Direct Access

>>> Microsoft Serveur 2012 R2

Description :

Le but de ce cours est de vous apprendre à configurer une solution de connexion à distance au système d'information de manière sécurisé appelé Direct Access.

Direct Access

>>> Microsoft Serveur 2012 R2

Sommaire :

I) Introduction

Microsoft Direct Access

Direct Access est une solution VPN (Virtual Private Network) développée par Microsoft et disponible depuis la version Windows Server 2008 R2. La particularité de Direct Access est que l'établissement de la connexion est automatique et aucune action de l'utilisateur n'est nécessaire. Lorsque le terminal est à l'extérieur du réseau de l'entreprise et qu'une connexion Internet est disponible, Direct Access va initier la connexion auprès du serveur Direct Access de l'entreprise. Pour déterminer s'il est connecté au LAN de l'entreprise ou à l'extérieur, le système va contacter une ressource disponible seulement en interne, par exemple l'Active Directory. Le système utilise deux techniques pour contacter la ressource interne, le ping ou la requête HTTP.

Les paramètres permettant au client de se connecter au serveur Direct Access sont déployés par GPO lorsque le terminal est connecté au réseau interne. La sécurité de cette solution est assurée par la création d'un tunnel SSL/TLS (à travers la carte IPHTTPS) entre le client et le serveur DirectAccess, de plus les informations transiteront sur un tunnel IPsec. Pour l'authentification, plusieurs méthodes sont possibles, le compte active Directory (Kerberos), un certificat ou encore un Dongle.

DirectAccess est une solution qui fonctionne en IPV6, la compatibilité avec l'IPV4 est assurée automatiquement grâce à des tunnels 6to4 et des cartes réseaux virtuelles IPv6.

Plusieurs pré-requis sont nécessaire à la mise en place d'une telle infrastructure :

- Le système exploitation sur le serveur DirectAccess doit être au minimum Windows Serveur 2008 R2.
- Un domaine Active Directory doit être présent dans l'entreprise
- La forêt et le domaine doivent avoir un niveau fonctionnelle minimum Windows 2003.
- L'OS client doit être Windows 8 Enterprise, possible avec Windows 7 Enterprise ou Ultimate avec ajout d'un Addon.

Dans cette démonstration, nous allons utiliser trois serveurs virtuels Windows Server 2012 R2 et 1 client Windows 8.1 Enterprise :

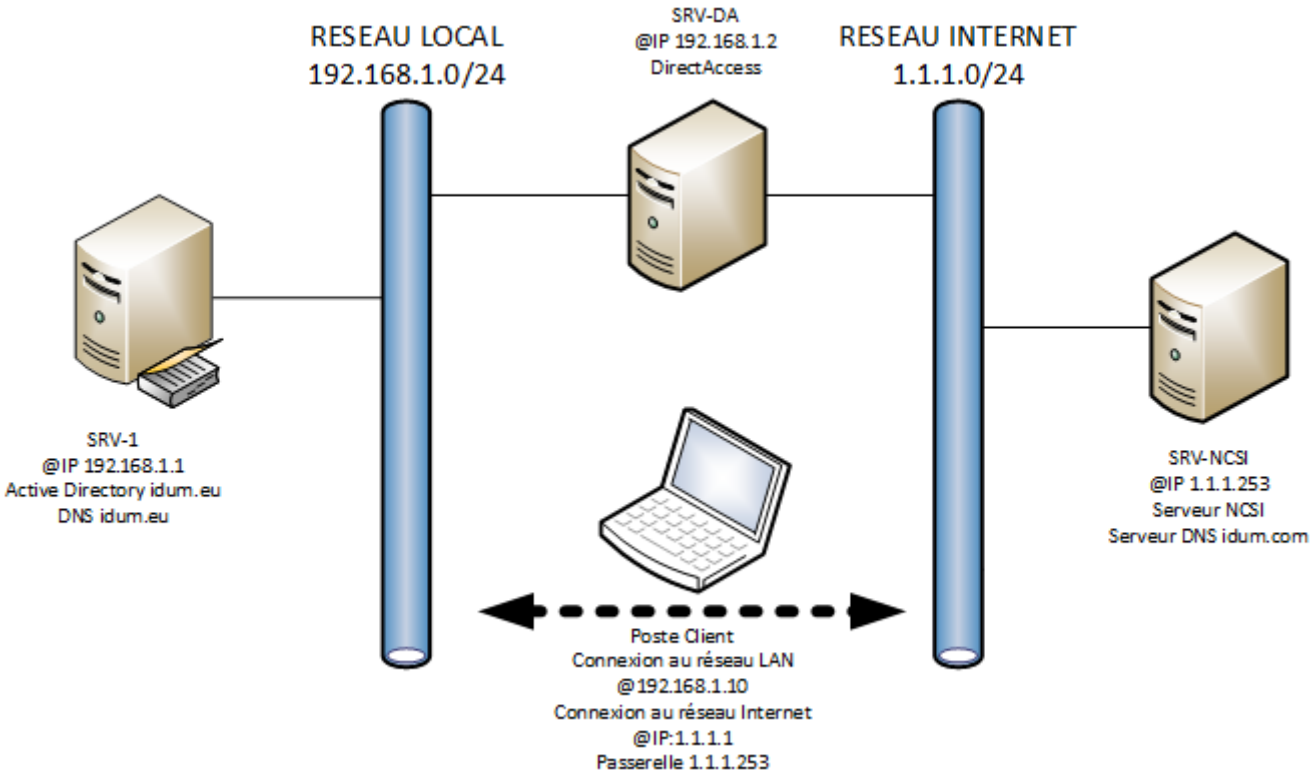
Notre labo est hors ligne, c'est à dire qu'il n'a pas accès à Internet, dans cet article pour que le client initie la connexion DirectAccess, la détection de l'accès Internet est nécessaire (Vous savez la petite icone en bas à droite à côté de l'heure !) . Nous allons donc mettre en place un petit serveur avec un service DNS et Web qui va simuler l'accès Internet, c'est un serveur Microsoft NCSI. -> Voir Chapitre "IV) Configuration du serveur ISP"

Description des serveurs utilisés :

- SRV-1 : Ce sera le contrôleur du domaine idum.eu son installation est expliquée dans cet article voir article->286
- SRV-DA : Ce sera le serveur DirectAccess, son installation est le but de cet article.Il sera doté de deux cartes réseaux (LAN et WAN)
- SRV-ISP : Ce sera le serveur qui simulera l'accès a Internet et hébergera la zone idum.com
- CLIENT : Il simulera l'accès LAN puis WAN pour les tests du DirectAccess.

Pour cette démonstration, les certificats utilisés seront des certificats auto-signés. Un article est paru le 19 octobre 2015 vous expliquant comment générer les certificats avec l'autorité de certification Windows.

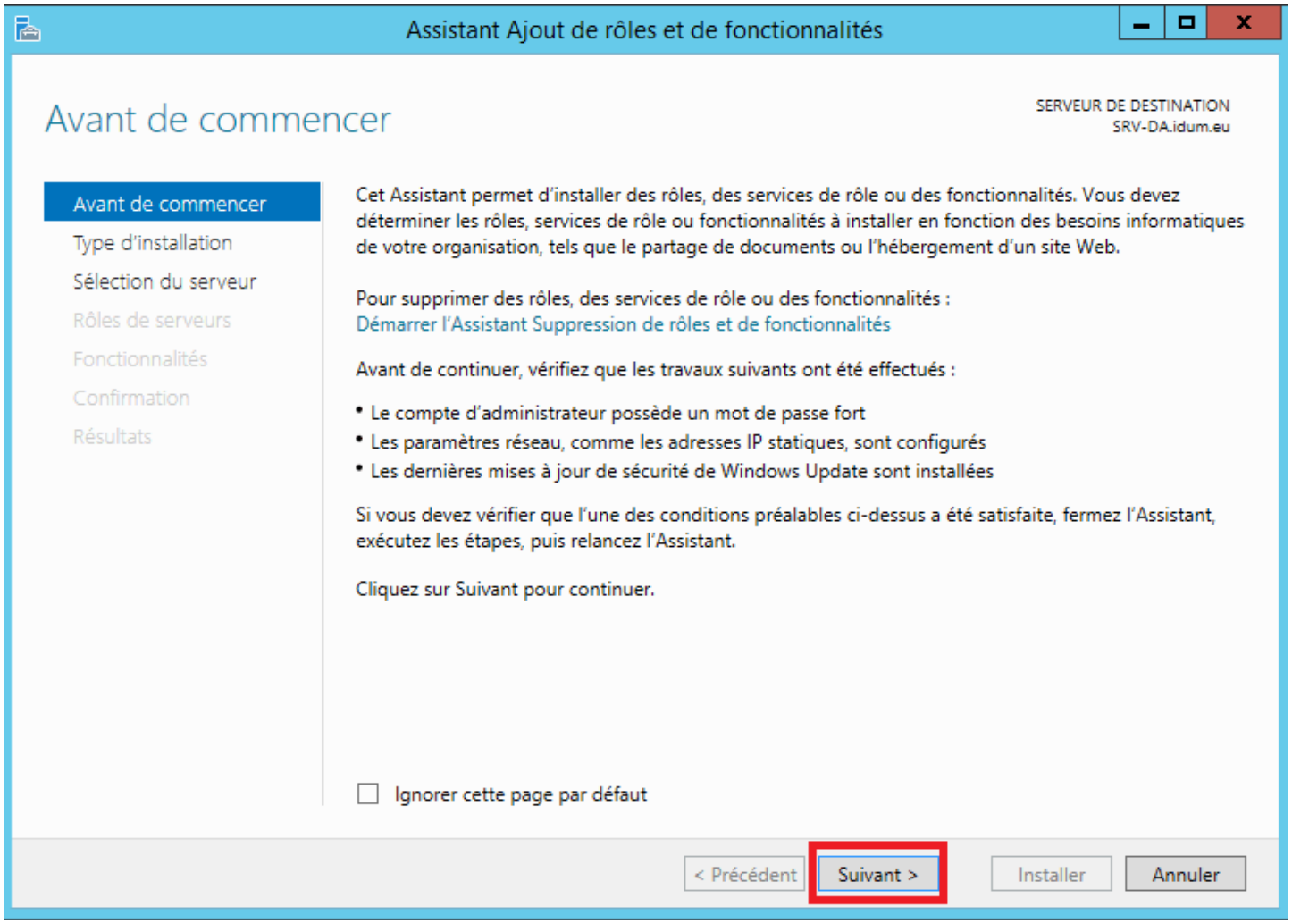
Voici le schéma du labo mis en place :



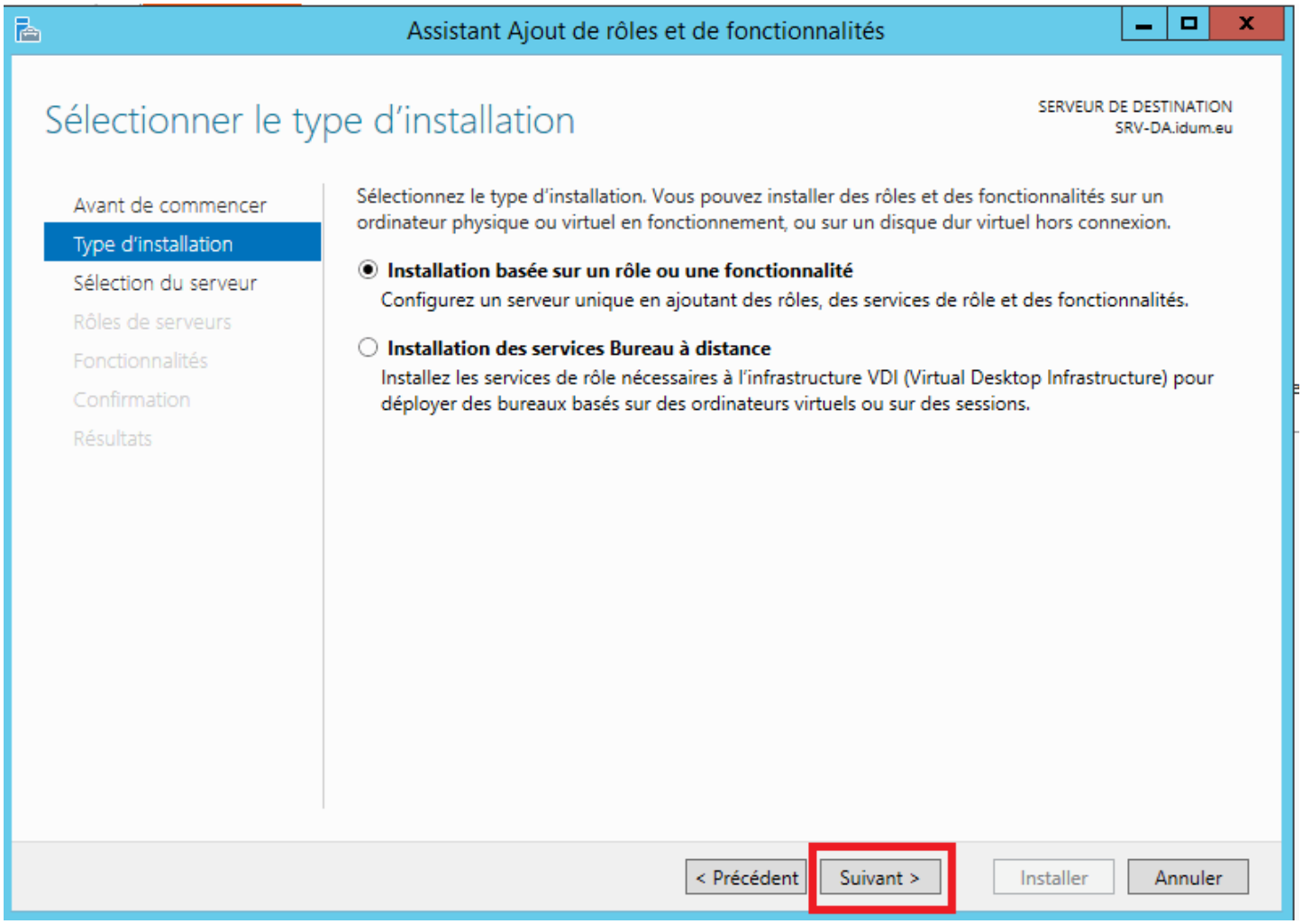
II) Installation du Rôle DirectAccess

Sur le serveur SRV-DA.
– Ouvrez le gestionnaire de serveur, puis cliquez sur **"Ajouter des rôles et des fonctionnalités"**.

