

## **Administration & Gestion des accès utilisateurs de l'infrastructure de STADIUM Company (AD,DNS,DHCP)**

### **Description du contexte de la mission :**

-Stadiumcompany est une société qui gère l'administration et la gestion des stades. Elle fait appel à Networking company pour mettre en place une infrastructure réseau qui répondras aux besoins du cahier de charges.

### **Ressources et outils utilisés :**

- *Windows serveur 2019*

- *VmWare*

-*pc dell*

### **Résultat attendu :**

-L'Implémentation et la configuration d'une solution pour que les utilisateurs soient authentifiés via le serveur Active Directory du domaine stadiumcompany.com. Il est configuré en regroupant les utilisateurs par service. Les UO suivantes sont présentes sur le serveur : Admin, WiFi, .....

### **Contraintes :**

- X Postes pour les employés

- Le site de stade dispose d'un service Active Directory, d'un service DHCP, et d'un DNS primaire sur une machine sous Windows 2019 Server. Celle-ci permet aussi le stockage des fichiers utilisateurs. Un serveur RSync et DNS Secondaire sous Linux Debian.

Extrait d'une GPO : service équipes → gpo\_equipes

- L'accès au panneau de configuration, aux paramètres réseau est interdit

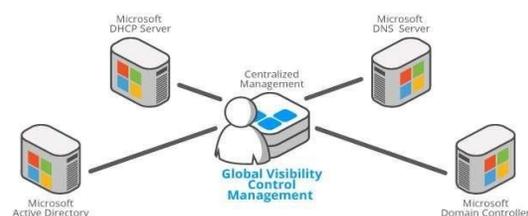
- Un script de démarrage Equipesstart.bat permet la connexion des lecteurs réseaux accédant aux dossiers partagés.

- Les utilisateurs démarrent avec un bureau imposé (barre de menu, fond d'écran...

**DNS** : Les serveurs DNS sont configurés pour résoudre la zone directe stadiumcompany.com et la zone inverse du 172.20.0.10 Le serveur primaire est hébergé sur une machine Windows 2012 Server et le DNS secondaire sur une Linux Debian.

**DHCP** : Une plage est définie sur le 172.20.0.10 avec des options de routeur renvoyant vers la passerelle/pare-feu IPCOP. Les serveurs DNS sont aussi transmis via les options DHCP.

### Installation d'Active Directory, du DNS et du DHCP :

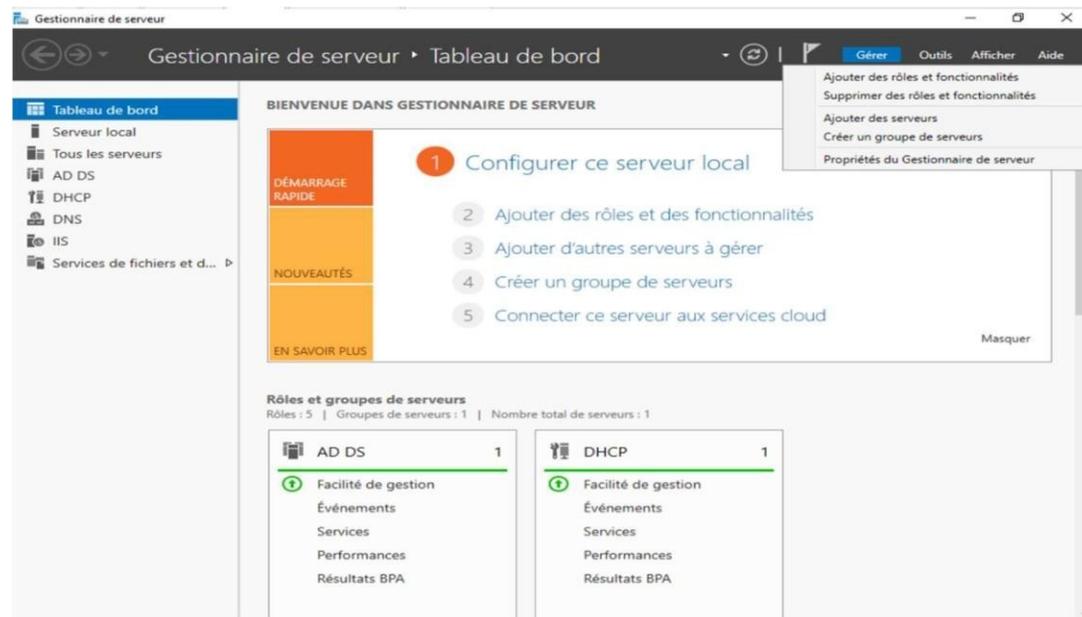


### Définition :

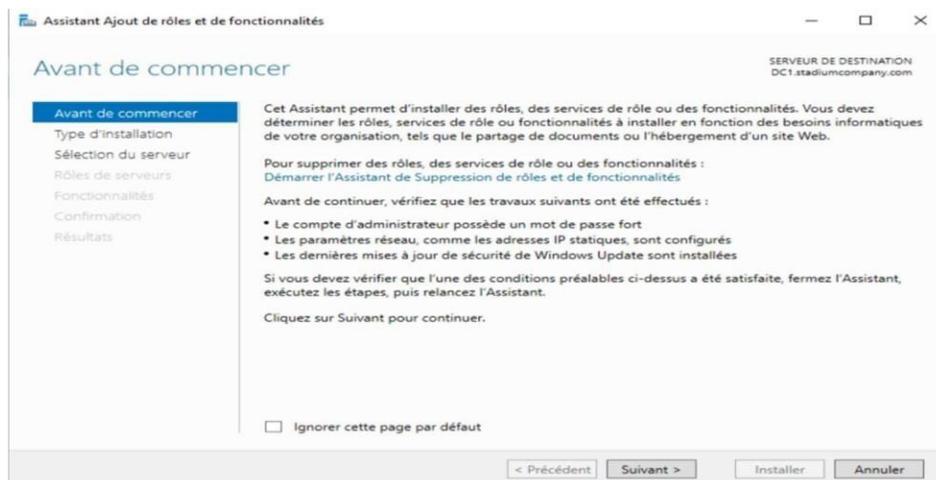
- Active Directory est un service annuaire LDAP mis en place par Microsoft pour les machines Windows Serveur. Il permet d'administrer des ressources telles que les ordinateurs, des dossiers de partages, mais aussi des comptes utilisateurs par l'intermédiaire d'un système d'Identification/Authentication. 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.
- Un serveur DHCP (ou service DHCP) est un serveur qui délivre des adresses IP aux ordinateurs qui se connectent sur le réseau.
- Le système DNS d'Internet fonctionne comme un annuaire téléphonique en gérant le mappage entre les noms et les numéros. Un serveur DNS (ou système DNS) traduit les demandes de noms e adresses IP en contrôlant à quel serveur un utilisateur va se connecter quand il tapera un nom de domaine dans son navigateur. Ces demandes sont appelées requêtes.

## Installation des rôles AD, DNS, DHCP :

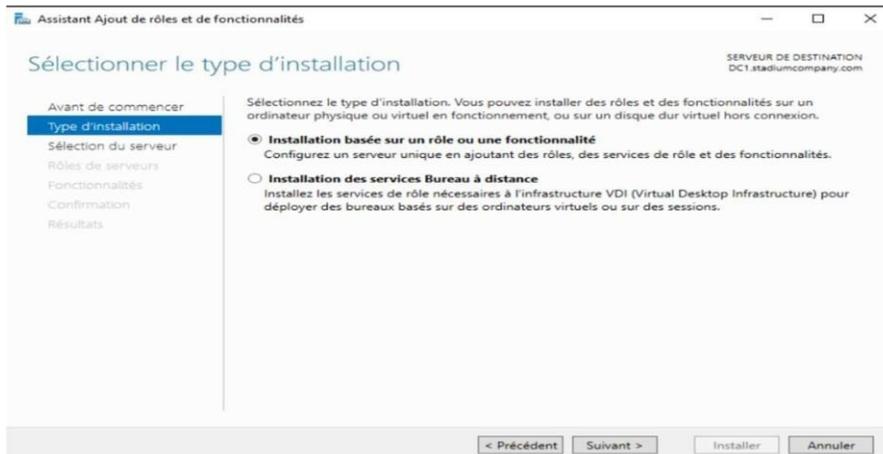
- Depuis le Gestionnaire de serveur, cliquer sur gérer puis « Ajouter des rôles et des fonctionnalités »



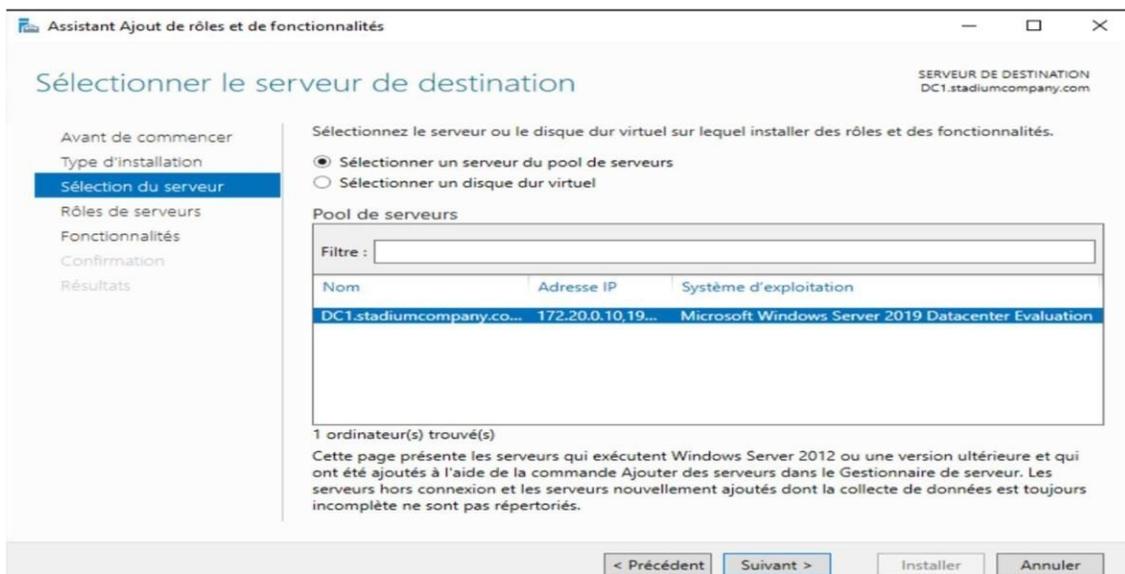
- Sur l'Assistant Ajout de rôles et de fonctionnalités, passer l'introduction avec **suivant**.



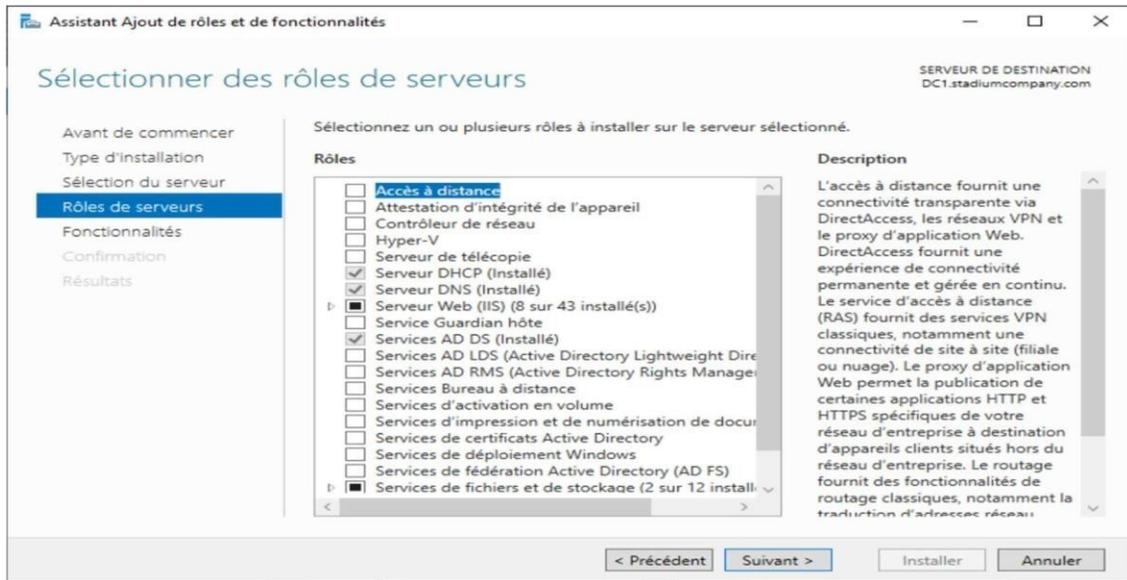
- Sélectionner le type d'installation basée sur un rôle ou une fonctionnalité.



