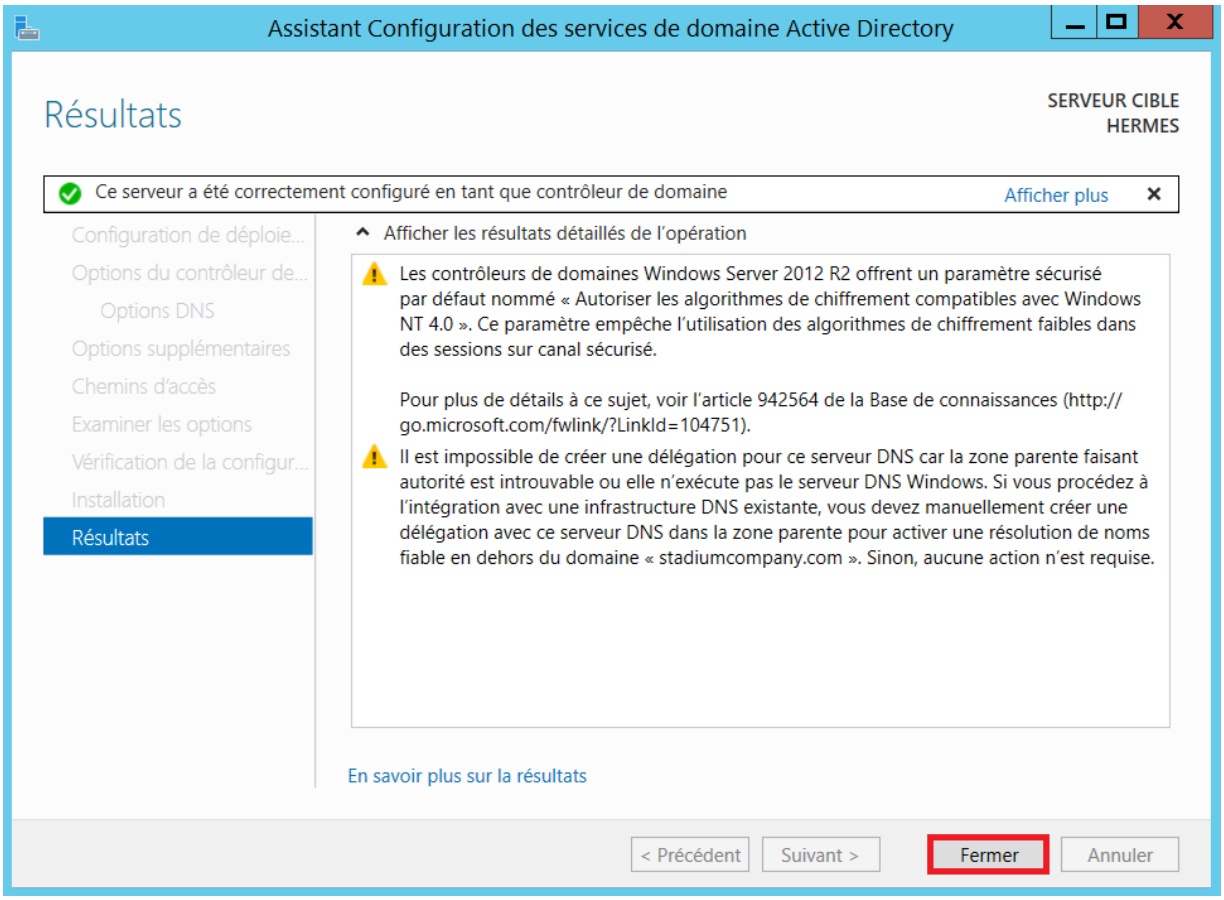
- Conf:Airmer la sélection, faire **suivant**.



- Lancer l'**installation**.

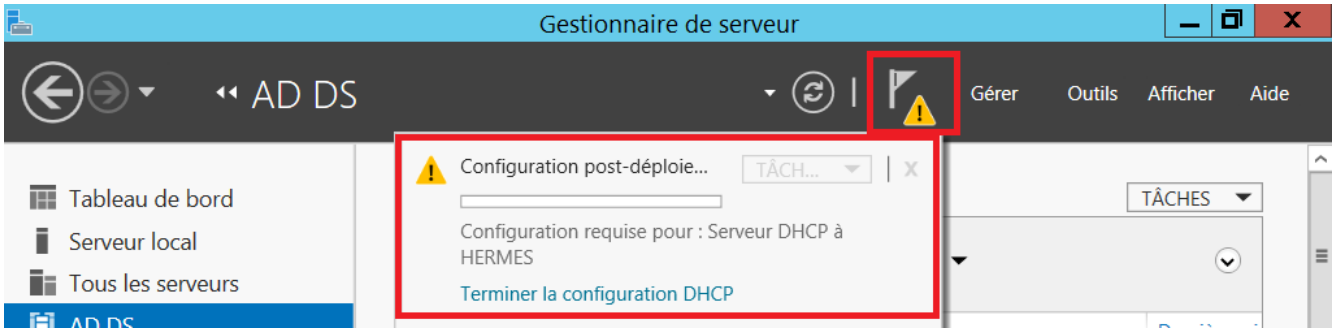


- **Fermer** l'Assistance du domaine Active Directory ce qui redémarre la machine.

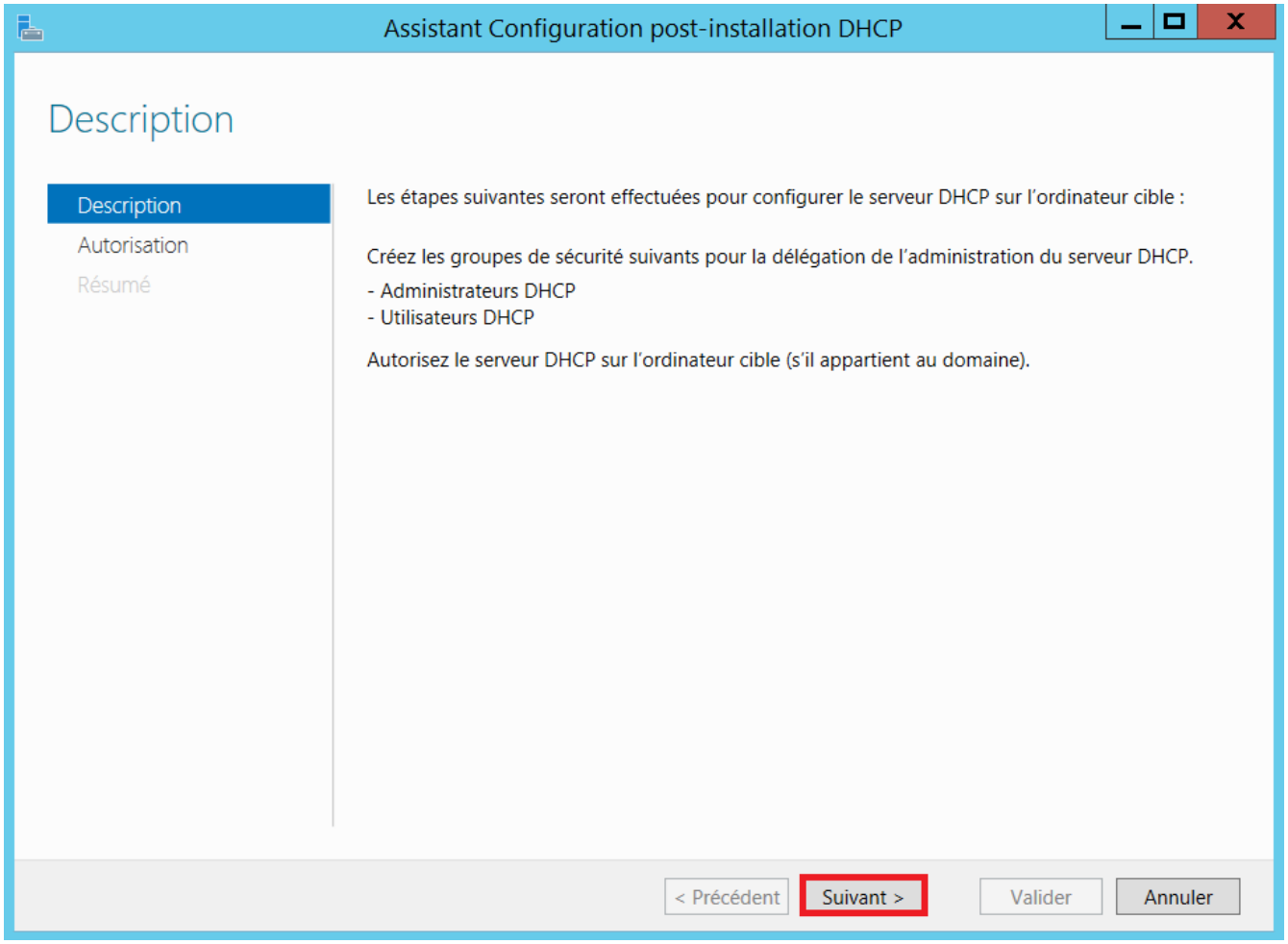


Configuration du DHCP

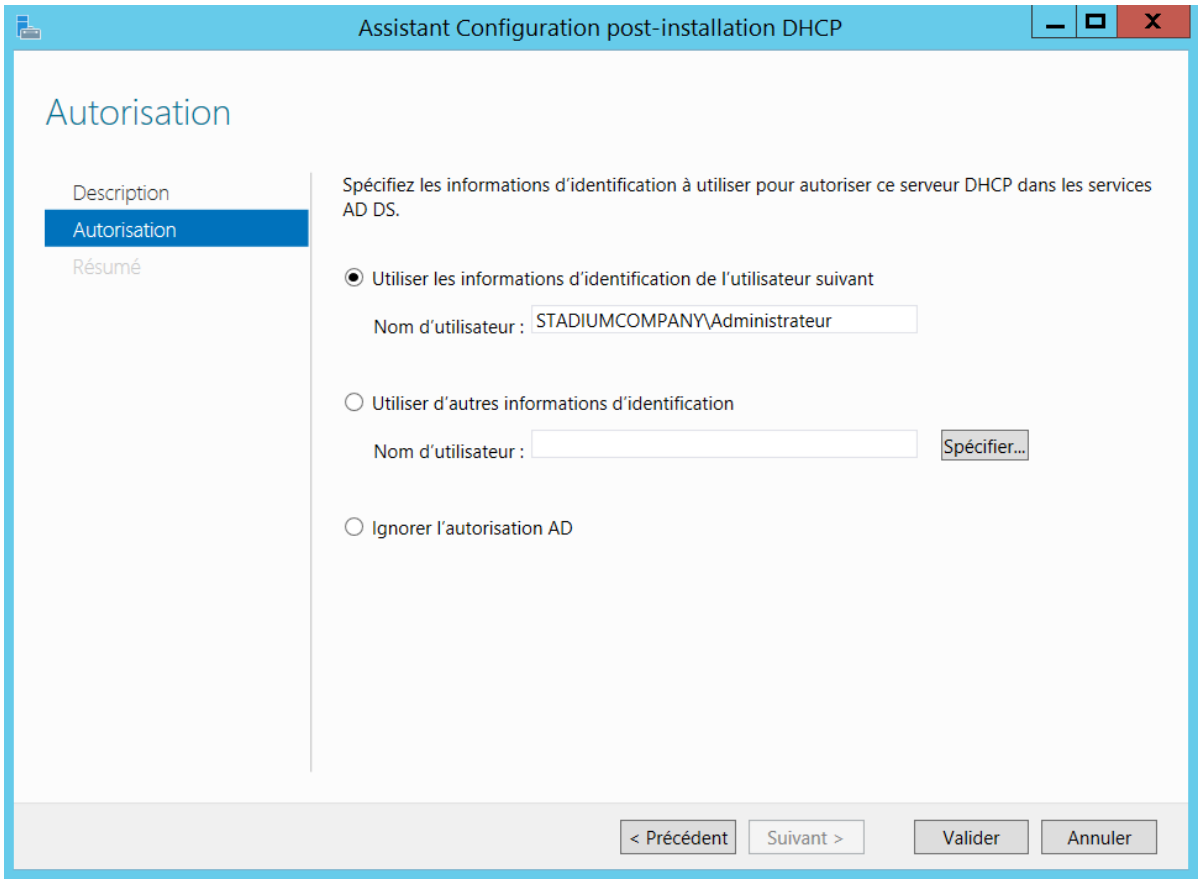
- Sur le gestionnaire de serveur, cliquer sur le drapeau, cliquer sur « Terminer la configuration DHCP ».



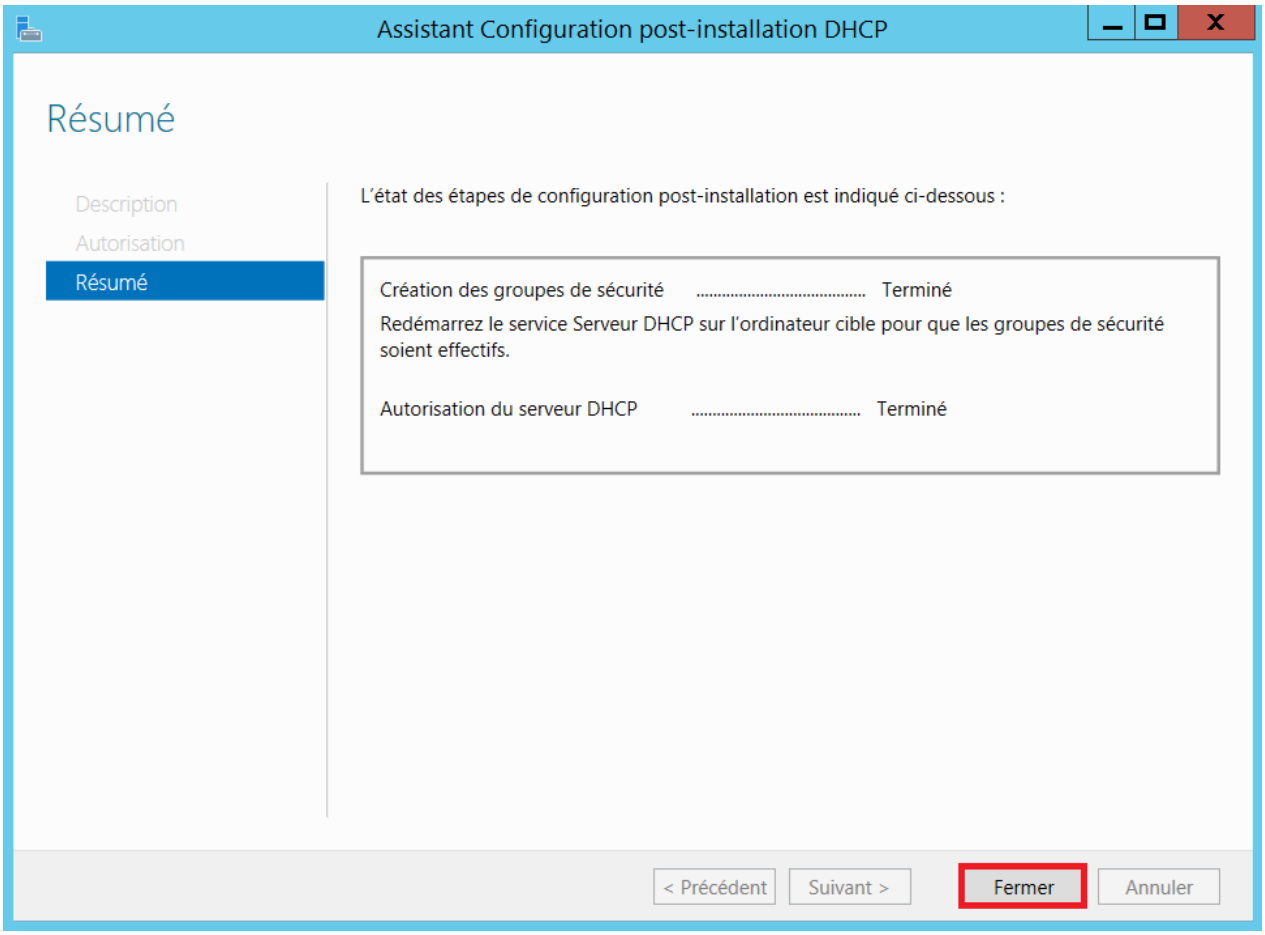
- Passer l'introduction de la configuration du DHCP, faire **suivant**.



- Autorisation de l'installation de configuration avec le compte administrateur de domaine, faire **valider**.

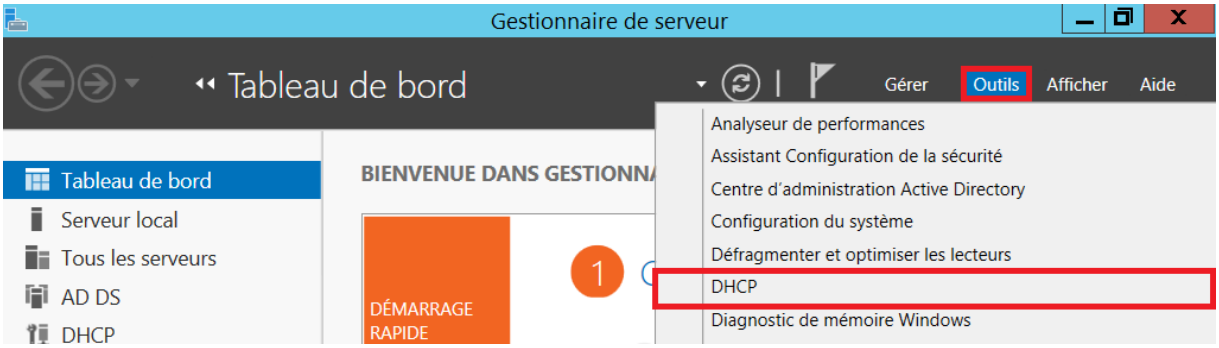


- **Fermer** le résumer de la configuration installer.

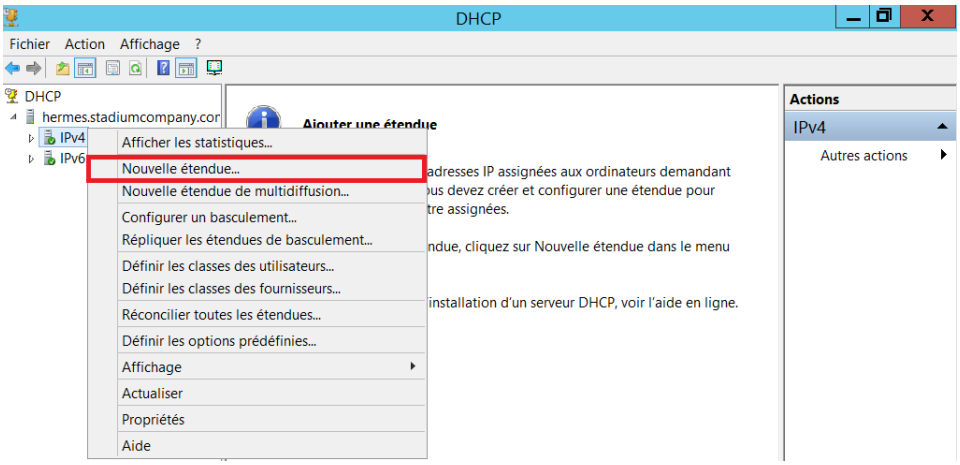


<u>Création des plages d'adresses :</u>

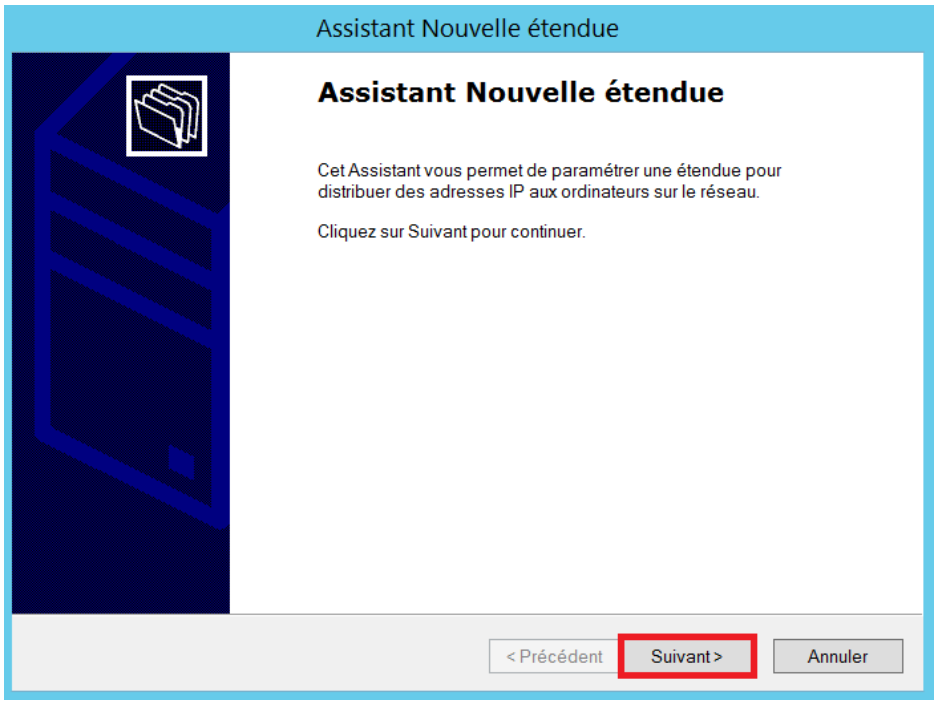
- Gestionnaire de serveur, Outils, **DHCP**.



- DHCP → hermes.stadiumcompany.local → Clic droit IPv4 → **Nouvelle étendue…**



- Passer l'intro d'Assistant Nouvelle étendue, faire **suivant.**



- Renseigner le **nom** et la **description** de la nouvelle étendue, faire **suivant**.

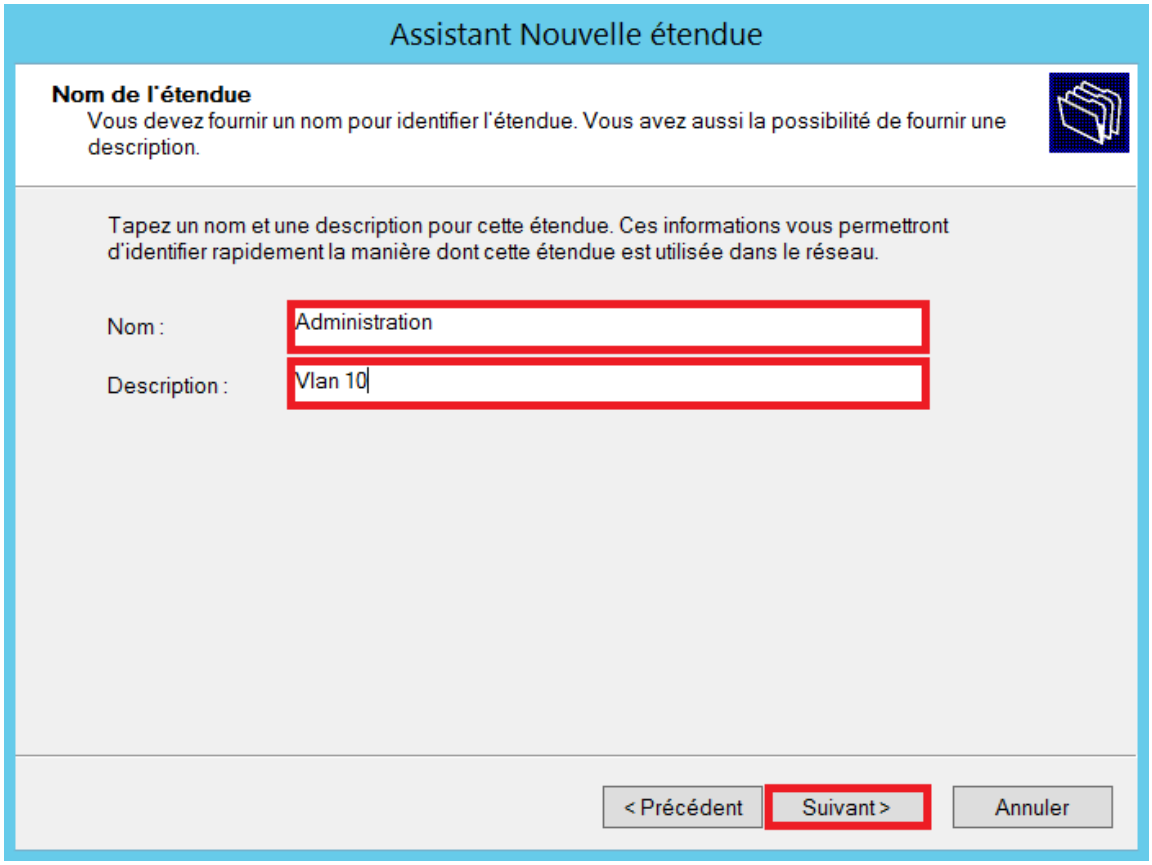


Tableau des noms et détails des étendu stadiumcompany.local bn

	Noms	Descriptions
Étendu 1	Administration	Vlan 10
Étendu 2	Equipes	Vlan 20
Étendu 3	WIFI	Vlan 30
Étendu 4	Camera-IP	Vlan 40
Étendu 5	VIP-Presse	Vlan 50
Étendu 6	Fournisseurs	Vlan 60
Étendu 7	Restaurant	Vlan 70

172.10.0.1

- Indiquer **l'adresse IP de début**, **l'adresse IP de fin**, la **longueur** du **masque et le masque du sous-réseau**.