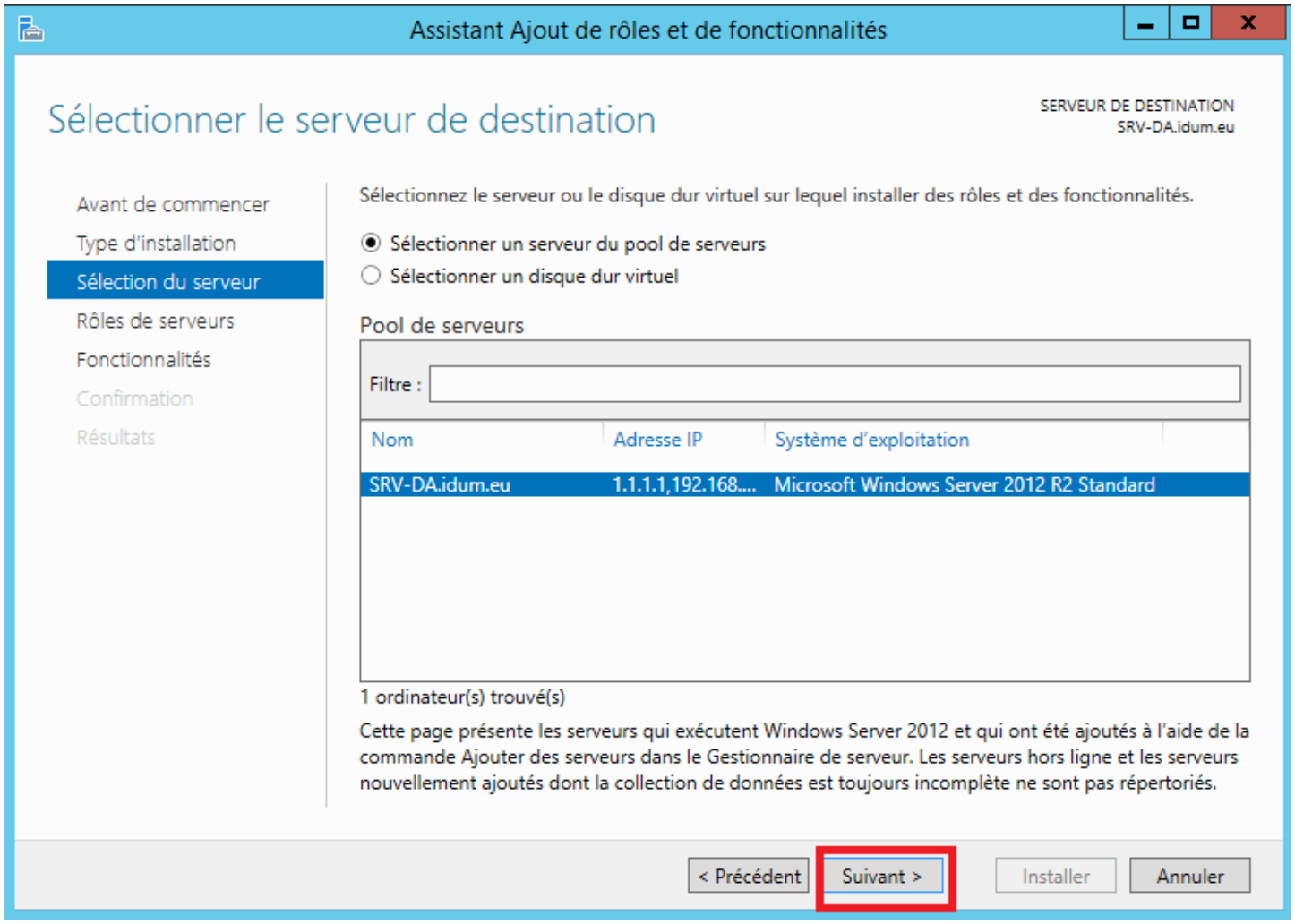
- Cliquez sur **"Suivant"**.



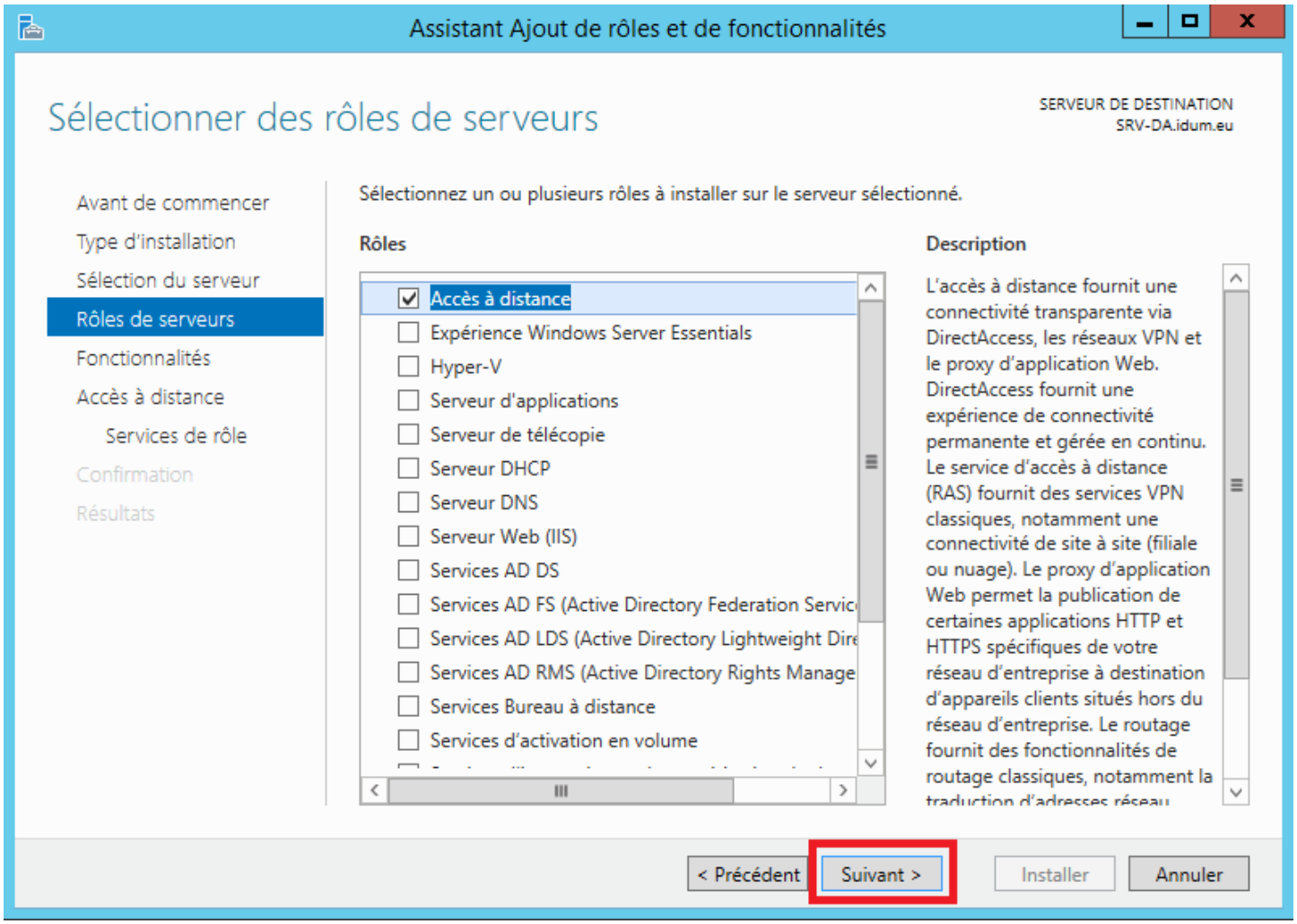
- Cliquez sur **"Suivant"**.



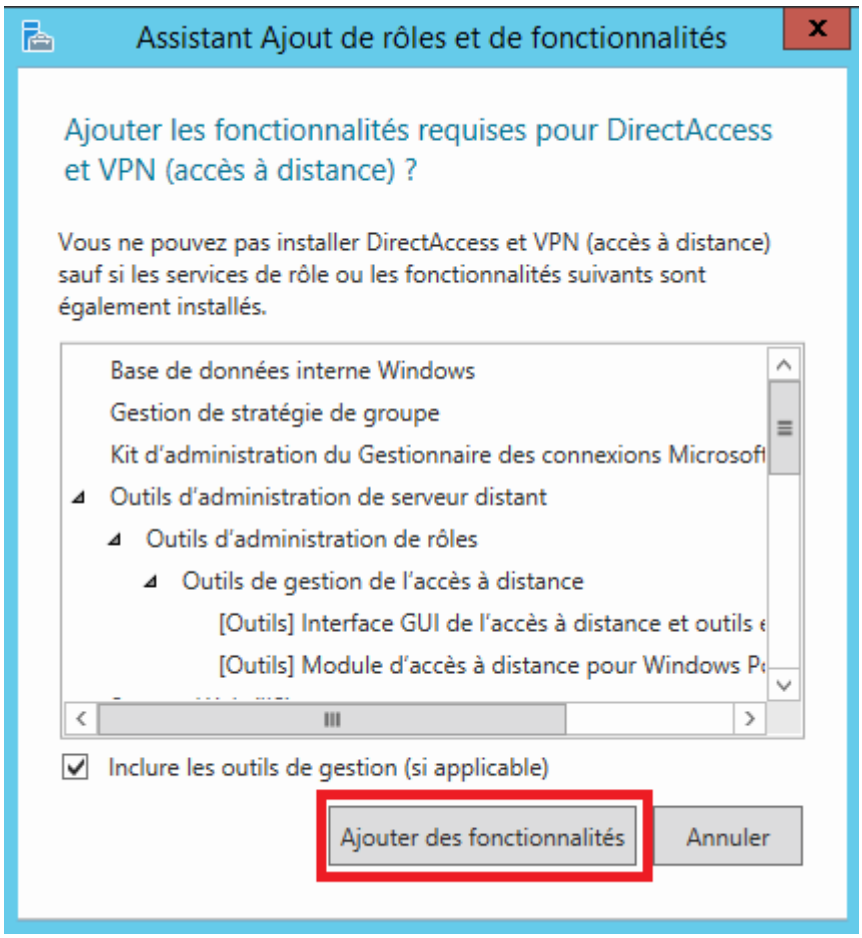
- Vérifiez que le serveur SRV-DA soit sélectionné et cliquez sur **"Suivant"**.



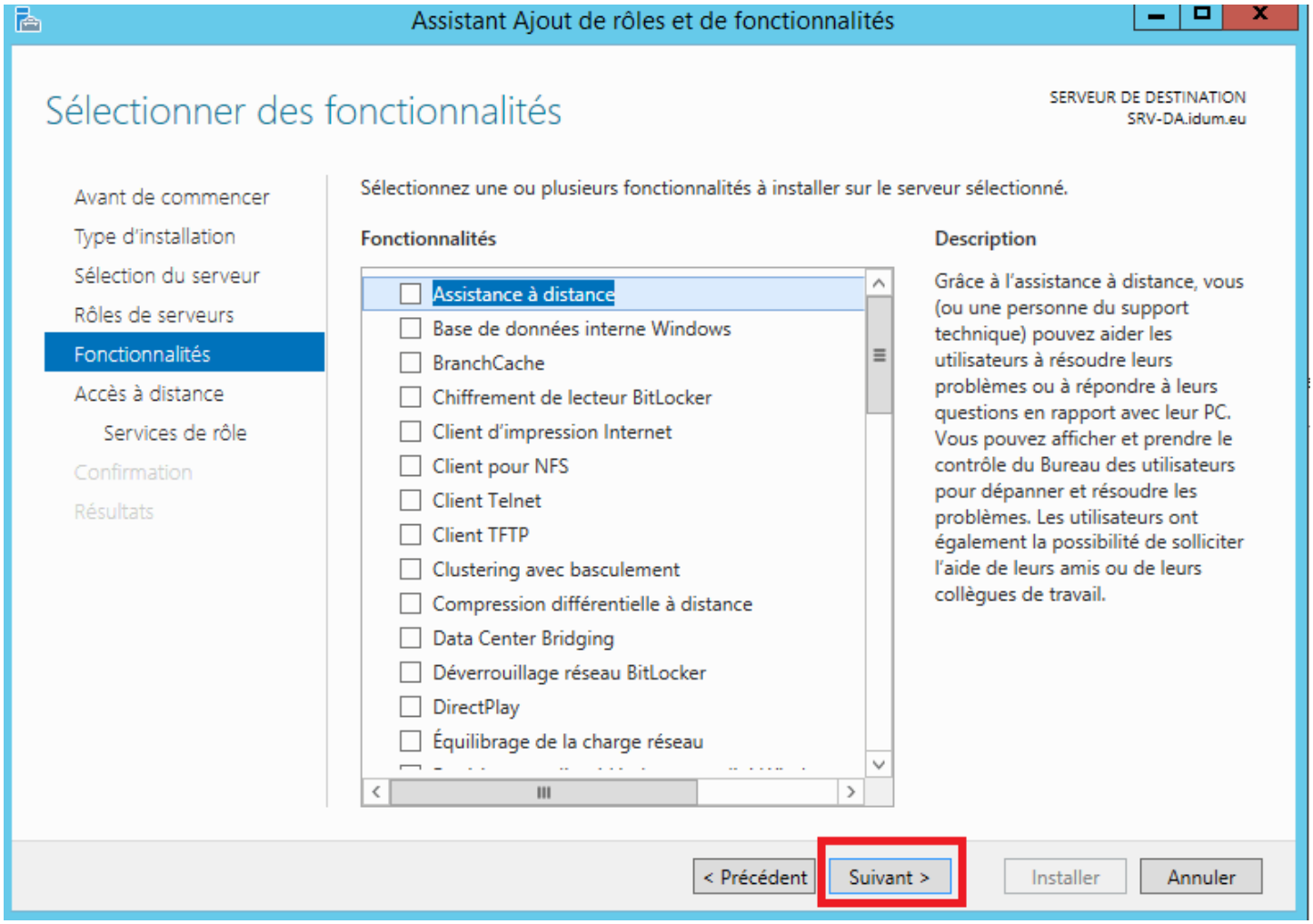
- Cochez **"Accès à distance"** et Cliquez sur **"Suivant"**.



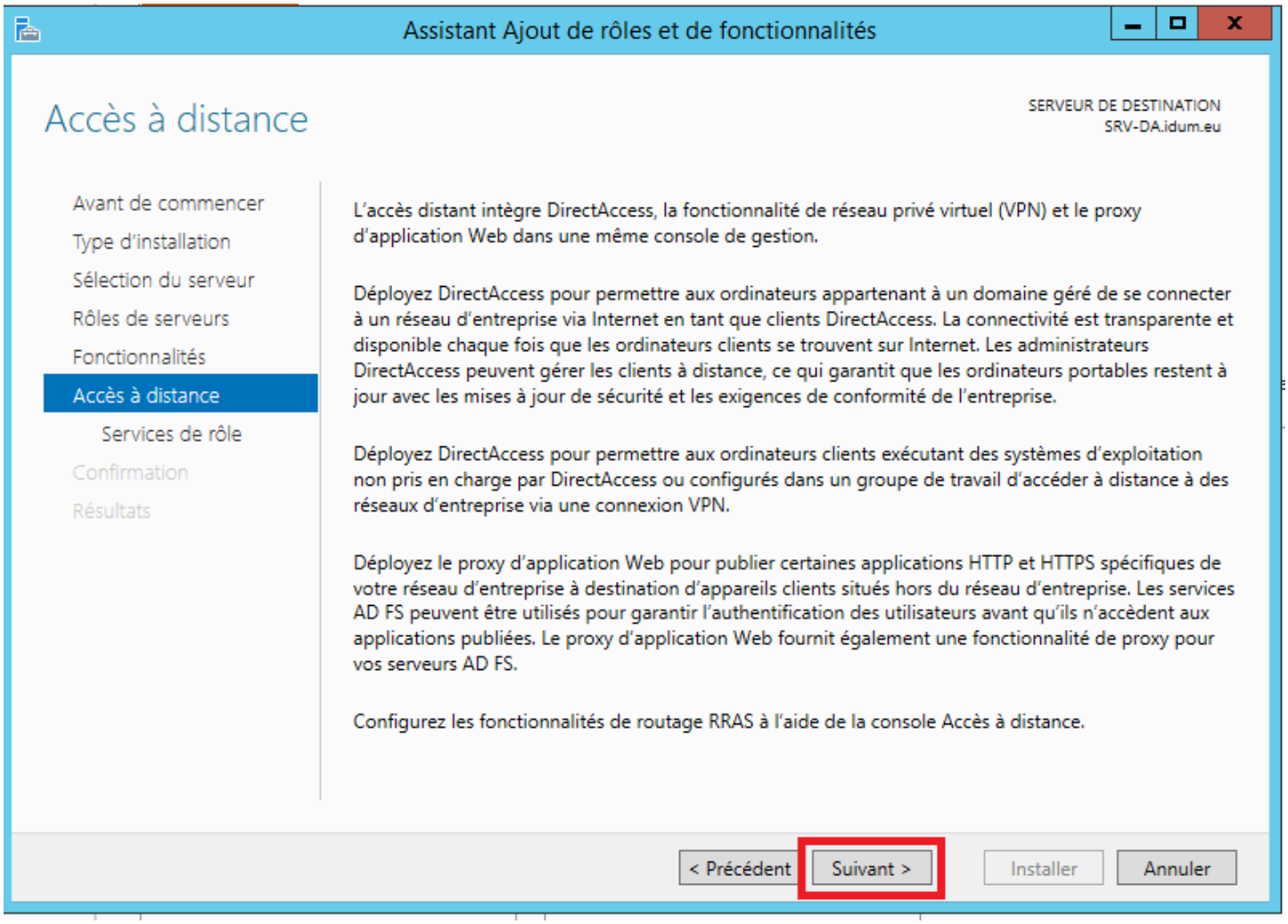
- Cliquez sur "**Ajouter des fonctionnalités**".