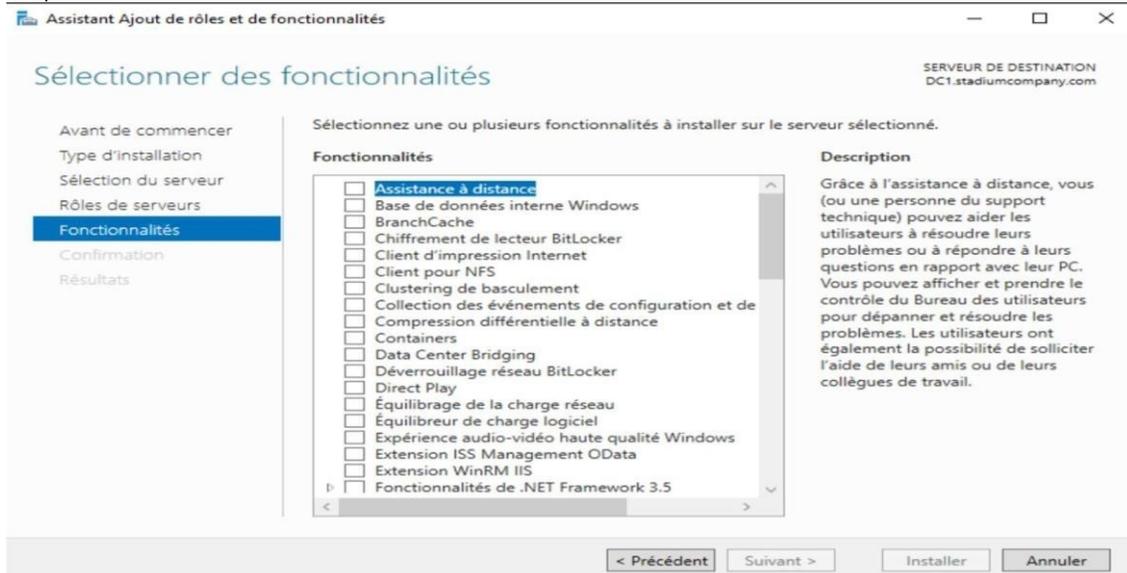
-Sélectionner son serveur pool pour installer les rôles et suivant.



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



-Ne pas sélectionner de fonctionnalités et suivant.

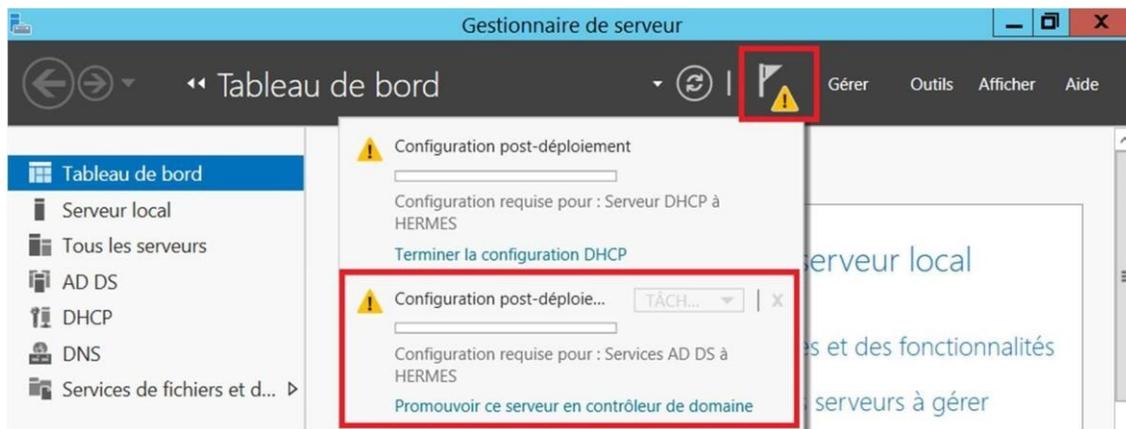


- Passer les explications du DHCP, du DNS et de l'Active Directory et suivant, après confirmer l'installation en cliquant sur installer.

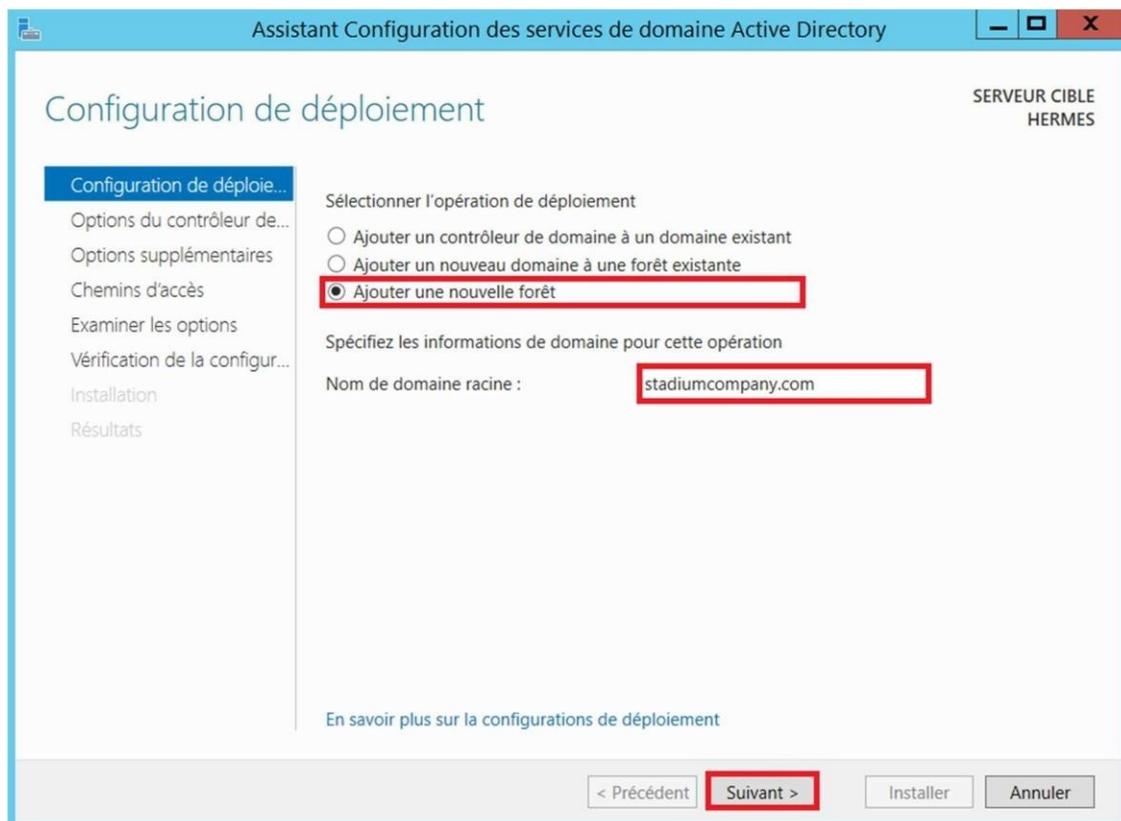
## Configuration de l'Active Directory

### Création du domaine

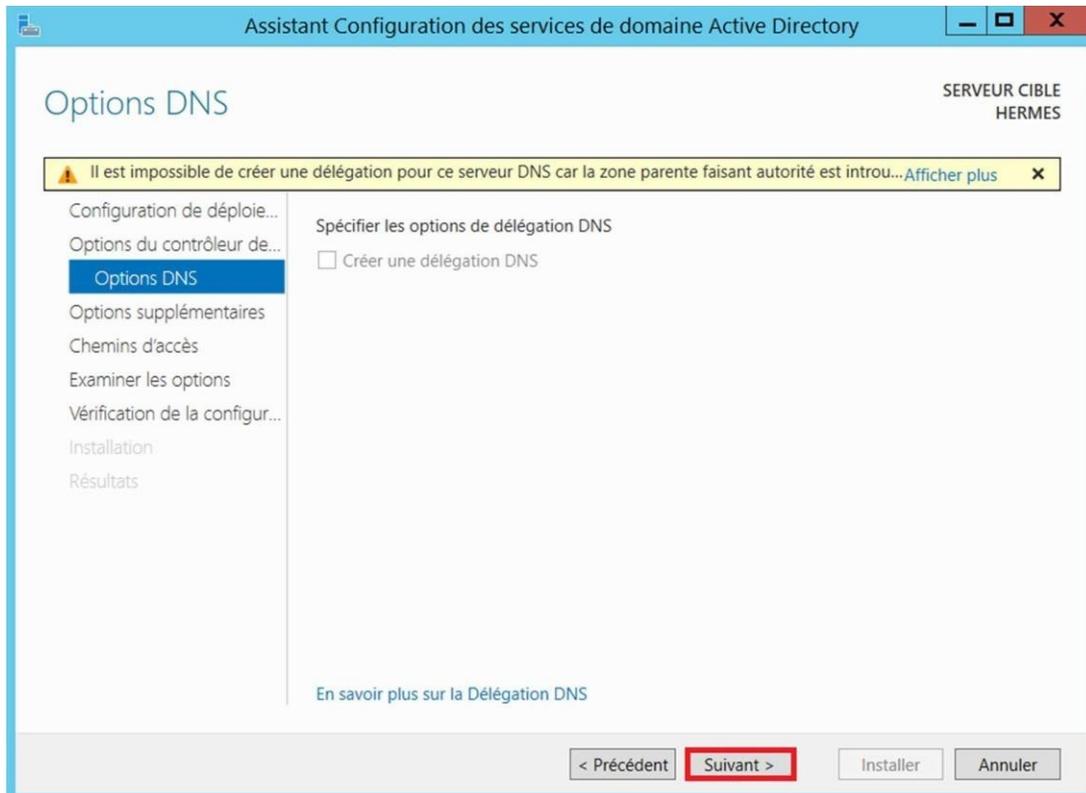
- Sur le gestionnaire de serveur, Cliquer sur le drapeau, puis cliquer sur « Promouvoir ce serveur en contrôleur de domaine ».



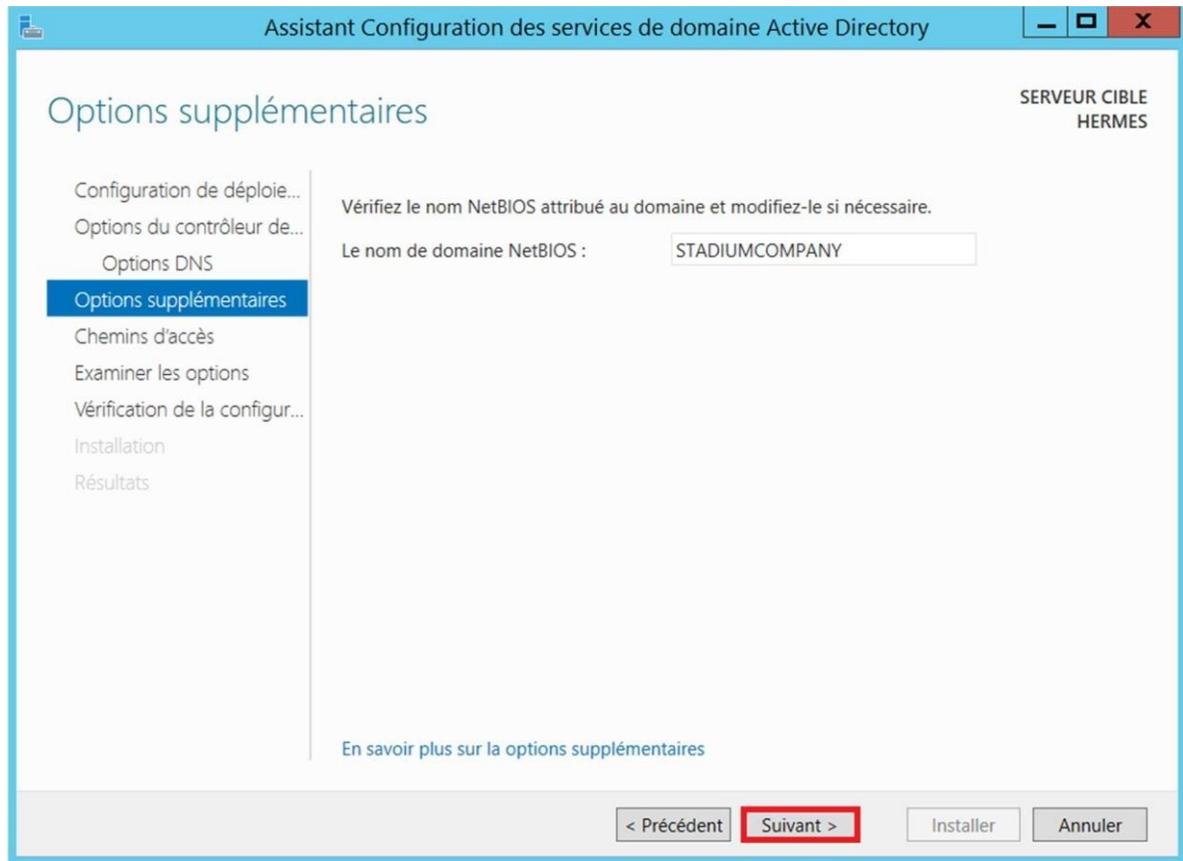
- Ajouter une nouvelle forêt, le nom de domaine est stadiumcompany.com.



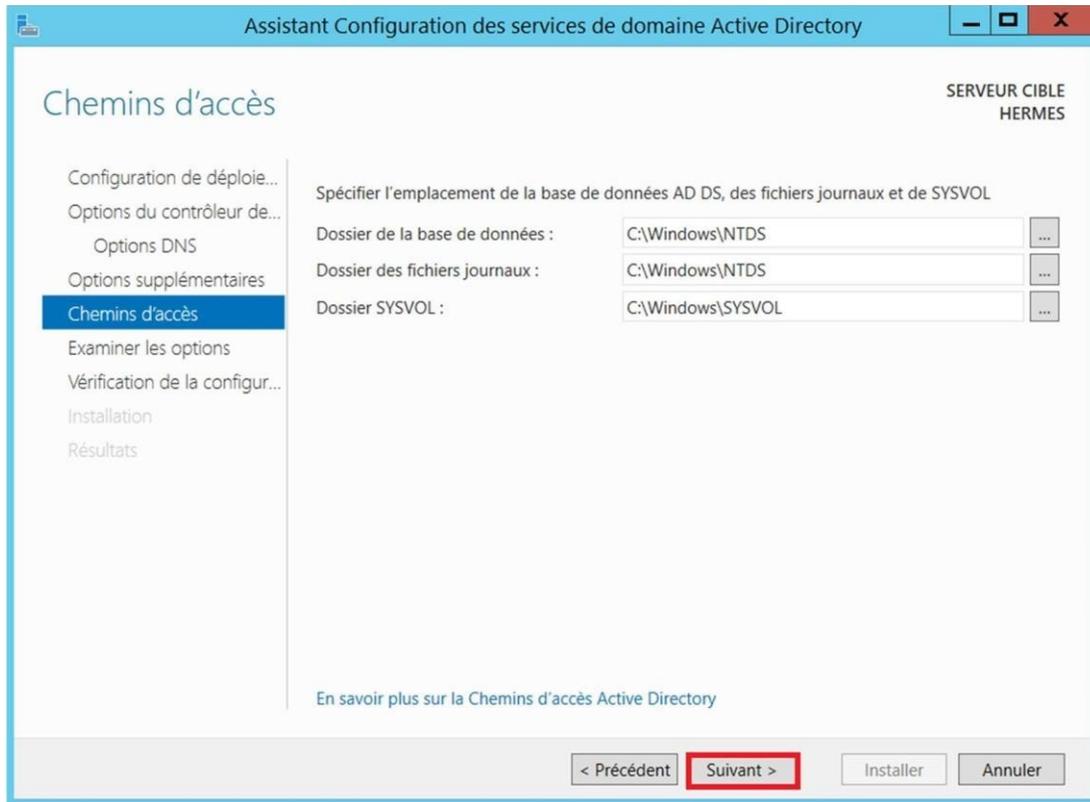
- Informer le mot de passe du domaine. Le mot de passe sera : Bts2022\$
- Passer l'option DNS car le rôle a déjà été installé, faire suivant.