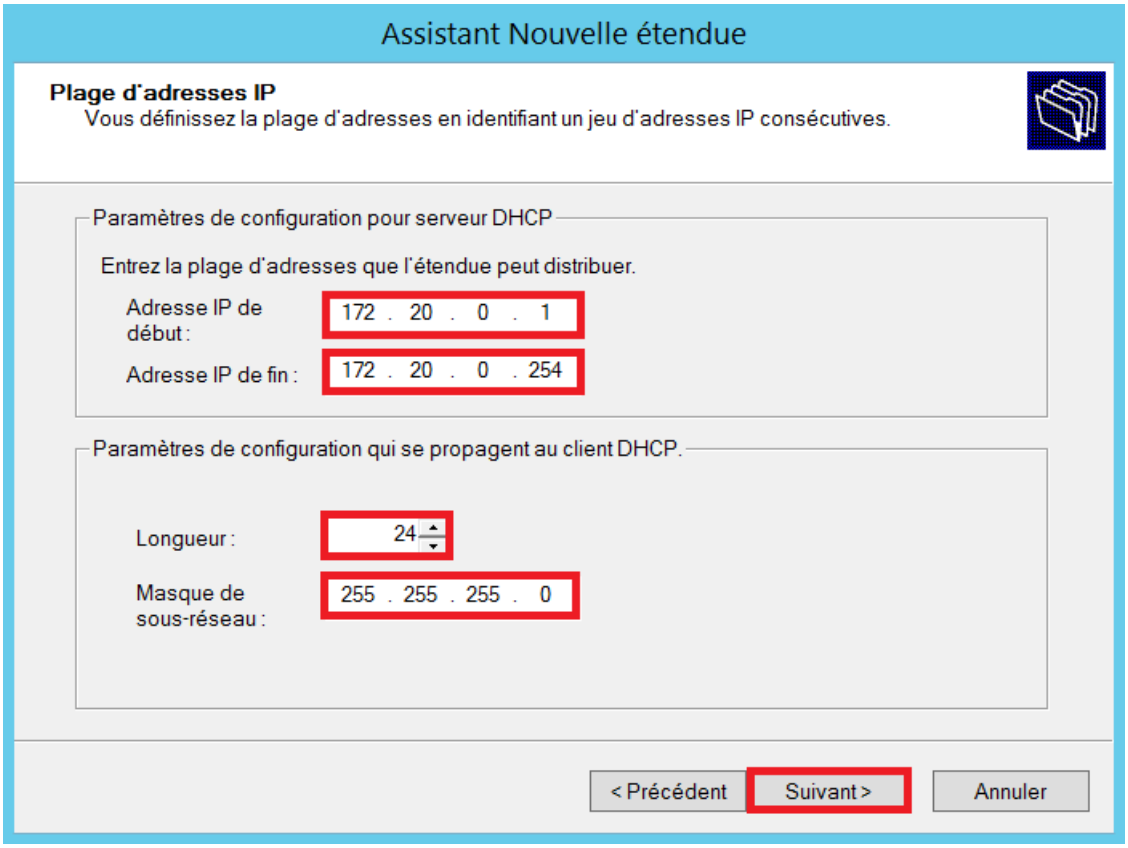
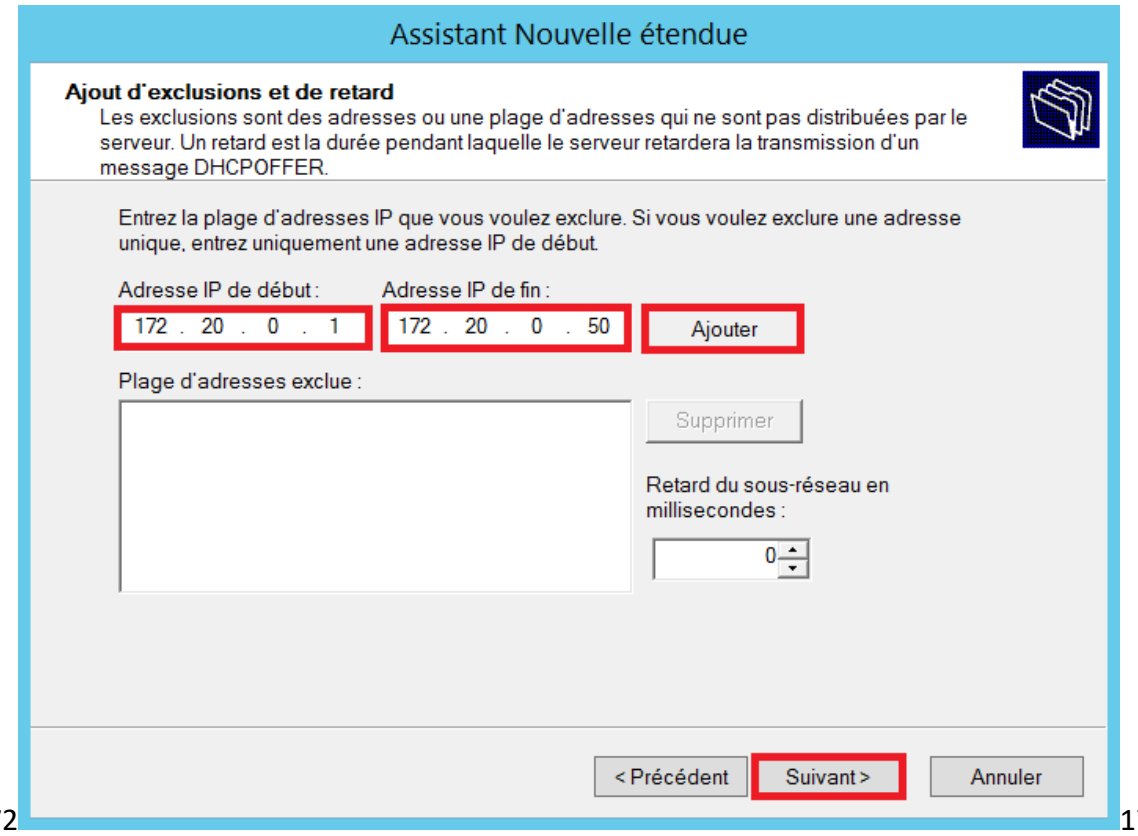


Tableau des adressages des étendu stadiumcompany.local :

Rang	Service / VLAN	Hôtes Requis	Masque	Adresse Réseau	Première Valable	Dernière Valable	Broadcast
1	VLAN 10 - Administration	170	/24	172.20.0.0	172.20.0.1	172.20.0.254	172.20.0.255
2	VLAN 20 - Équipes	164	/24	172.20.1.0	172.20.1.1	172.20.1.254	172.20.1.255
3	VLAN 30 - WiFi	100	/24	172.20.2.0	172.20.2.1	172.20.2.254	172.20.2.255
4	VLAN 40 - VIP-Presse	80	/25	172.20.3.0	172.20.3.1	172.20.3.126	172.20.3.127

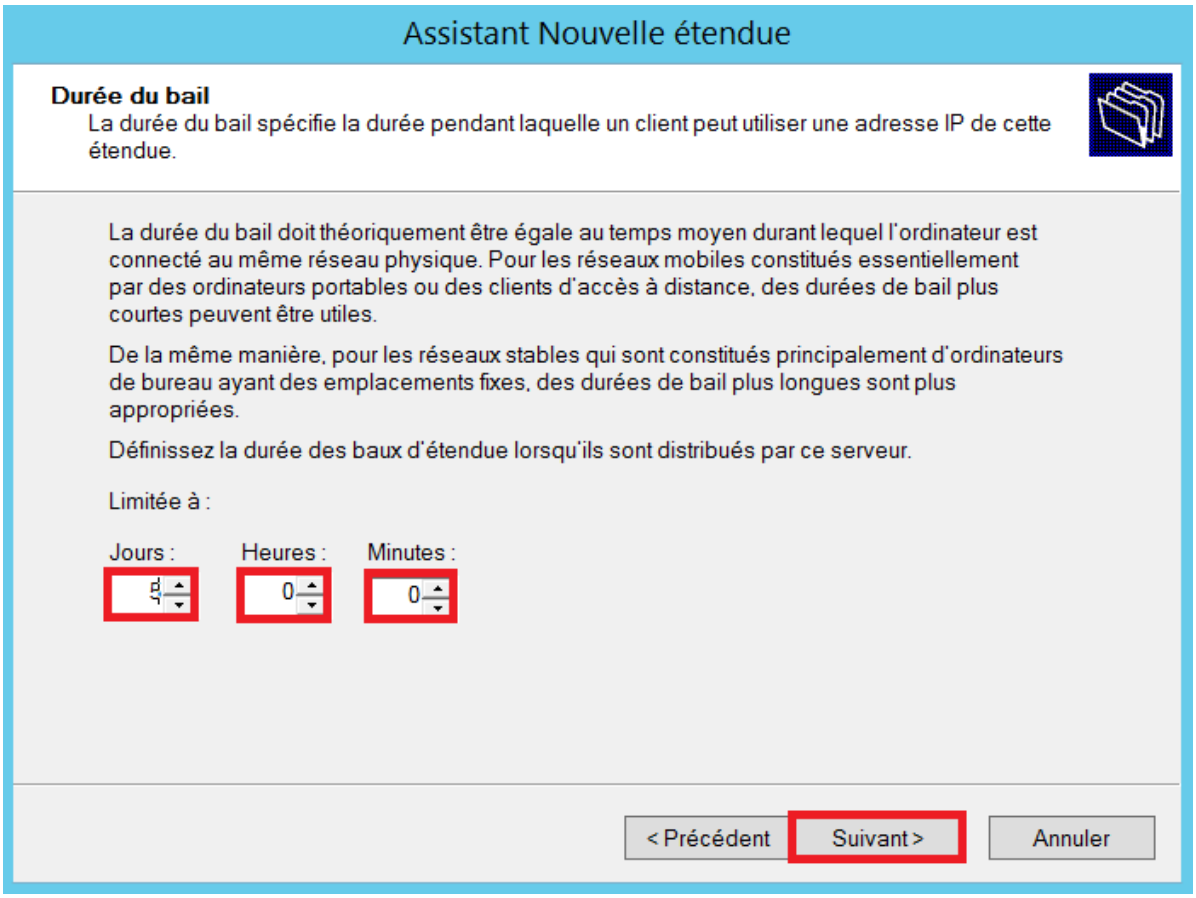
5	VLAN 50 - Caméras IP	80	/25	172.20.3.128	172.20.3.129	172.20.3.254	172.20.3.255
6	VLAN 60 - Fournisseurs	44	/26	172.20.4.0	172.20.4.1	172.20.4.62	172.20.4.63
7	VLAN 70 - Restaurant	14	/27	172.20.4.64	172.20.4.65	172.20.4.94	172.20.4.95

- Exclure la plage d'adresse (que dans l'étendue 1 : 172.20.0.1 à 172.20.0.25), faire **suivant**.

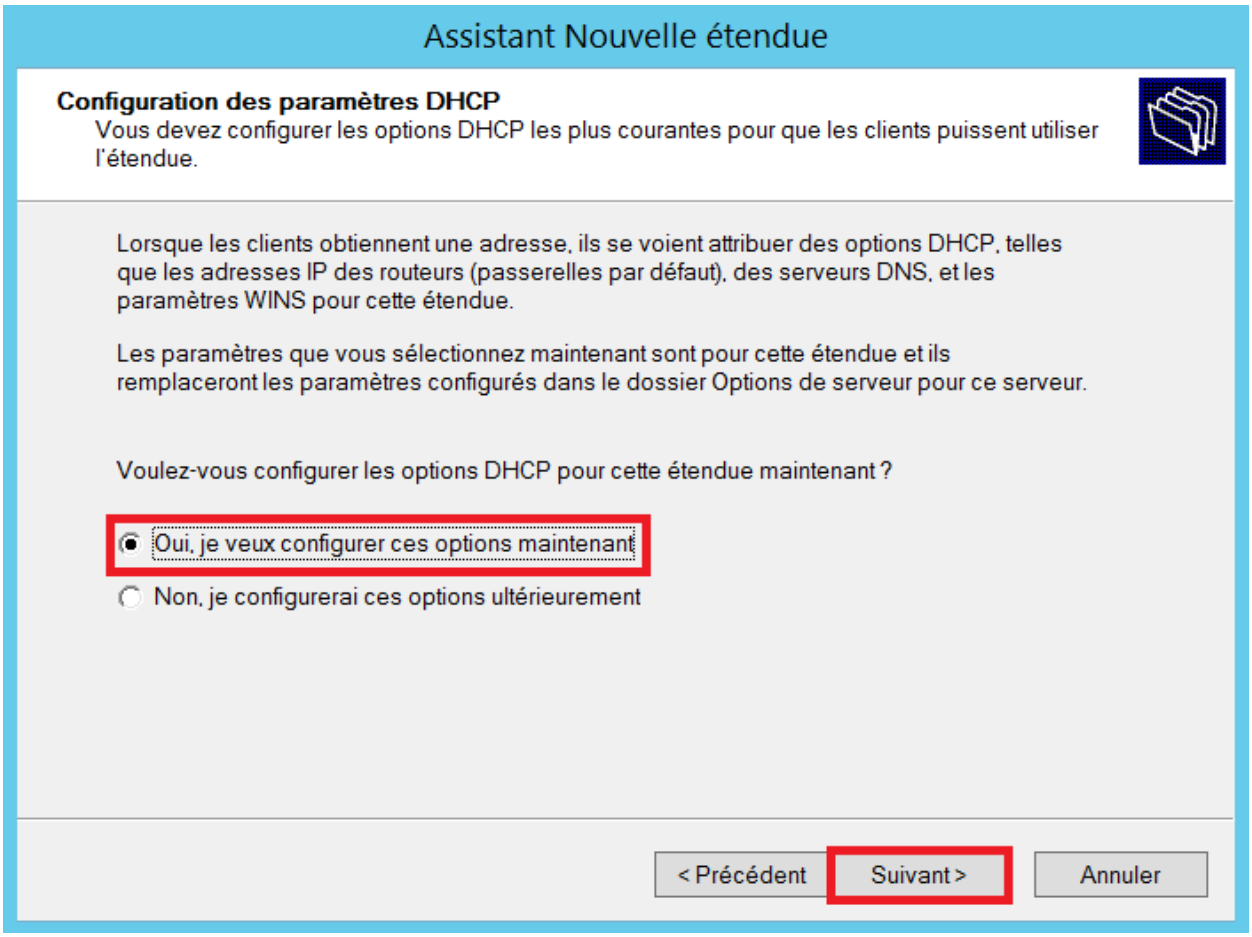


172 172

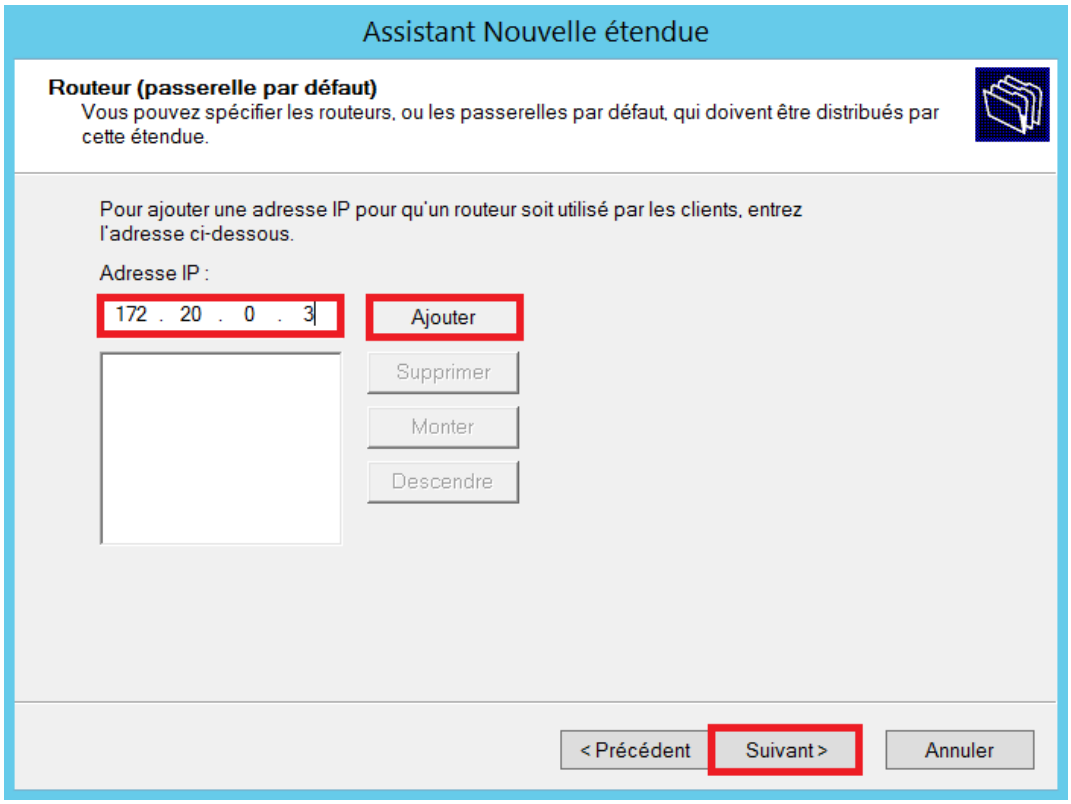
- Imposer la durée du bail (5 jours), faire **suivant**.



- Configurer les options maintenant sur tous les étendues, faire **suivant**.

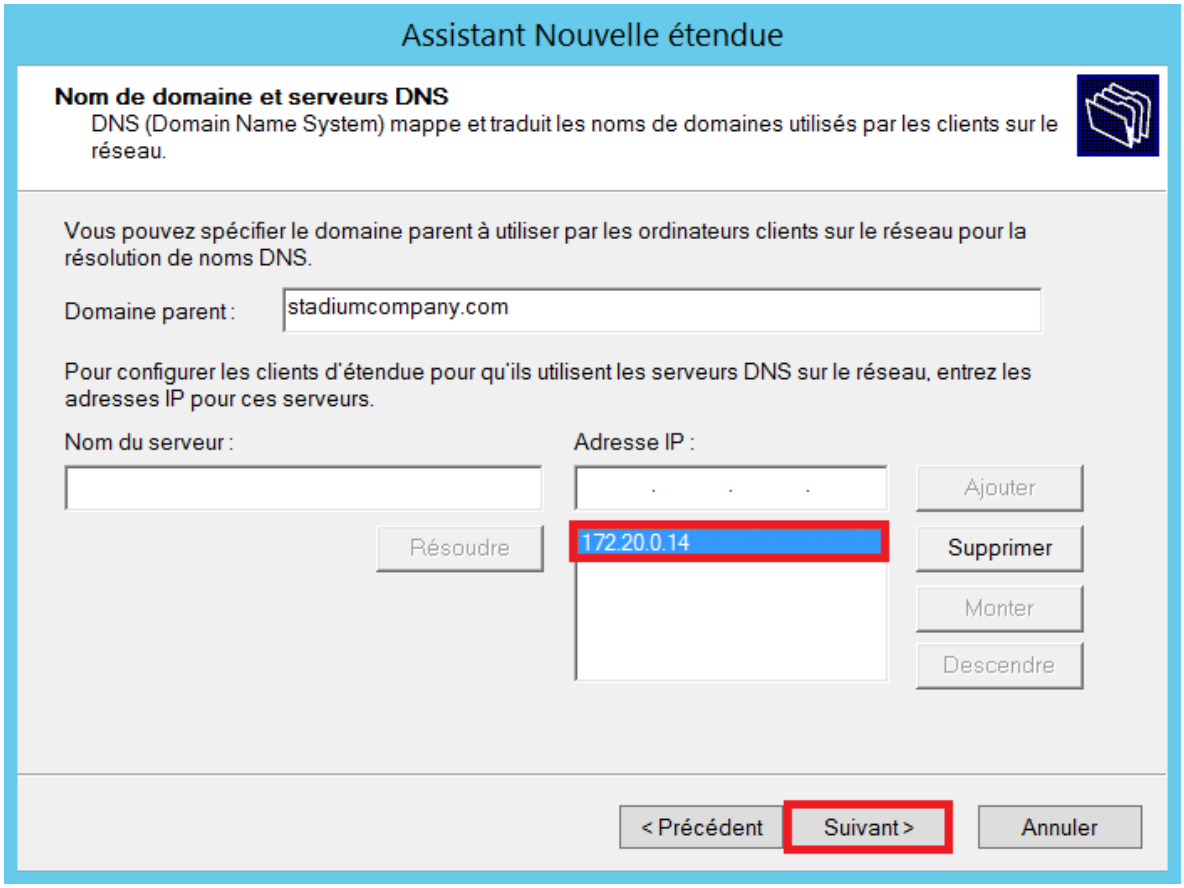


- Indiquer l'adresse du routeur (Ici le routeur virtuel HSRP 172.20.0.3), faire **suivant**.

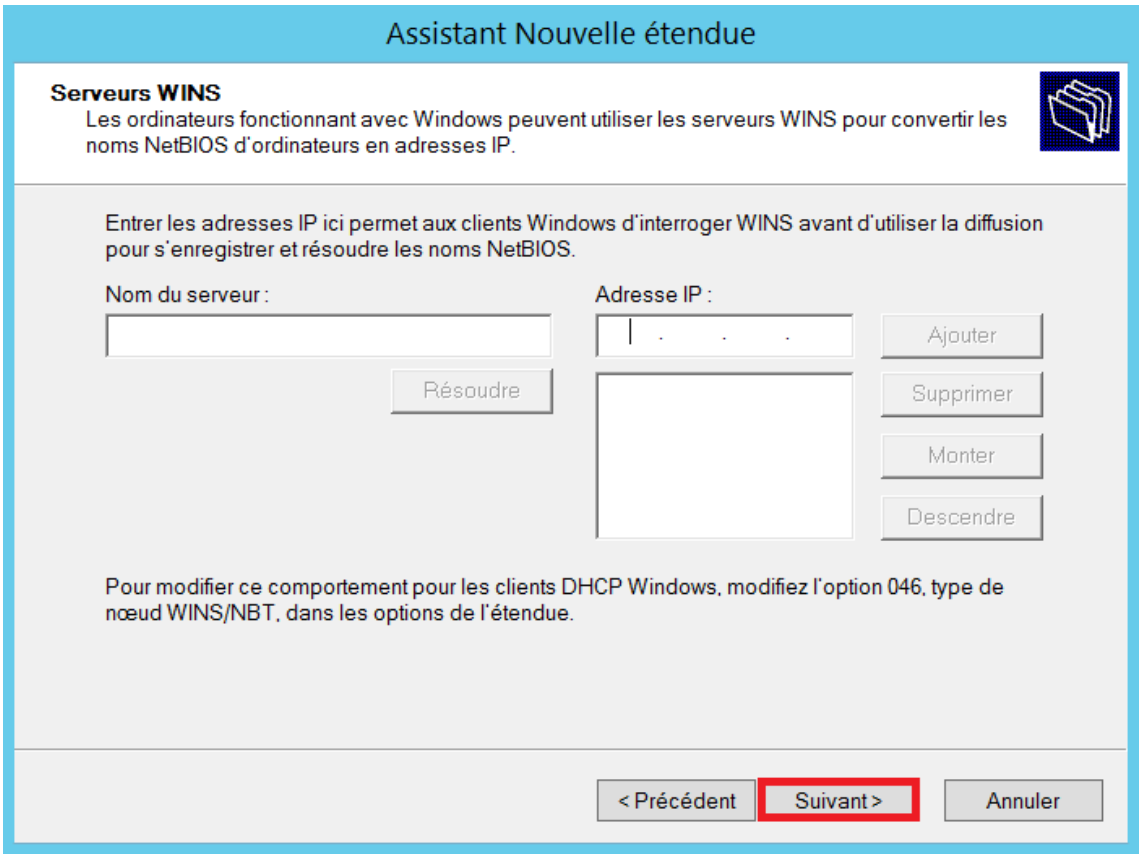


172

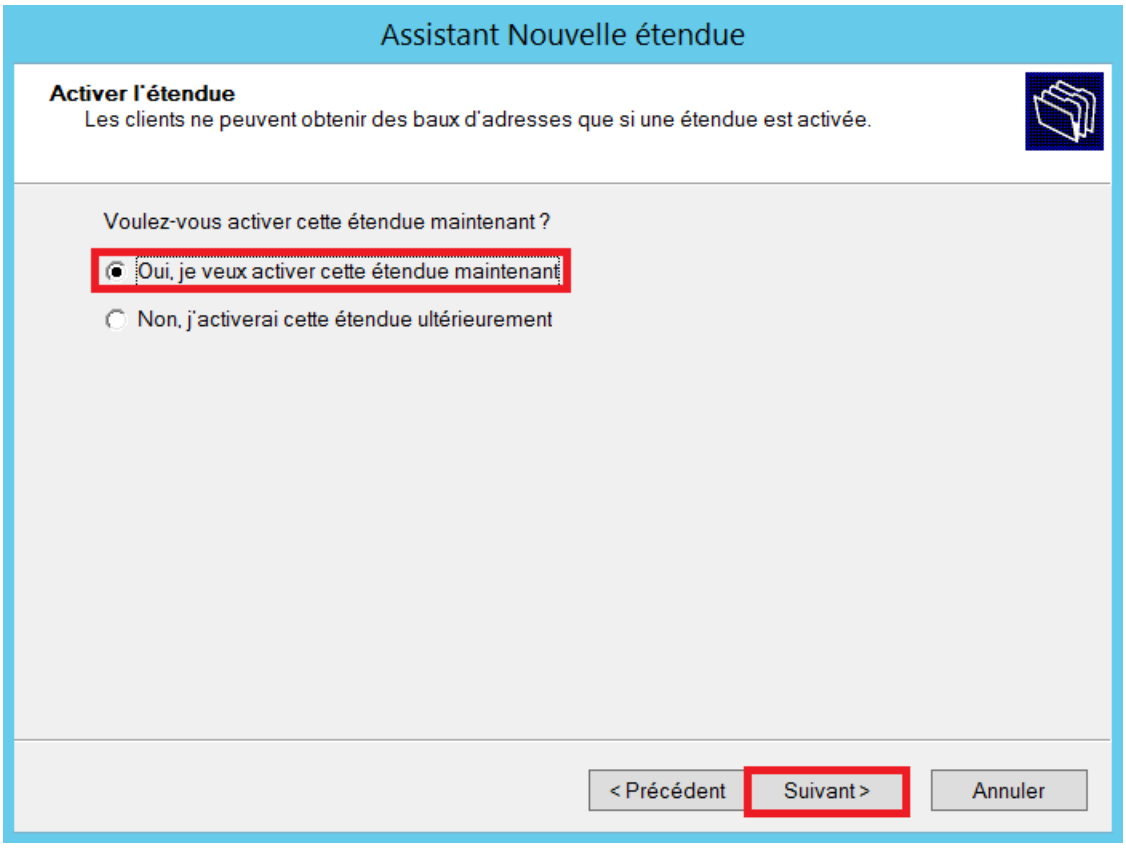
- Ajouter le **DNS** (stadiumcompany.local : 172.20.0.14) Automatique.