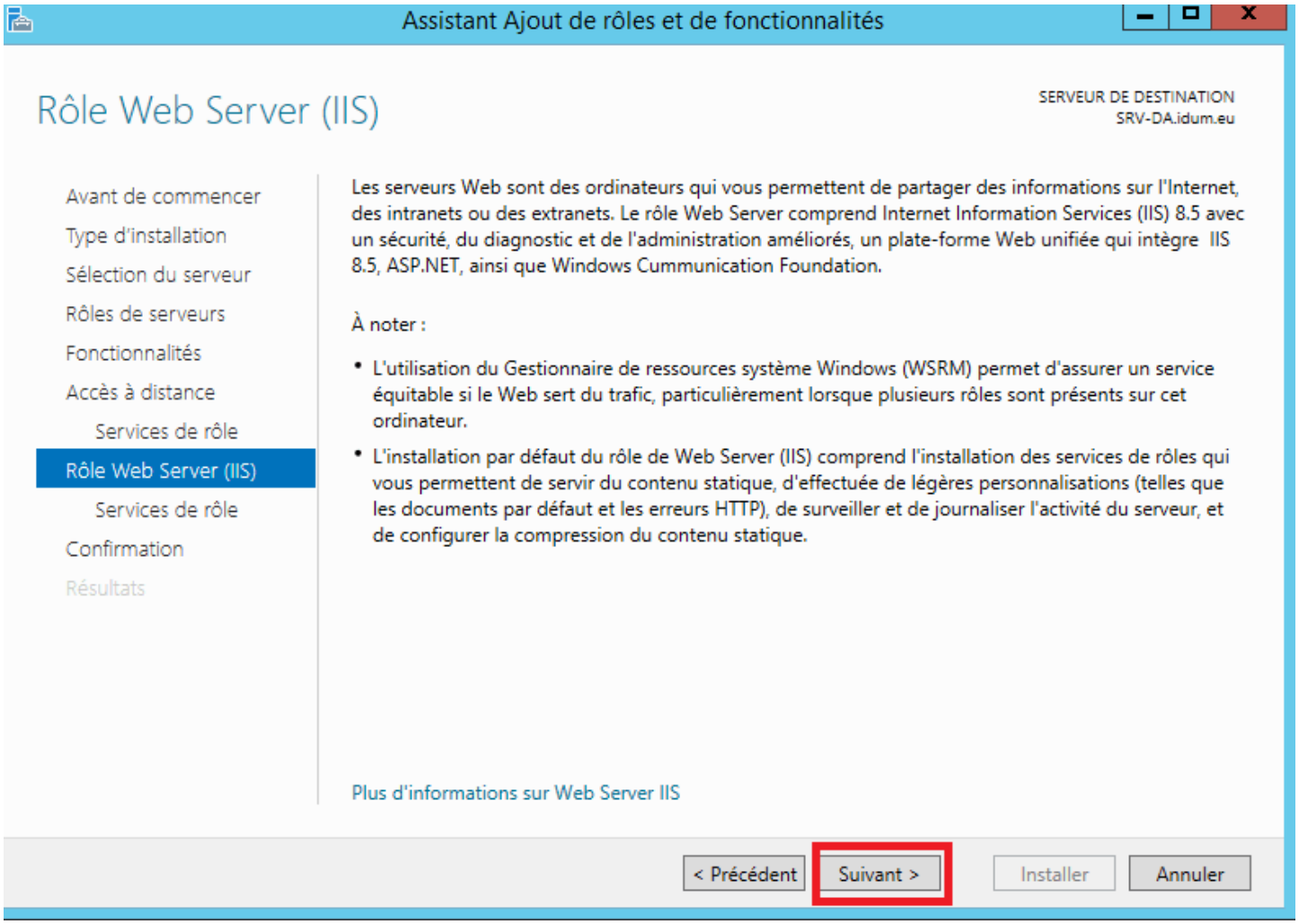
- Il n'y a rien de plus à faire sur ces pages, cliquez sur "**suivant**".



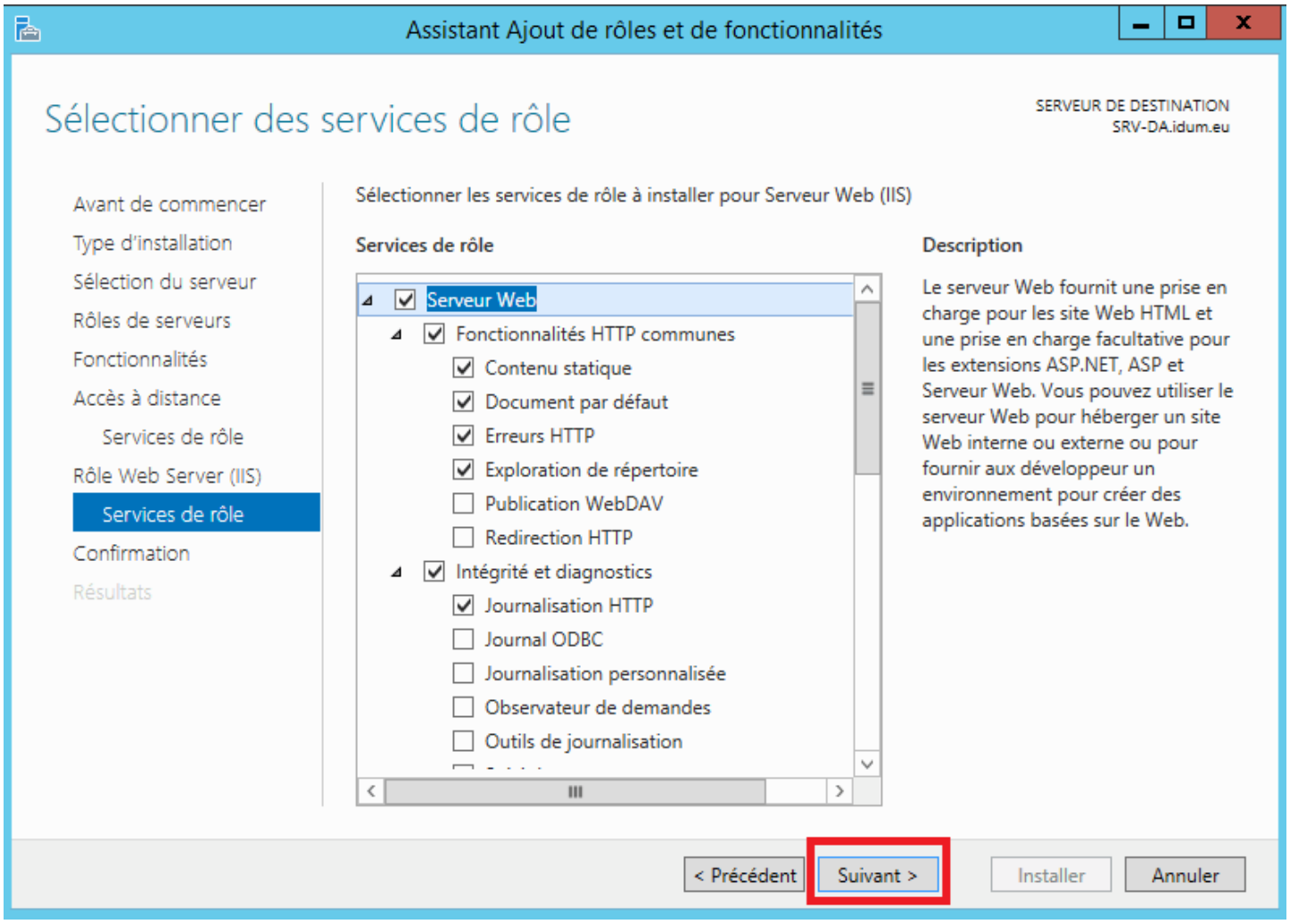
- Cliquez sur **"Suivant"**.



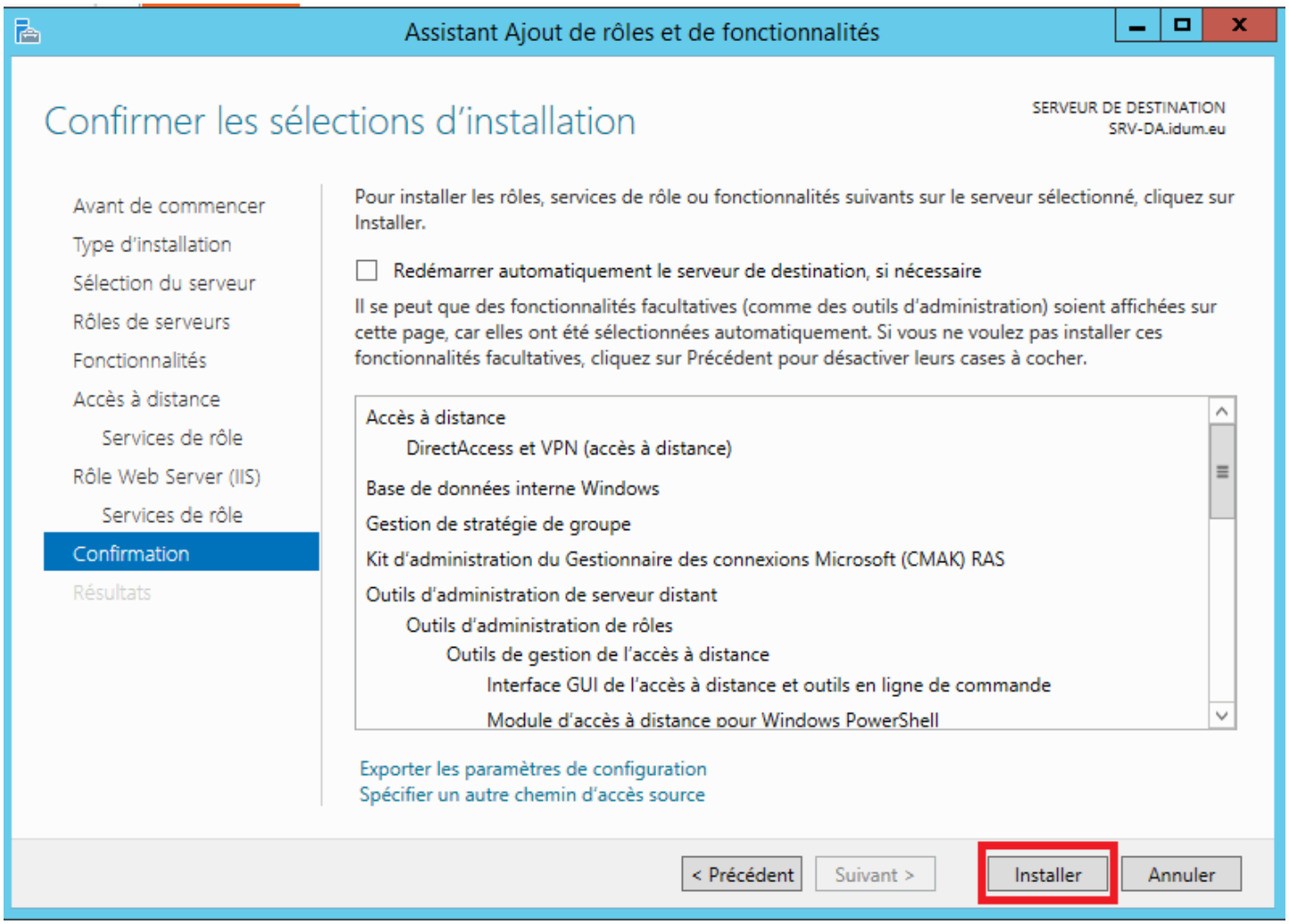
- Cliquez sur **"Suivant"**.



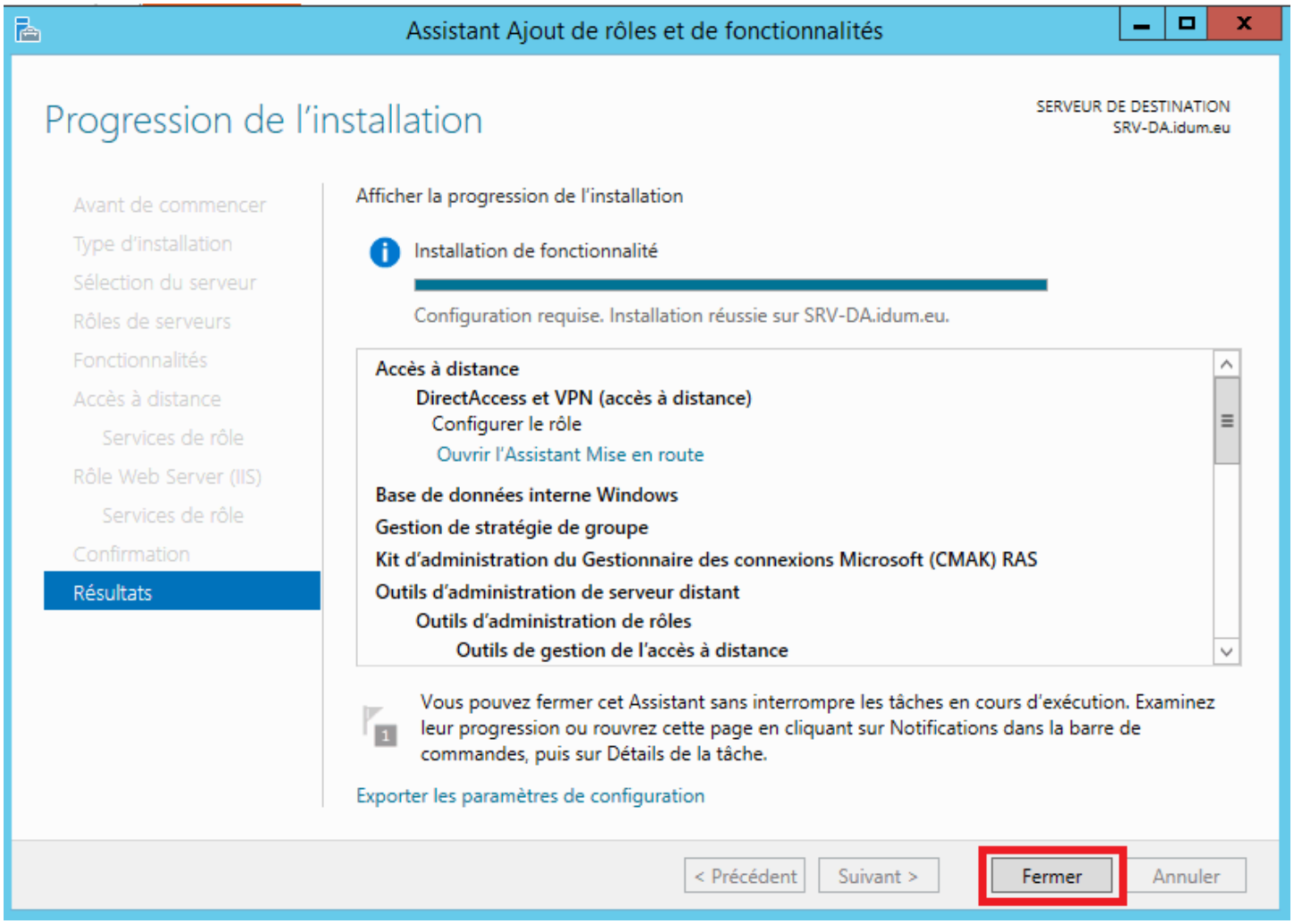
- Cliquez sur **"Suivant"**.