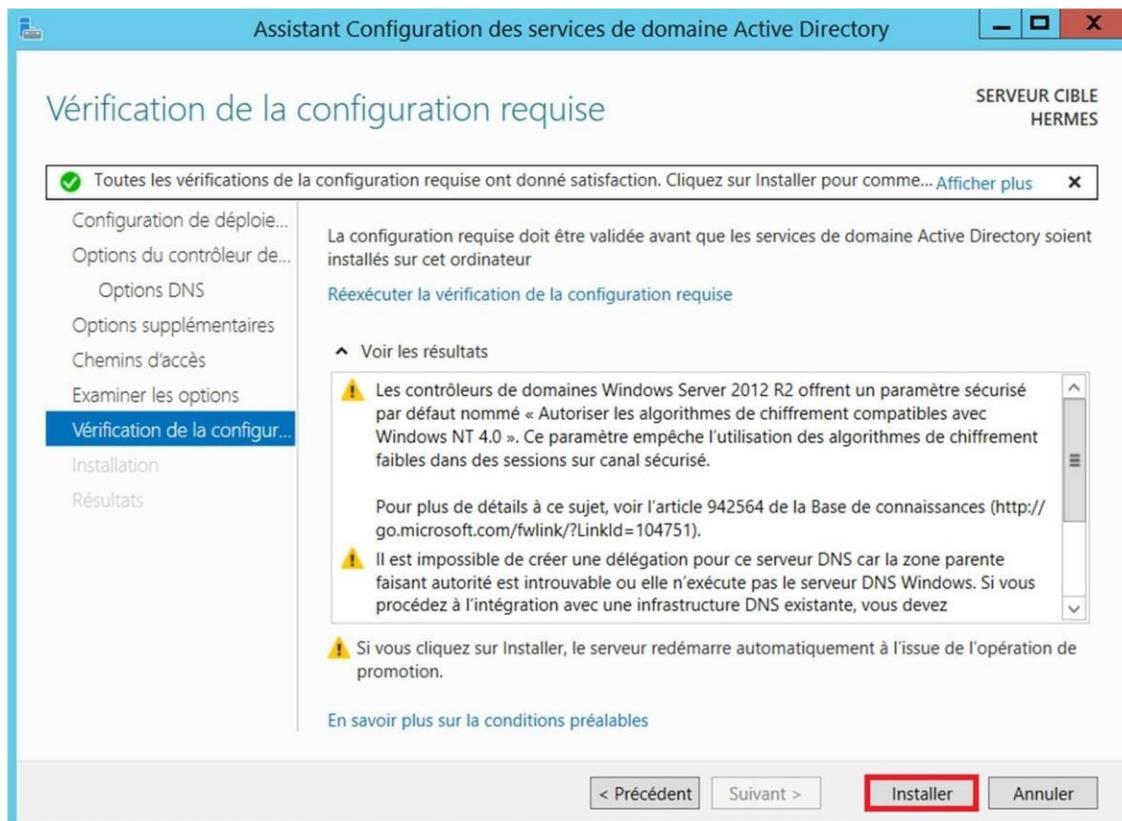
- Confirmer le nom NetBIOS, faire suivant.



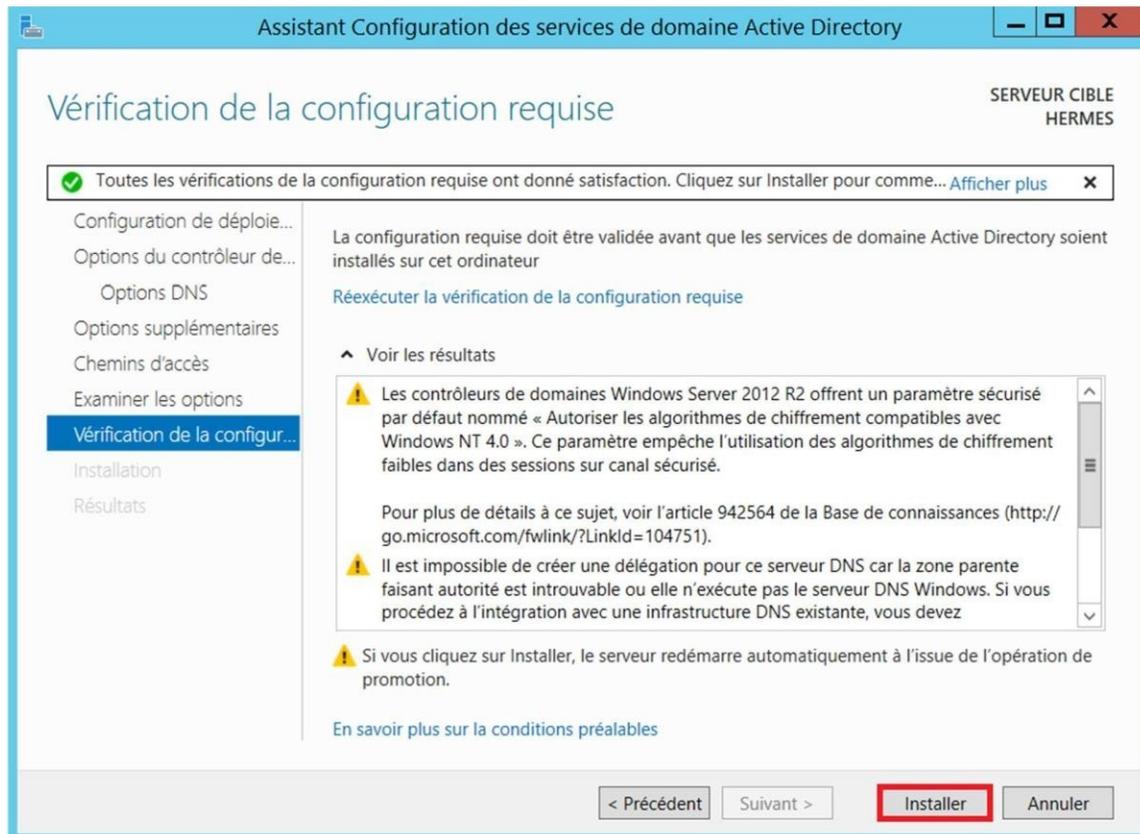
- Garder le chemin d'accès par défauts, faire suivant.



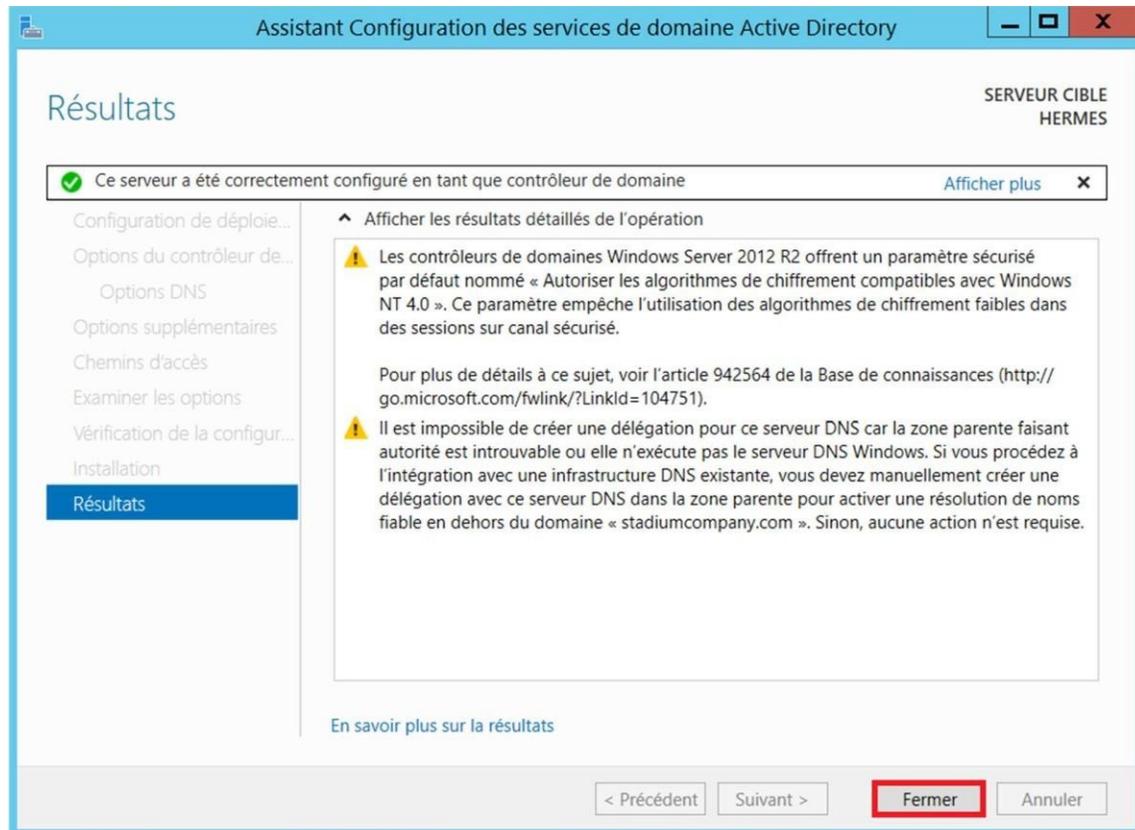
- Confirmer la sélection, faire suivant.



- Lancer l'installation.

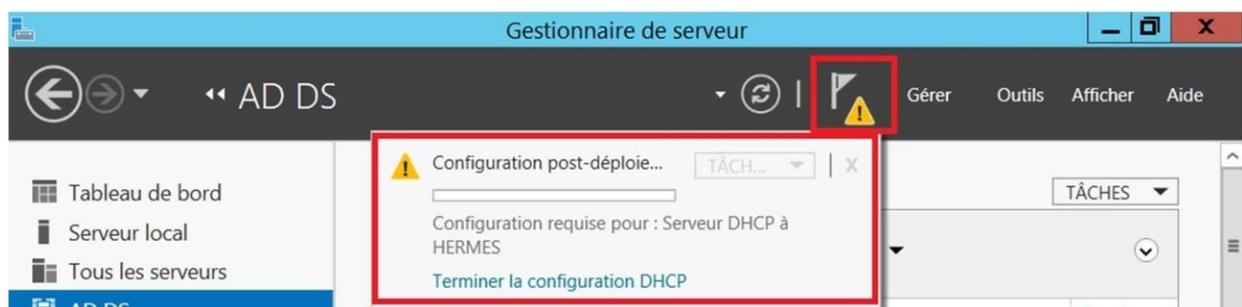


- Fermer l'Assistance du domaine Active Directory ce qui redémarre la machine.