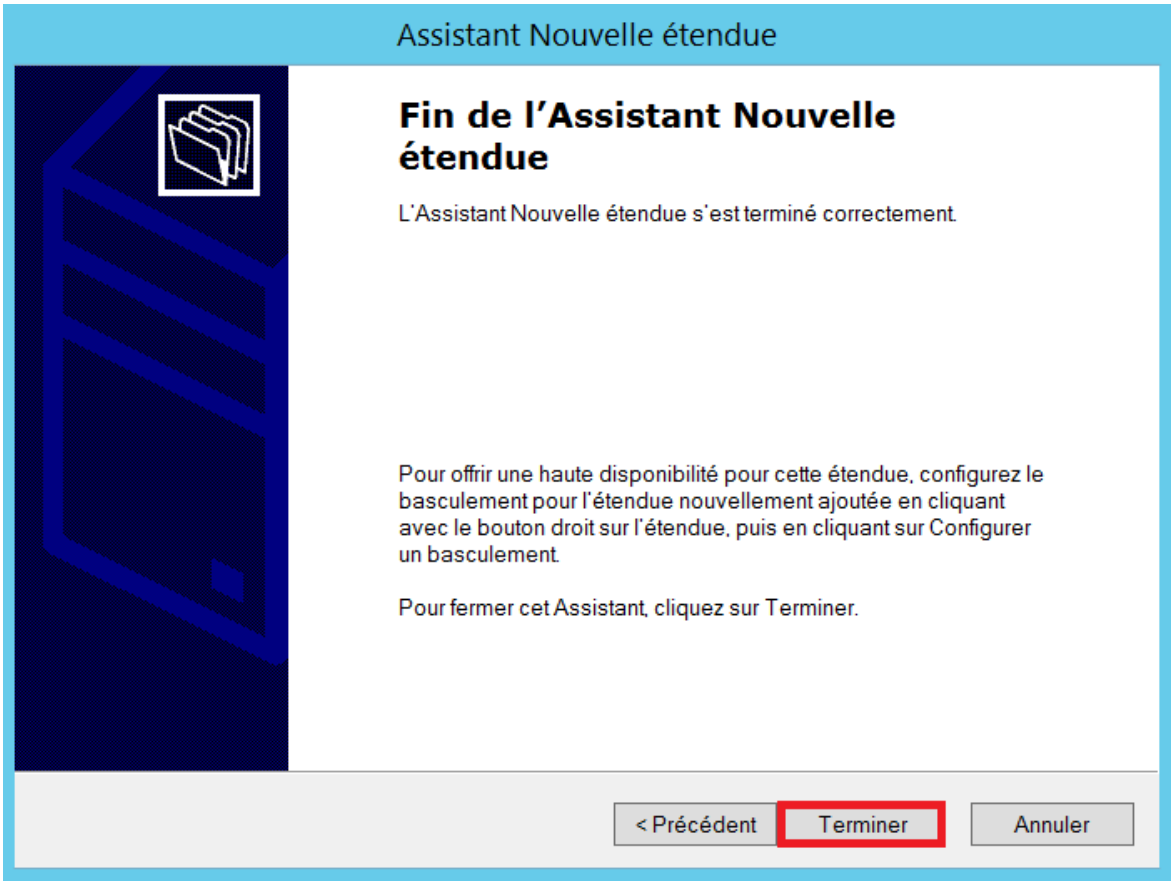
- Pas de serveur WINS NetBIOS, faire **suivant**.



- **Activer** l'étendue maintenant.



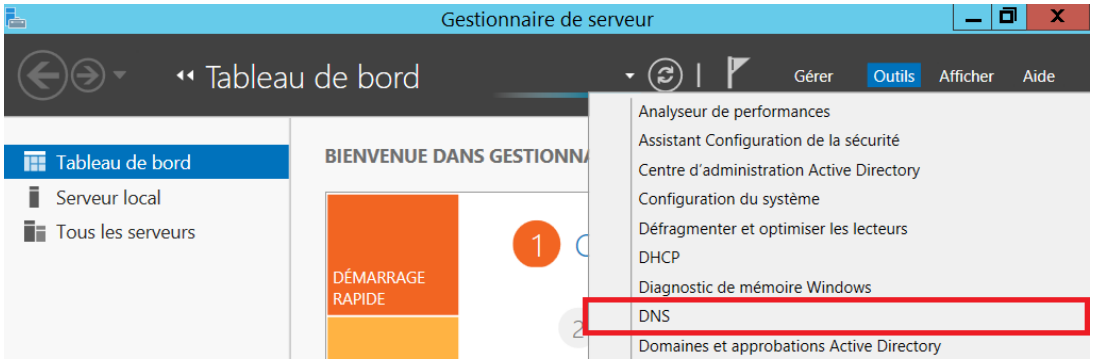
- **Terminer** la création de l'étendu.



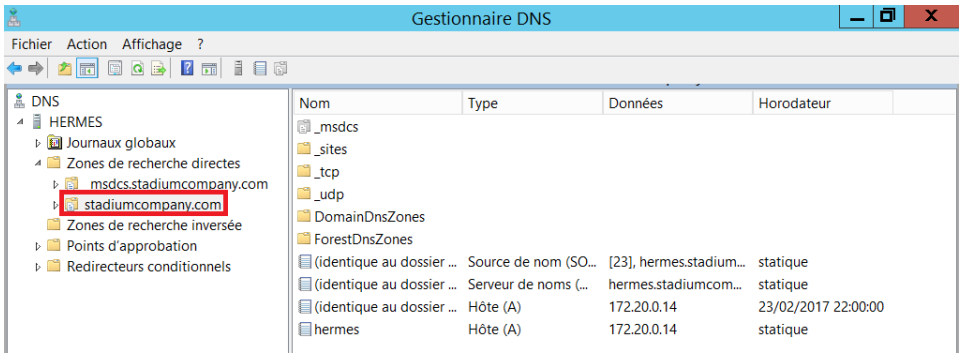
Configuration DNS

<u>Vérifications de zones de recherche directe :</u>

- Gestionnaire de serveur → Outils → DNS.



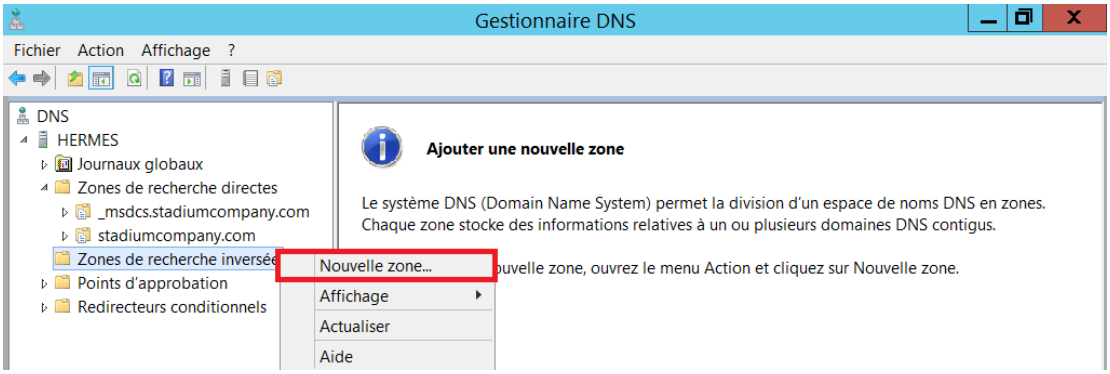
- DNS → HERMES → Zones de recherches directes → Vérifier que la zone stadiumcompany.local a bien été créé.



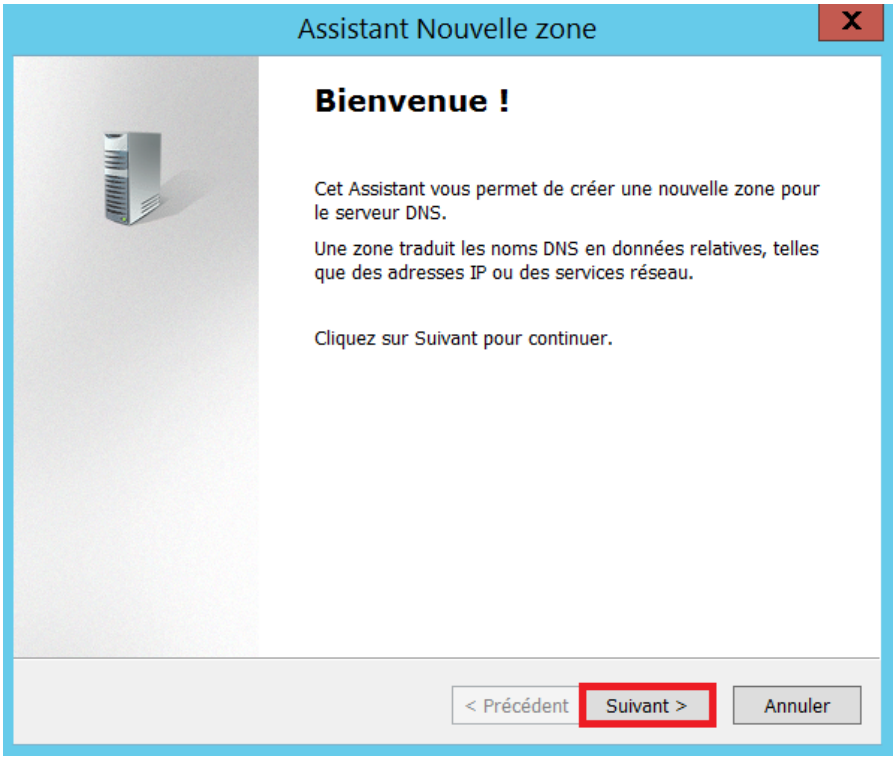
E

<u>Nouvelle Zone inversé :</u>

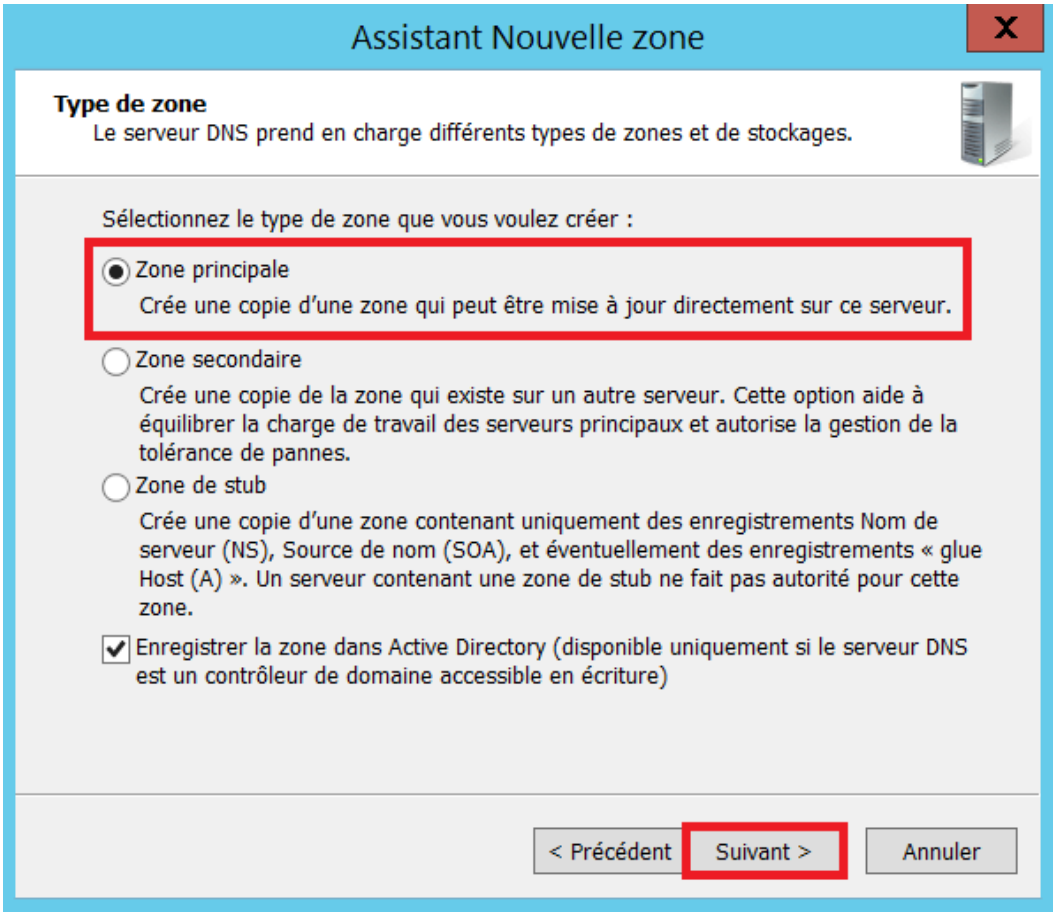
- Clic droit sur Zones de recherche inversée → Nouvelle zones…



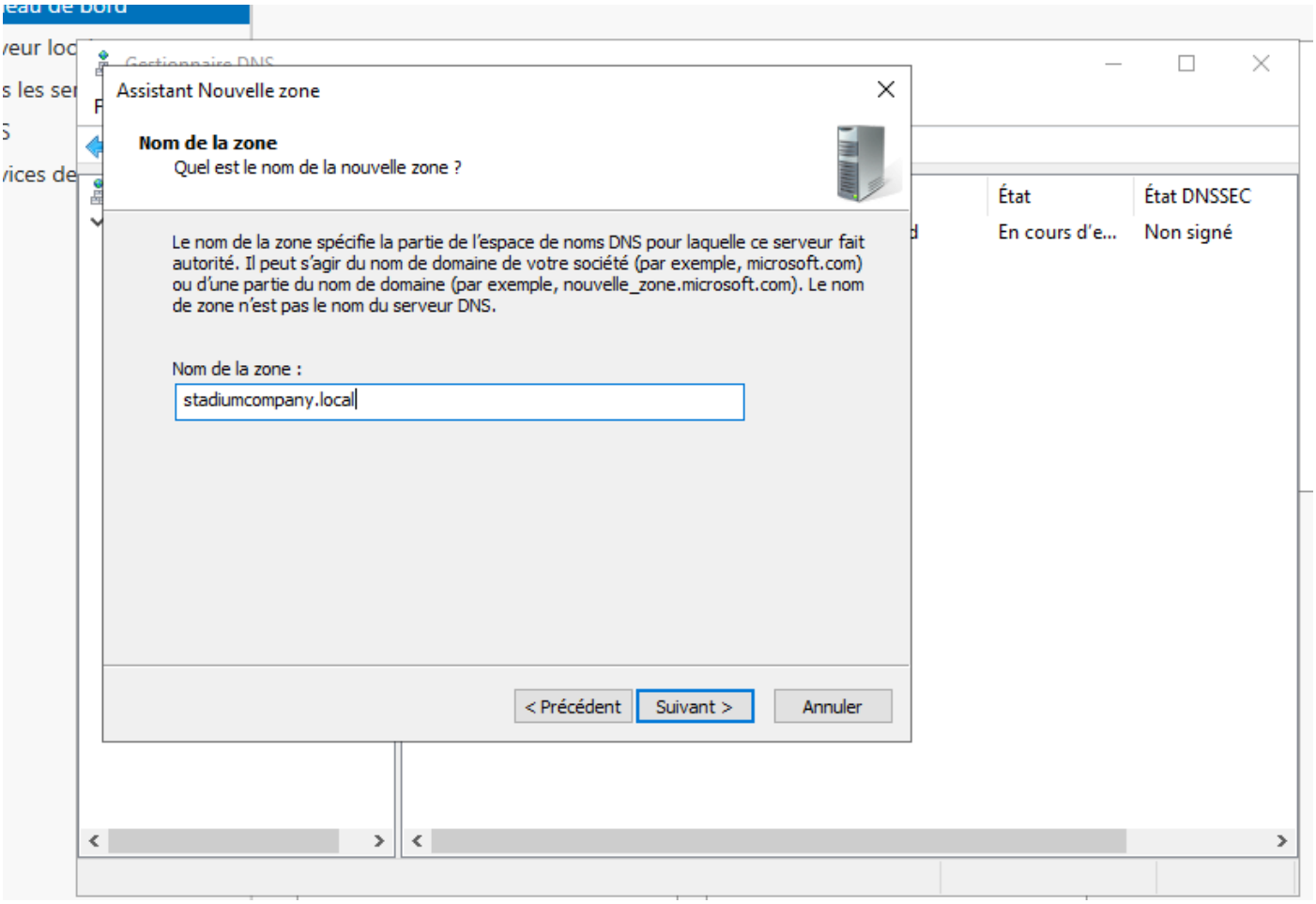
- Passer l'intro de la création de la nouvelle zone, faire **suivant**.



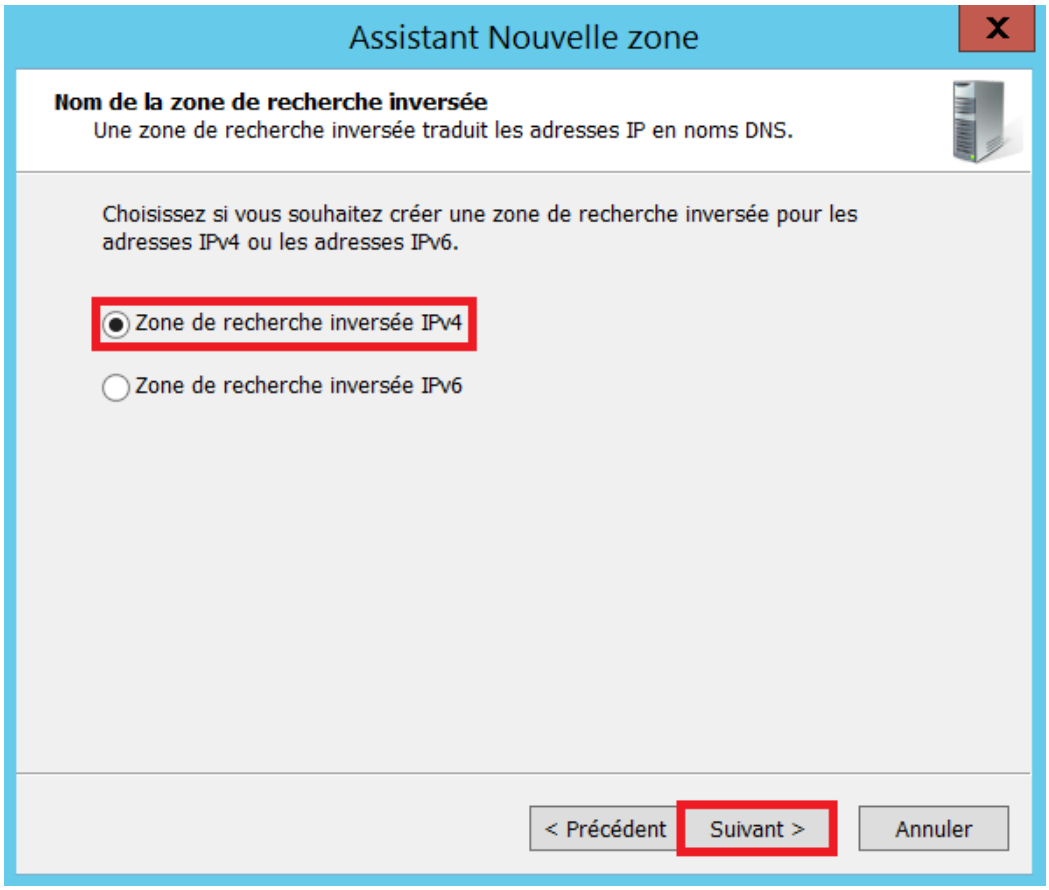
- Sélectionner « **Zone principale** », faire **suivant**.



- Sélectionner **« Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : stadiumcompany.local »**, faire **suivant**.

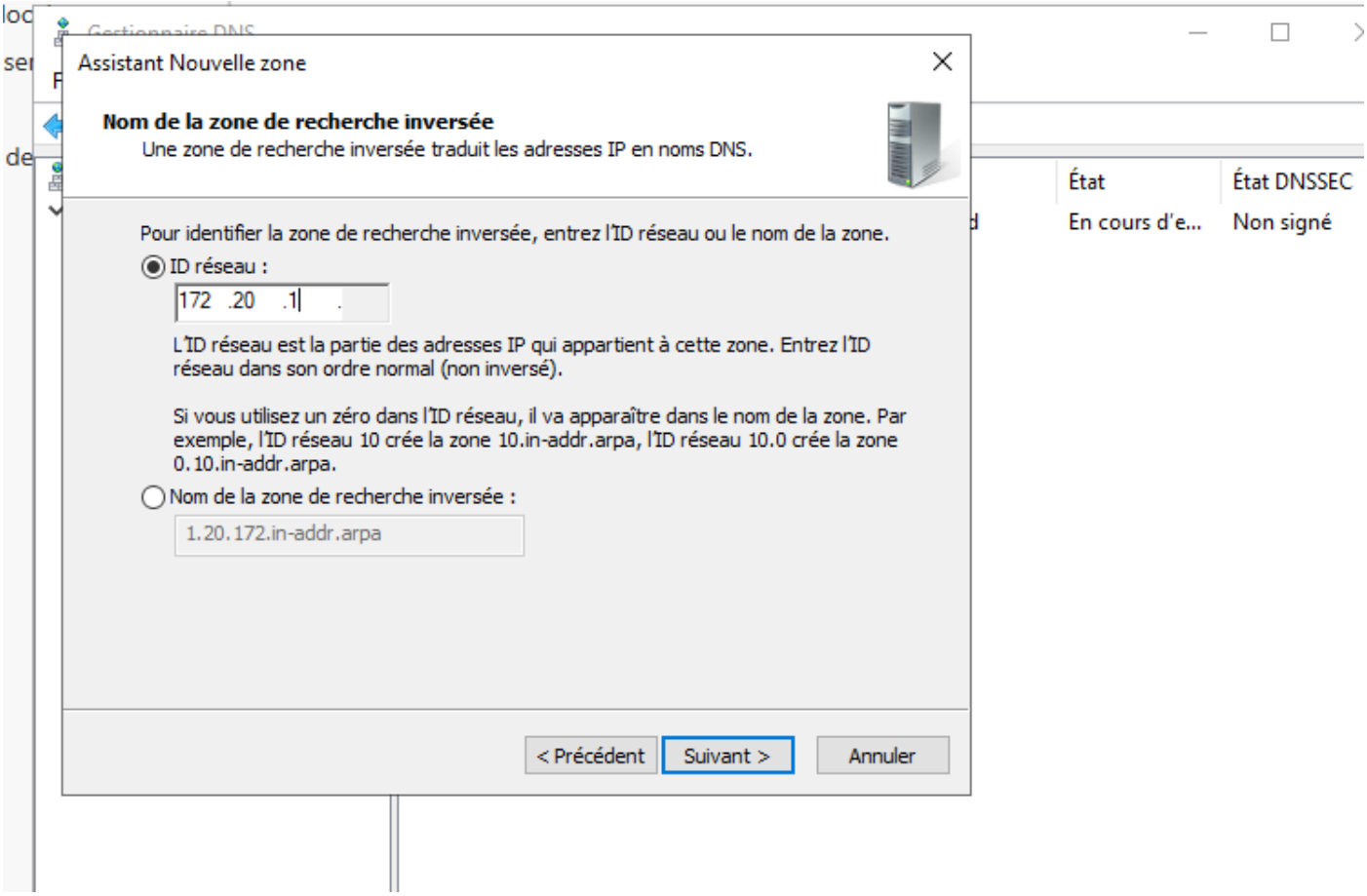


- Sélectionner **« Zone de recherche inversée IPv4 »**, puis **suivant.**

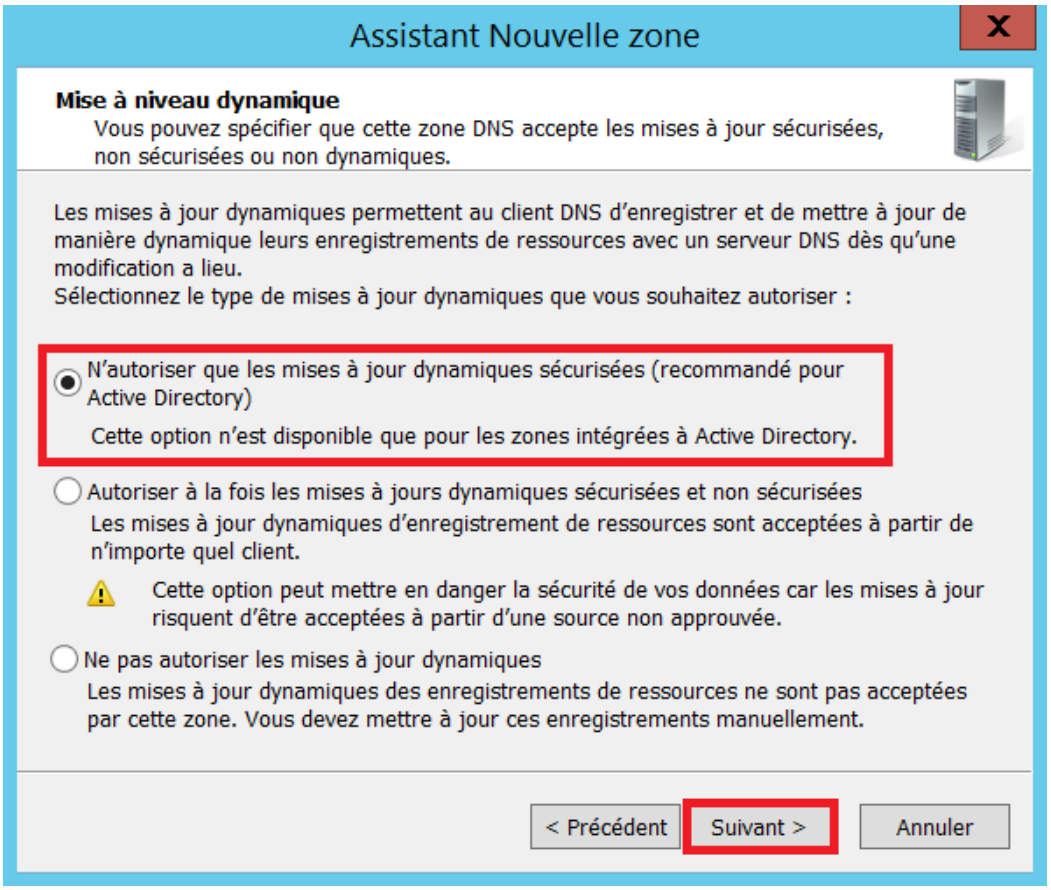

Assistant Nouvelle zone
Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.
Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.
Zone de recherche inversée IPv4
Zone de recherche inversée IPv6
< Précédent
Suivant >
Annuler