- Cliquez sur **"Installer"** et patientez jusqu'à la fin de l'opération.



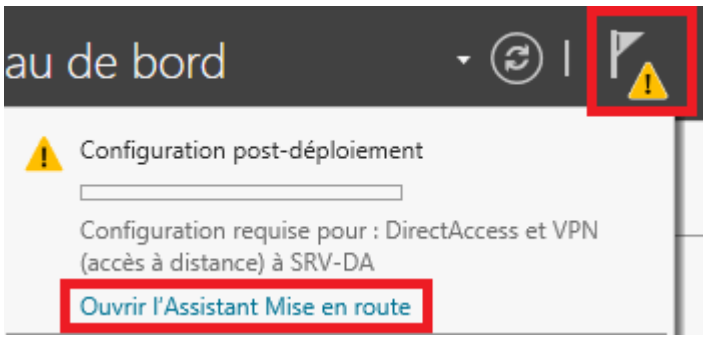
- Une fois terminée, cliquez sur **"Fermer"**.



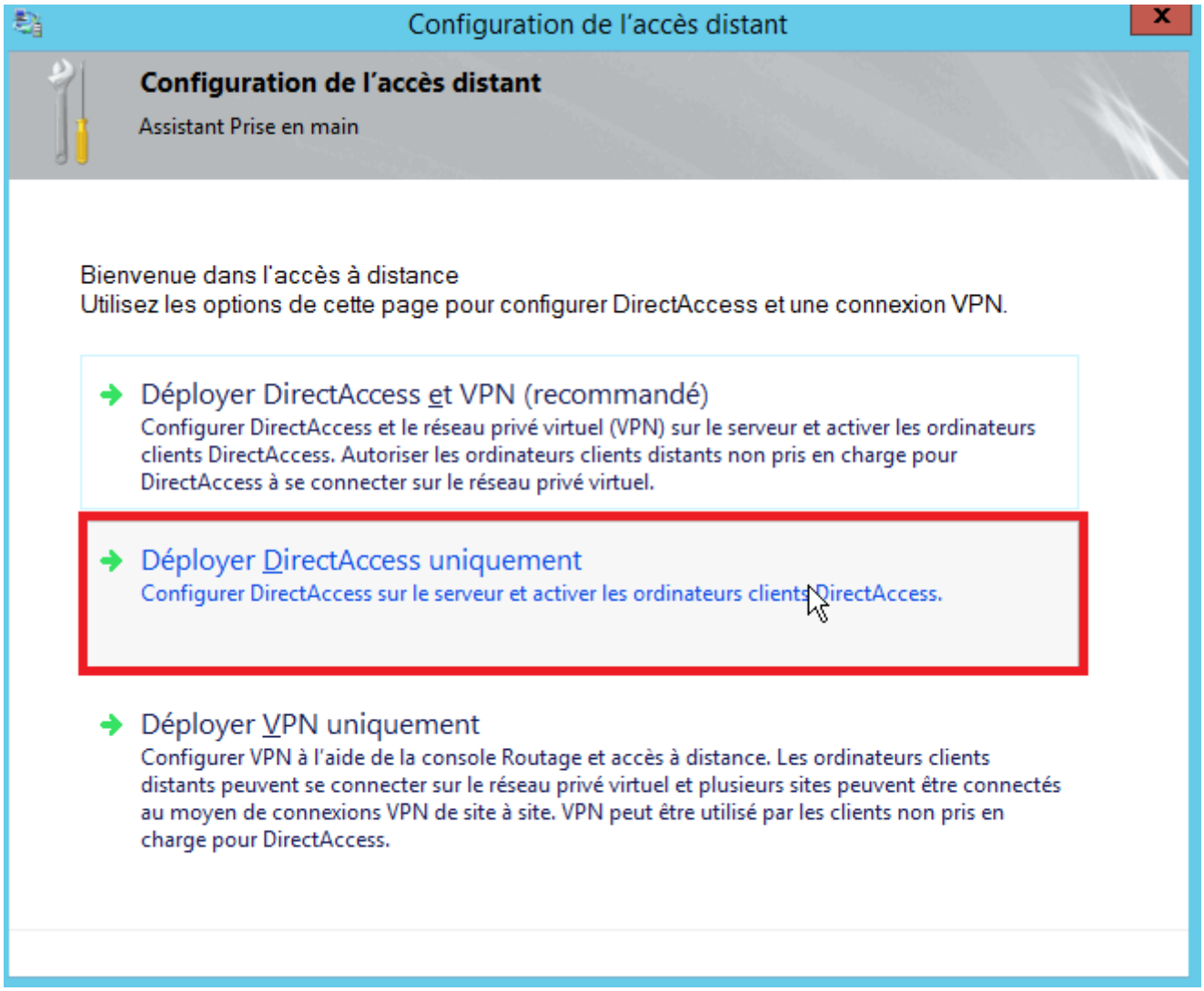
III) Configuration de DirectAccess

1) Configuration générale

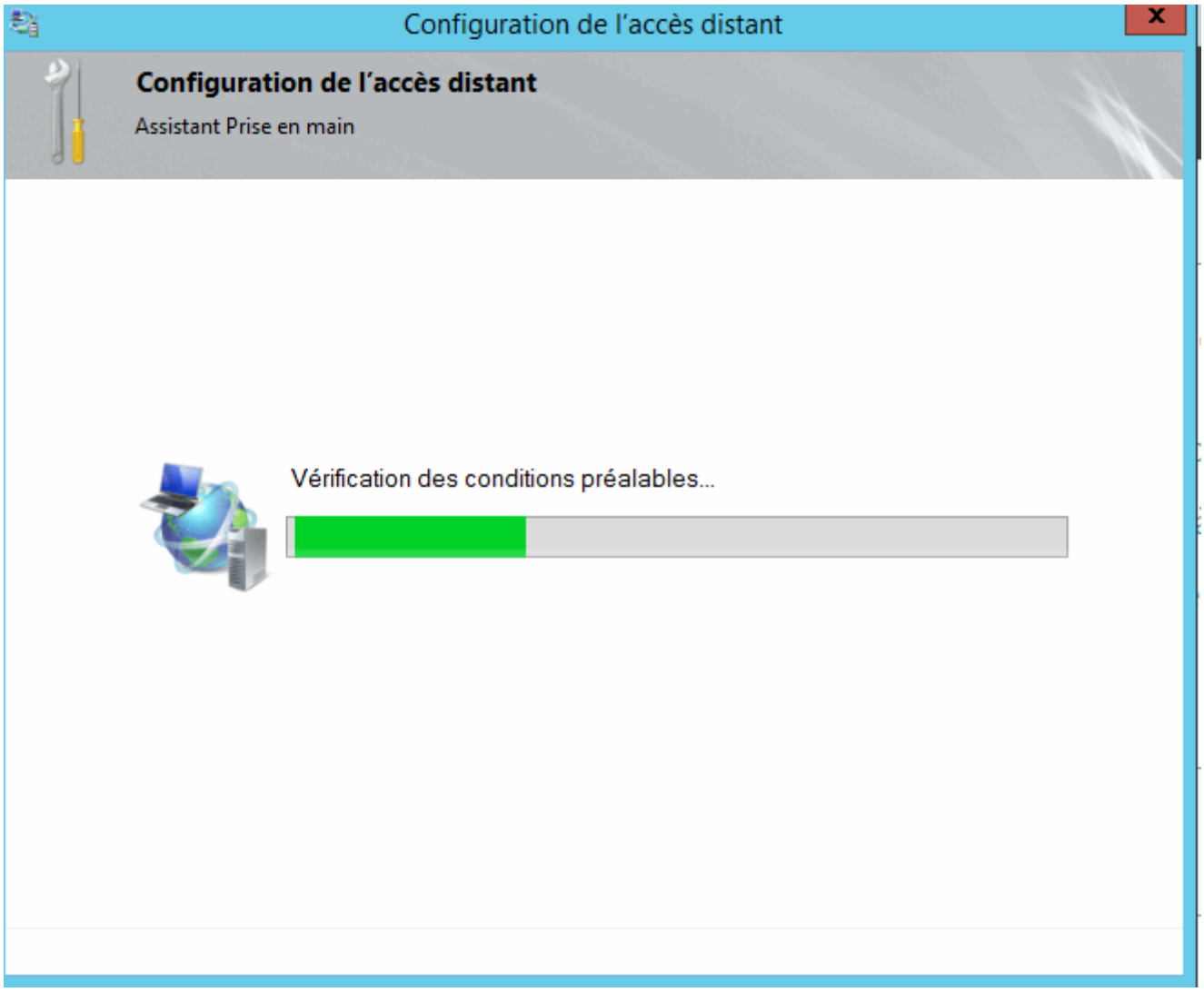
- Une fois le rôle installé, cliquez sur les actions à réaliser et ouvrez l'Assistant de Mise en route.



- Sélectionnez **"Déployez DirectAccess uniquement"**.

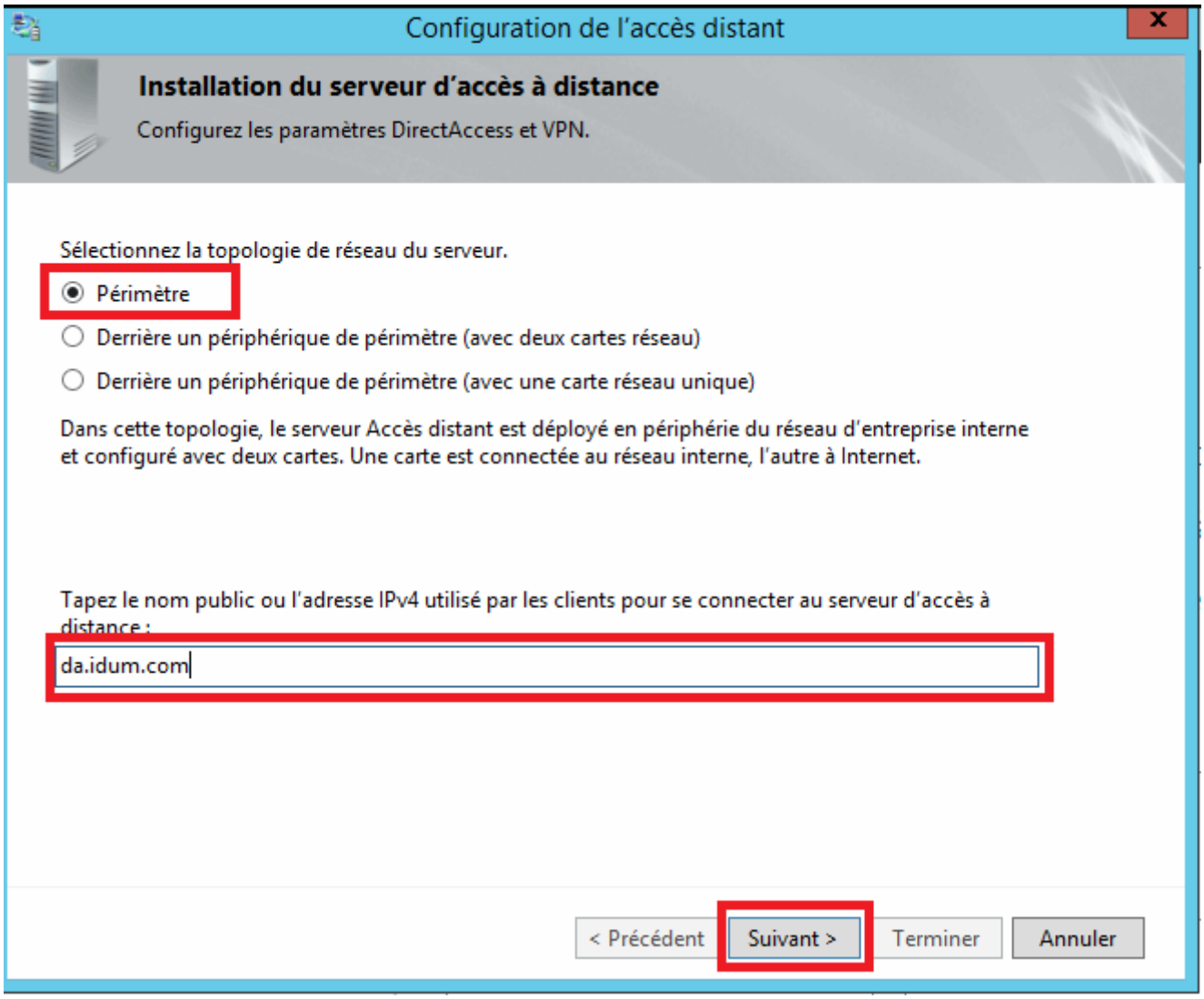


- Patientez durant les tests de faisabilité du service.

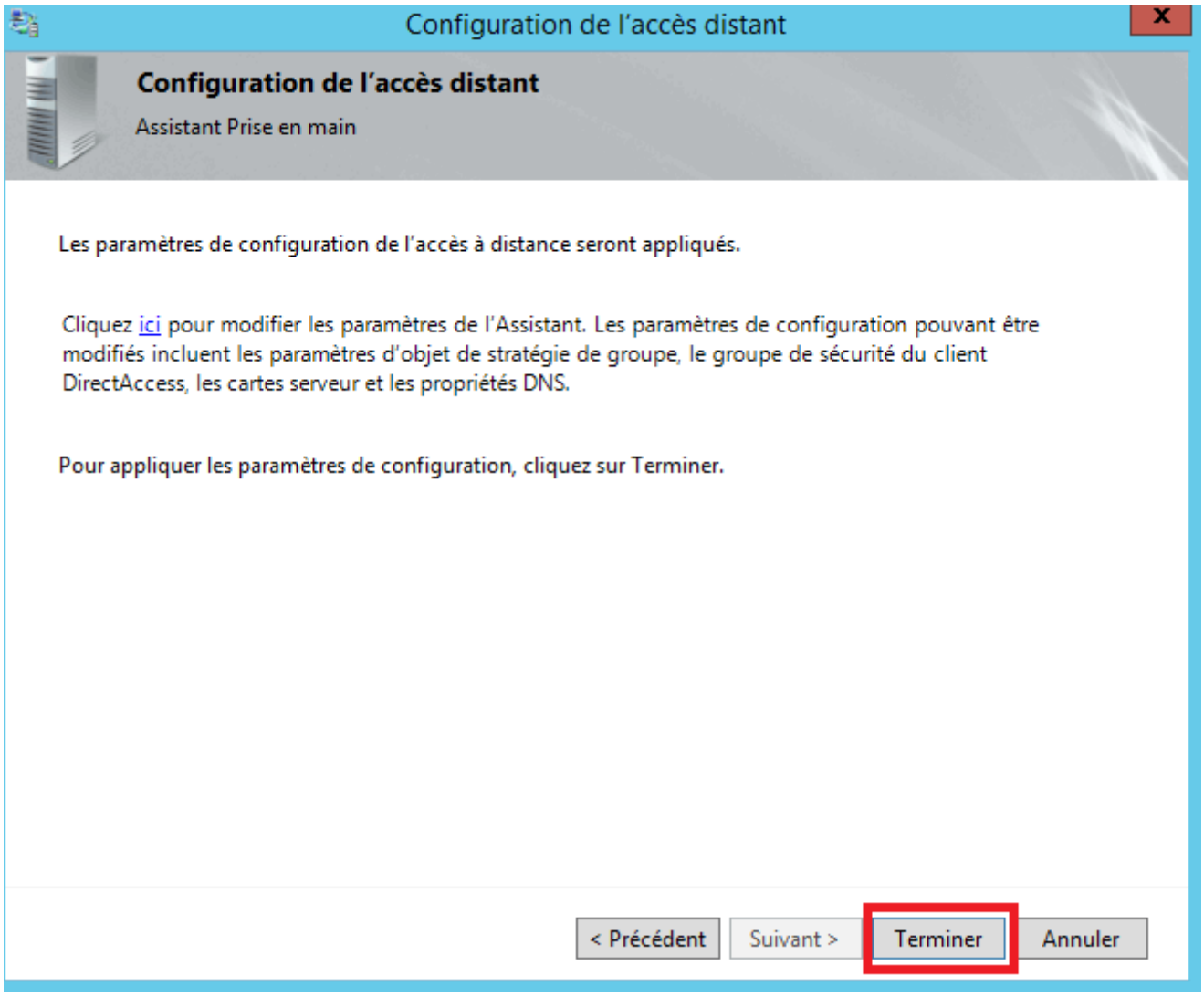


- Sélectionnez **"Périmètre"** : c'est à dire que notre serveur possède une interface dans le LAN et une interface dans le WAN. La seconde option est utilisée dans le cas où le serveur Direct Access est situé dans une DMZ et possède une interface dans le LAN. La dernière est utile quand le serveur Direct Access est situé dans une DMZ sans accès au LAN.