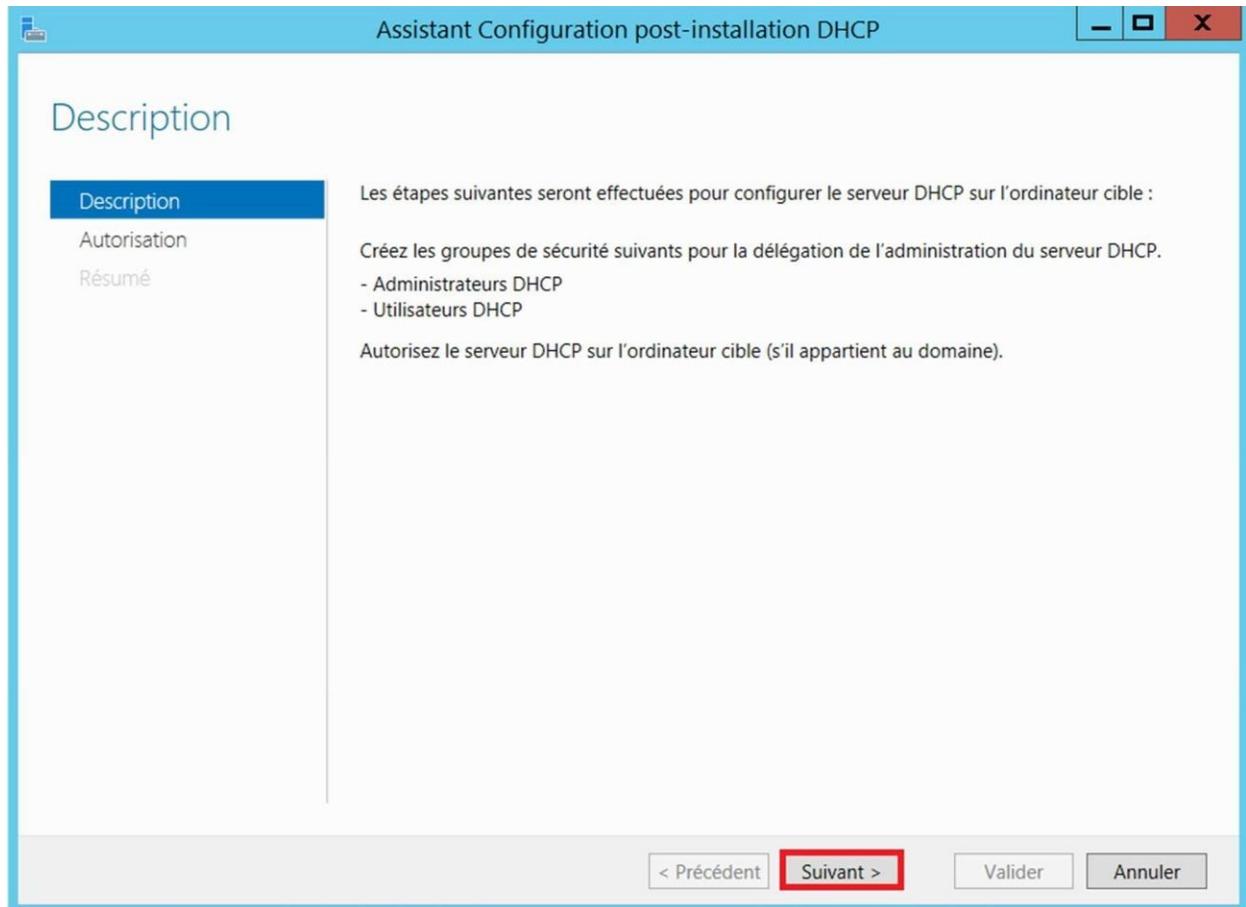


## Configuration du DHCP

- 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.

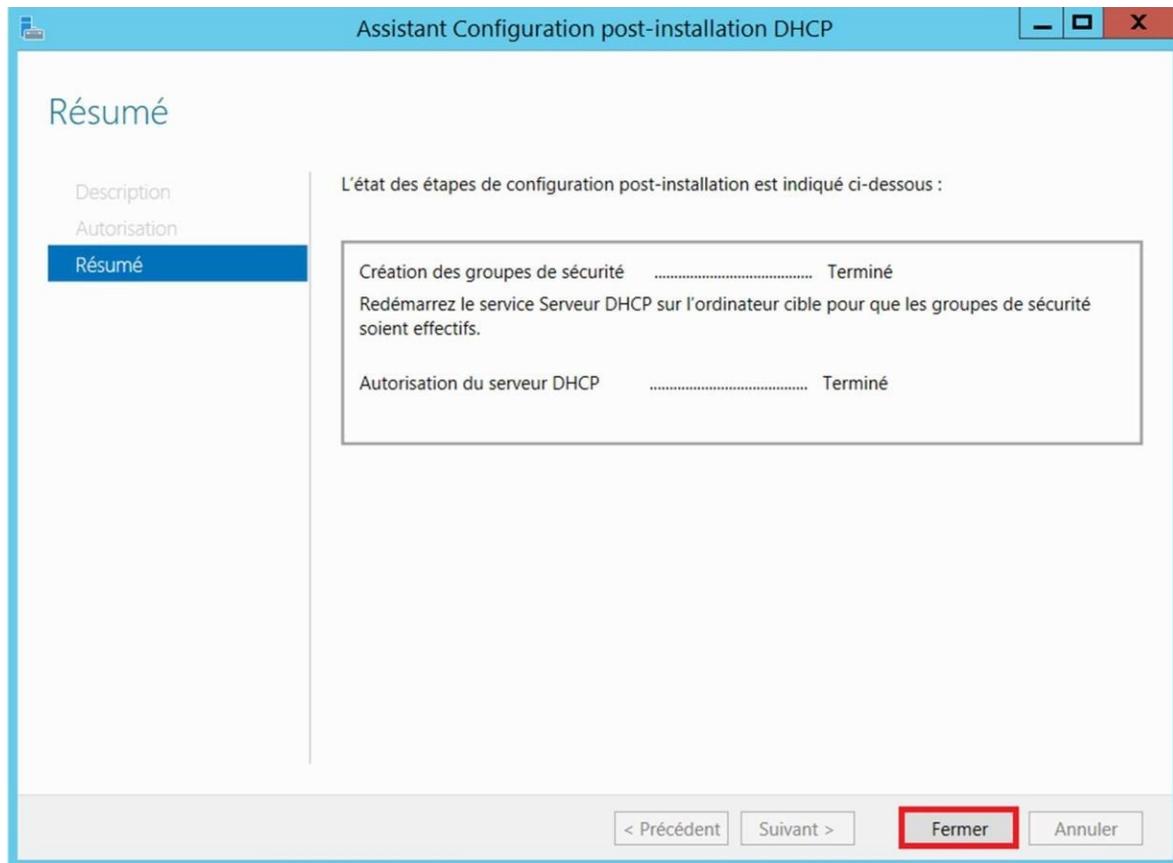
The screenshot shows a Windows window titled "Assistant Configuration post-installation DHCP". The window has a blue header bar with standard Windows window controls (minimize, maximize, close). The main content area is titled "Autorisation" and contains a sidebar on the left with three items: "Description", "Autorisation" (highlighted in blue), and "Résumé". The main area contains the following text and controls:

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

- Utiliser les informations d'identification de l'utilisateur suivant  
Nom d'utilisateur :
- Utiliser d'autres informations d'identification  
Nom d'utilisateur :
- Ignorer l'autorisation AD

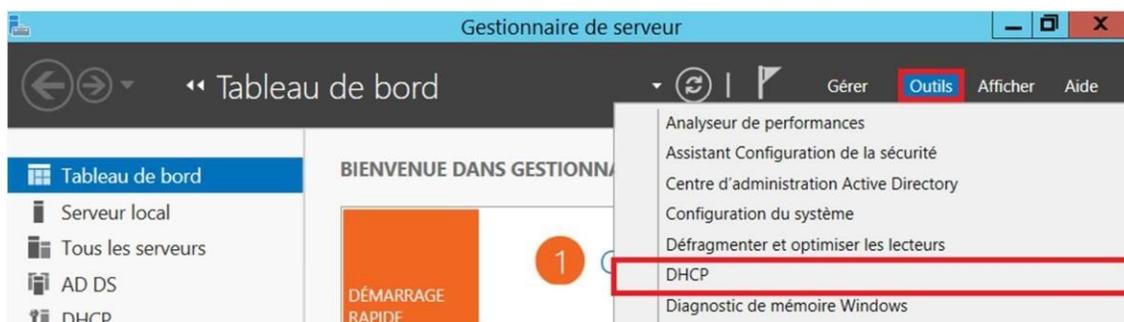
At the bottom of the window, there are four buttons: "< Précédent", "Suivant >", "Valider", and "Annuler".

- Fermer le résumer de la configuration installer.



Création des plages d'adresses :

- Gestionnaire de serveur, Outils, DHCP.



- DHCP → DC1.stadiumcompany.com → Clic droit IPv4 → Nouvelle étendue...

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

## Assistant Nouvelle étendue

**Nom de l'étendue**

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



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

Nom :

Description :

< Précédent **Suivant >** Annuler

## 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

## Tableau des noms et détails des étendu stadiumcompany.com

	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
Étendu 8	Sécurité	Vlan 80

## 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 :

[< Précédent](#)[Suivant >](#)[Annuler](#)

## 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 :

[< Précédent](#)[Suivant >](#)[Annuler](#)

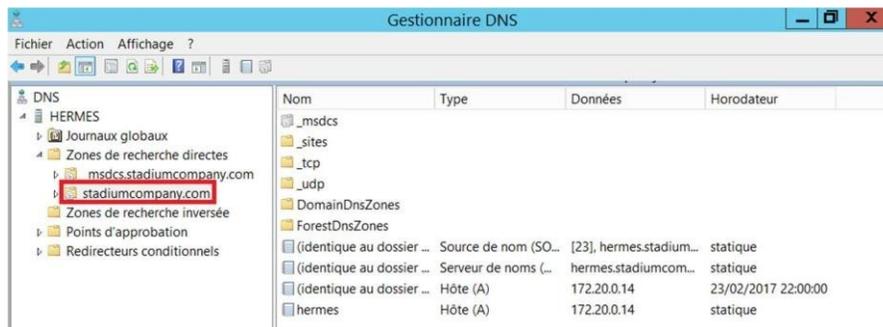
## Configuration DNS

Vérifications de zones de recherche directe :

Gestionnaire de serveur → Outils → DNS.

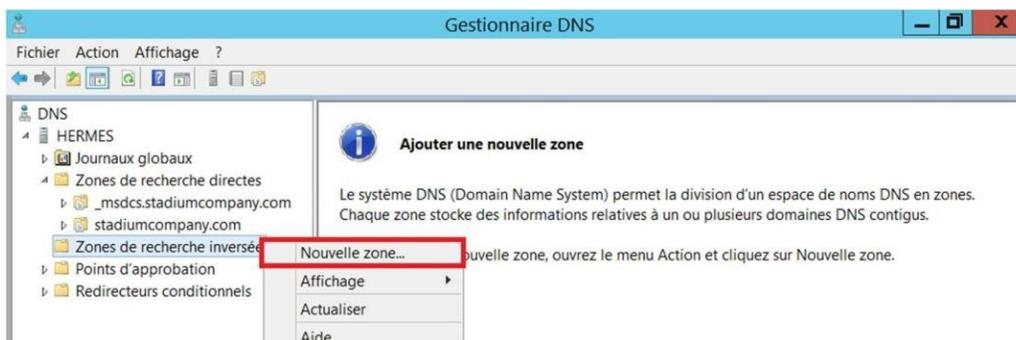


DNS → DC1 → Zones de recherches directes → Vérifier que la zone stadiumcompany.com a bien été créé.



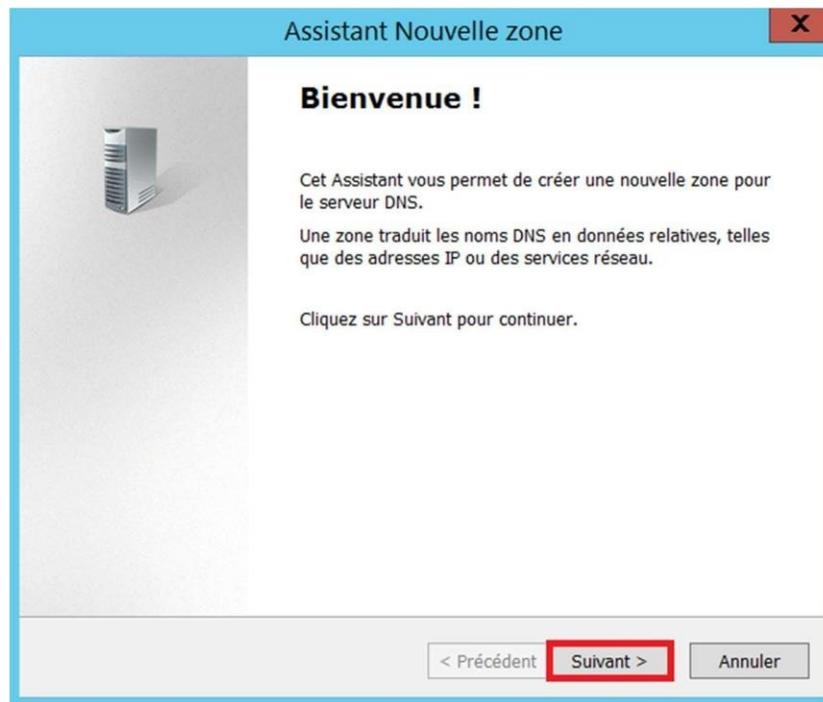
Nouvelle Zone inversé :

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.

**Assistant Nouvelle zone** ✕

**Type de zone**  
Le serveur DNS prend en charge différents types de zones et de stockages. 

Sélectionnez le type de zone que vous voulez créer :

- Zone principale**  
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
- Zone secondaire**  
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
- Zone de stub**  
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.
- Enregistrer la zone dans Active Directory** (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent Suivant > Annuler

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

Assistant Nouvelle zone

**Étendue de la zone de réplication de Active Directory**  
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

Choisissez la façon dont les données de la zone doivent être répliquées :

Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : stadiumcompany.com

Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : stadiumcompany.com

Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : stadiumcompany.com

Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

< Précédent Suivant > Annuler

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

Sélectionner « L'ID réseau 172.20.0.X »

**Assistant Nouvelle zone**

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

172 .20 .0

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :

0.20.172.in-addr.arpa

< Précédent **Suivant >** Annuler

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. 