- Sélectionné **« L'ID réseau 172.20.1.X »**

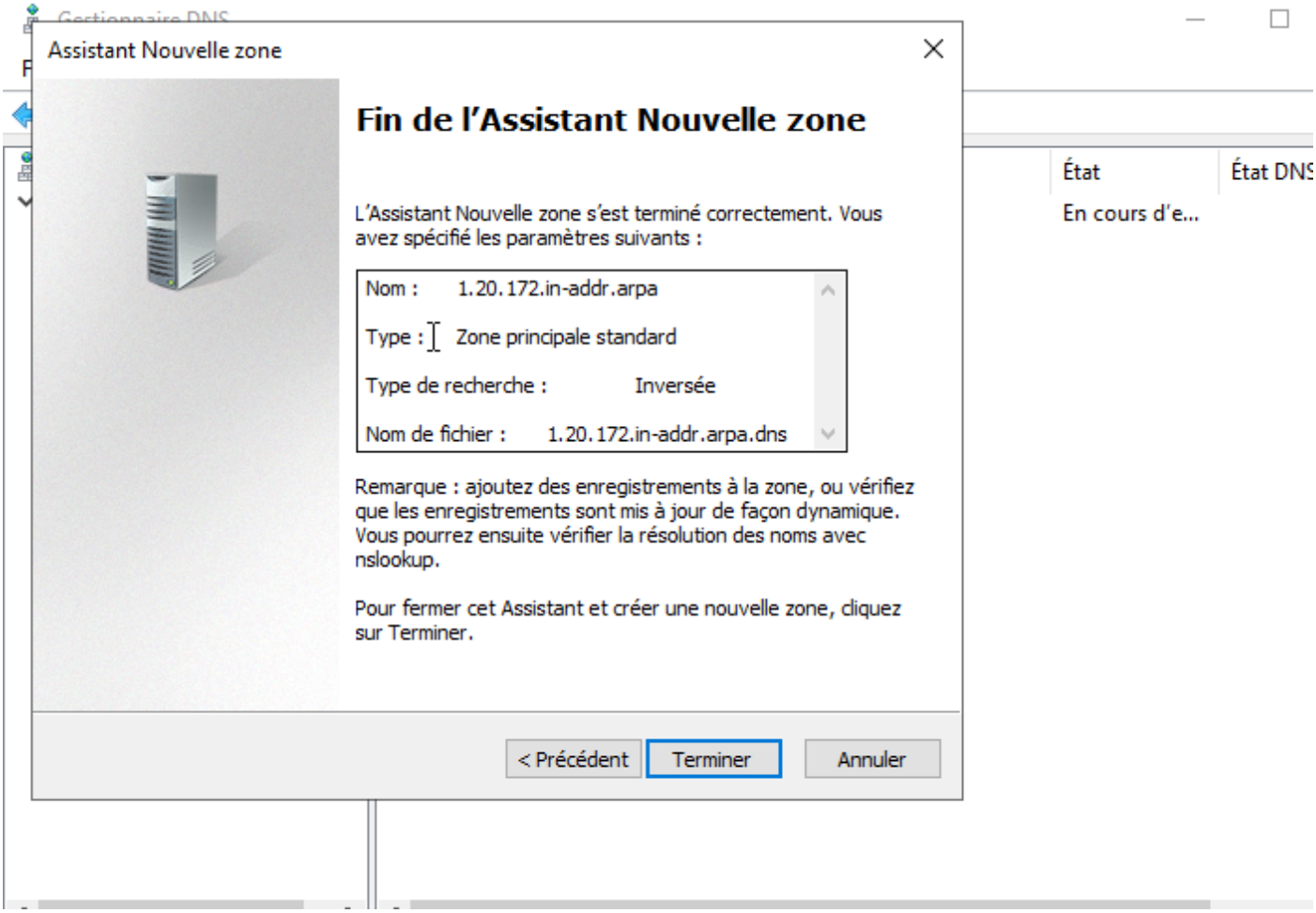
.



- Sélectionner **« N'autoriser que les mises à jour dynamiques sécurisées »**, faire **suivant**.


Assistant Nouvelle zone
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 jours 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

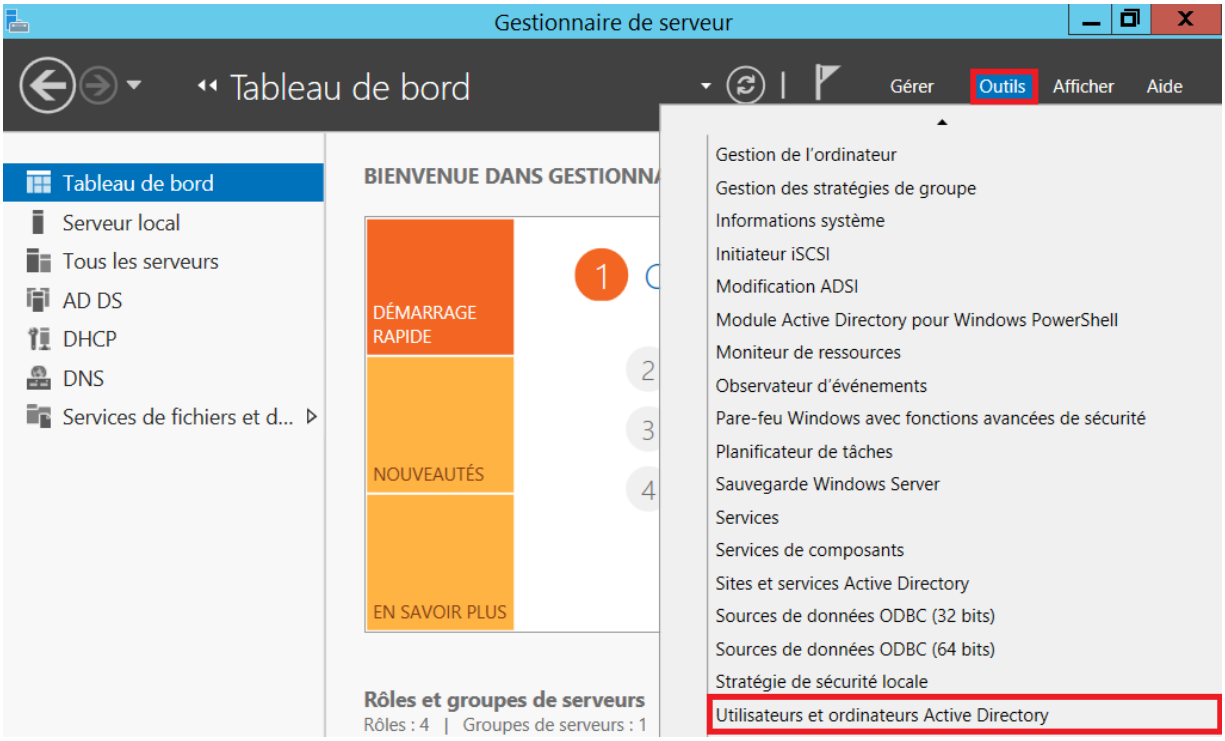
- Finaliser la création de la nouvelle zone, faire **terminer**.



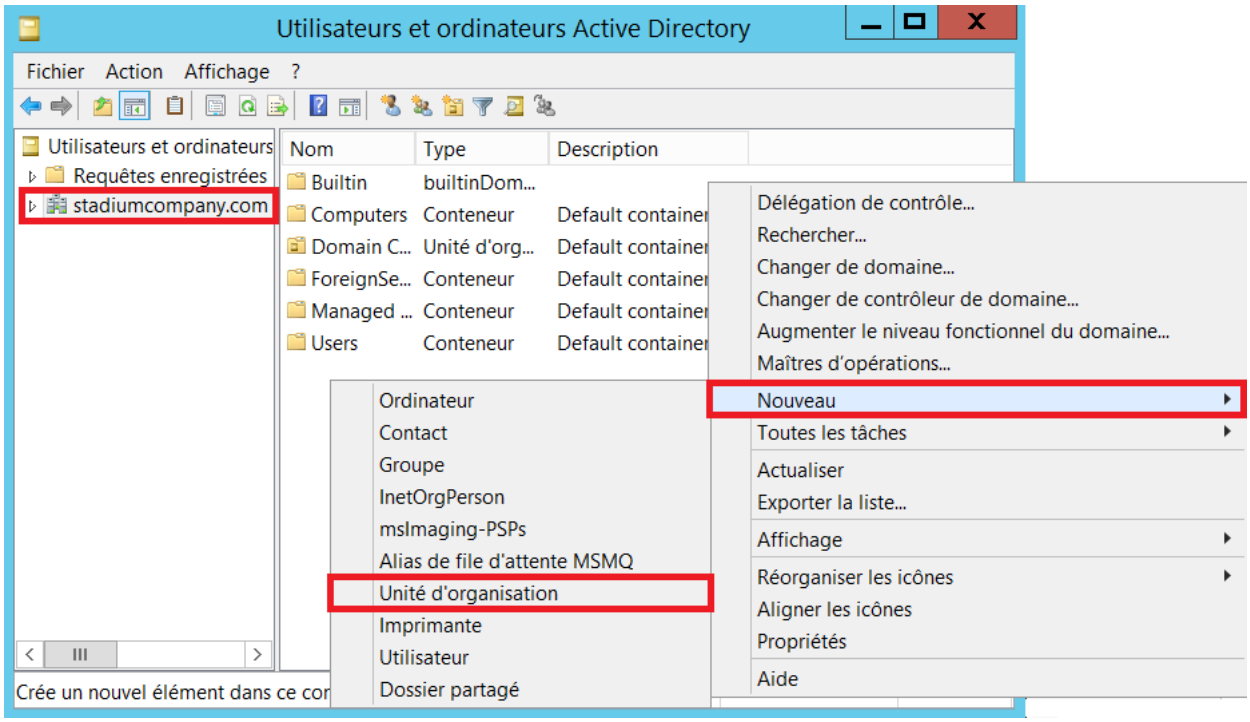
Configuration des outils d'Active Directory

Création des unités d'organisation

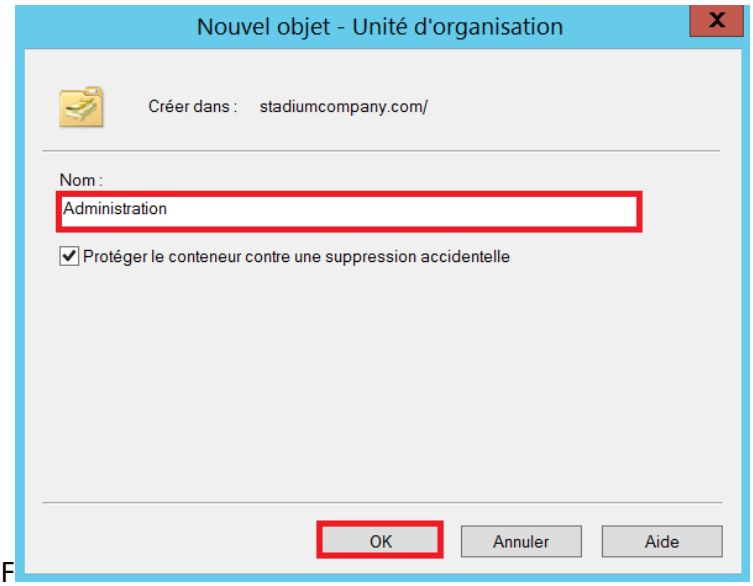
- Sur le gestionnaire de serveur → Outils → Clique sur **Utilisateurs et ordinateurs Active Directory**.



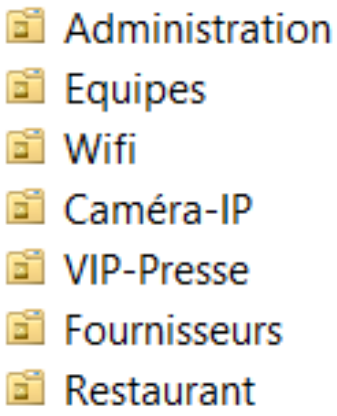
- Dans Utilisateurs et ordinateurs Active Directory → Domaine (stadiumcompany.local) → Clic droit → Nouveau → **Unité d'organisation**.


Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs
Requêtes enregistrées
stadiumcompany.com
Nom Type Description
Builtin builtinDom...
Computers Conteneur Default container
Domain C... Unité d'org... Default container
ForeignSe... Conteneur Default container
Managed ... Conteneur Default container
Users Conteneur Default container
Ordinateur
Contact
Groupe
InetOrgPerson
msImaging-PSPs
Alias de file d'attente MSMQ
Unité d'organisation
Imprimante
Utilisateur
Dossier partagé
Délégation de contrôle...
Rechercher...
Changer de domaine...
Changer de contrôleur de domaine...
Augmenter le niveau fonctionnel du domaine...
Maîtres d'opérations...
Nouveau
Toutes les tâches
Actualiser
Exporter la liste...
Affichage
Réorganiser les icônes
Aligner les icônes
Propriétés
Aide
Crée un nouvel élément dans ce cor

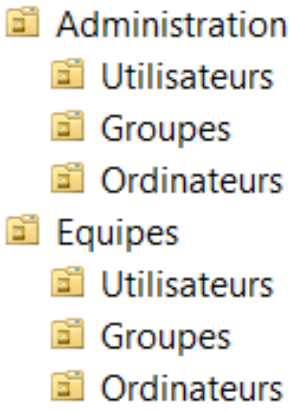
- Création des UO services (Administration, Equipe, Wifi, Caméra-IP, VIP-Presse, Fournisseurs et Restaurant).



F



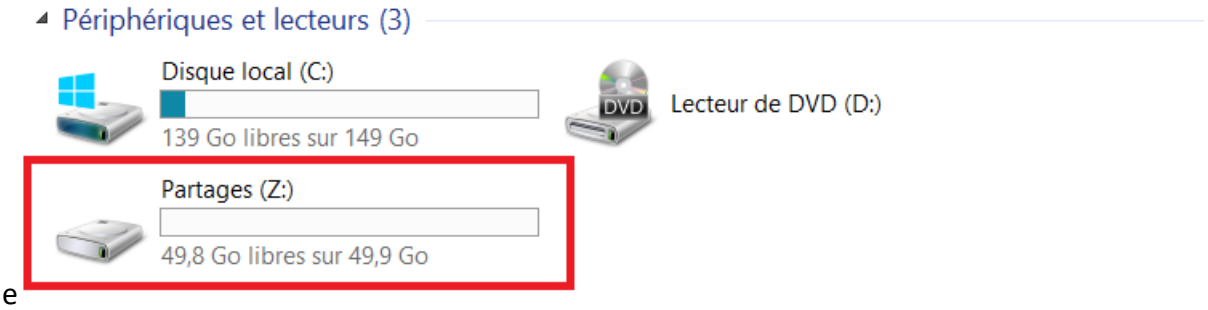
- Création des sous-UO (Utilisateurs, Groupes et ordinateurs) pour les services Administration, Equipes, Fournisseurs, Restaurant et VIP-Presse.



Les stratégies de groupe

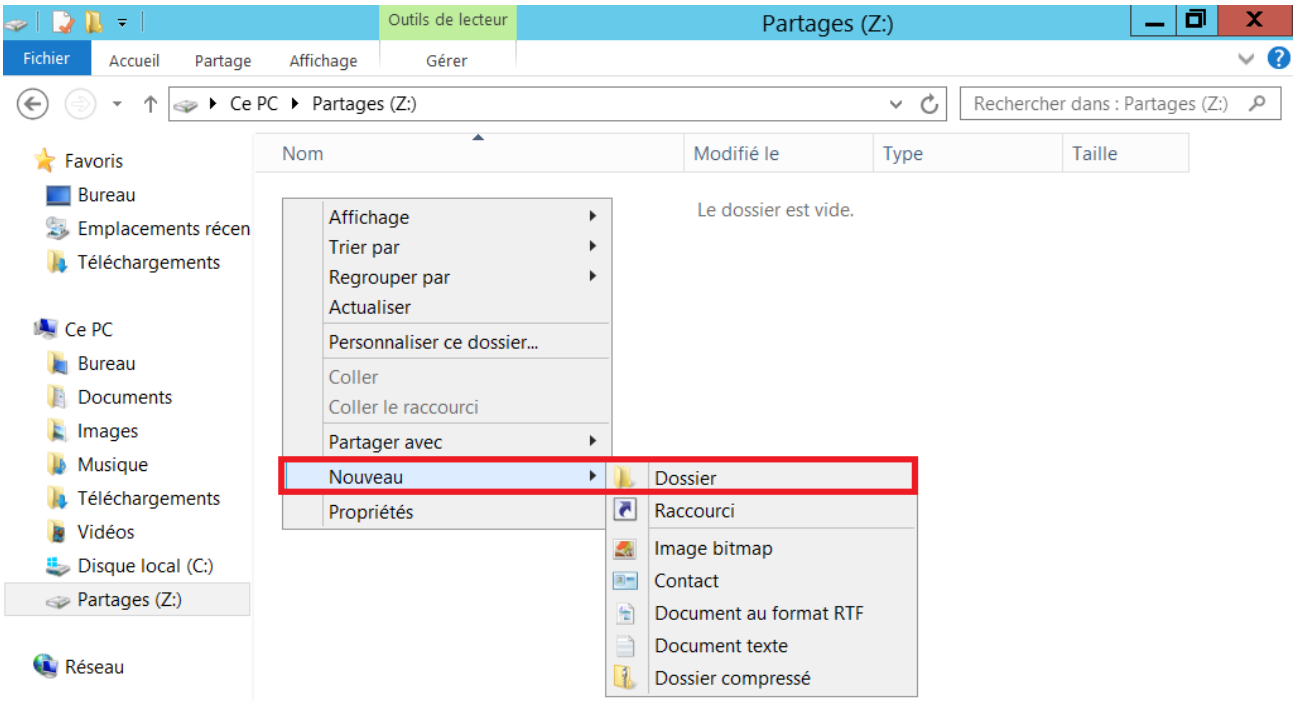
Forcer le fond d'écran (GPO)

- Sur le deuxième disque dur nous allons créer un dossier qui sera partagé avec tous les ordinateurs de l'Active Directory en lecture seule.
- Aller sur ordinateur → Deuxième disque (Partages Z pour moi).



e

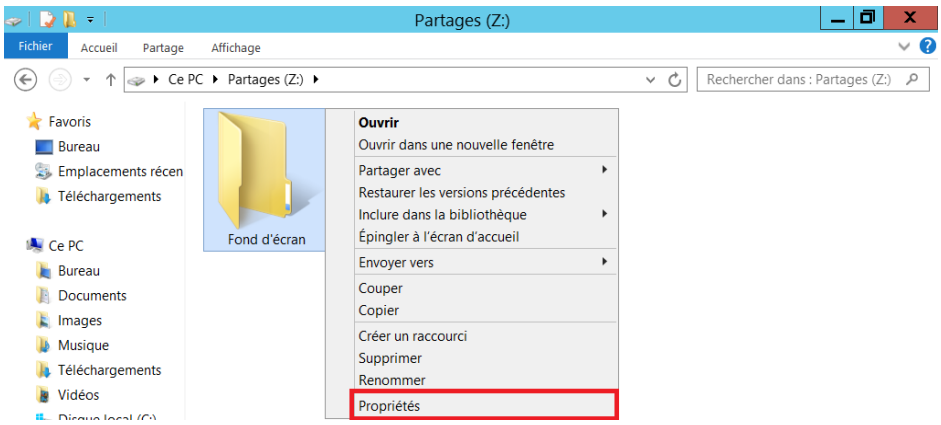
- Clic droit → Nouveau → Dossier → Nommer le (Exemple Fond d'écran).



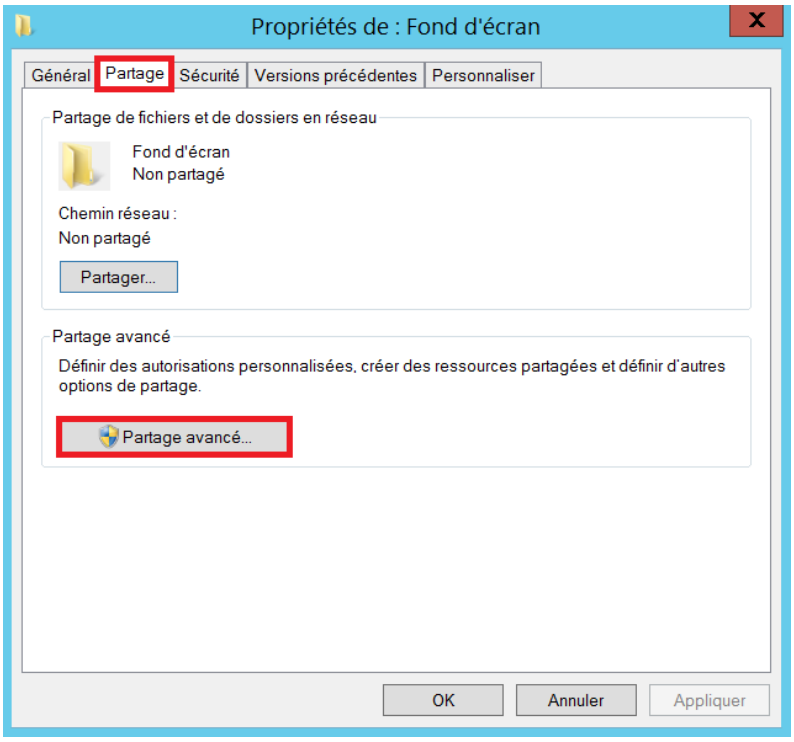
- Aller dans le dossier → Ajouter l'image qui sera à chaque écran.