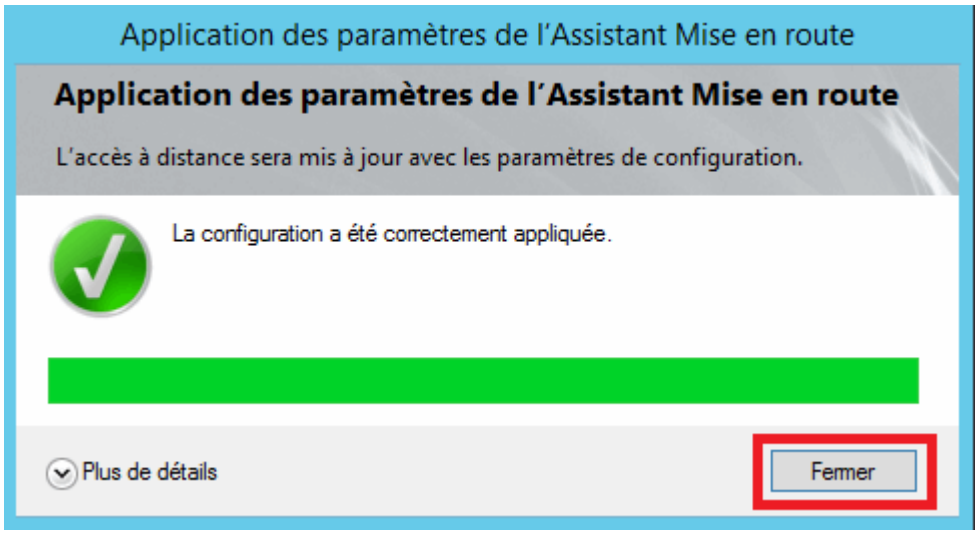
- Le nom public est le nom sur lequel les clients vont connecter leurs VPN, pour nous ce sera **"da.idum.com"**.



- Cliquez sur **"Terminer"** pour lancer la configuration.



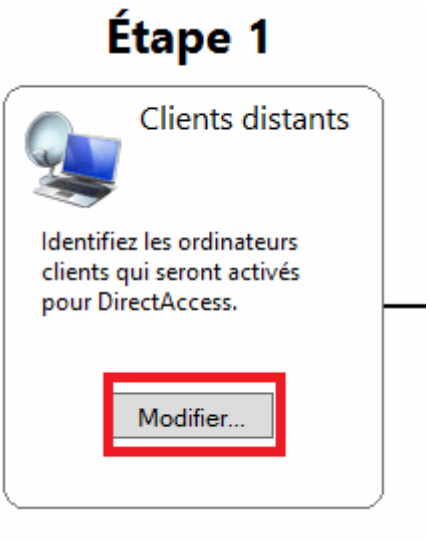
- Patientez jusqu'à la fin de la configuration, puis cliquez sur **"Fermer"**.



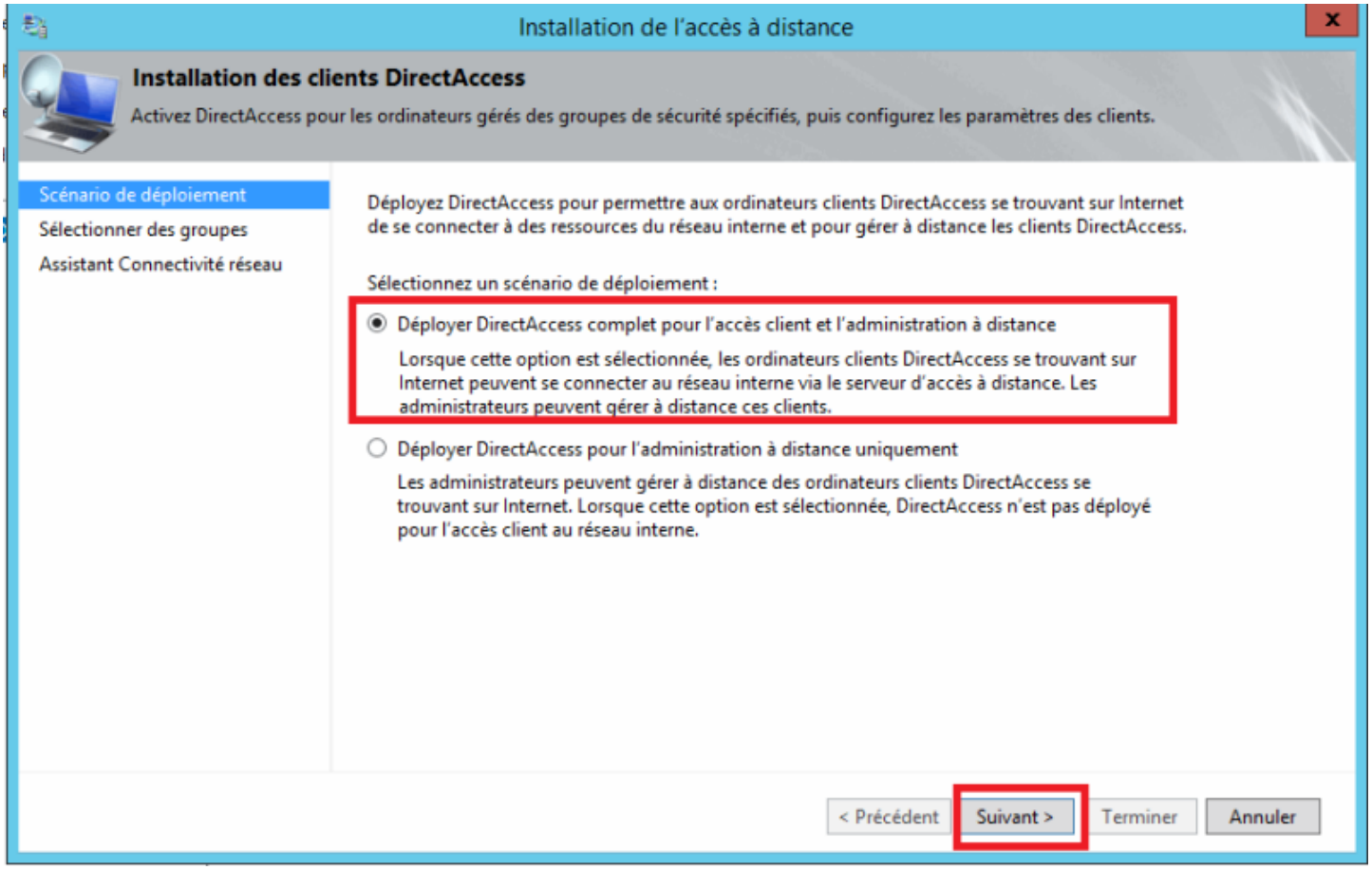
2) Configuration des paramètres des clients distant

Nous allons maintenant configurer la partie qui sera déployé sur les postes clients.

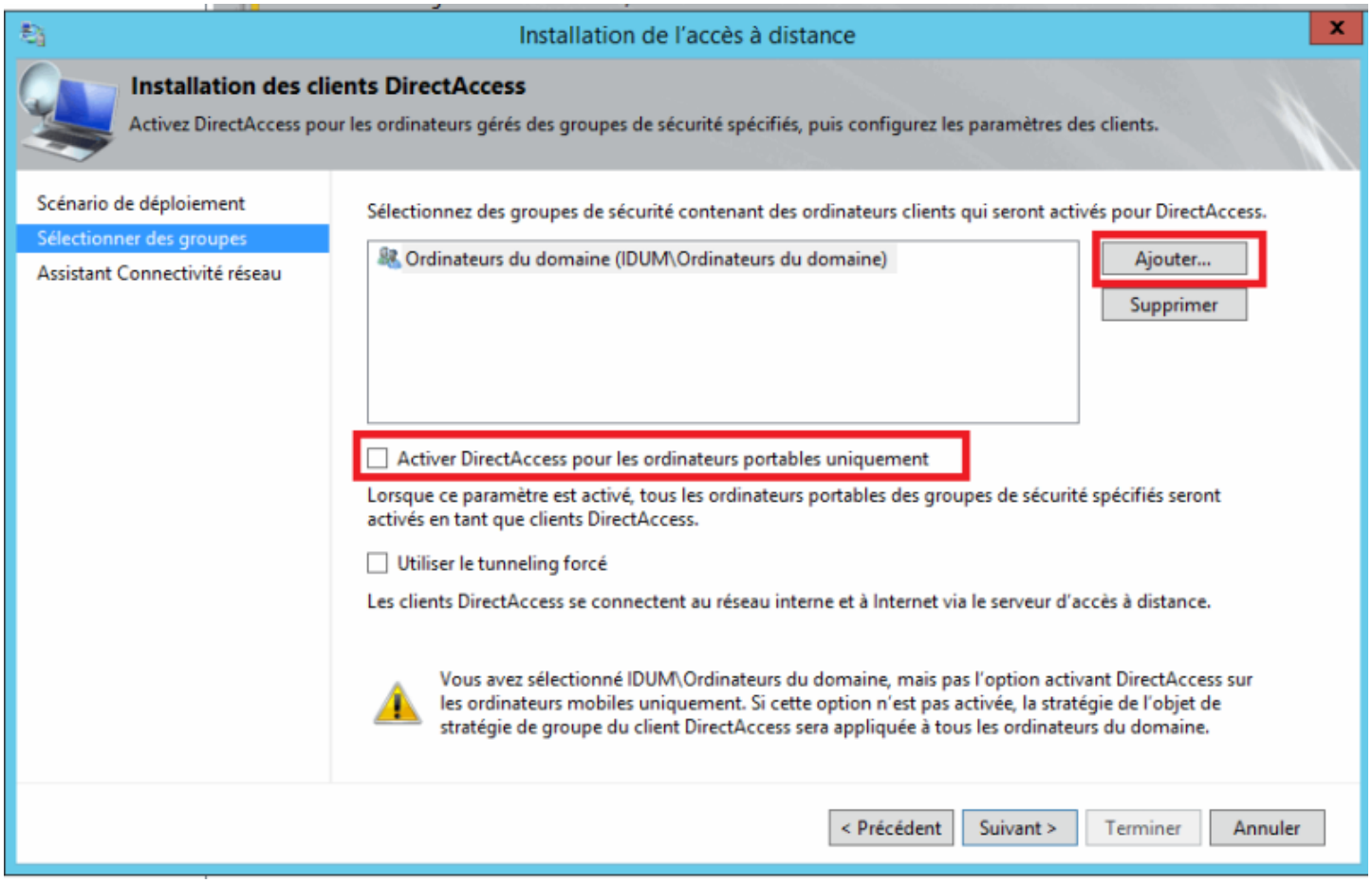
- Cliquez sur **"Modifier"**.



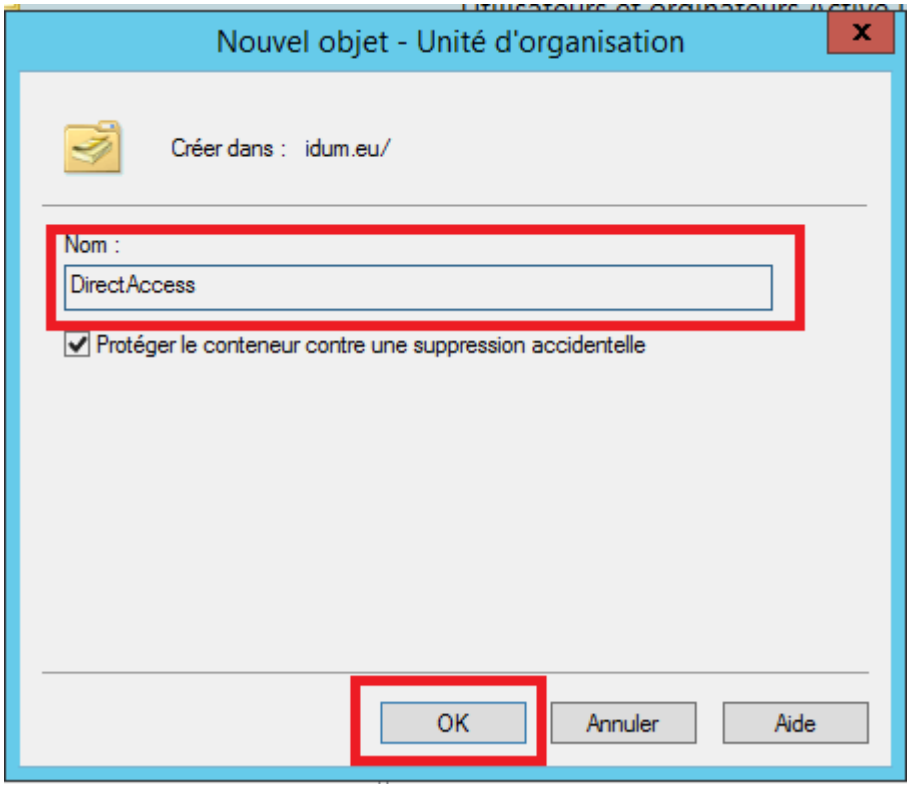
- Sélectionnez la première option et cliquer sur **"Suivant"**.



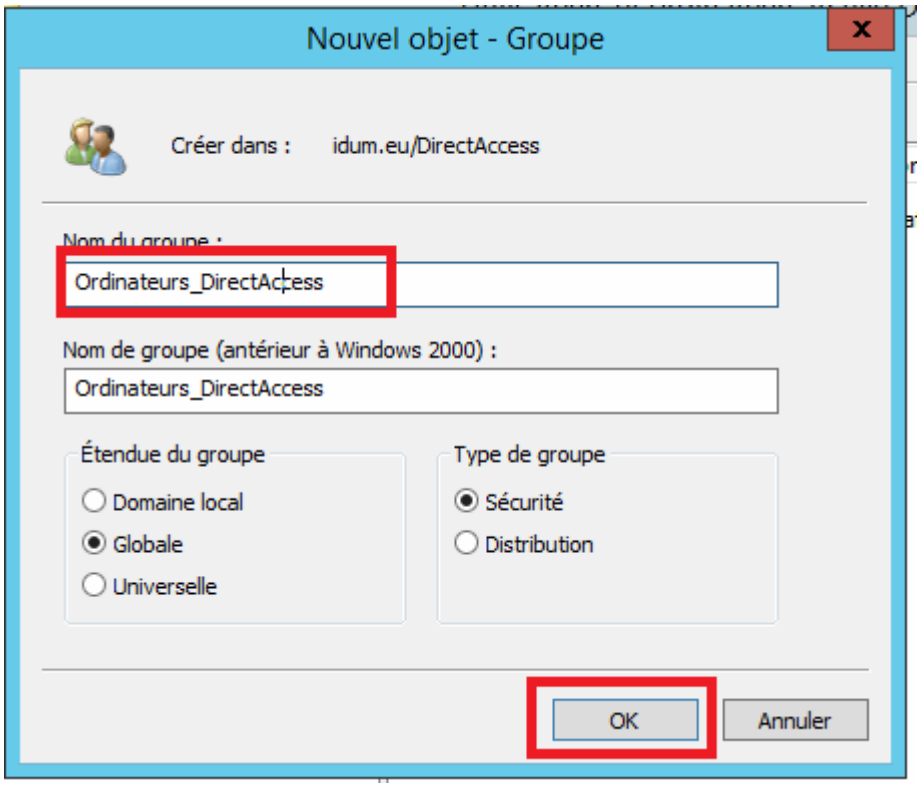
- Par défaut, l'assistant de configuration nous propose de déployer DirectAccess sur tous les ordinateurs du domaine, dans notre exemple, nous allons créer un groupe d'ordinateur spécial pour les clients DirectAccess.