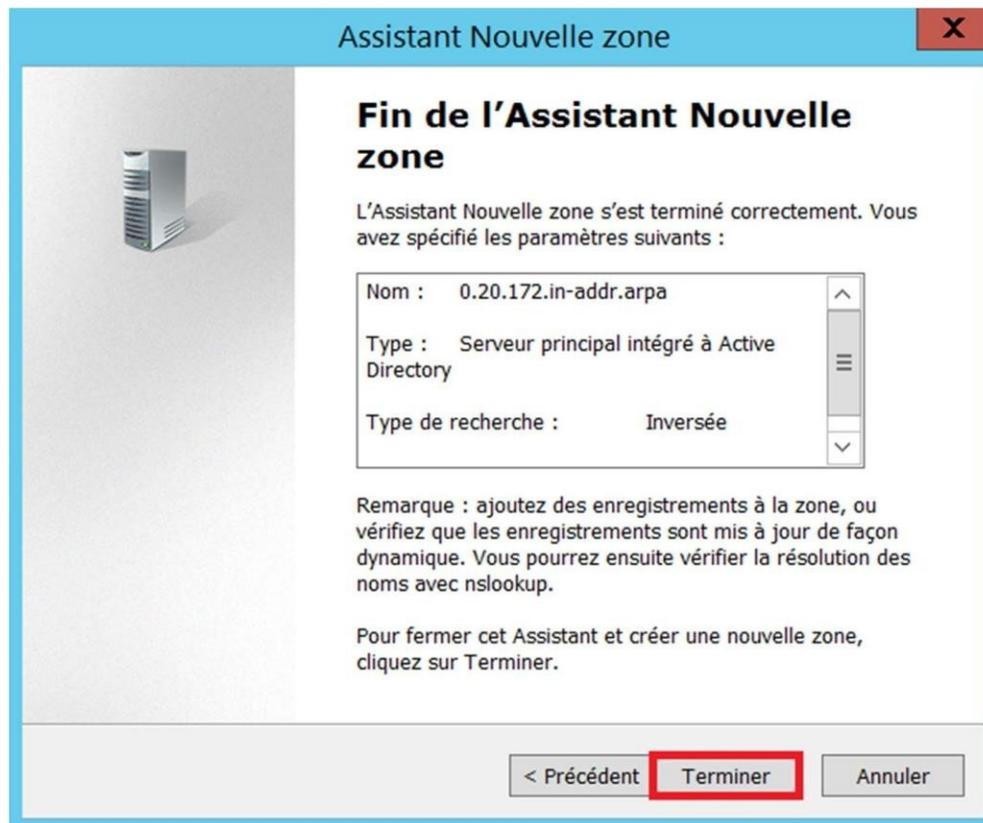
Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

**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.

Finaliser la création de la nouvelle zone, faire terminer.



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

Assistant Nouvelle zone ✕

**Étendue de la zone de réplication de Active Directory**  
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau. 

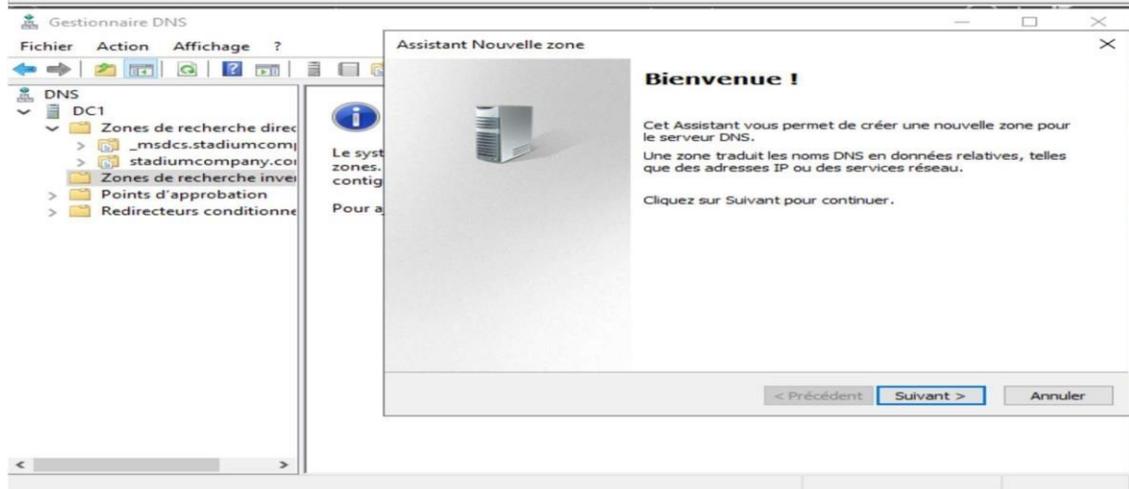
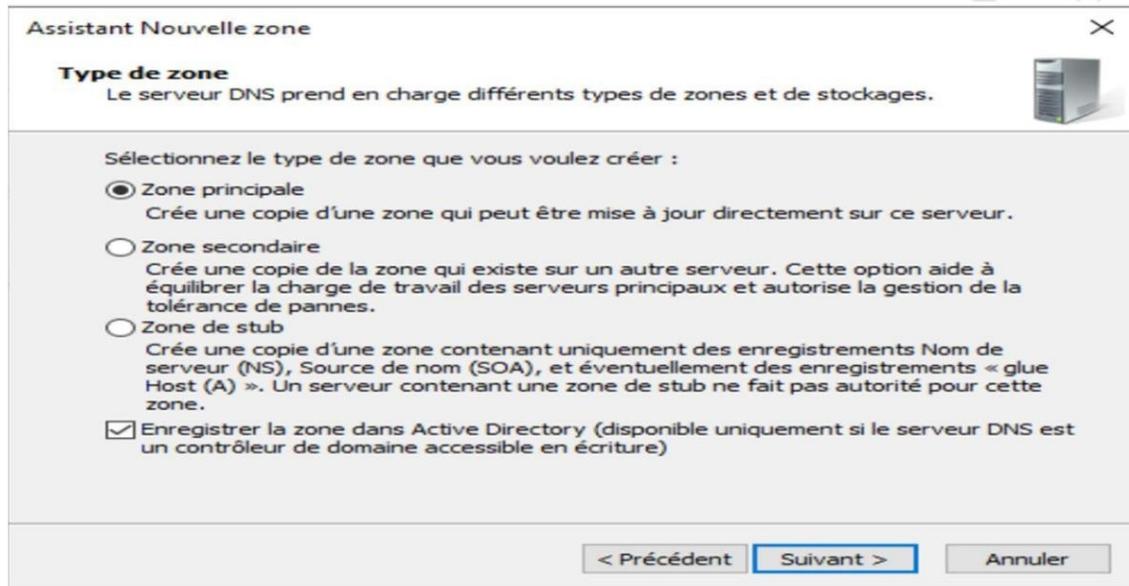
Choisissez la façon dont les données de la zone doivent être répliquées :

Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : stadiumcompany.com

Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : stadiumcompany.com

Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : stadiumcompany.com

Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :



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

Assistant Nouvelle zone ✕

**Nom de la zone de recherche inversée**  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

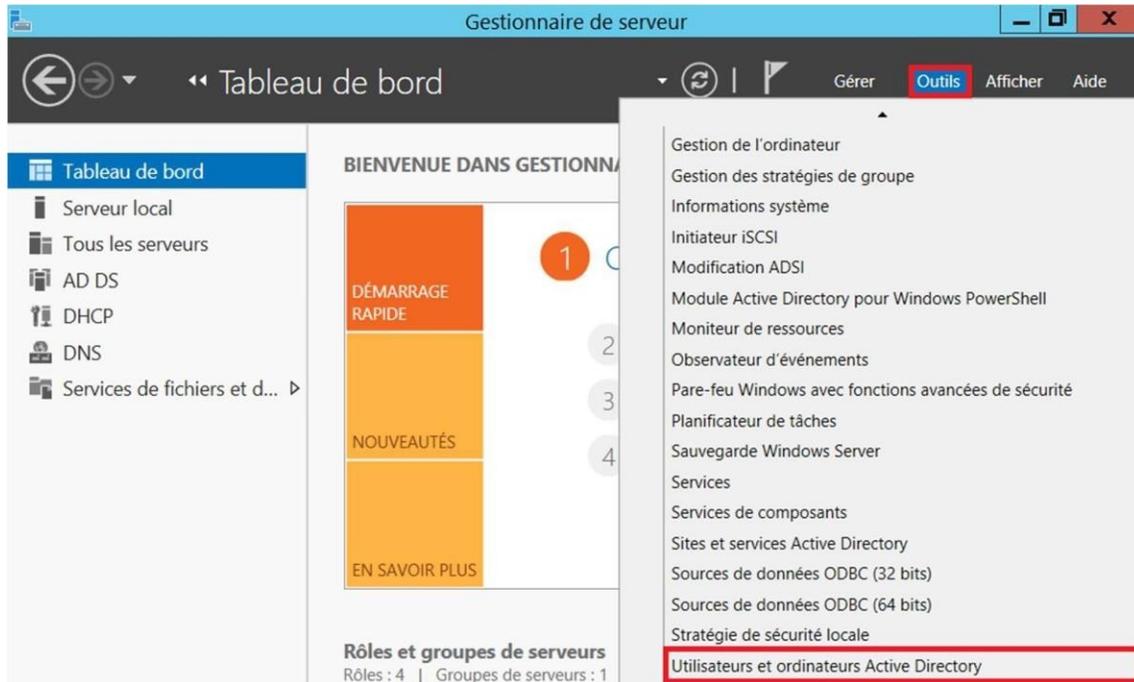
Nom de la zone de recherche inversée :

< Précédent **Suivant >** Annuler

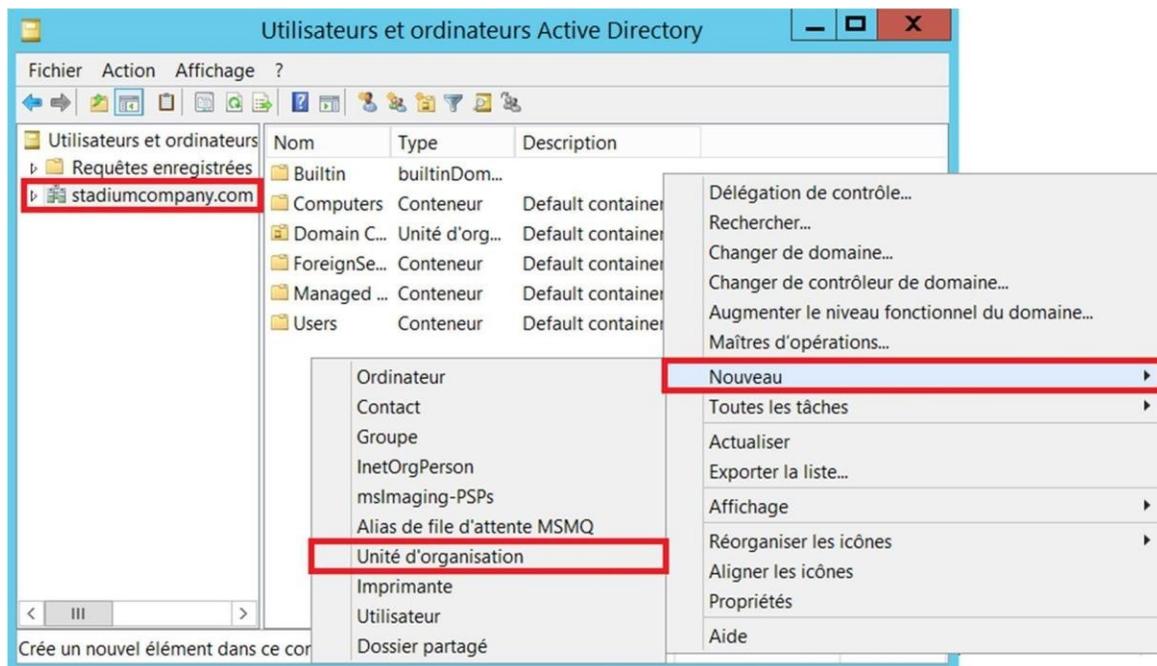
## Configuration des outils d'Active Directory

### Création des unités d'organisation

Sur le gestionnaire de serveur → Outils → Cliquez sur Utilisateurs et ordinateurs Active Directory.