- Clic droit sur le dossier Fond d'écran → **Propriétés.**

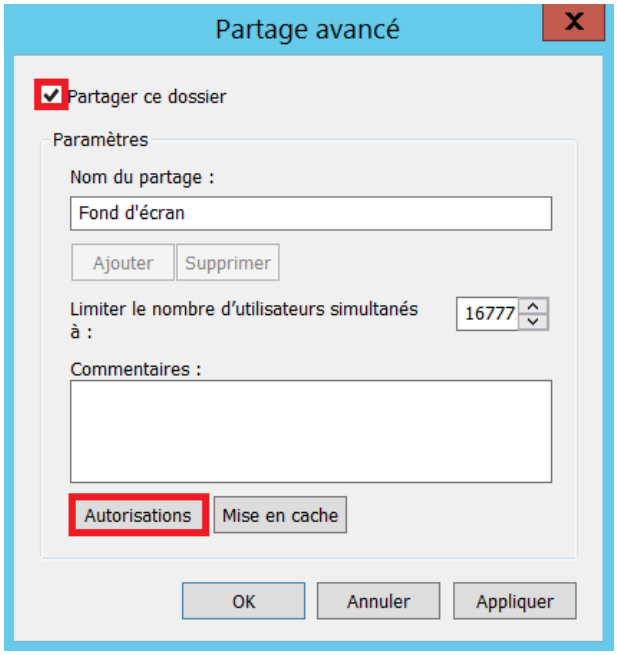
Fond

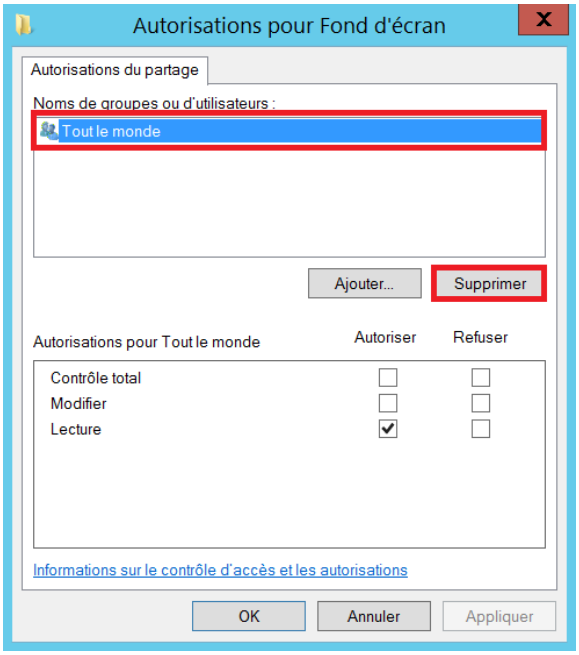


- Dans l'onglet partage → **Partage avancé**…

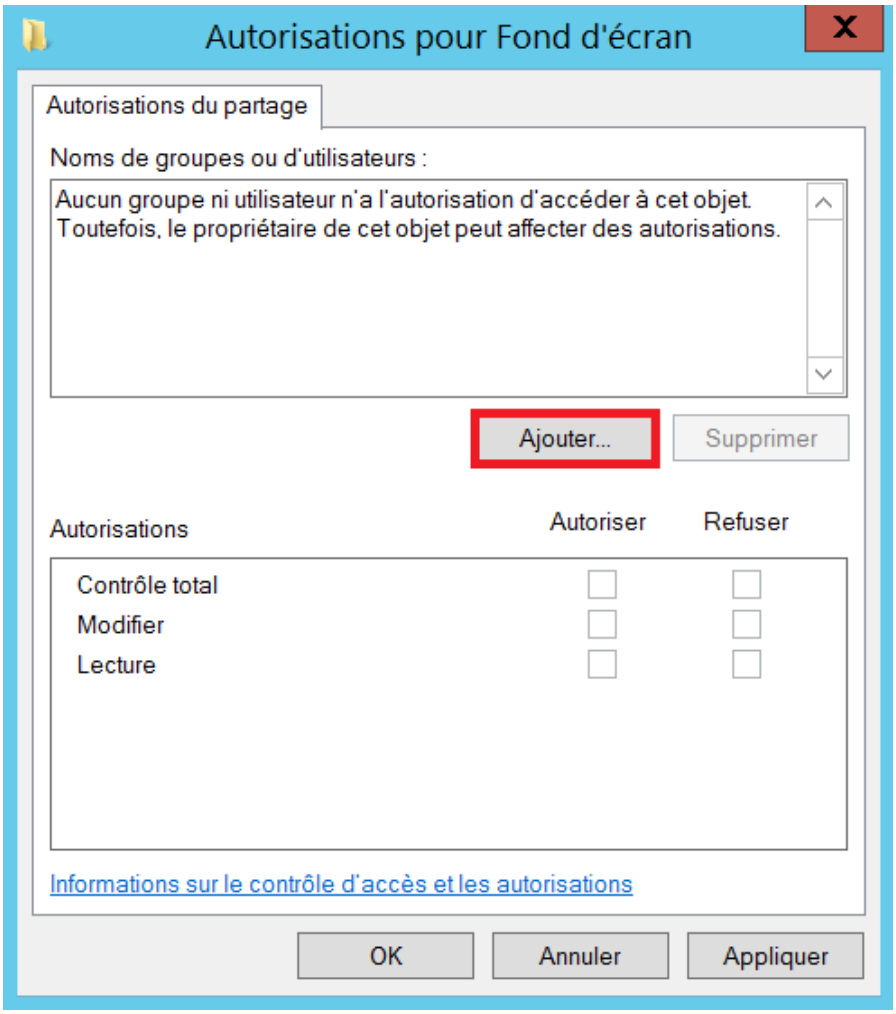


- Cocher « Partager ce dossier » et aller sur **Autorisations → Supprimer le groupe Tout le monde**.
-

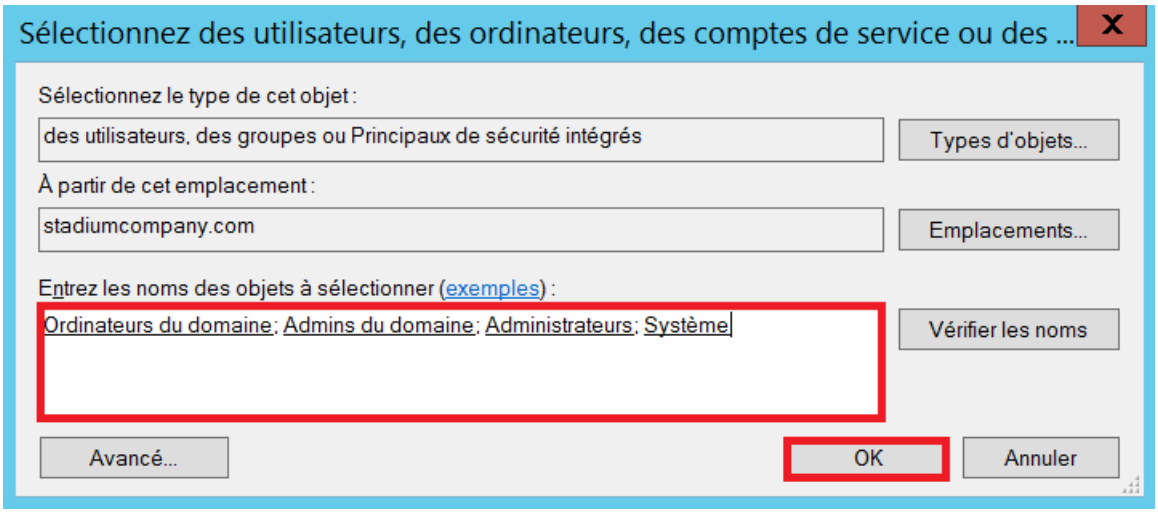




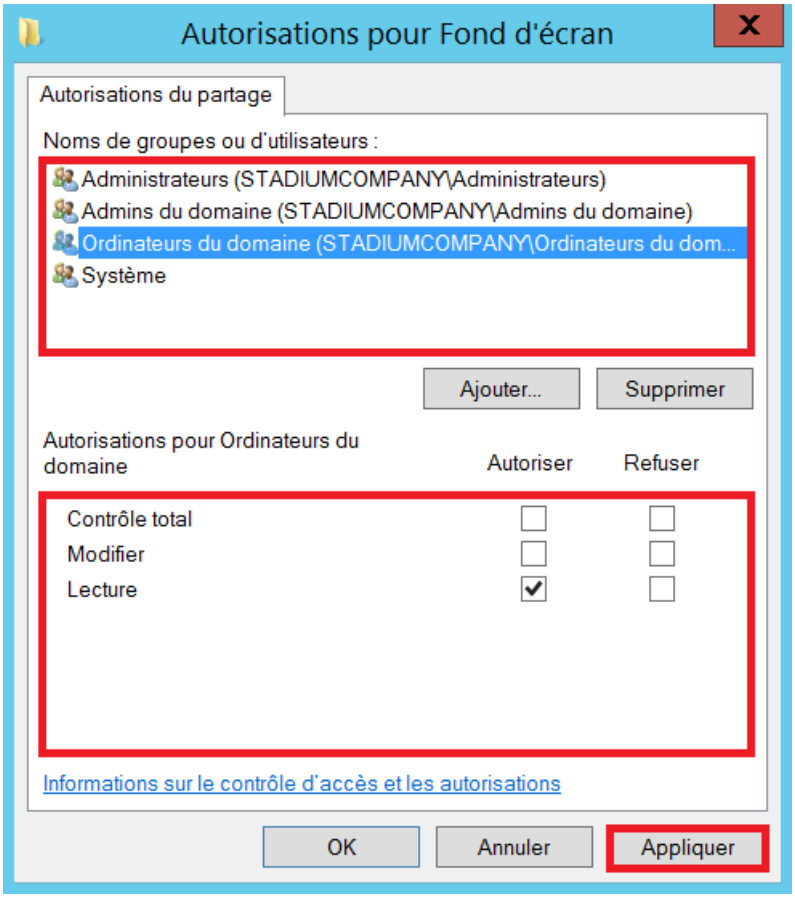
- Cliquer sur **Ajouter…**


Autorisations pour Fond d'écran
Autorisations du partage
Noms de groupes ou d'utilisateurs :
Aucun groupe ni utilisateur n'a l'autorisation d'accéder à cet objet.
Toutefois, le propriétaire de cet objet peut affecter des autorisations.
Ajouter...
Supprimer
Autorisations
Autoriser
Refuser
Contrôle total
Modifier
Lecture
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer

- Ajouter : « Ordinateurs du domaine ; Admins du domaine ; Administrateurs ; Système »

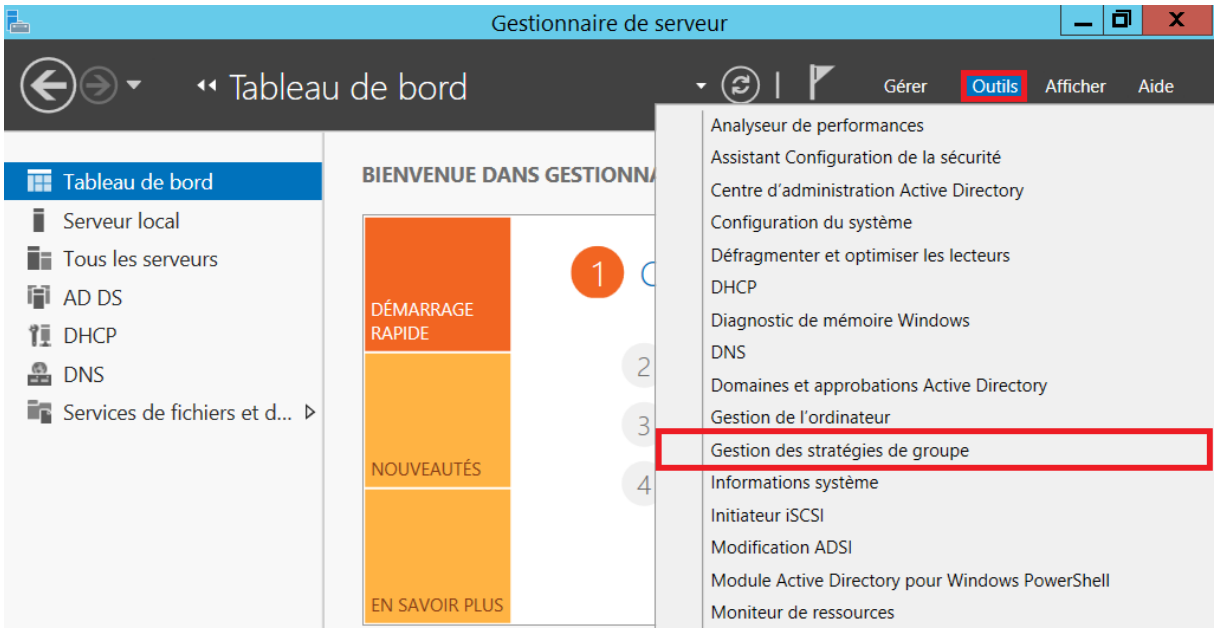


- Ajouter les Autorisation :
  - Contrôle total pour Admins du domaine
  - Modification pour Administrateurs
  - Lecture pour Ordinateurs du domaine et Système

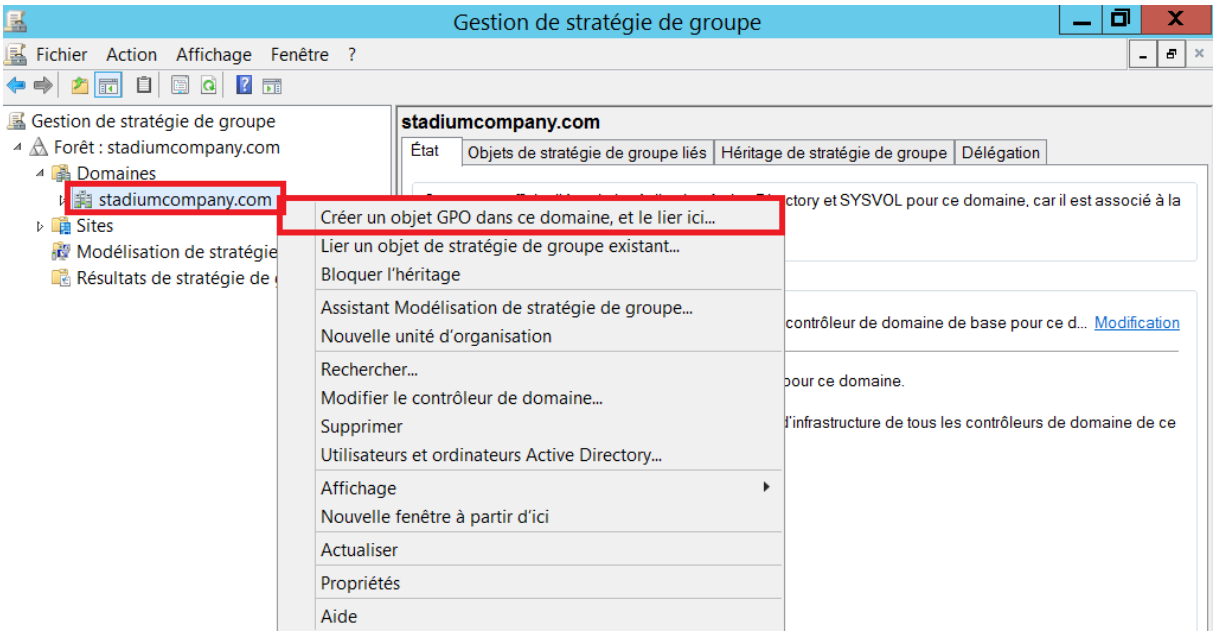


Création d'un paramètre pour copier le fichier sur l'ordinateur. Ainsi l'ordinateur récupèrera le fond d'écran directement en local ce qui empêcheras les ordinateurs de récupérer l'image l'AD à chaque démarrage, pouvant entrainer un temps de traitement supplémentaire su il y a du monde.

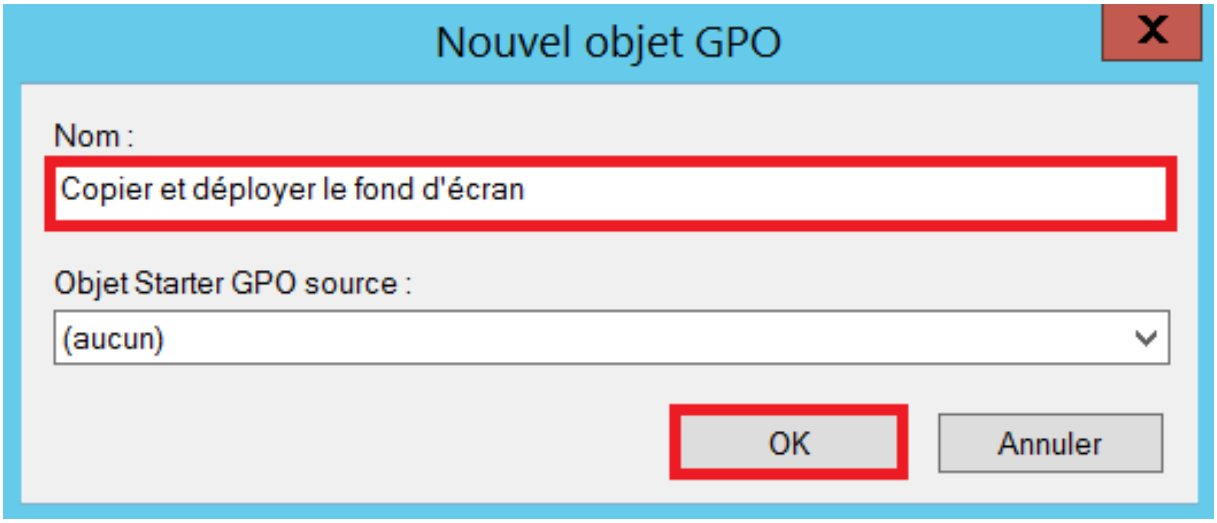
- Gestionnaire de serveur → Outils → **Gestion des stratégies de groupe.**



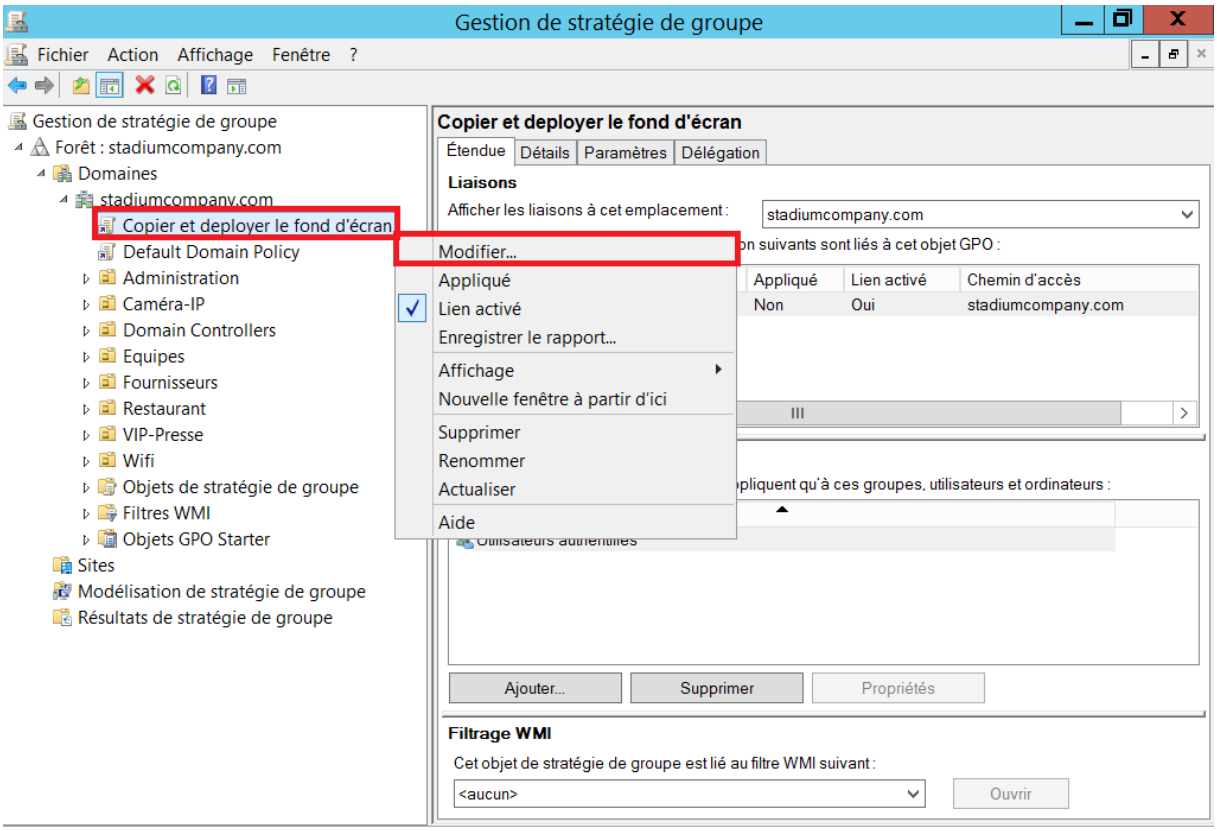
- Gestion de Stratégie de groupe → Forêt : stadiumcompany.local → Domaines → Stadiumcompany.local → Créer un objet GPO dans ce domaine, et le lier ici…



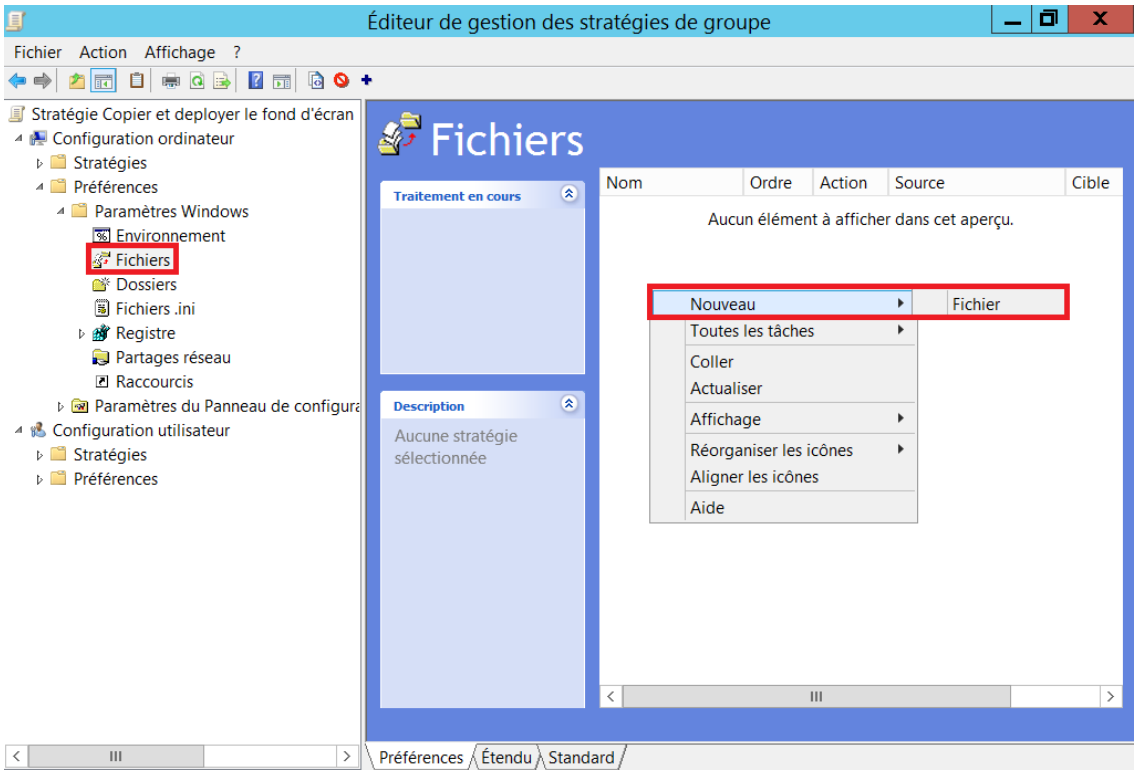
- Nommer la GPO (Copier et déployer le fond d'écran).