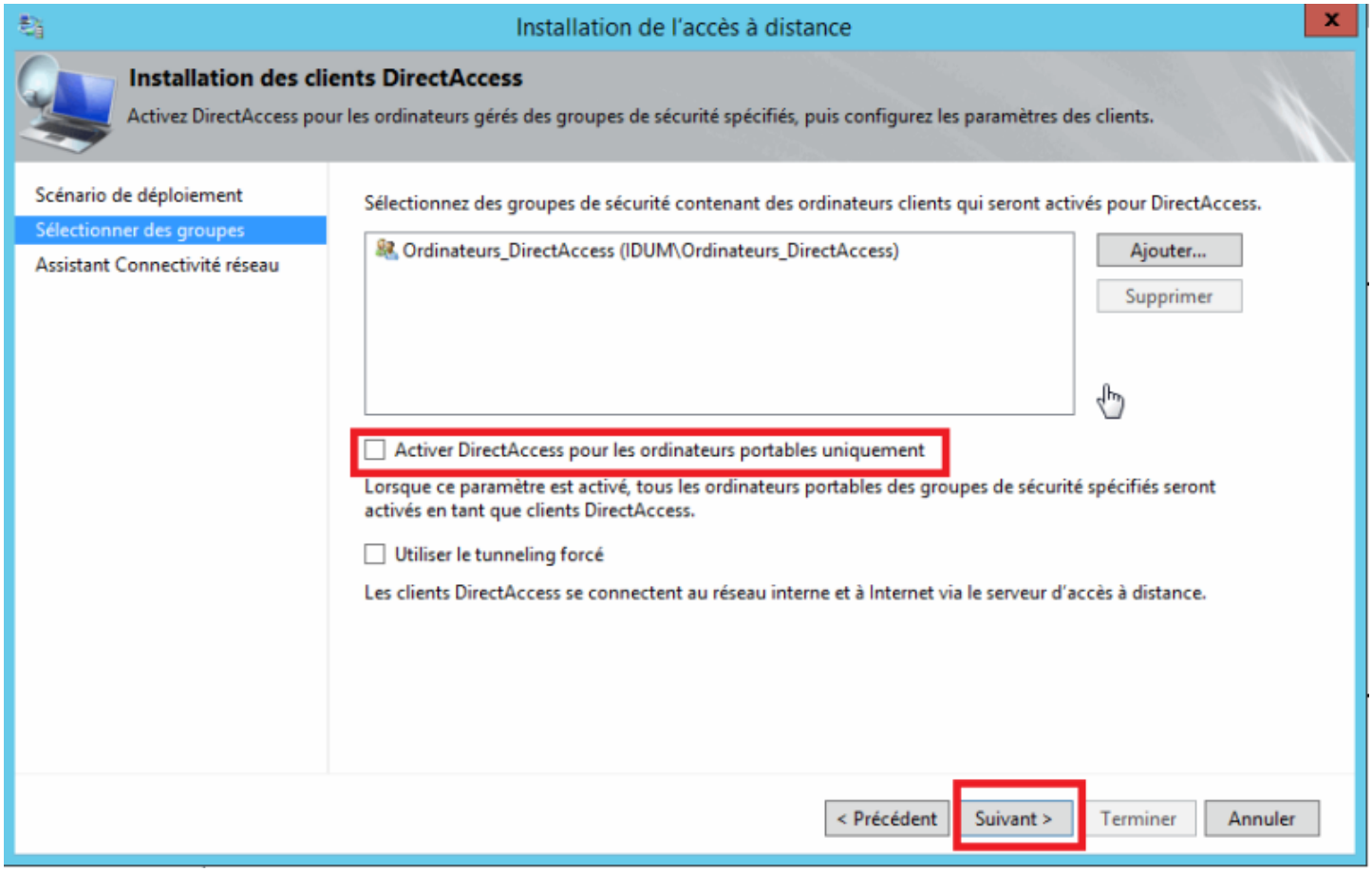
- Sur l'ActiveDirectory, créez une OU (Unité organisationnelle) et créez un groupe dans cette OU. Dans l'outil **"Utilisateurs et ordinateurs du domaine"**, faites un clic droit sur le domaine et sélectionnez **"nouveau"** puis **"Unité d'organisation"**. Nommez-la comme vous voulez.



- A l'intérieur de cette OU, créez un groupe et nommez le comme vous voulez.

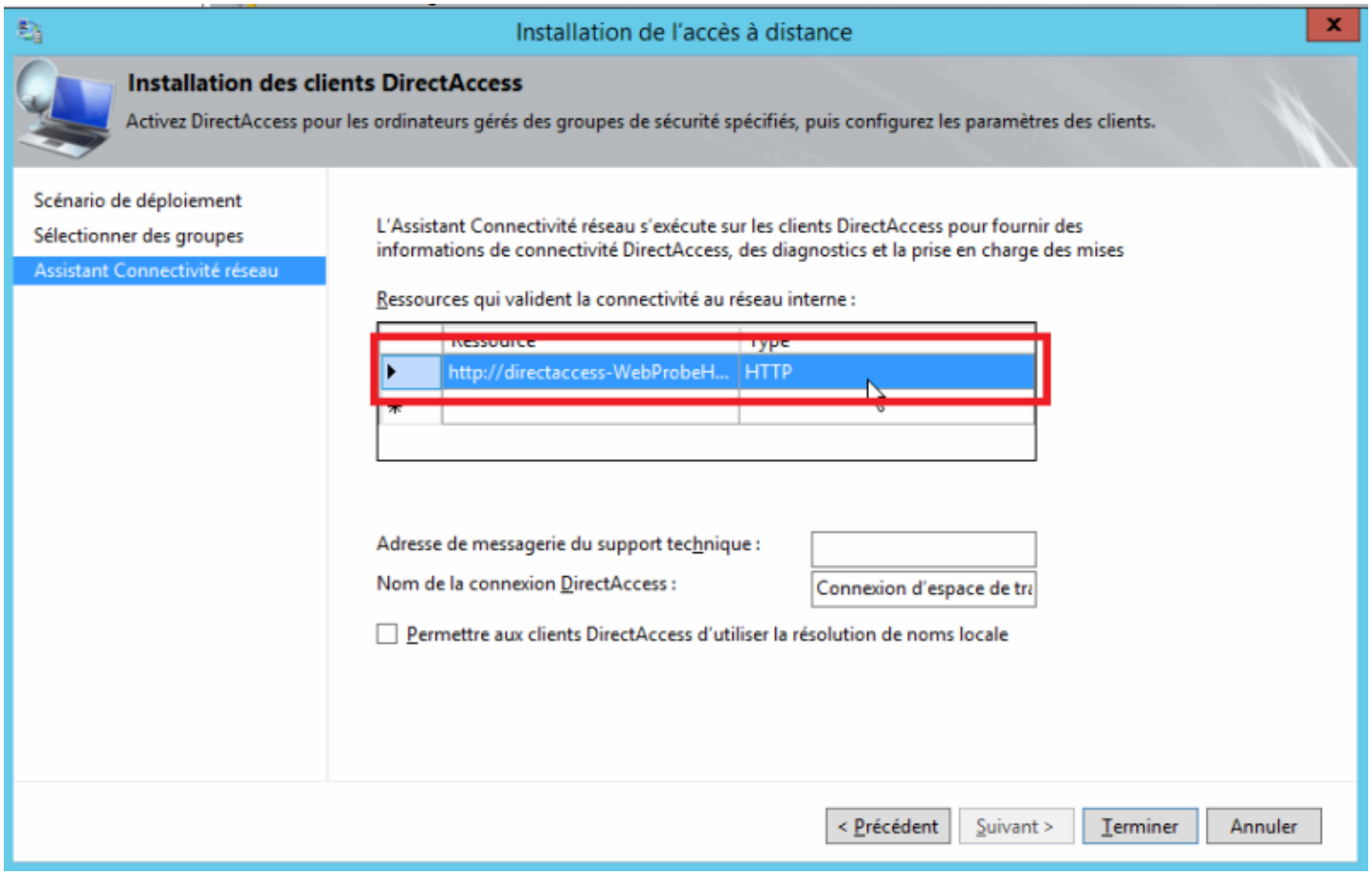


- Revenons à l'assistant de configuration, sélectionnez **"Ajouter"** et entrer le nom de votre groupe. En passant, décocher l'option **"Activez DirectAccess pour les ordinateurs portables uniquement"**.

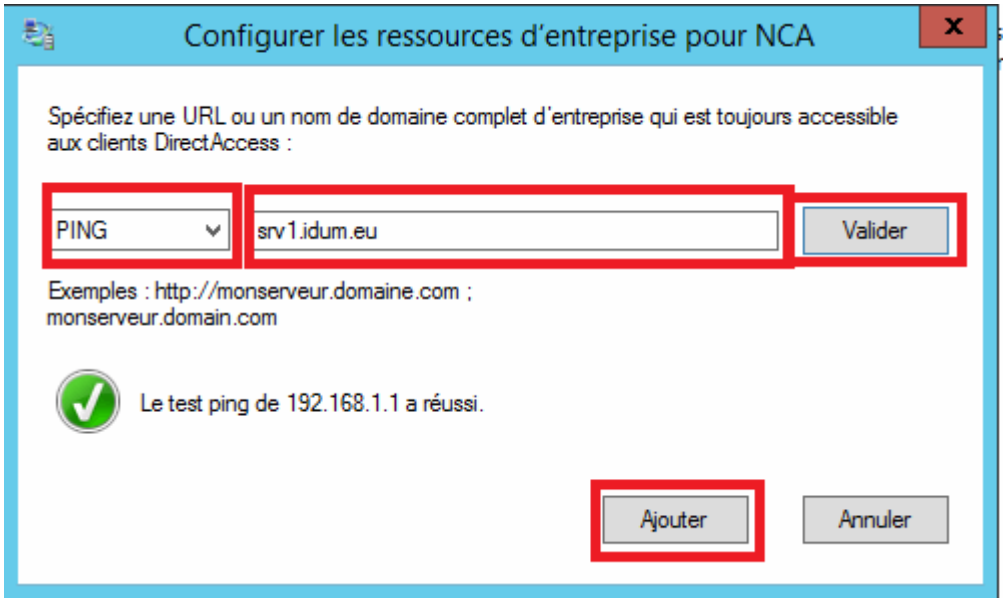


L'assistant de connectivité réseau c'est le protocole de test pour savoir si l'ordinateur se trouve dans le LAN ou bien s'il est hors du réseau local. Pour notre démonstration, nous allons faire un ping vers le serveur ActiveDirectory, à savoir srv1.idum.eu.

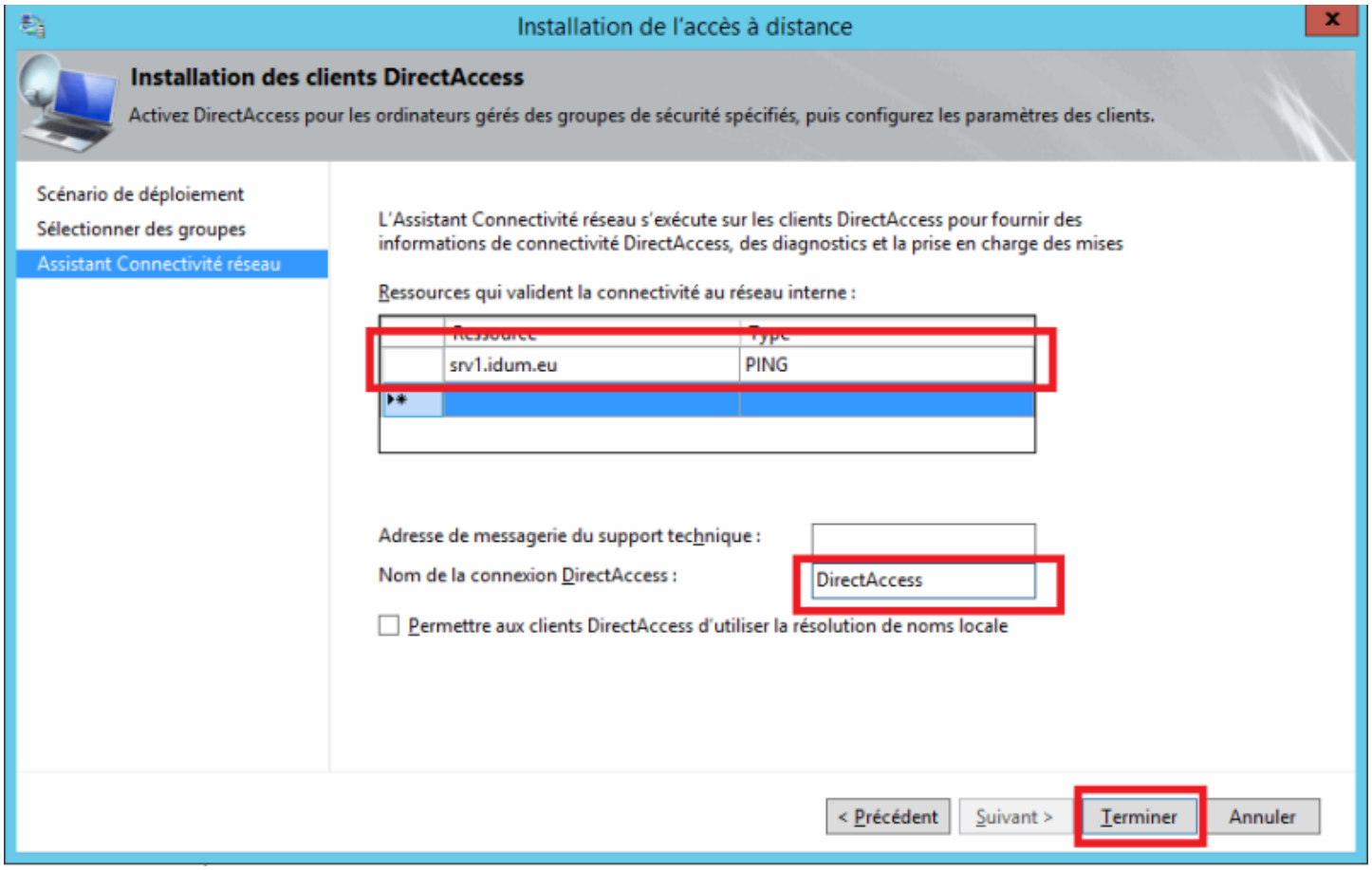
- Faites un clic droit sur la ligne déjà proposé et cliquez sur **"Supprimer"**. Faîte un clic droit sur la ligne vide et cliquez sur **"Nouveau"**.



- Dans la première case sélectionnez **"Ping"** et dans la seconde entrez le nom du serveur à contacter. Cliquez sur **"Valider"** et sur **"Ajouter"**.

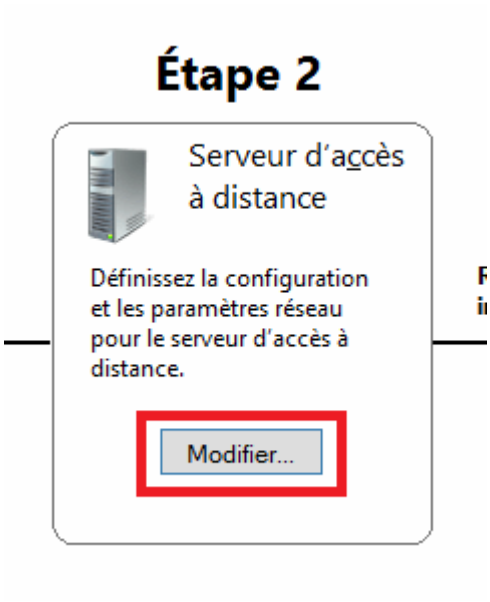


- Dans **"Nom de la connexion"** entrer le nom que vous souhaitez voir apparaître sur le client.