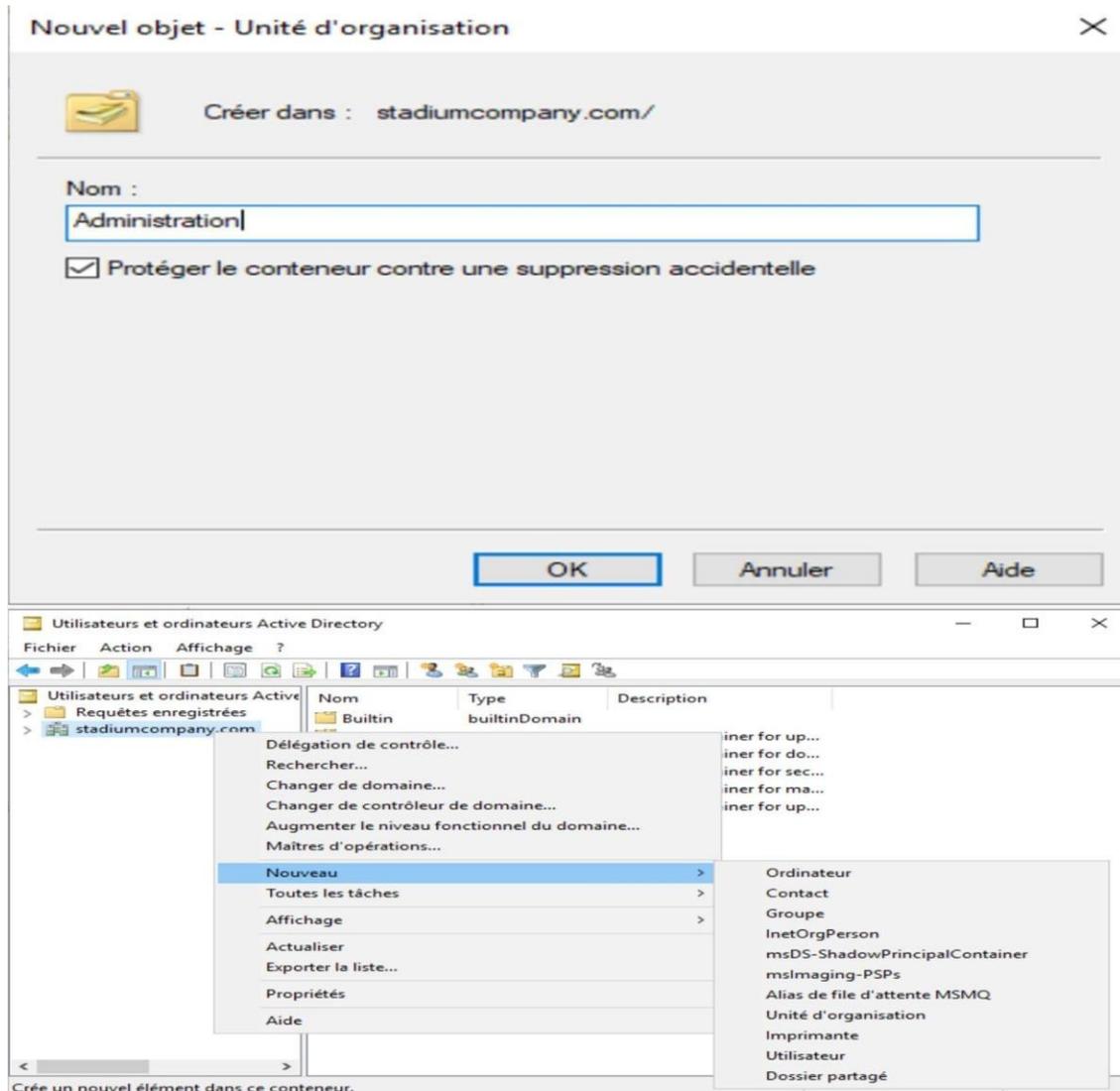


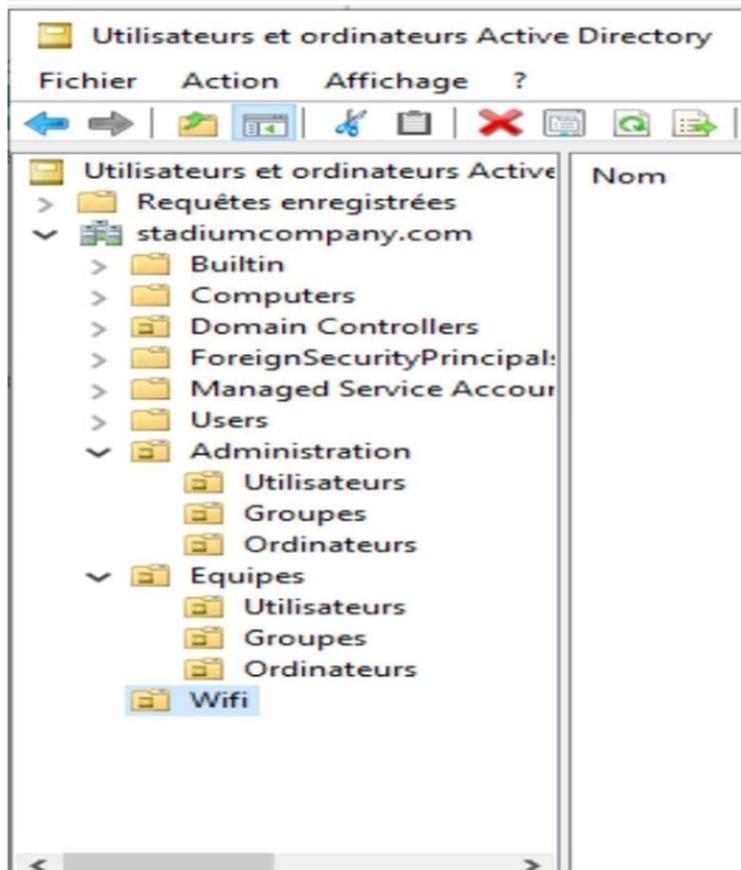
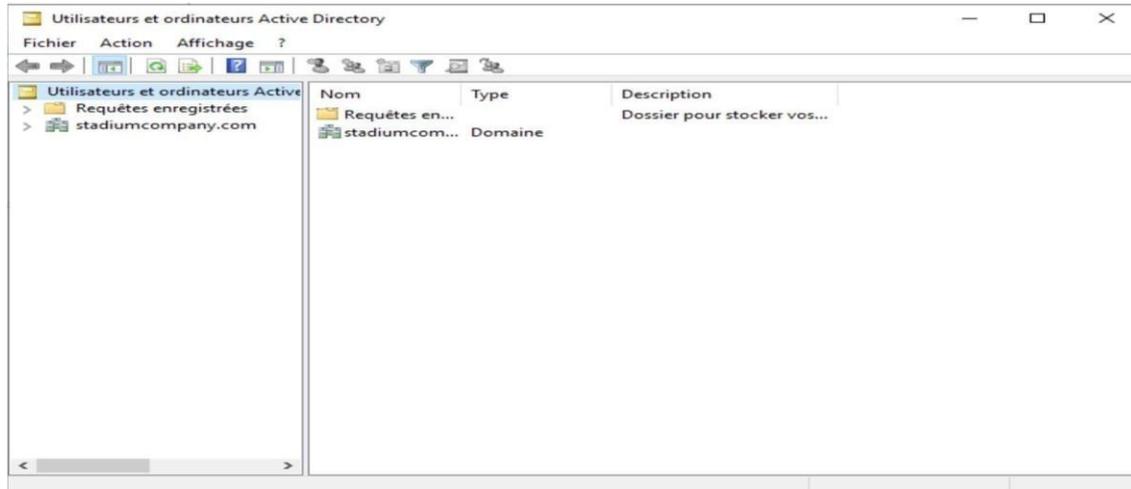
Dans Utilisateurs et ordinateurs Active Directory → Domaine (stadiumcompany.com) → Clic droit → Nouveau → Unité d'organisation.

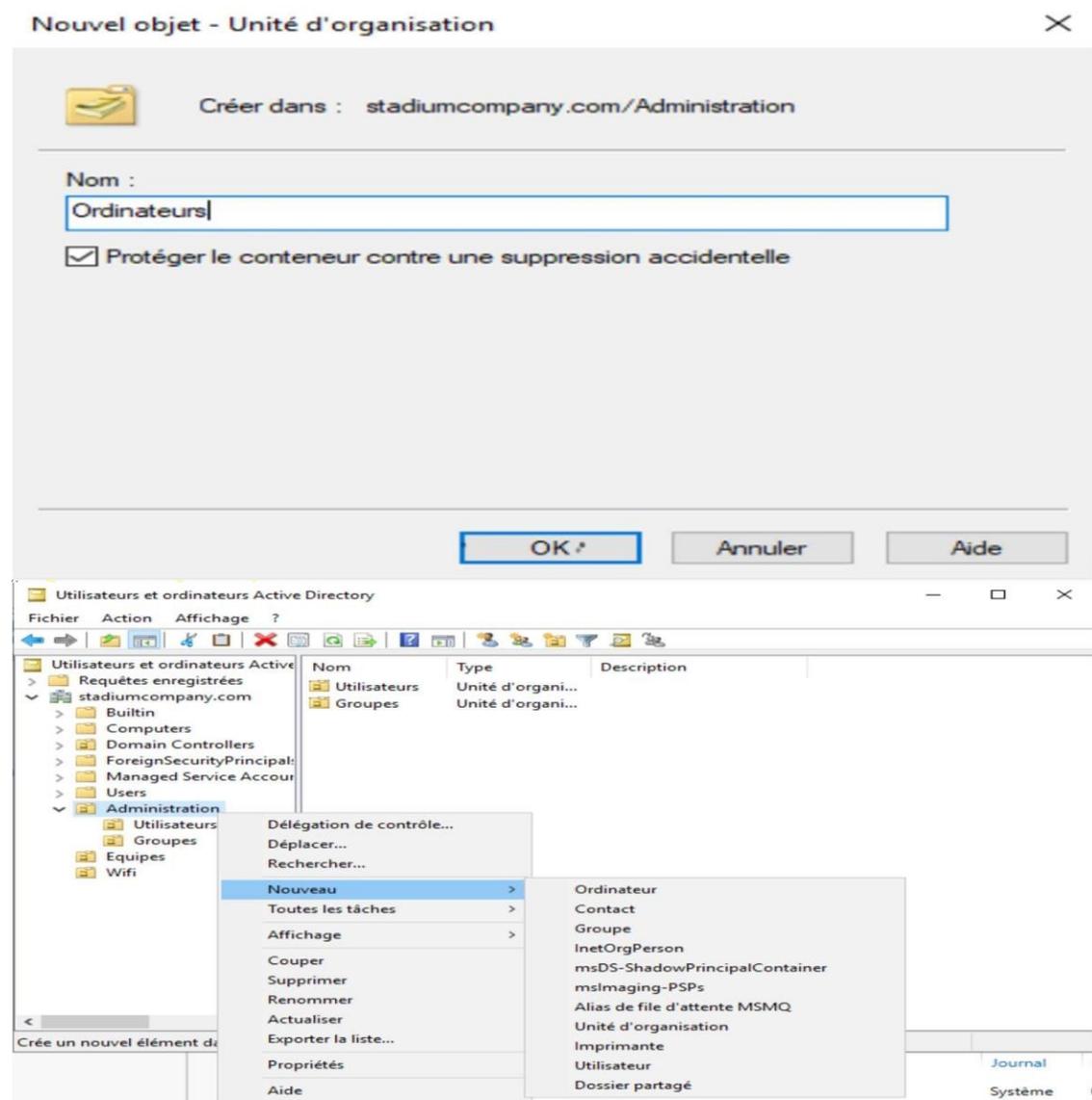




Création des UO services (Administration, Equipe, Wifi, Caméra-IP, VIP-Pressé, Fournisseurs et Restaurant).







## Les stratégies de groupe

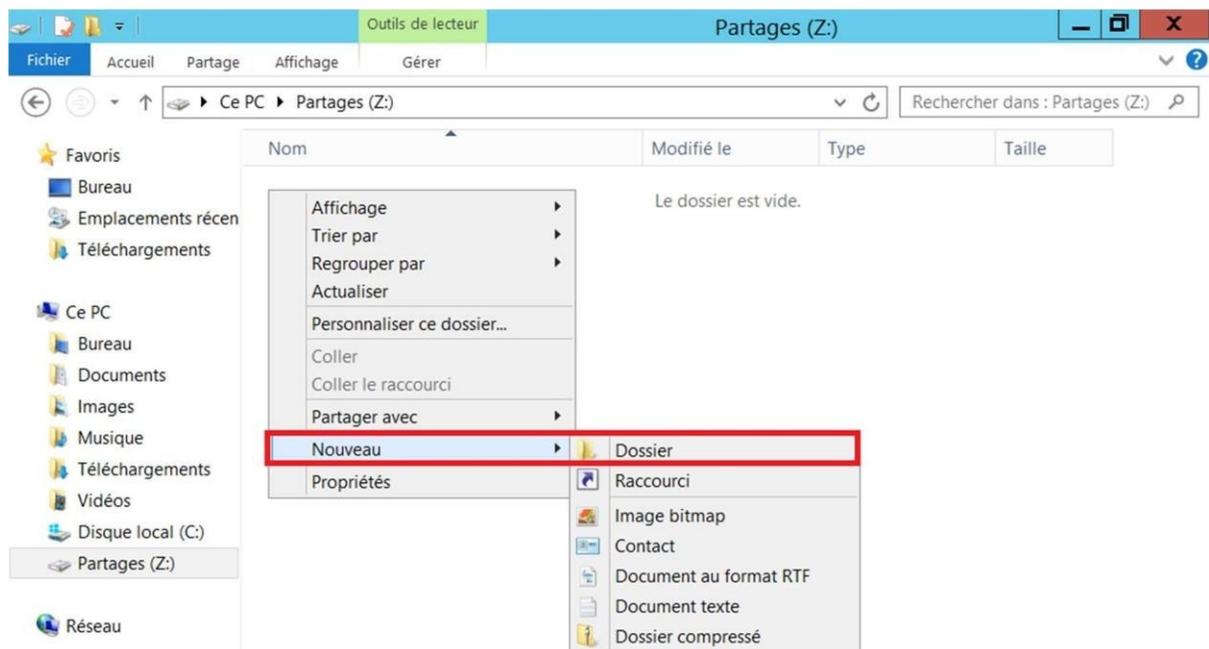
### Forcer le fond d'écran (GPO)

- 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).

## Périphériques et lecteurs (3)



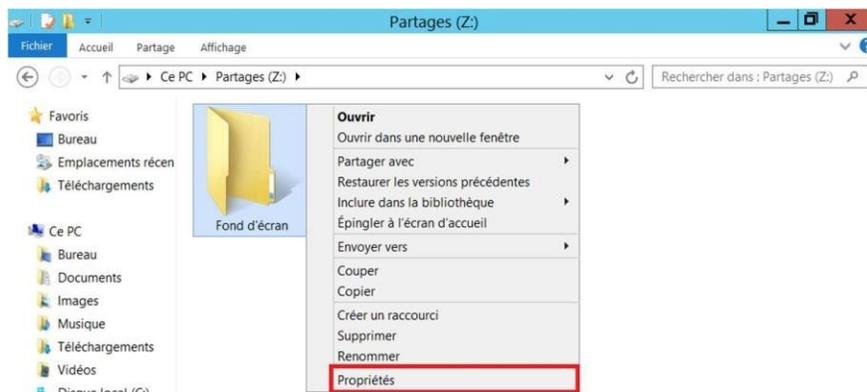
Clic droit → Nouveau → Dossier → Nommer le (Exemple Fond d'écran).