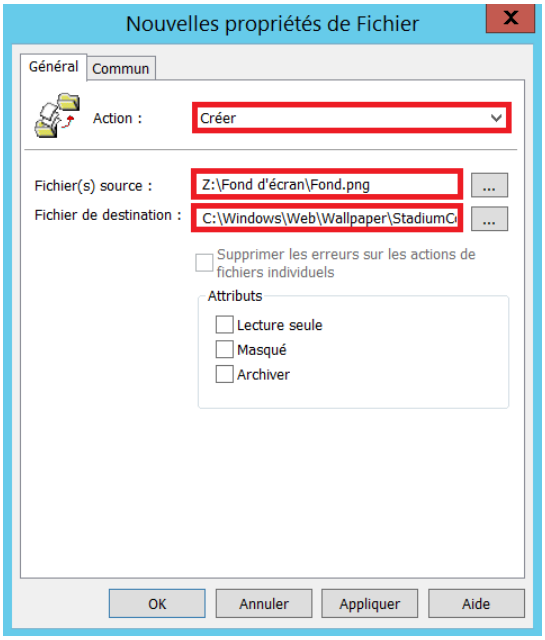
- Clic droit sur la GPO Copier et déployer le fond d'écran → Modifier…



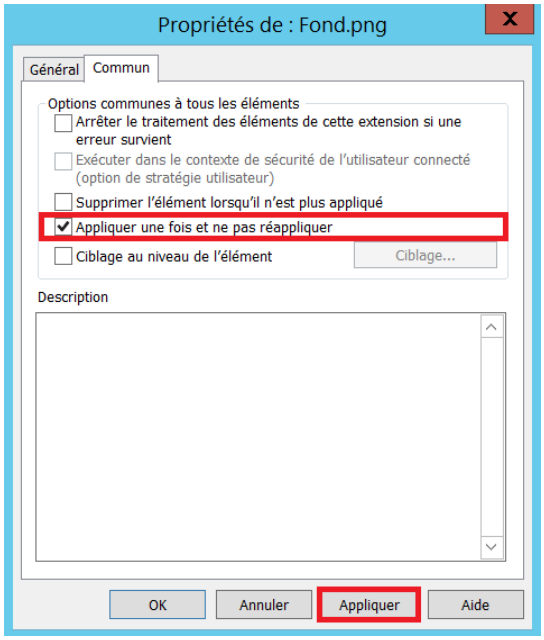
- Stratégie Copier et déployer le fond d'écran → Configuration ordinateur → Préférences → Paramètres Windows → Fichiers → Clic droit → Nouveau → Fichier



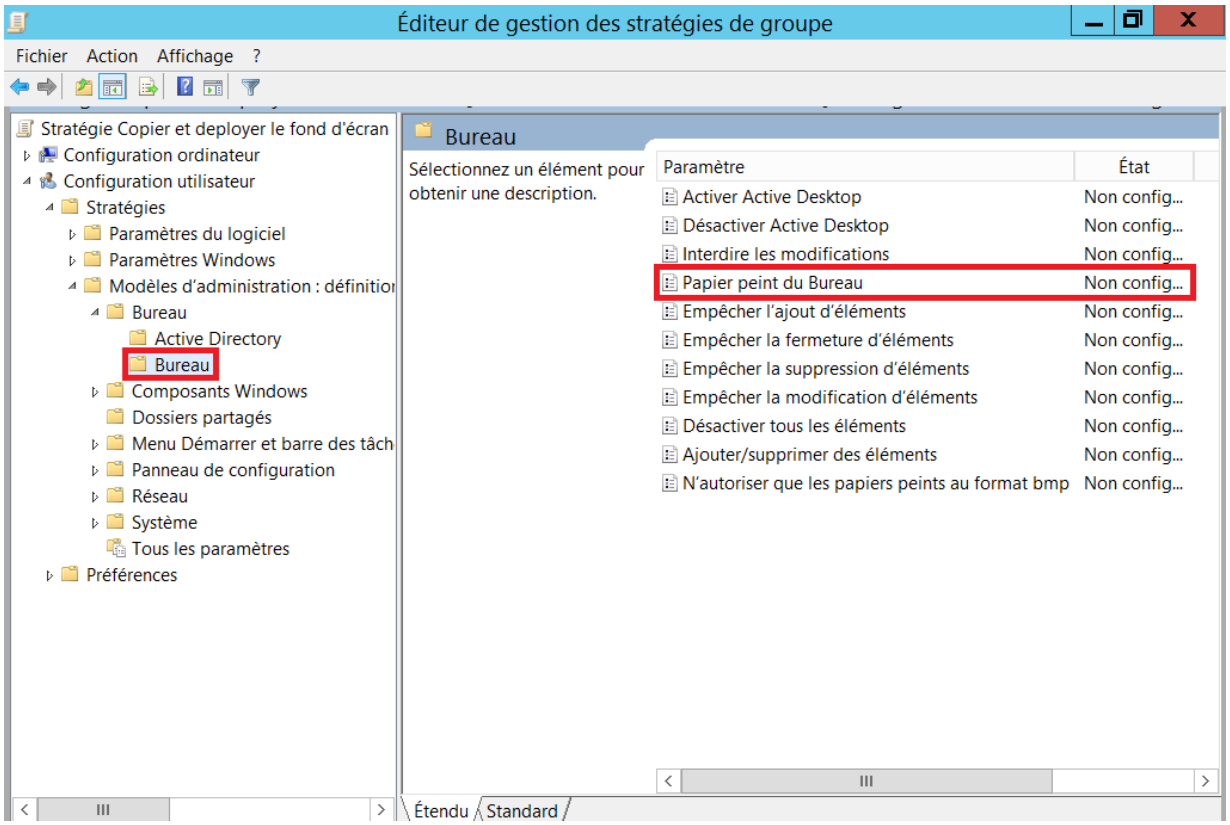
- Action → Créer (puisque ce fichier n'existe pas)
- Fichier(s) source → Z:\Fond d'écran\Fonf.png
- Fichier de destination → C:\windows\Web\Wallpaper\StadiumCompany\Fond.png
- Commun → Appliquer une fois et ne pas réappliquer



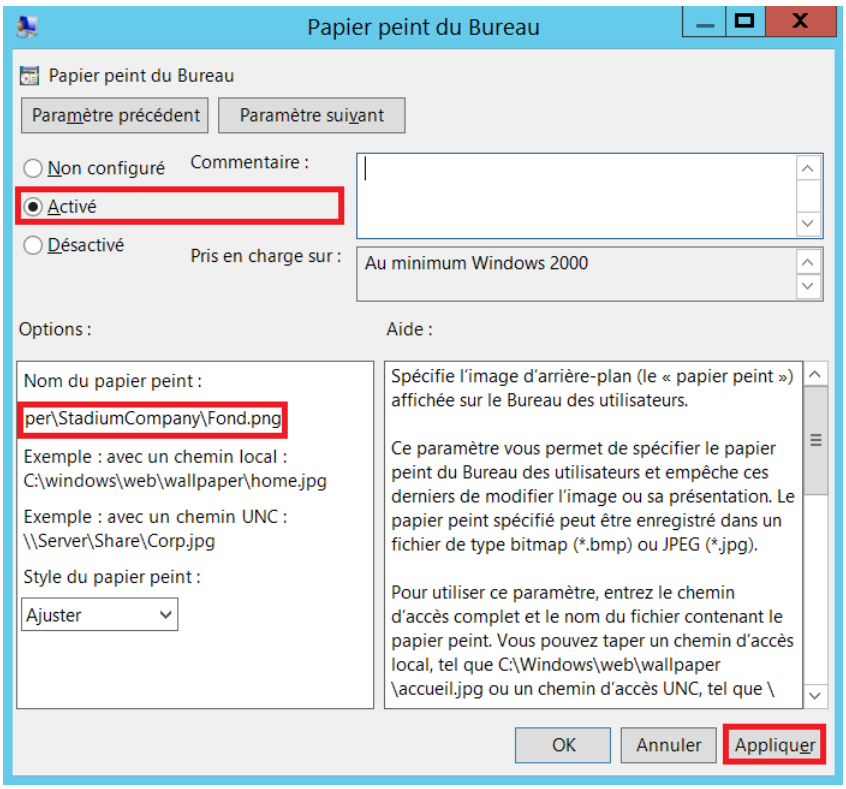
\



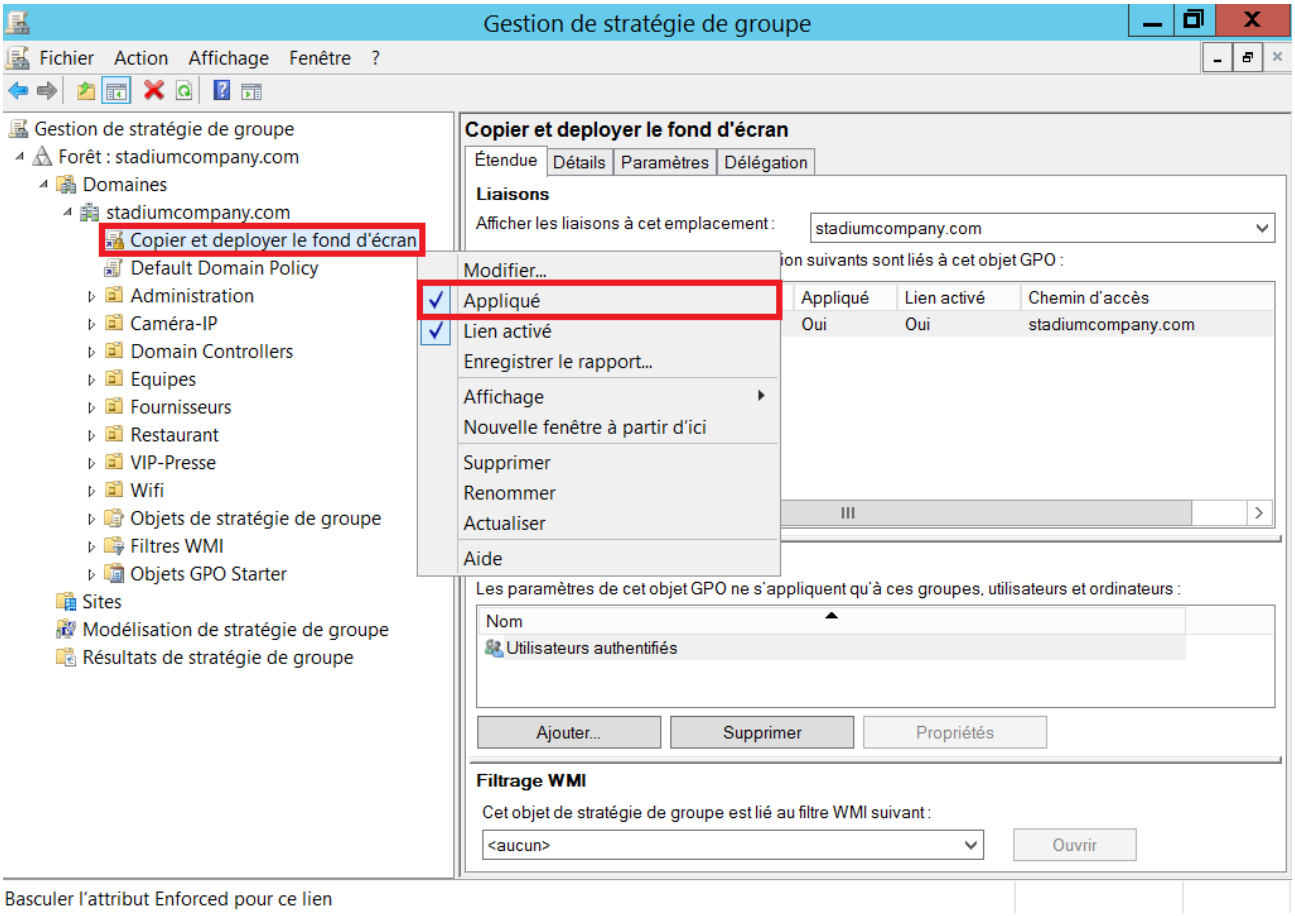
- Stratégie Copier et déployer le fond d'écran → Stratégies → Configuration utilisateur → Modèles d'administration → Bureau → Bureau → Papier peint du Bureau.



- Activé et renseigner le chemin (C:\windows\Web\Wallpaper\StadiumCompany\Fond.png)



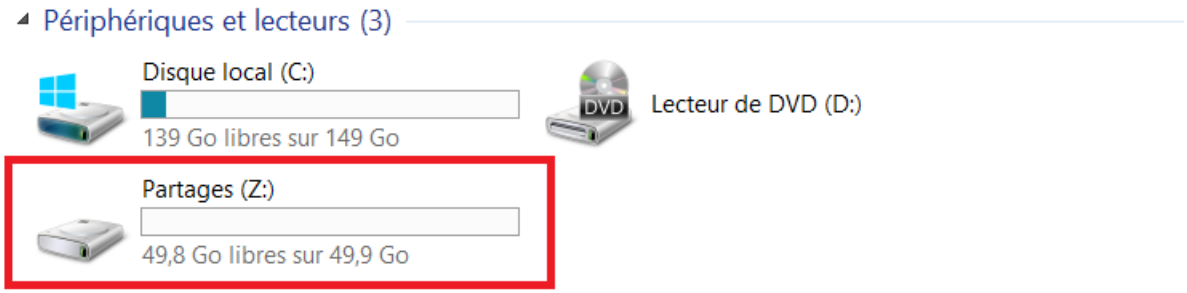
- Appliquer la GPO (clic droit sur Copier et déployer le fond d'écran → Appliqué.



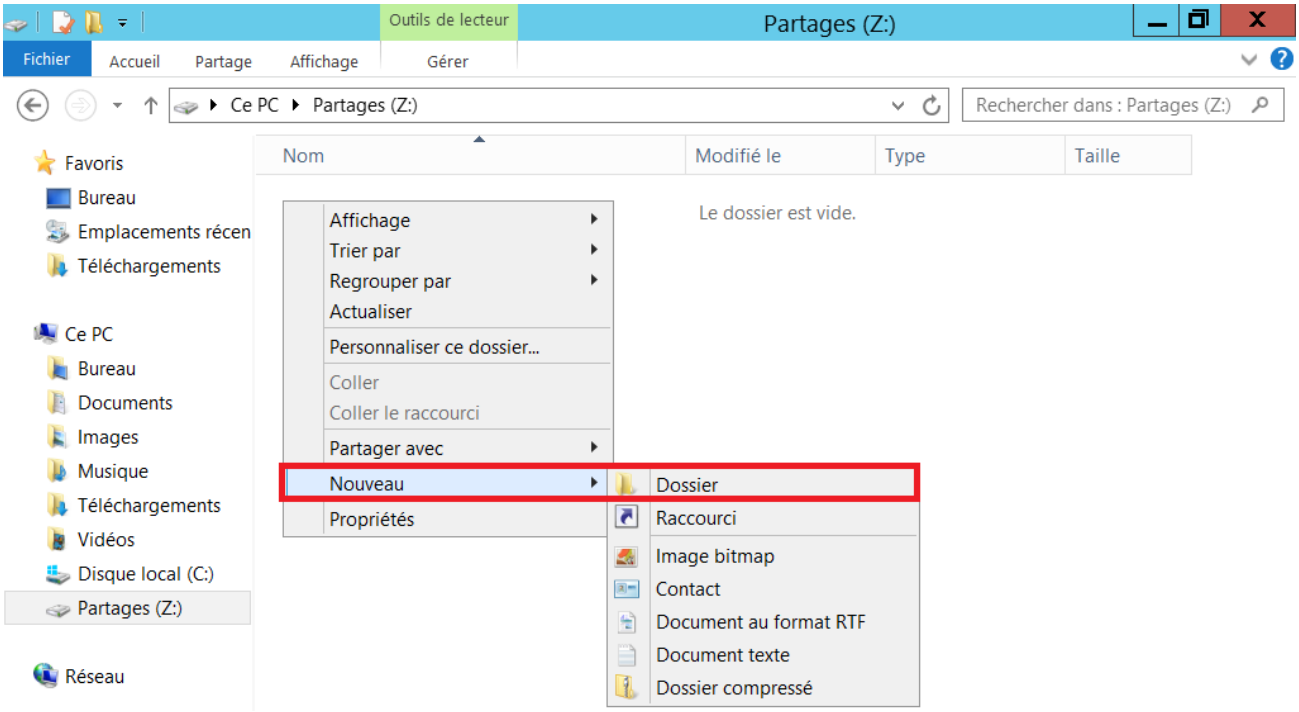
Création d'un script de démarrage permettant aux utilisateurs une connexion aux dossiers partagés

Sur le deuxième disque dur nous allons créer un dossier qui sera partagé avec tous les utilisateurs en lecture.

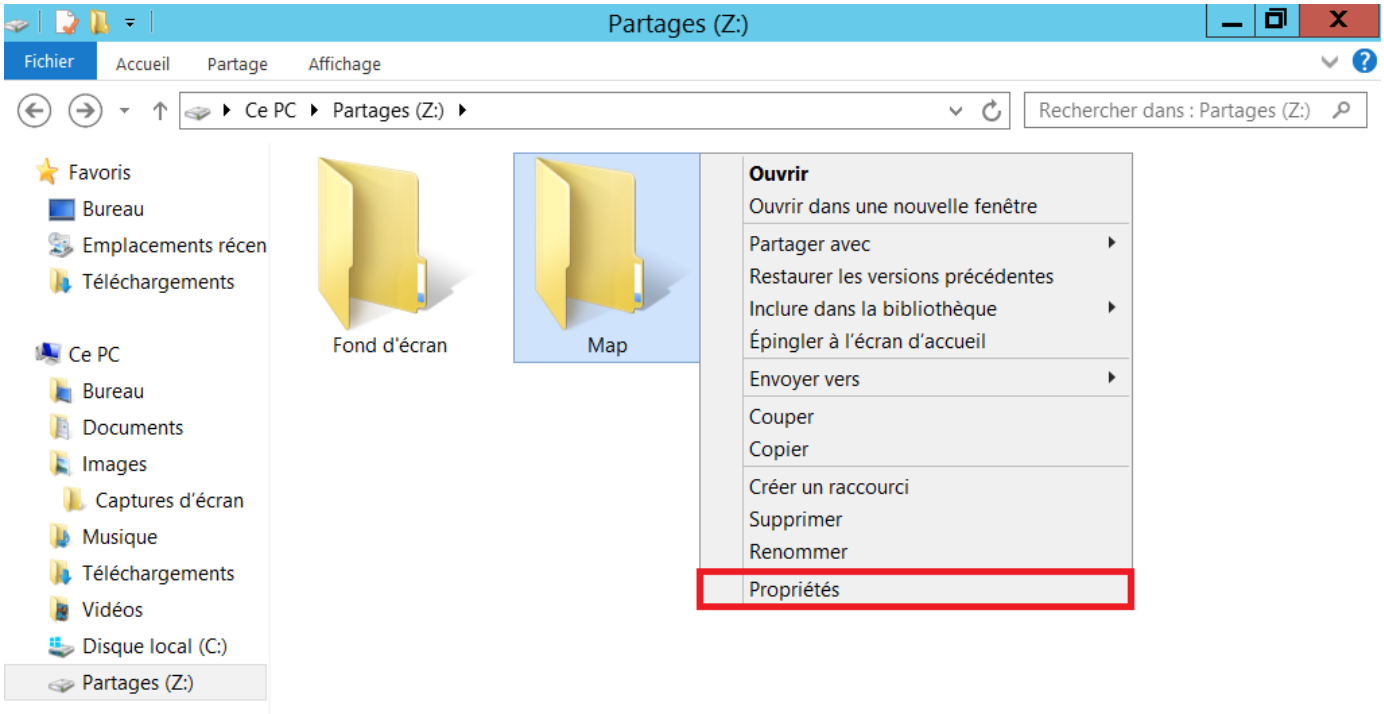
- Aller sur ordinateur → Deuxième disque (Partages Z pour moi).



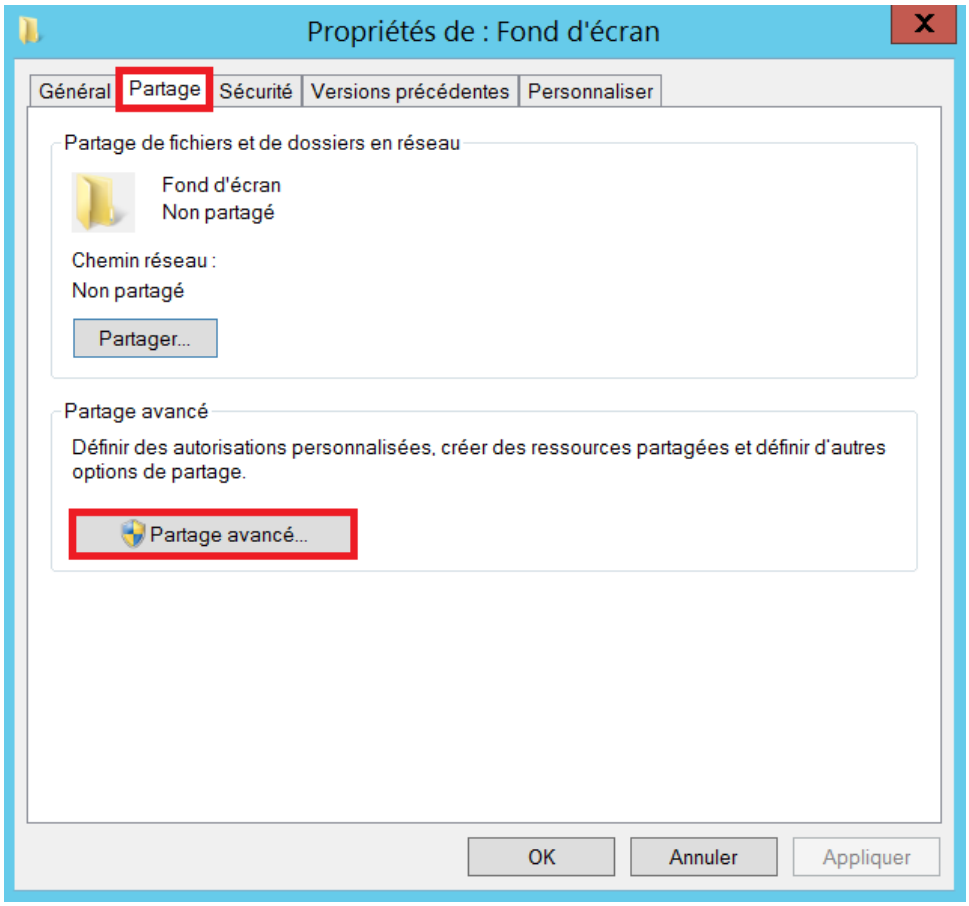
- Clic droit → Nouveau → Dossier → Nommer le (Map).



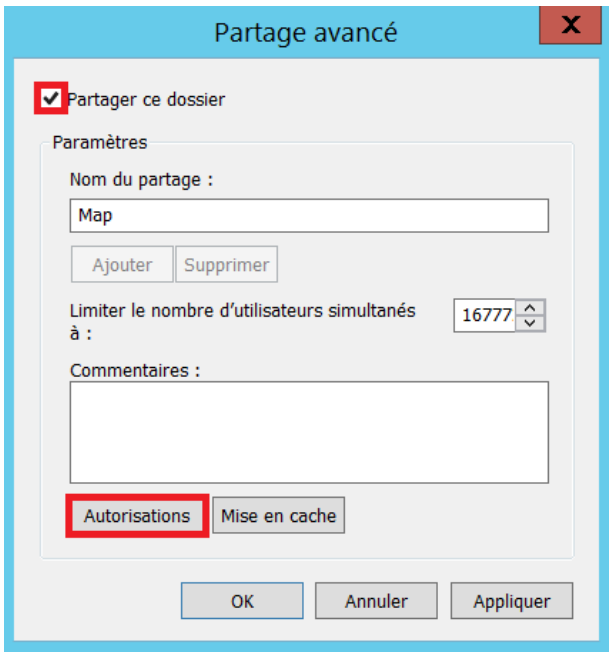
- Clic droit sur le dossier Map → Propriétés.

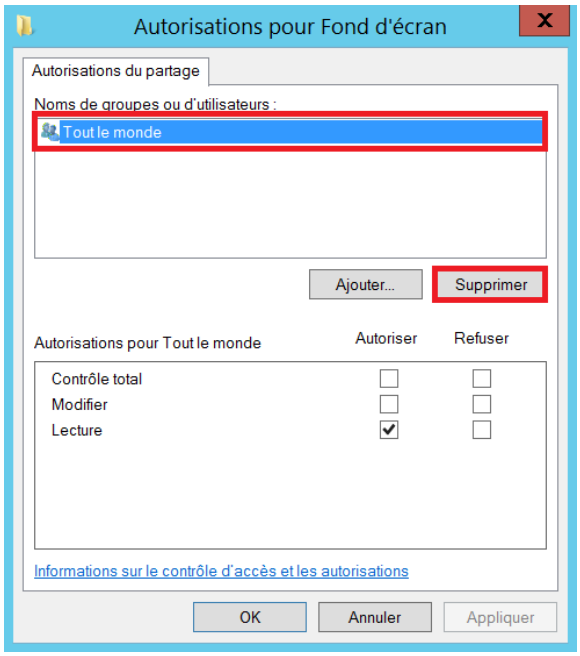


- Dans l'onglet partage → Partage avancé…

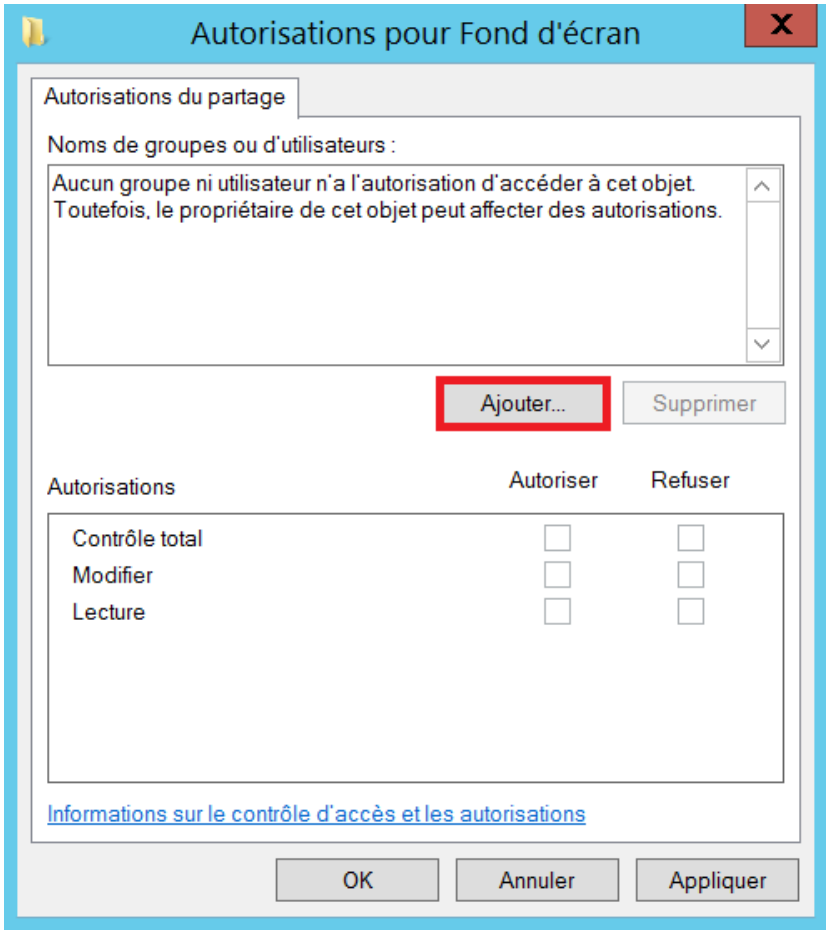


- Cocher Partager ce dossier et aller sur Autorisations → Supprimer Tout le monde.