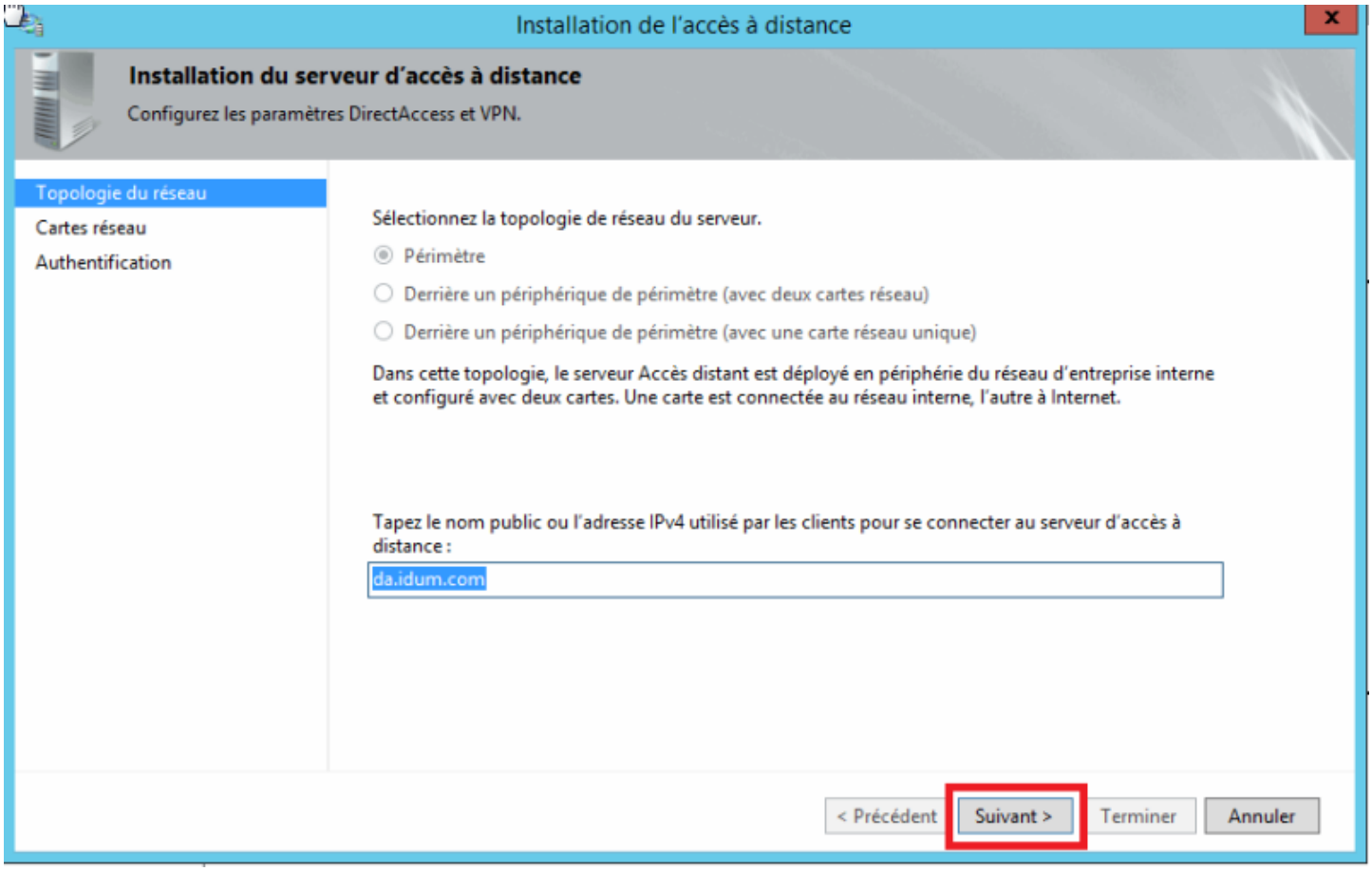


3) Configuration du serveur d'accès à distance

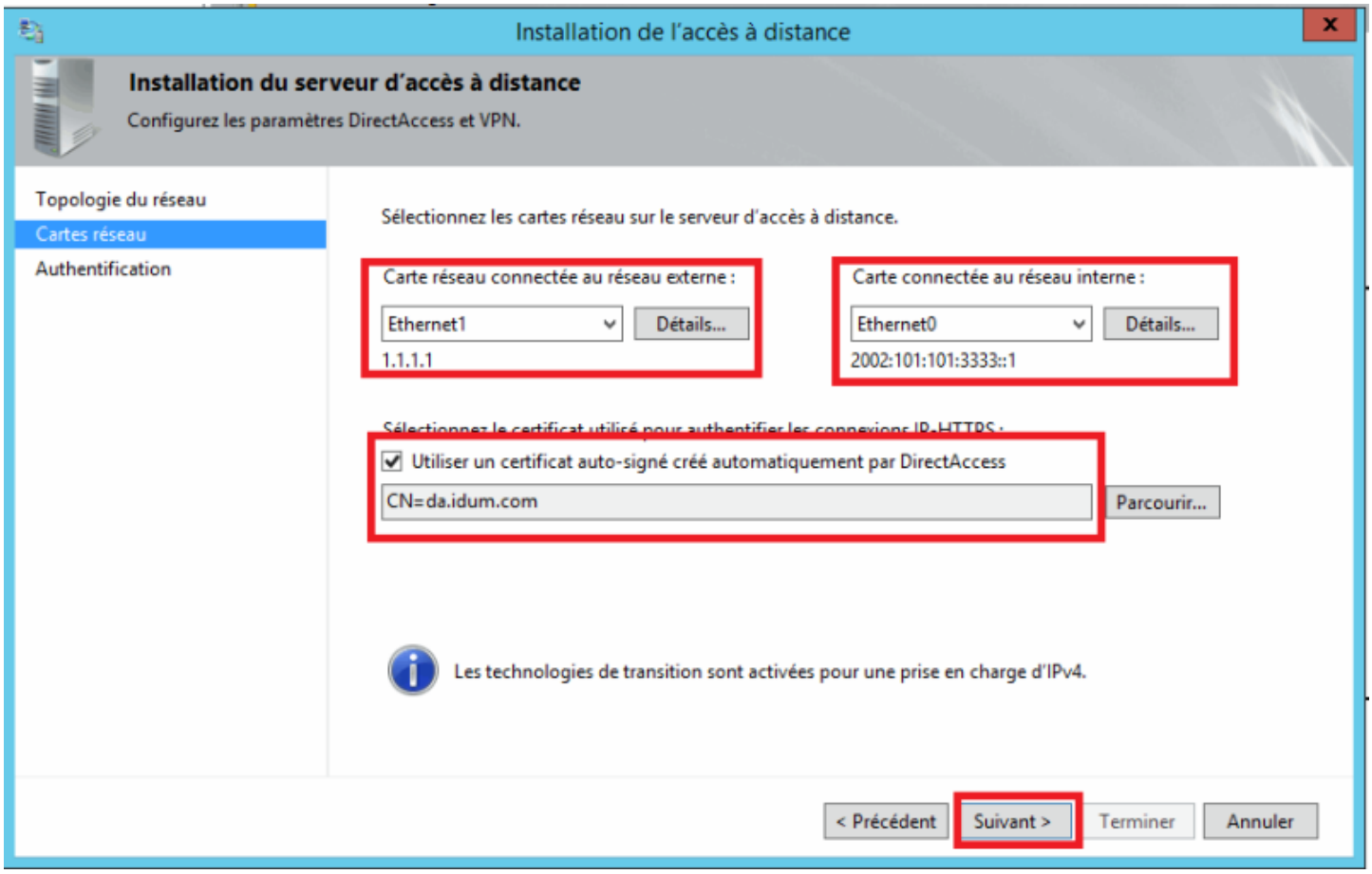
- Nous allons passez à l'étape 2, cliquez sur "**Modifier**".



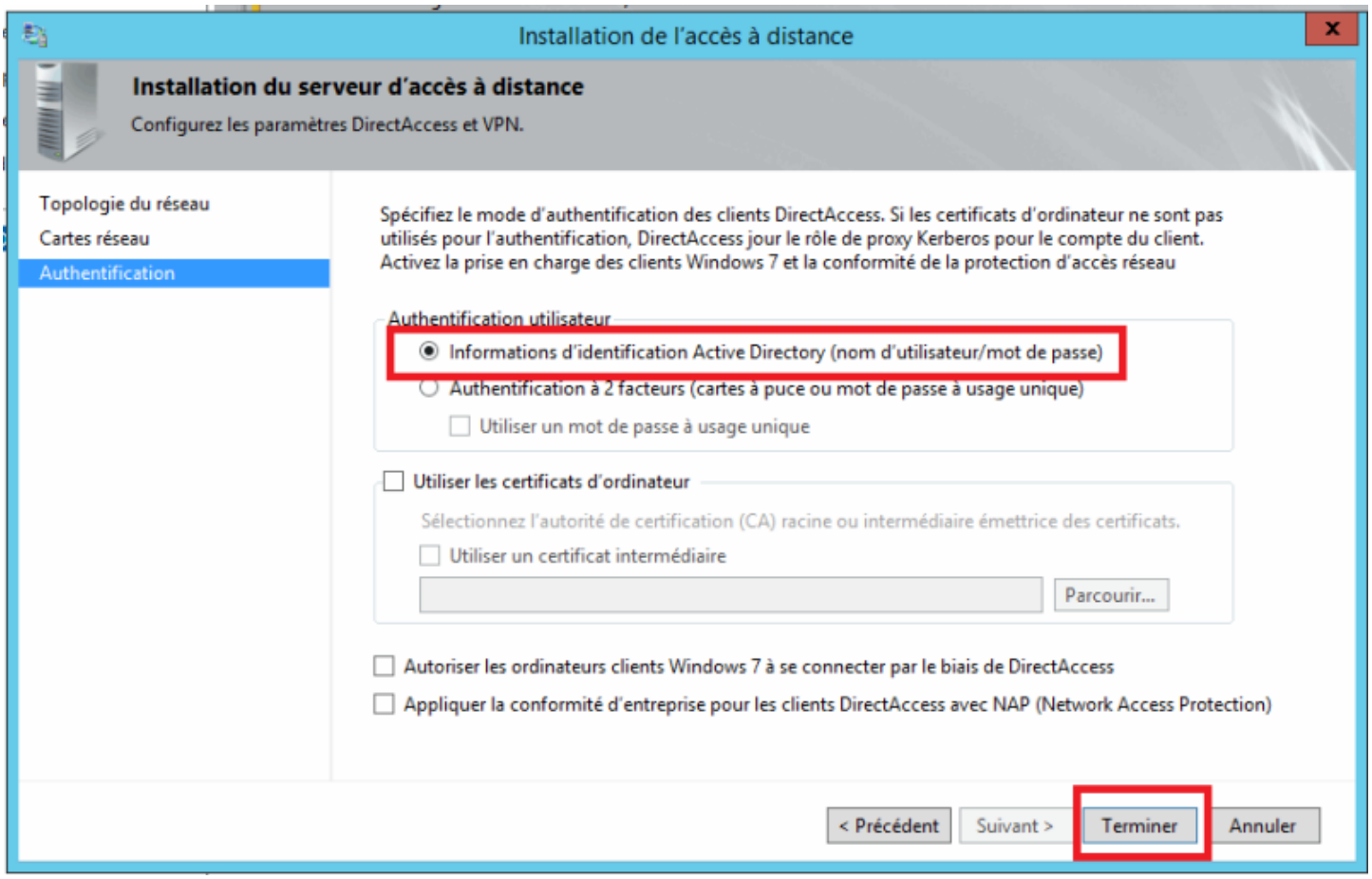
- Vous retrouvez ici le paramètre défini avant, ne modifiez rien et cliquez sur "**Suivant**".



- Vérifiez que l'affectation des cartes réseaux est correcte, et cliquez sur "**Suivant**".

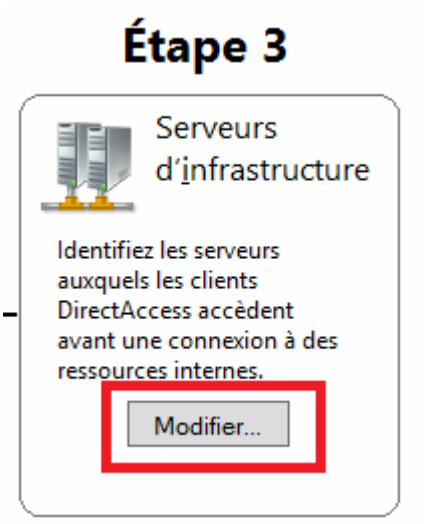


- Pour authentifier l'utilisateur, nous utiliserons le login/mot de passe Active Directory, cliquez sur "**Terminer**".