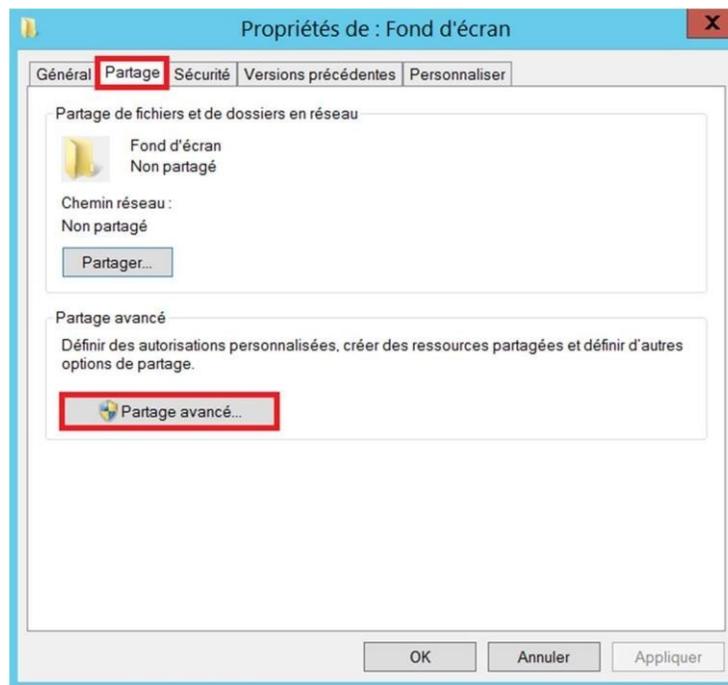
Aller dans le dossier → Ajouter l'image qui sera à chaque écran.



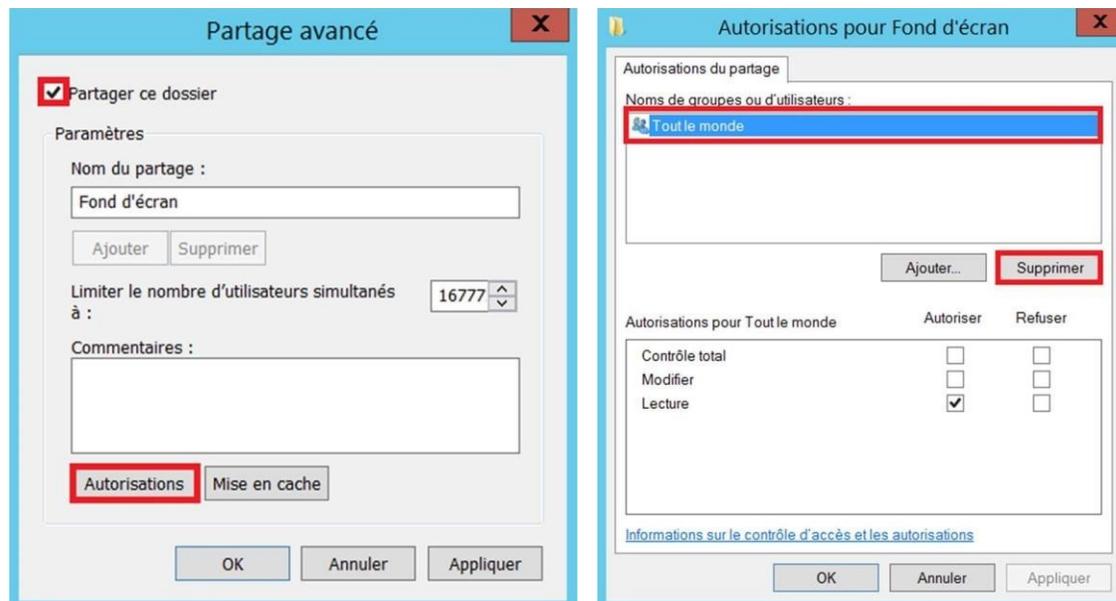
Clic droit sur le dossier Fond d'écran → Propriétés.



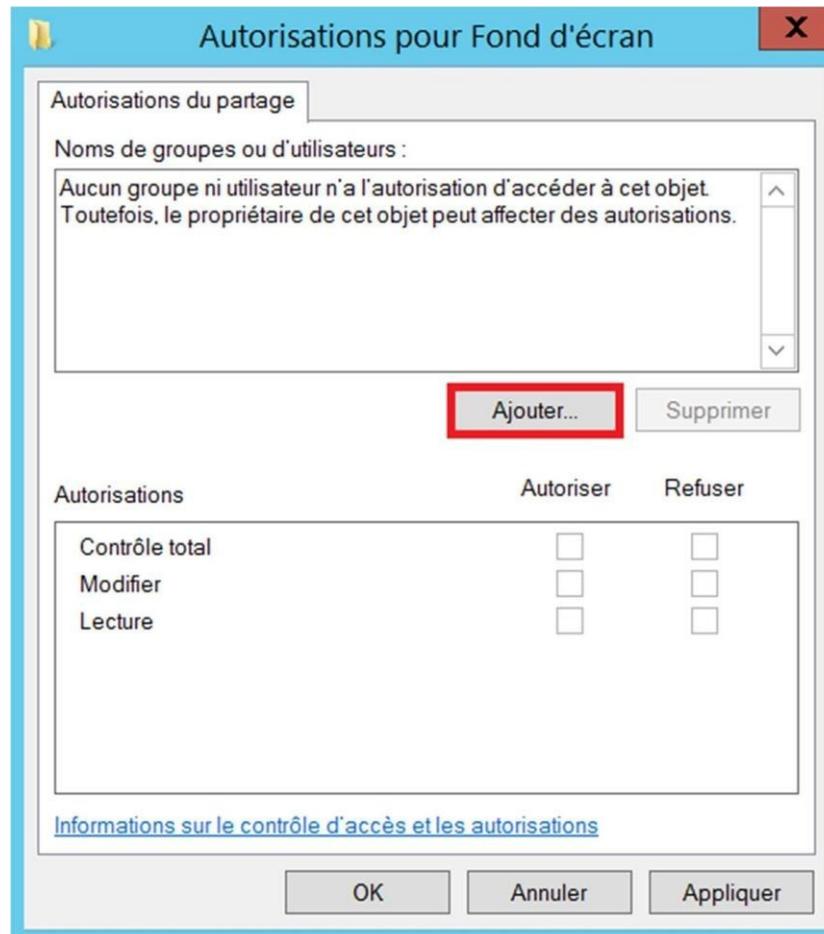
Dans l'onglet partage → Partage avancé...



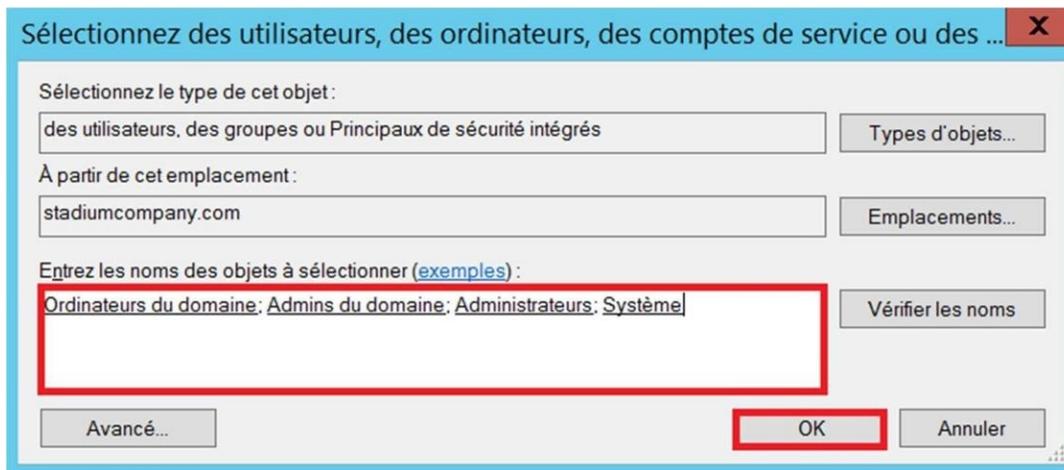
Cocher « Partager ce dossier » et aller sur Autorisations → Supprimer le groupe Tout le monde.



Cliquer sur Ajouter...



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



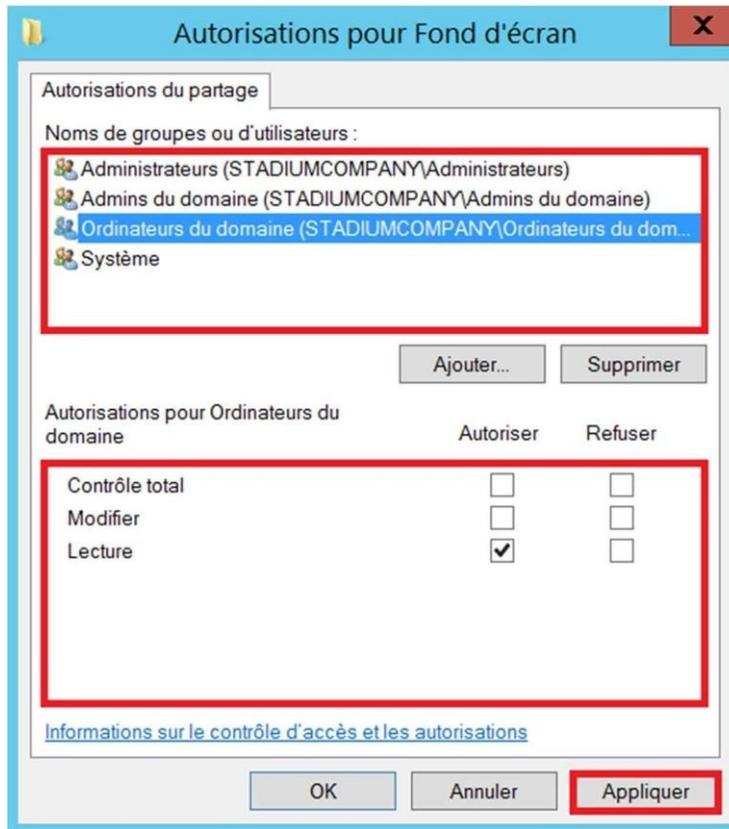
The image shows a Windows dialog box titled "Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des ...". The dialog has a light blue border and a red 'X' in the top right corner. It contains the following fields and buttons:

- Sélectionnez le type de cet objet :** A text box containing "des utilisateurs, des groupes ou Principaux de sécurité intégrés" and a "Types d'objets..." button.
- À partir de cet emplacement :** A text box containing "stadiumcompany.com" and an "Emplacements..." button.
- Entrez les noms des objets à sélectionner (exemples) :** A text box containing "Ordinateurs du domaine; Admins du domaine; Administrateurs; Système" and a "Vérifier les noms" button.
- Buttons at the bottom: "Avancé...", "OK", and "Annuler".

Red boxes highlight the text input field for object names and the "OK" button.

Ajouter les Autorisation :

- Contrôle total pour Admins du domaine
- Modification pour Administrateurs
- Lecture pour Ordinateurs du domaine et Système

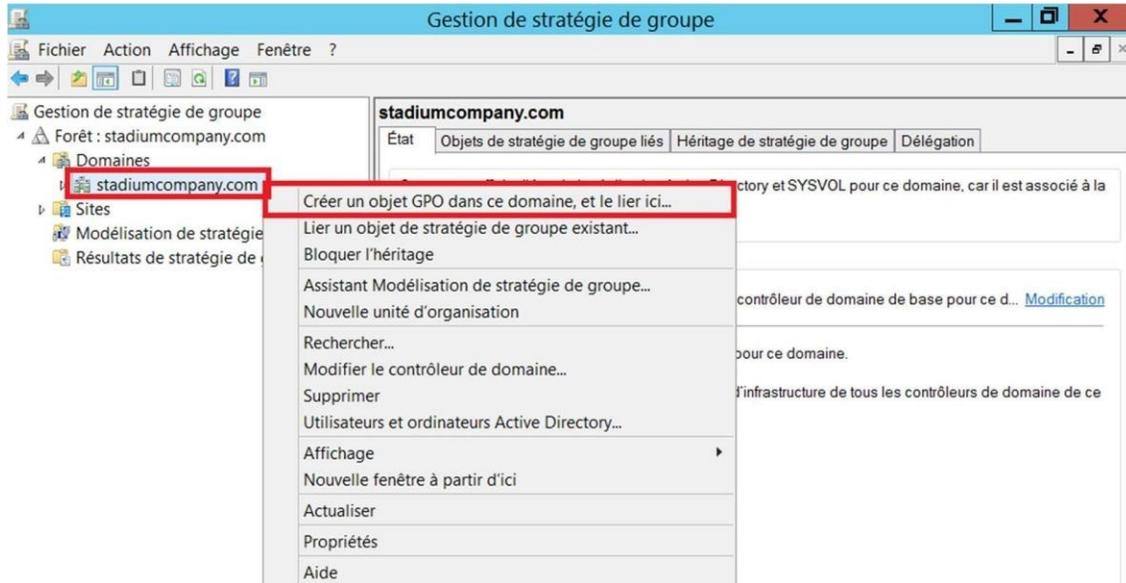


Création d'un paramètre pour copier le fichier sur l'ordinateur. Ainsi l'ordinateur récupèrera le fond d'écran directement en local ce qui empêchera les ordinateurs de récupérer l'image l'AD à chaque démarrage, pouvant entrainer un temps de traitement supplémentaire sur il y a du monde.