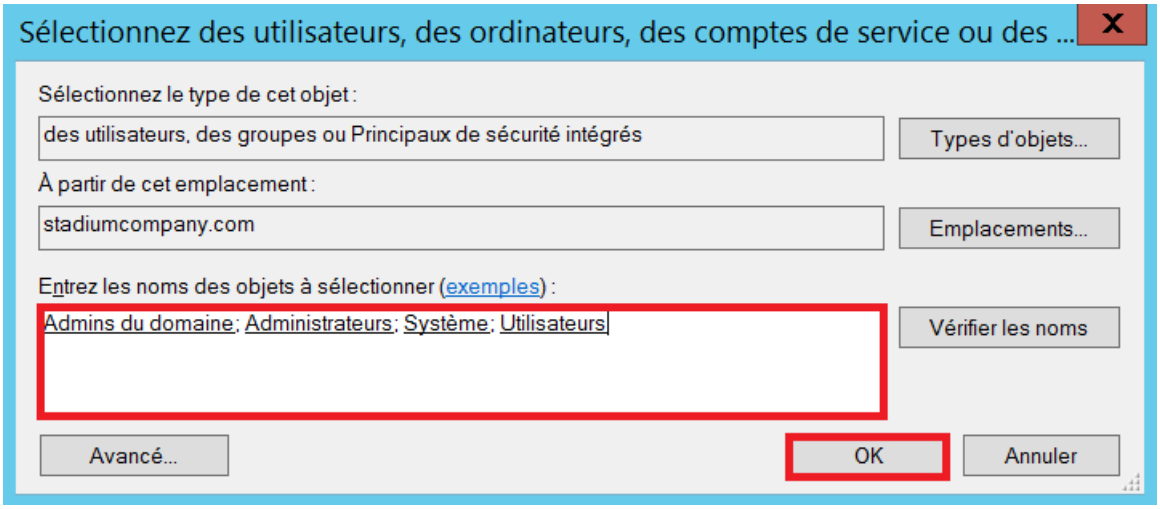




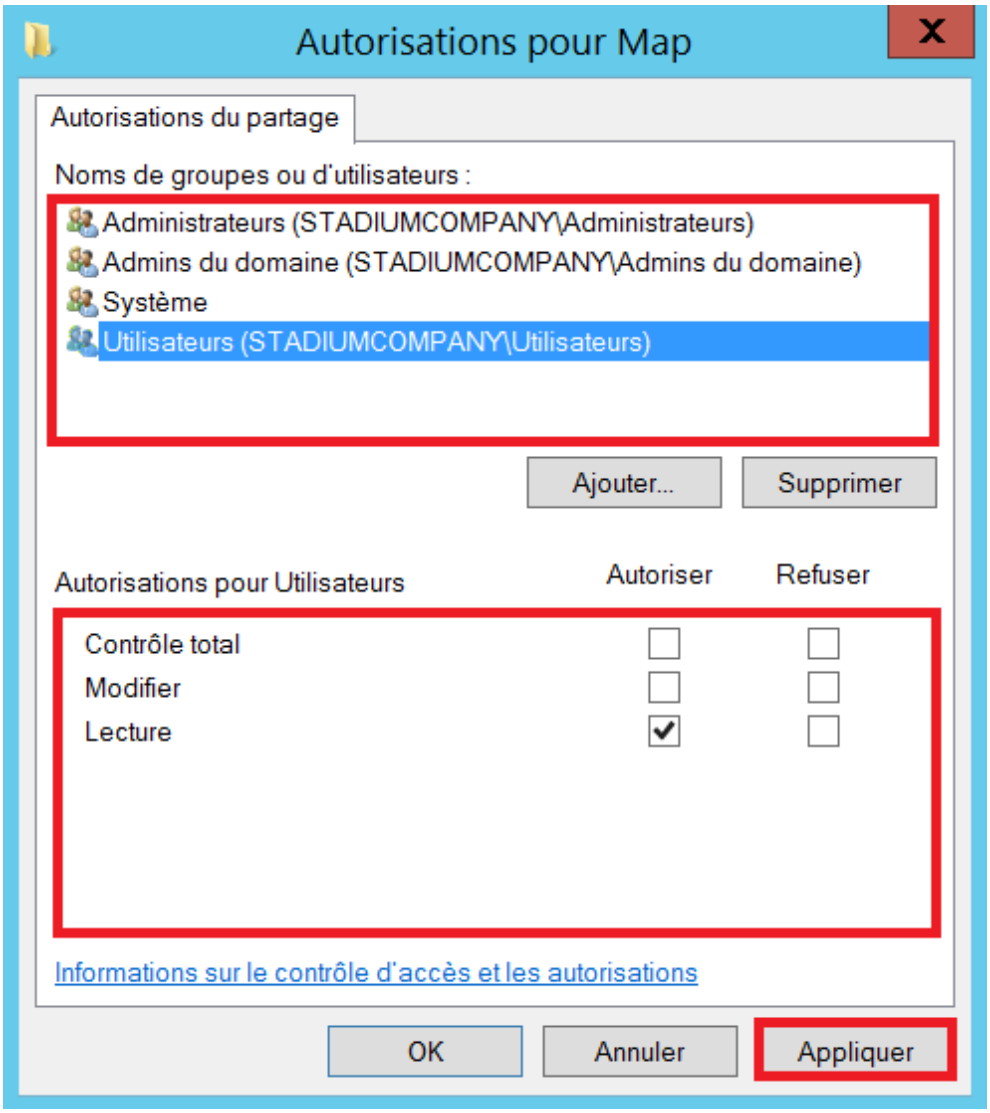
- Aller sur Ajouter…



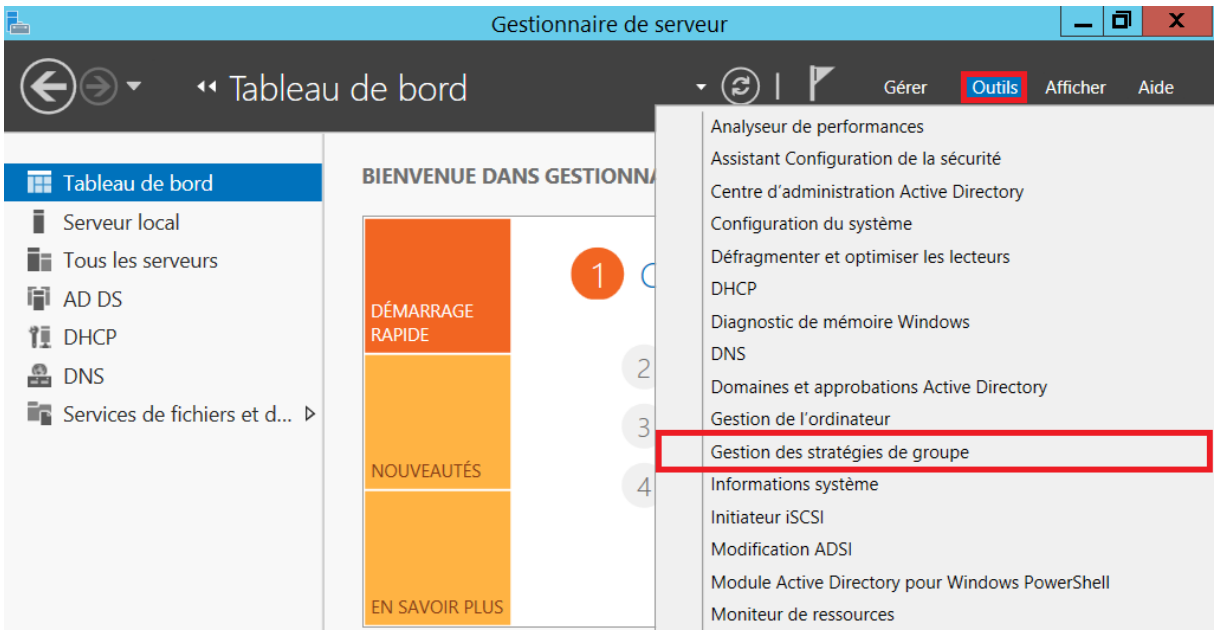
- Ajouter : Admins du domaine ; Administrateurs ; Système ; Utilisateurs



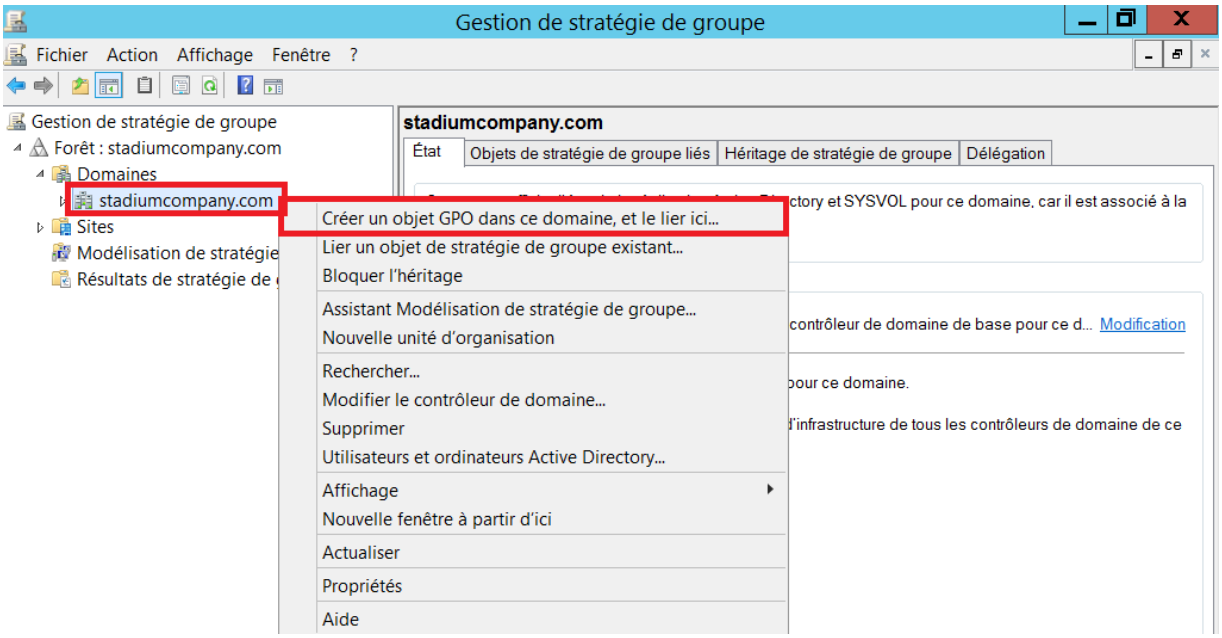
- Ajouter les Autorisation :
  - Contrôle total pour Admins du domaine
  - Modification pour Administrateurs
  - Lecture pour Utilisateurs et Système



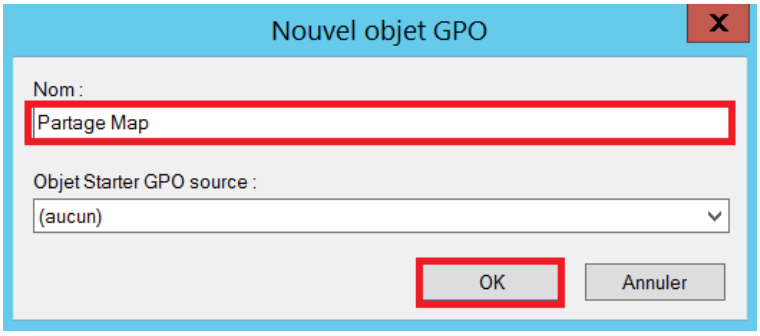
- Gestionnaire de serveur → Outils → Gestion des stratégies de groupe.



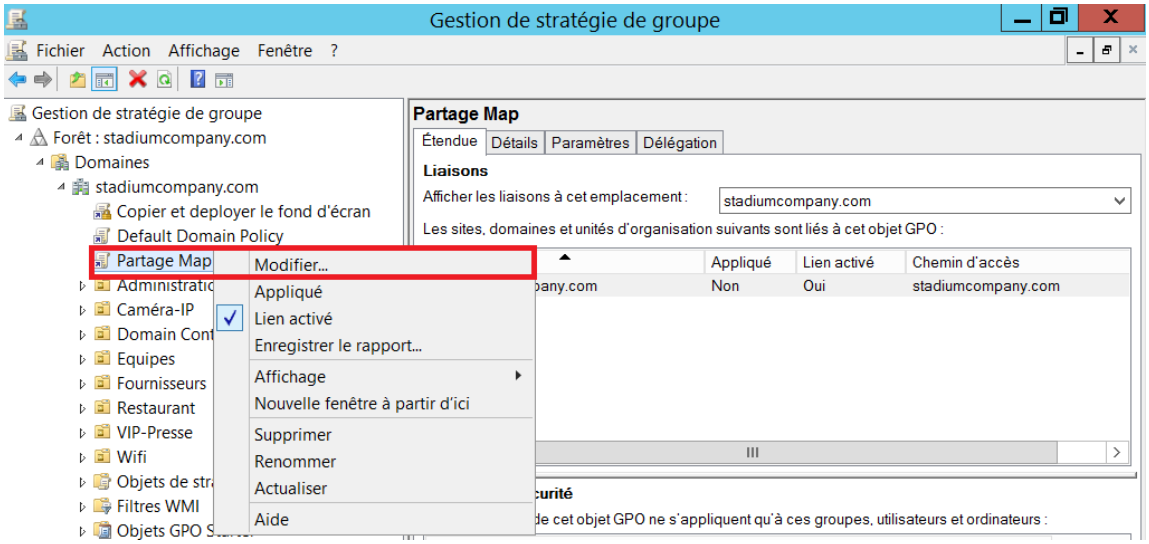
- Gestion de Stratégie de groupe → Forêt : stadiumcompany.local → Domaines → Stadiumcompany.local → Créer un objet GPO dans ce domaine, et le lier ici…



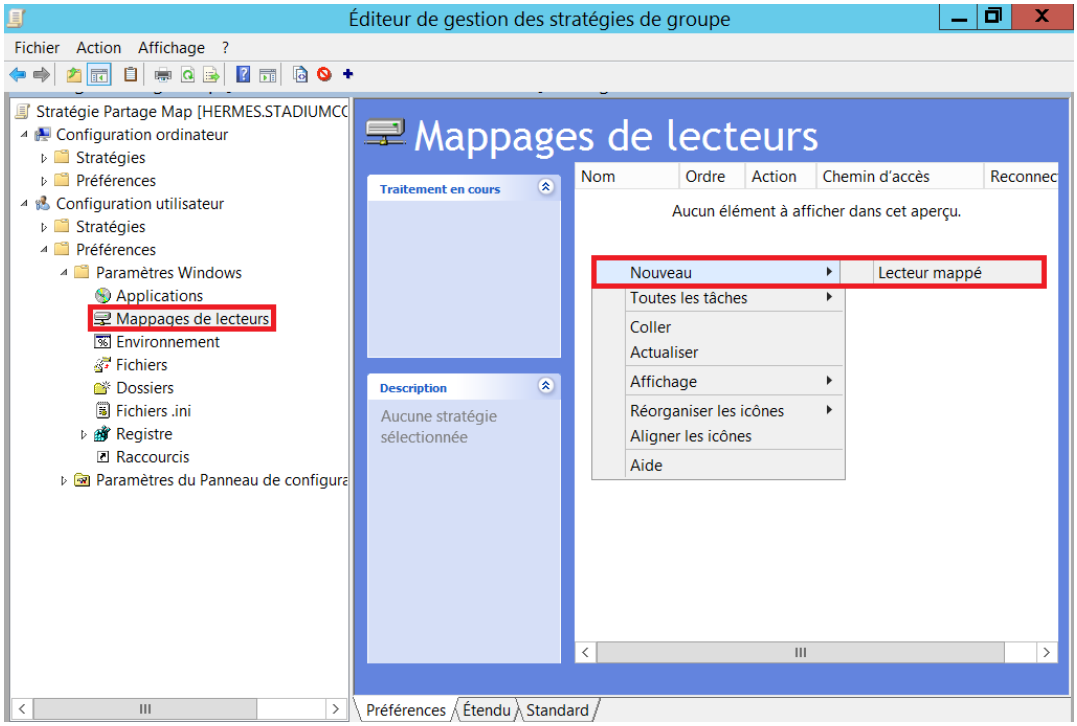
- Nommer la GPO (Partage Map).



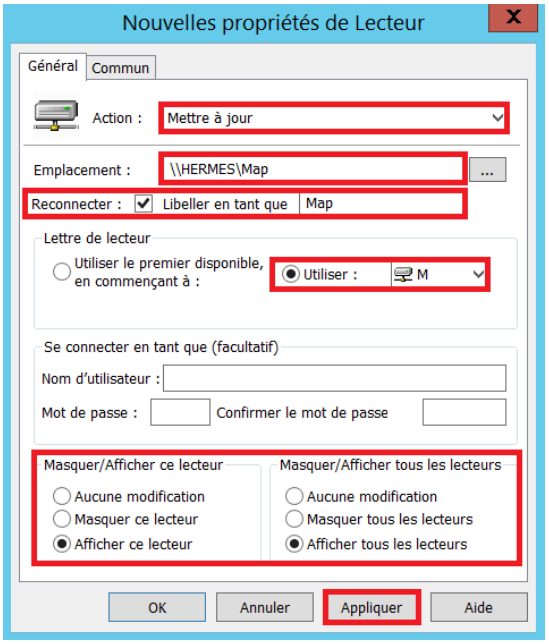
- Clic droit sur la GPO Copier et déployer le fond d'écran → Modifier…



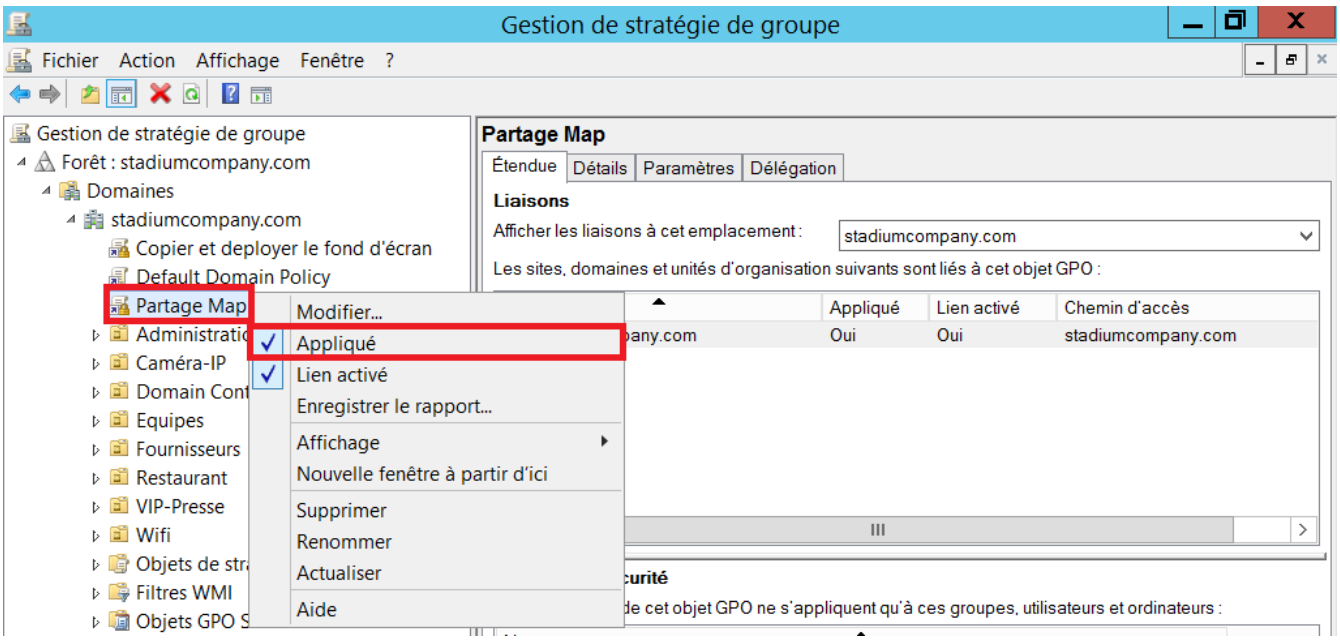
- Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs → Clic droit → Nouveau → Lecteur Mappé.



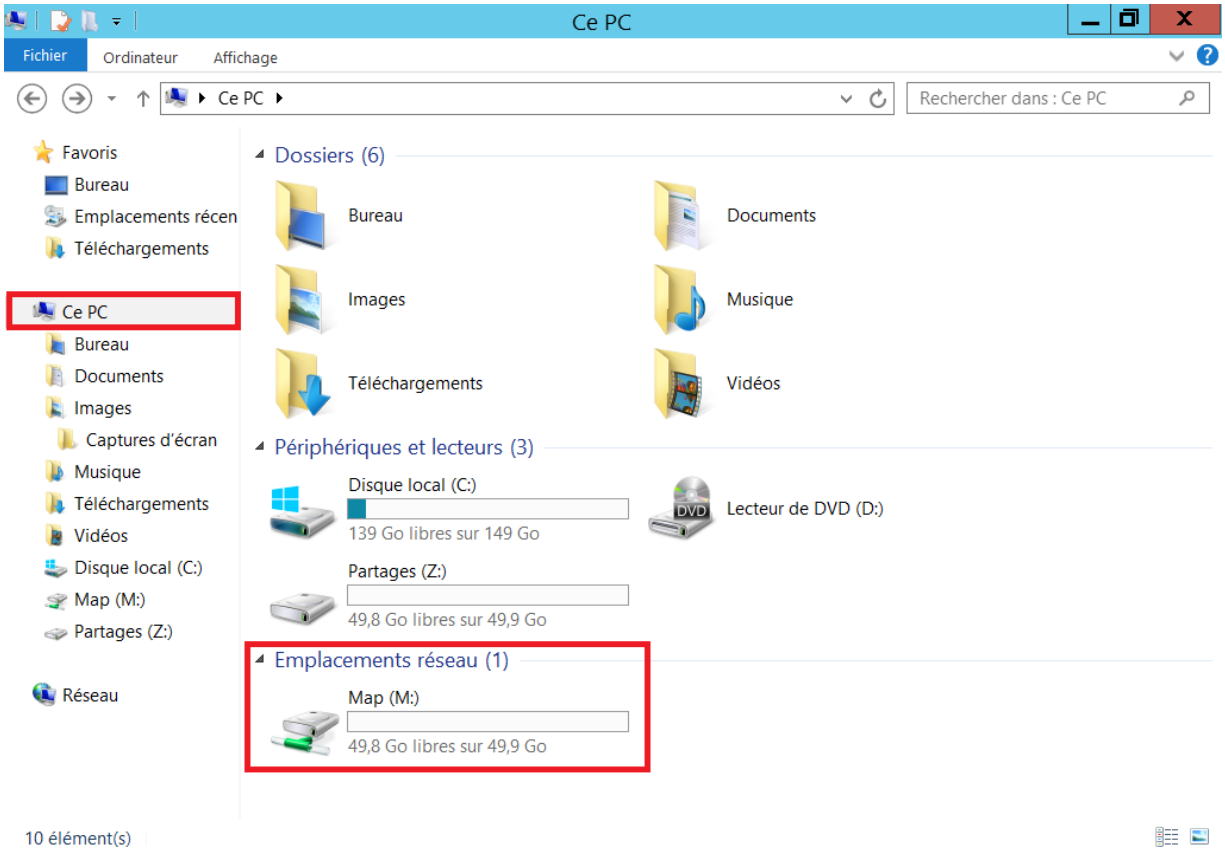
- Action → Mettre à jour
- Emplacement → \\HERMES\Map
- Libeller → Map
- Lettre de lecteur → M
- Afficher ce lecteur et Afficher tous les lecteurs



- Appliquer la GPO (clic droit sur Partage Map) → Appliqué.

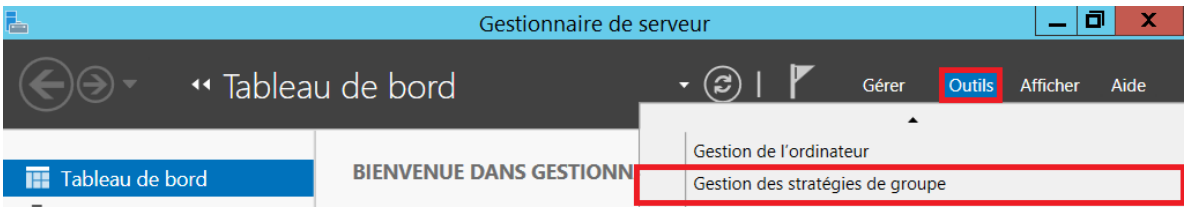


- Map (M :) est bien présent dans ordinateur.

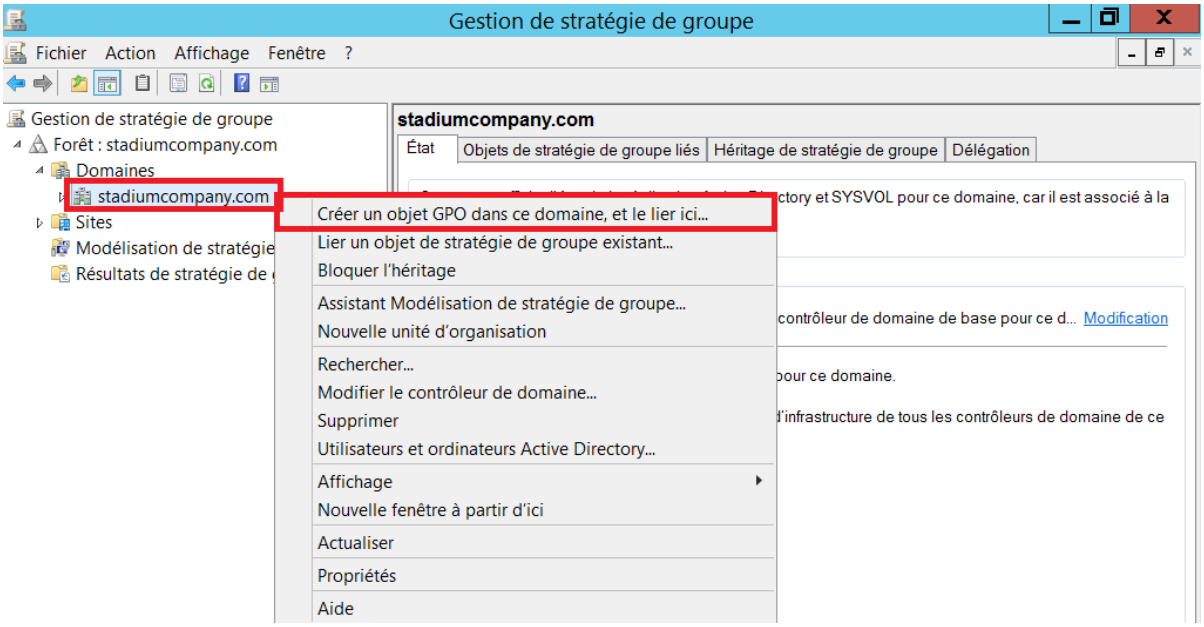


Empêcher l'accès au panneau de configuration

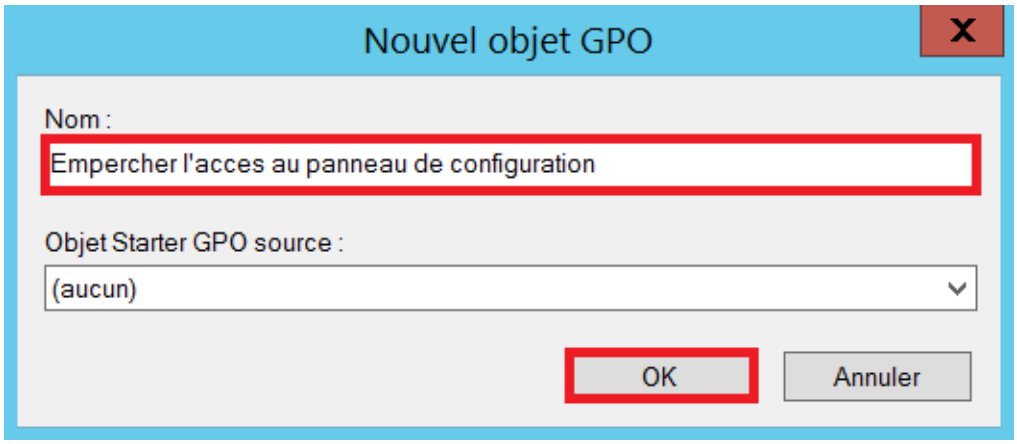
- Gestionnaire de serveur → Outils → Gestion des stratégies de groupe.



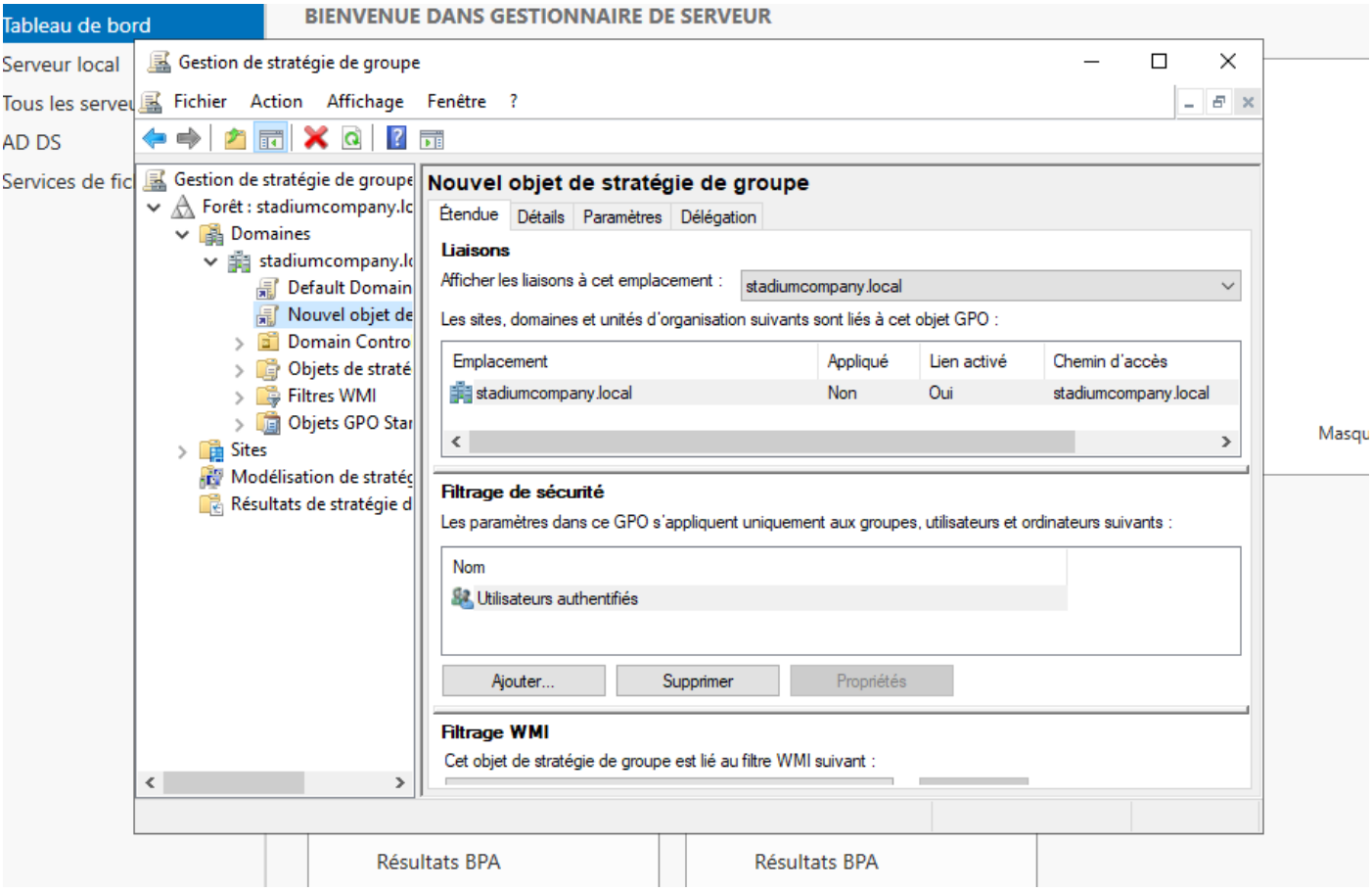
- Gestion de Stratégie de groupe → Forêt : stadiumcompany.local → Domaines → Stadiumcompany.local → Créer un objet GPO dans ce domaine, et le lier ici…



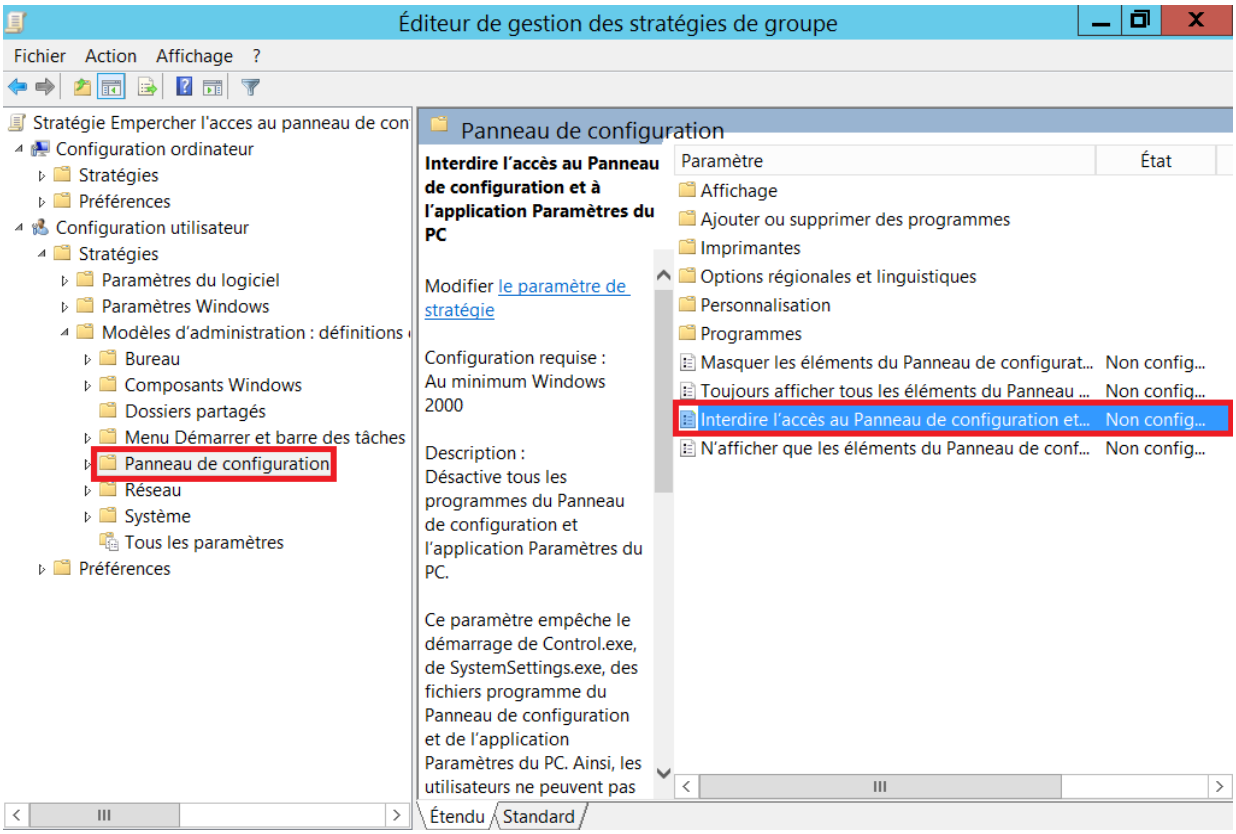
- Nommer la GPO (Empêcher l'accès au panneau de configuration).



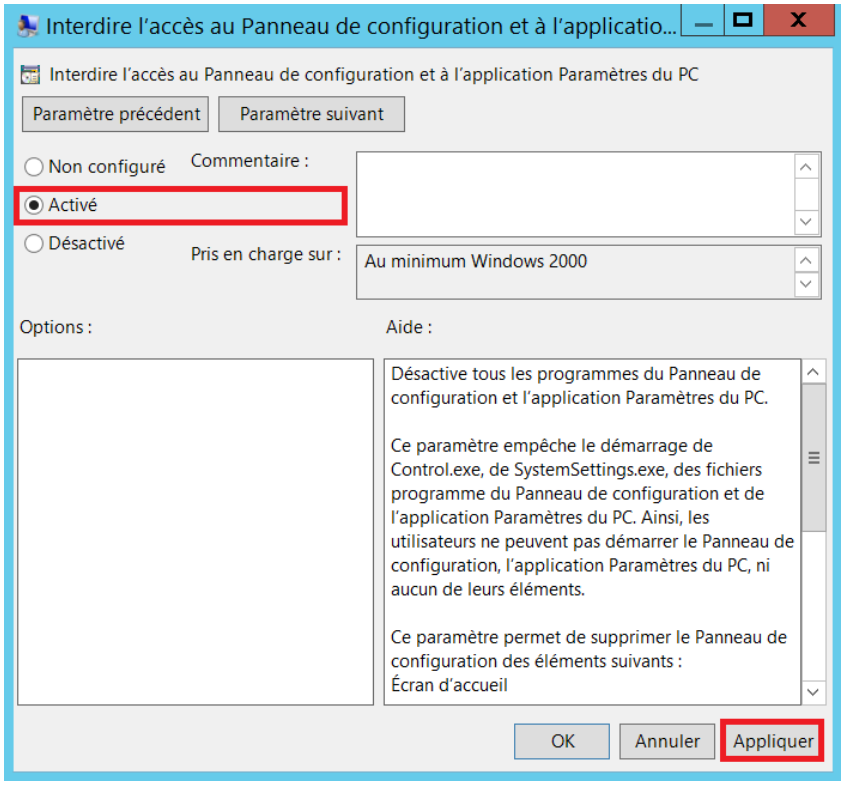
- Clic droit sur la GPO Empêcher l'accès au panneau de configuration → Modifier…



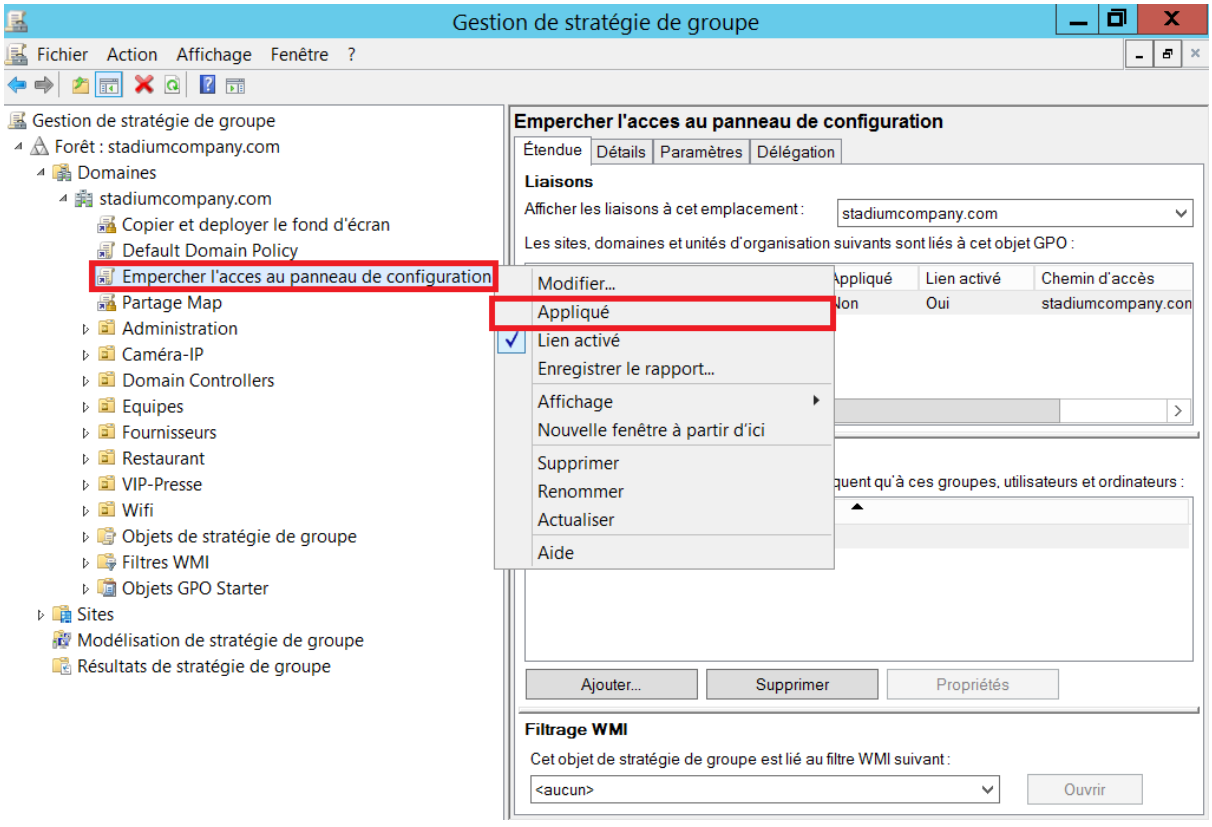
- Stratégie Empêcher l'accès au panneau de configuration → Configuration utilisateurs → stratégies → Modèles d'administration → Panneau de configuration → Interdire l'accès au Panneau de configuration et à l'application paramètre du PC.


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie Empercher l'acces au panneau de con
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Modèles d'administration : définitions
Bureau
Composants Windows
Dossiers partagés
Menu Démarrer et barre des tâches
Panneau de configuration
Réseau
Système
Tous les paramètres
Préférences
Panneau de configuration
Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC
Modifier le paramètre de stratégie
Configuration requise : Au minimum Windows 2000
Description : Désactive tous les programmes du Panneau de configuration et l'application Paramètres du PC.
Ce paramètre empêche le démarrage de Control.exe, de SystemSettings.exe, des fichiers programme du Panneau de configuration et de l'application Paramètres du PC. Ainsi, les utilisateurs ne peuvent pas
Paramètre
État
Affichage
Ajouter ou supprimer des programmes
Imprimantes
Options régionales et linguistiques
Personnalisation
Programmes
Masquer les éléments du Panneau de configurat...
Non config...
Toujours afficher tous les éléments du Panneau ...
Non config...
Interdire l'accès au Panneau de configuration et...
Non config...
N'afficher que les éléments du Panneau de conf...
Non config...
Étendu
Standard

- Activé et Appliquer

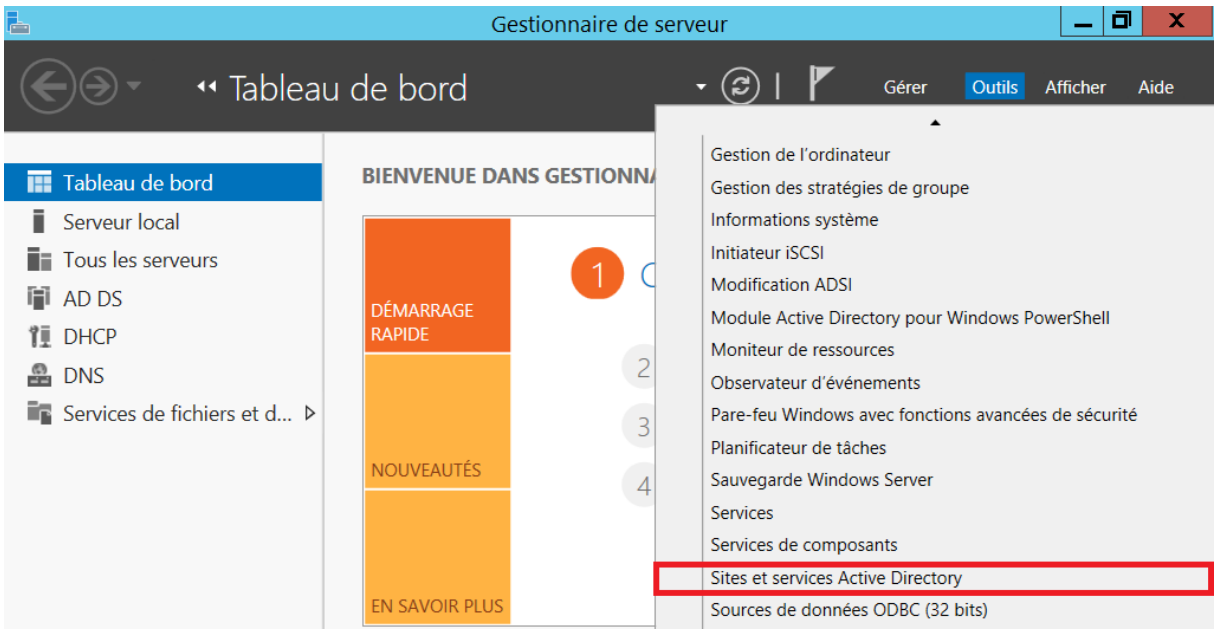


- Appliquer la GPO (clic droit sur Empêcher l'accès au panneau de configuration) → Appliqué

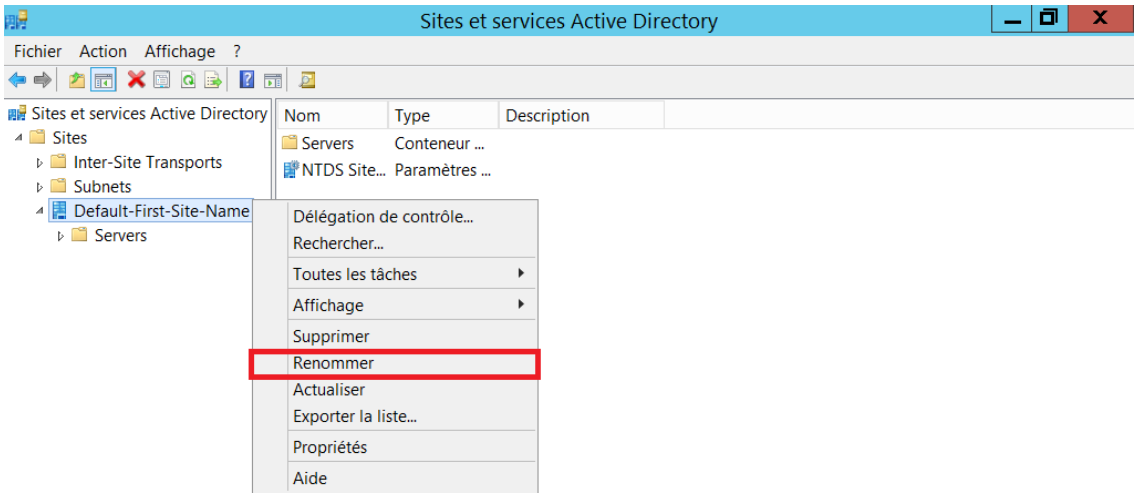


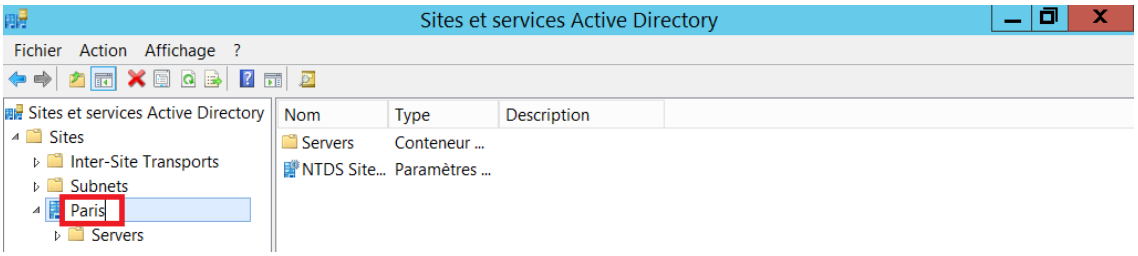
Création du Site de Paris

- Gestionnaire de serveur → Outils → Sites et service Active Directory.

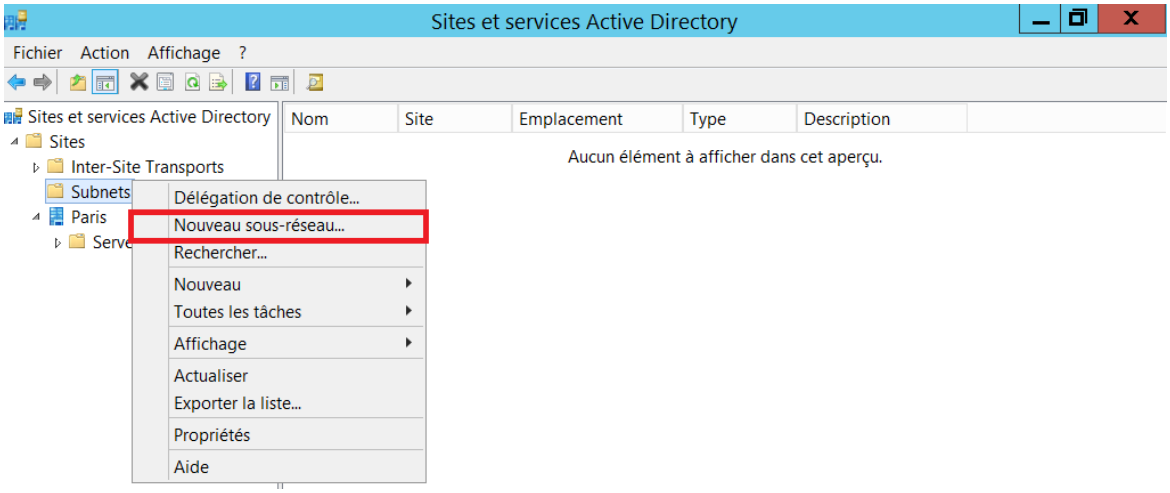


- Sites et services Active Directory → Sites → Clic droit sur Default-First-Site-Name → Renommer (Paris).





- Sites et services Active Directory → Sites → Clic droit sur Subnets → Nouveau sous-réseau…



- Préfixe : 172.20.0.0/24 et sélectionner PARIS.