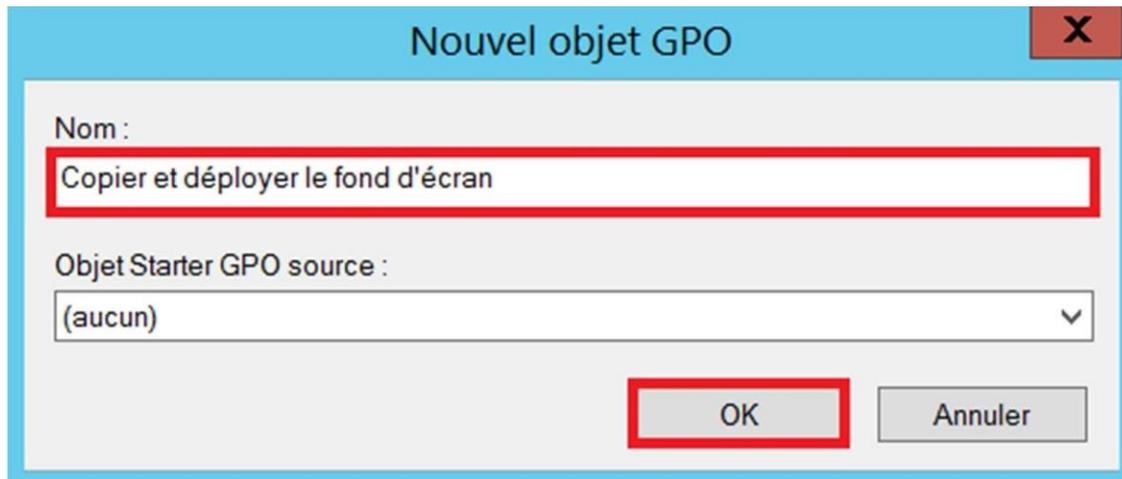
-Gestionnaire de serveur → Outils → Gestion des stratégies de groupe.



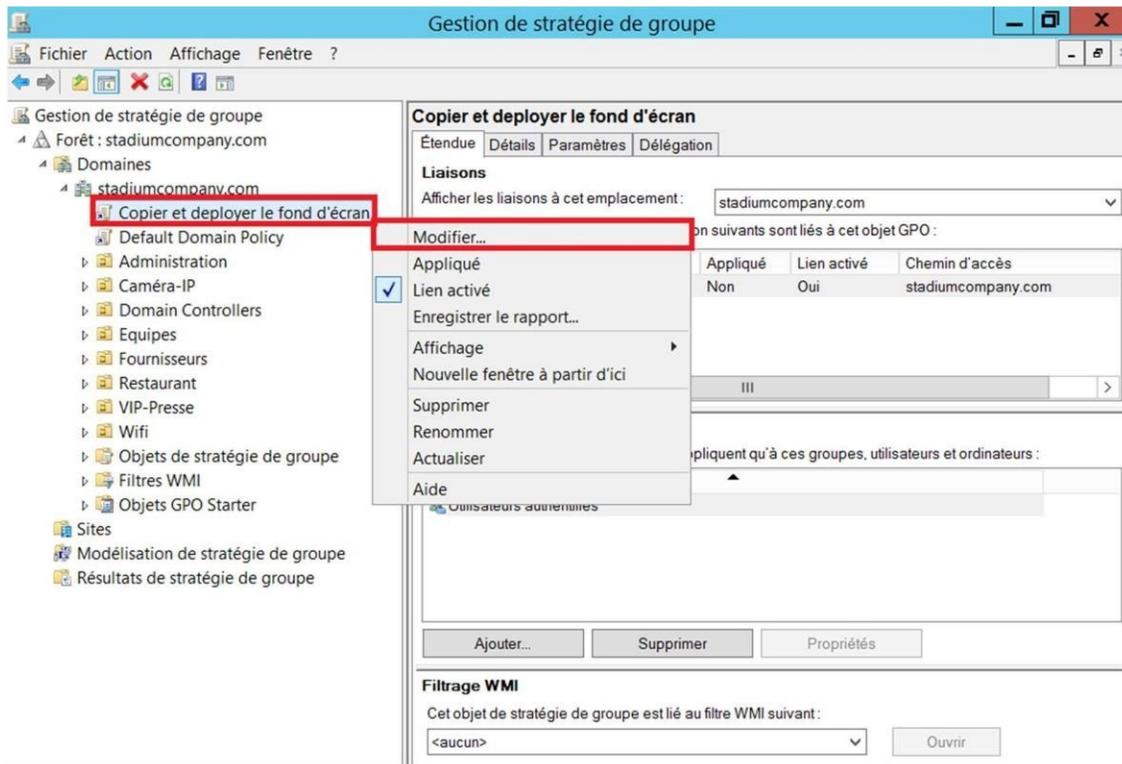
Gestion de Stratégie de groupe → Forêt : stadiumcompany.com → Domaines → Stadiumcompany.com → Créer un objet GPO dans ce domaine, et le lier ici...



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

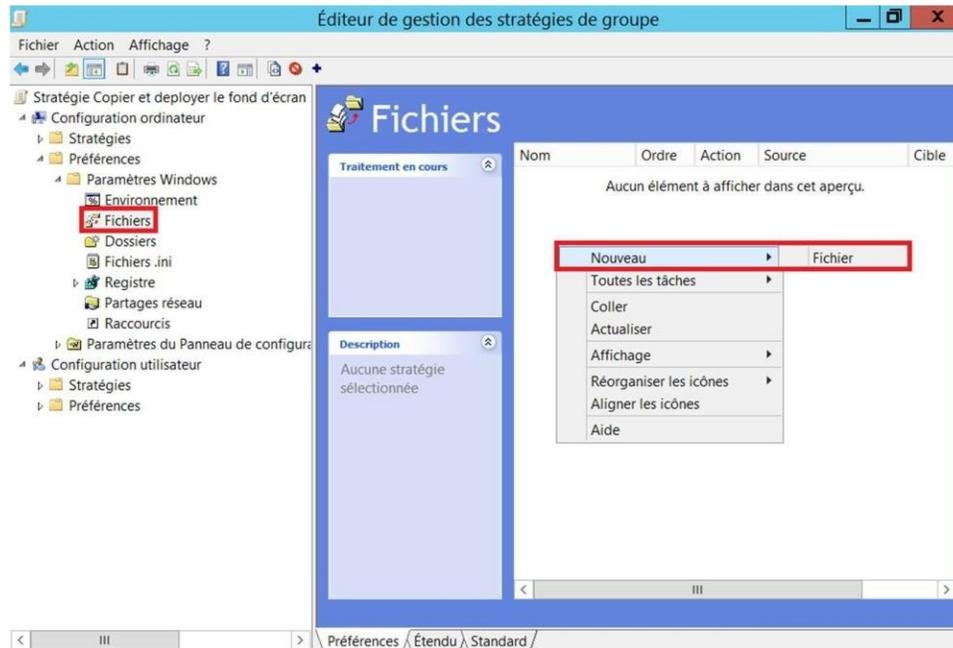


Clic droit sur la GPO Copier et déployer le fond d'écran → Modifier...

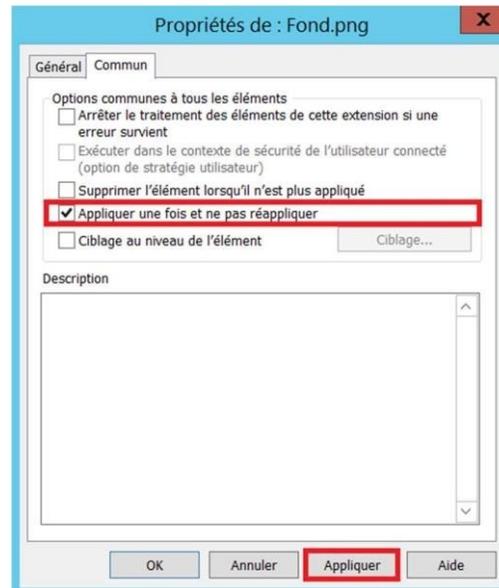
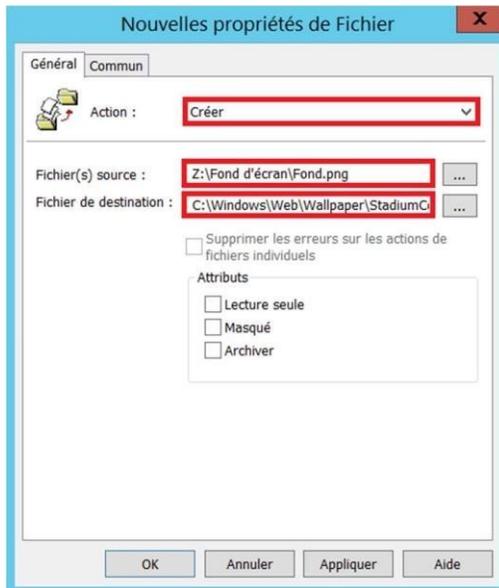




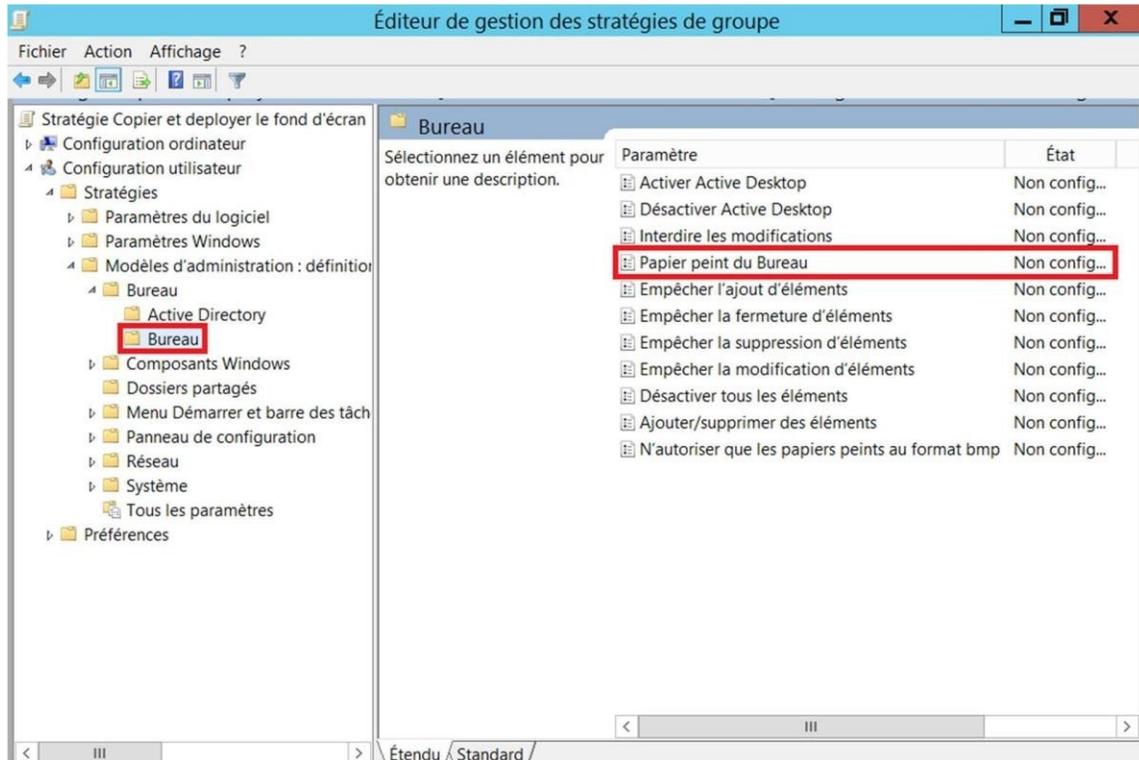
Stratégie Copier et déployer le fond d'écran → Configuration ordinateur  
 → Préférences → Paramètres Windows → Fichiers → Clic droit →  
 Nouveau → Fichier



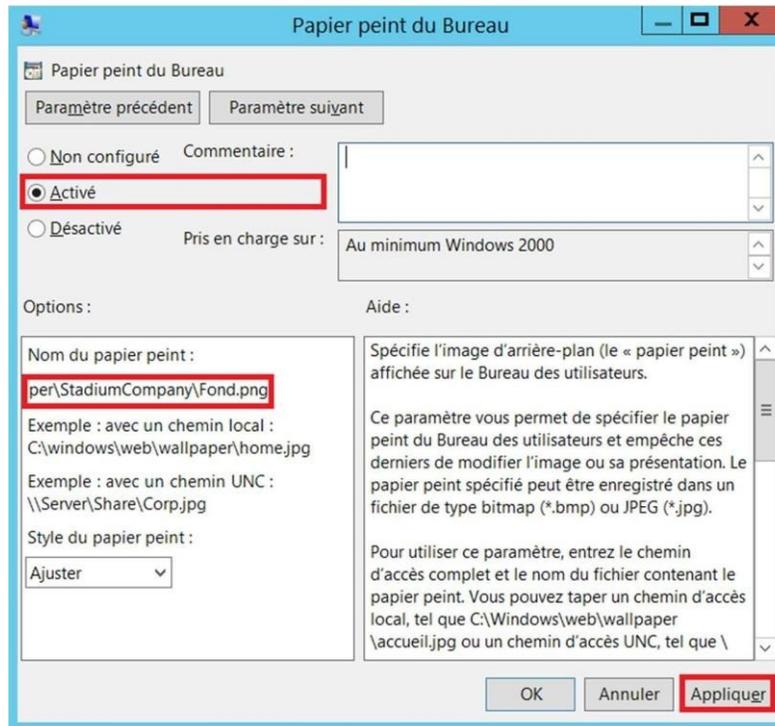
- Action → Créer (puisque ce fichier n'existe pas)
- Fichier(s) source → Z:\Fond d'écran\Fonf.png
- Fichier de destination → C:\windows\Web\Wallpaper\StadiumCompany\Fond.png
- Commun → Appliquer une fois et ne pas réappliquer



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.

The screenshot shows the Group Policy Management console for the domain 'stadiumcompany.com'. The left pane shows the hierarchy: Gestion de stratégie de groupe > Forêt : stadiumcompany.com > stadiumcompany.com > Copier et déployer le fond d'écran. A context menu is open over the selected GPO, with 'Appliqué' and 'Lien activé' checked. The main pane shows the 'Copier et déployer le fond d'écran' GPO details. The 'Liaisons' section shows a link to 'stadiumcompany.com' with 'Appliqué' and 'Lien activé' both set to 'Oui'. The 'Filtrage WMI' section shows the filter set to '<aucun>'. At the bottom, there is a button to 'Basculer l'attribut Enforced pour ce lien'.

Basculer l'attribut Enforced pour ce lien