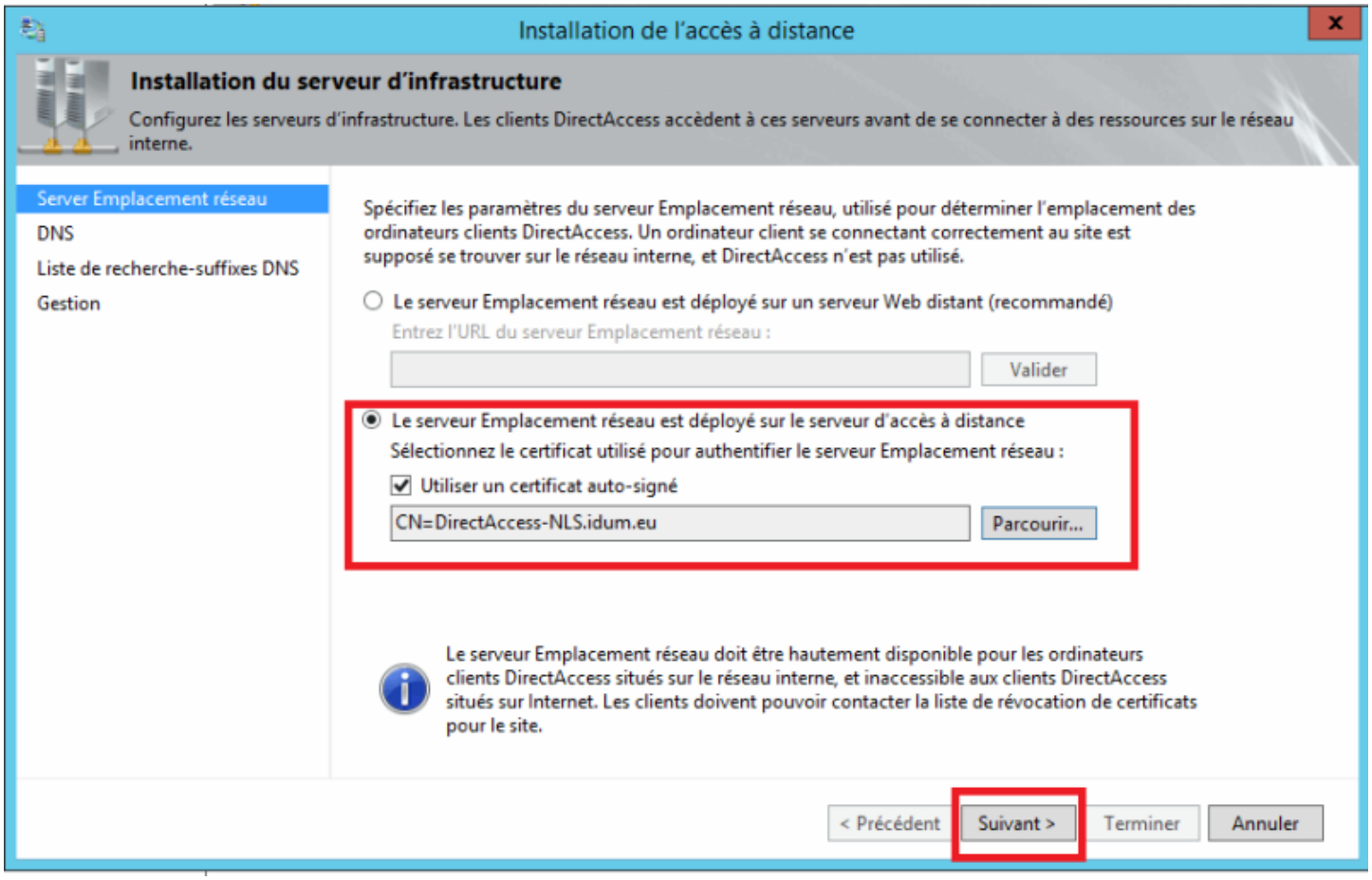


4)Configuration des ressources internet disponible à distance

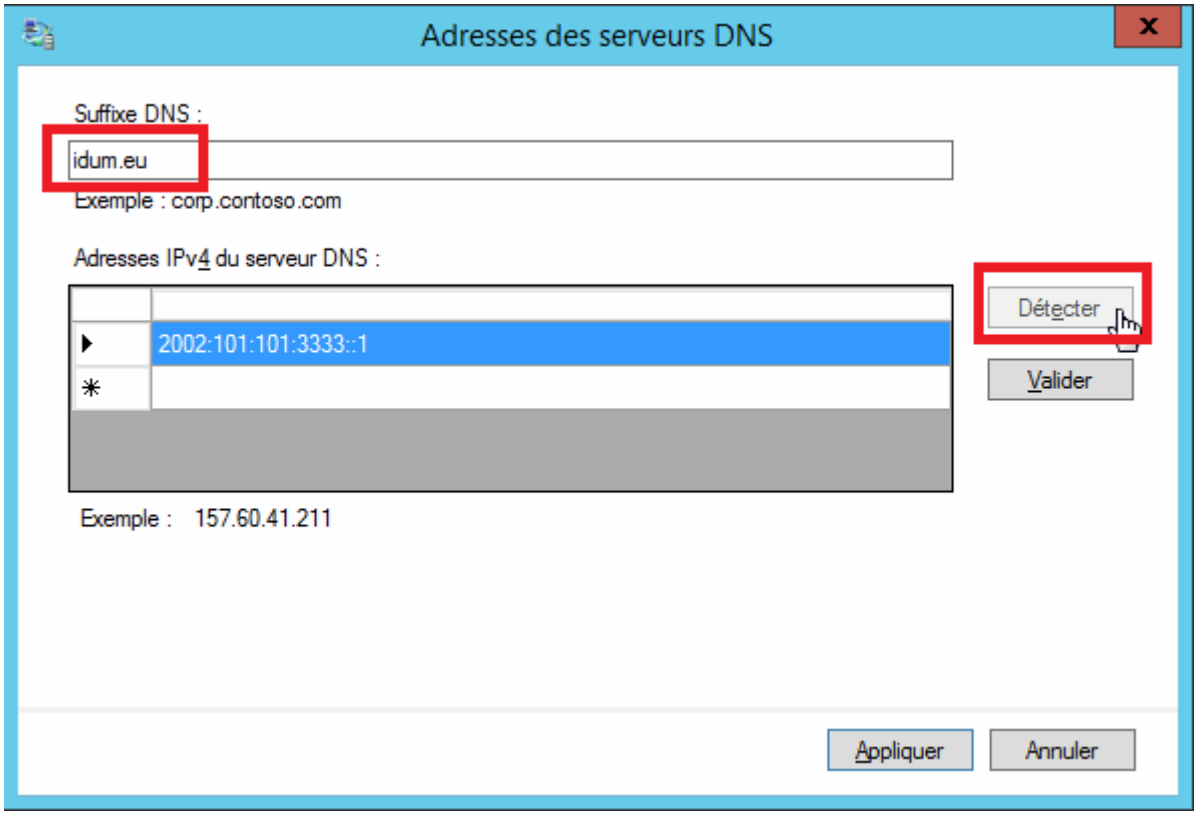
- Passons à la dernière étape de la configuration de DirectAccess :



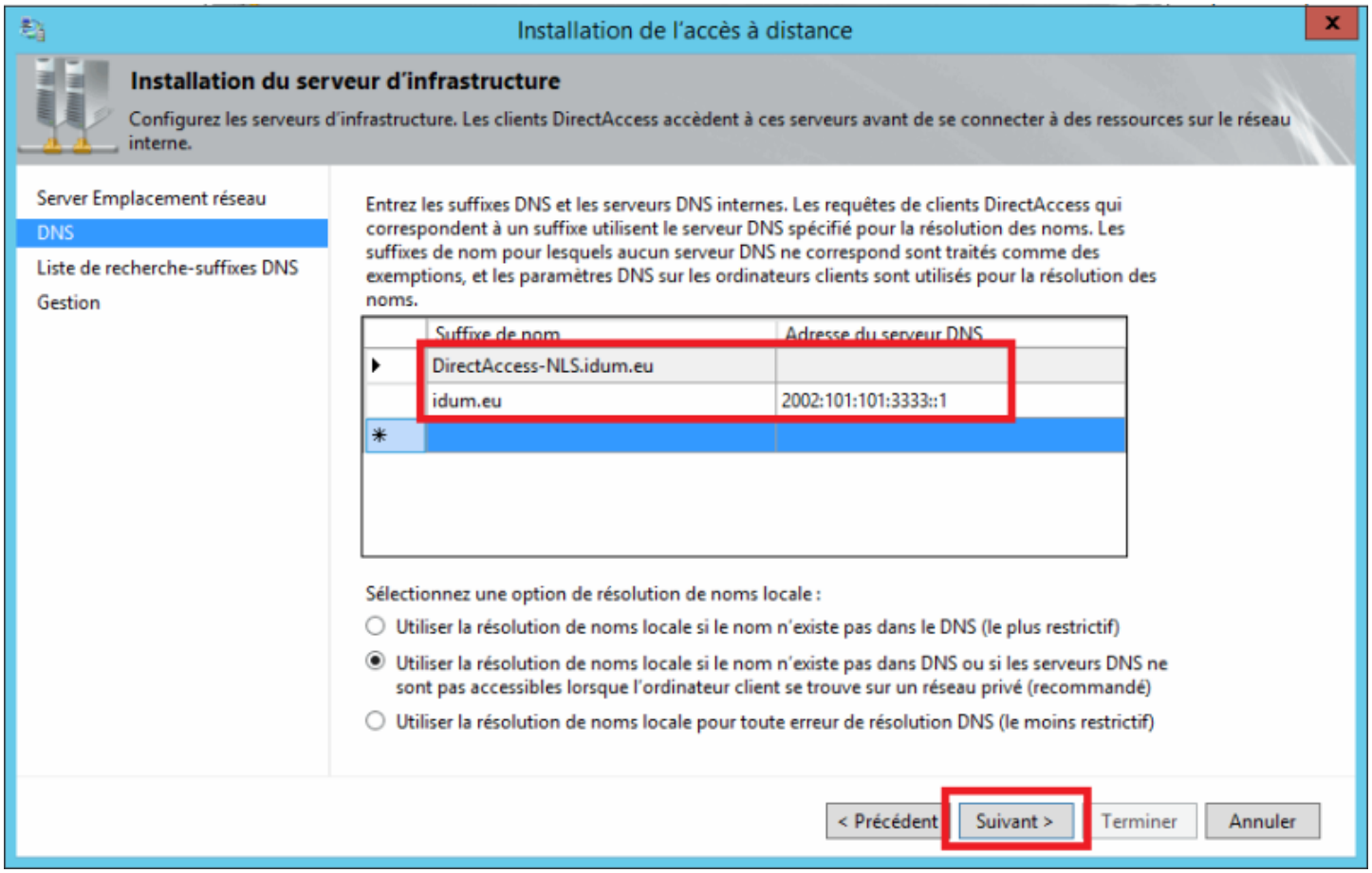
- Le serveur d'emplacement réseau, permet aussi au client de s'assurer qu'il se trouve sur le réseau local.



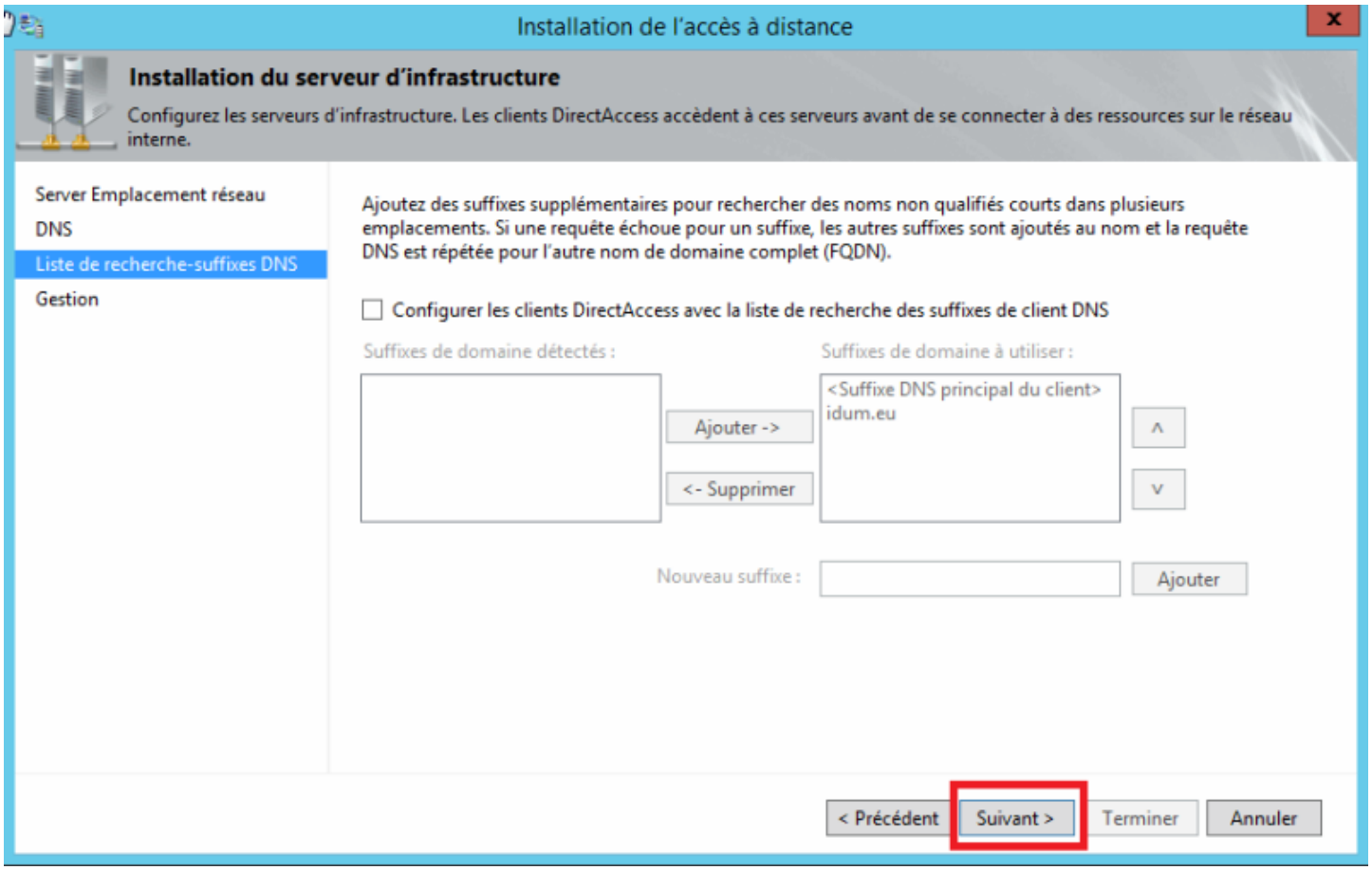
- Le client, une fois connecté en DirectAccess au réseau local, va utiliser le serveur DNS du domaine, on va ajouter le domaine idum.eu et cliquer sur détecter pour qu'il ajoute automatiquement l'adresse du DNS. L'adresse IPV6 du serveur doit s'afficher comme ici :



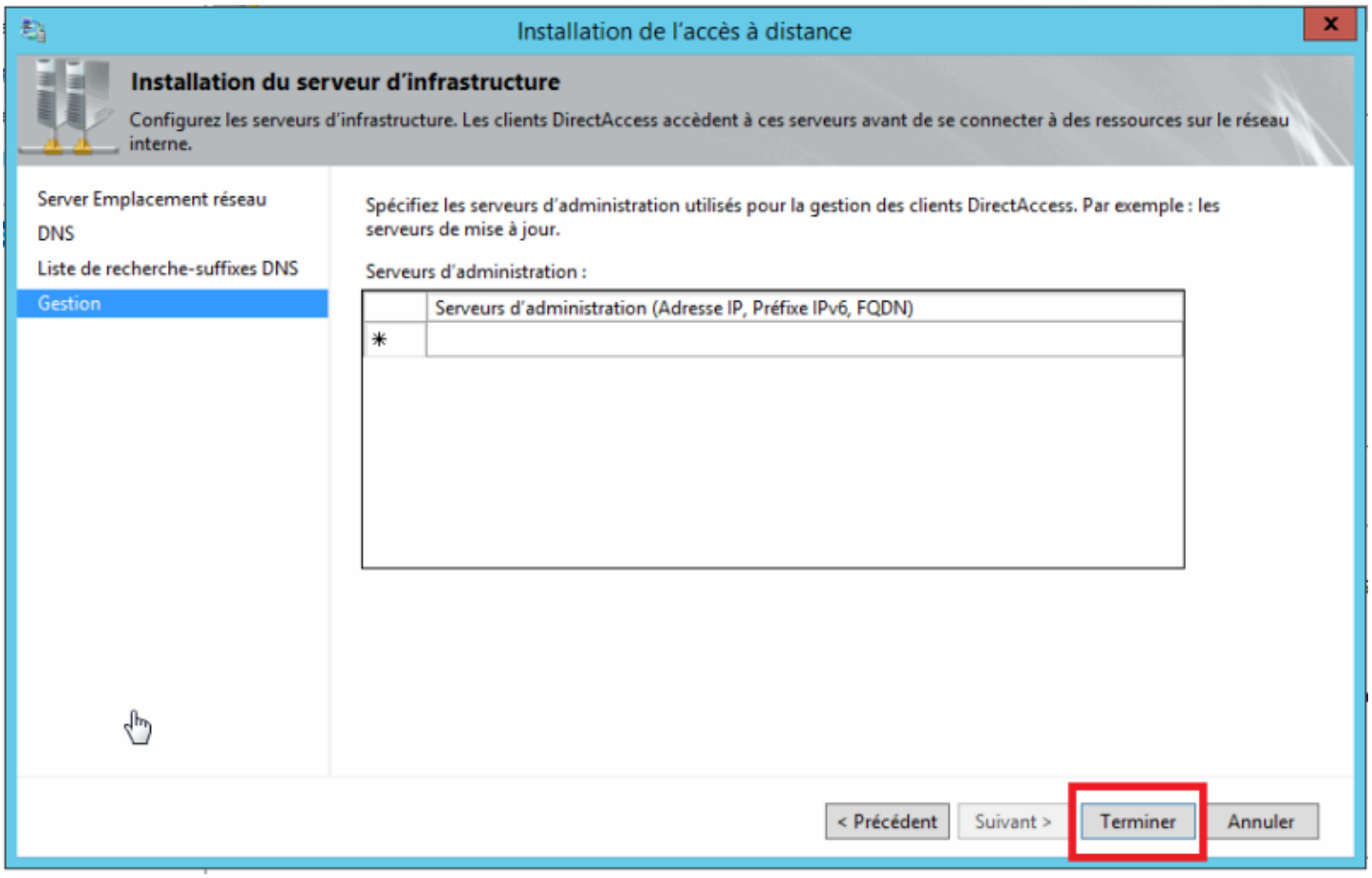
- Par défaut, on va signifier au client, que le DNS local va résoudre la zone idum.eu.



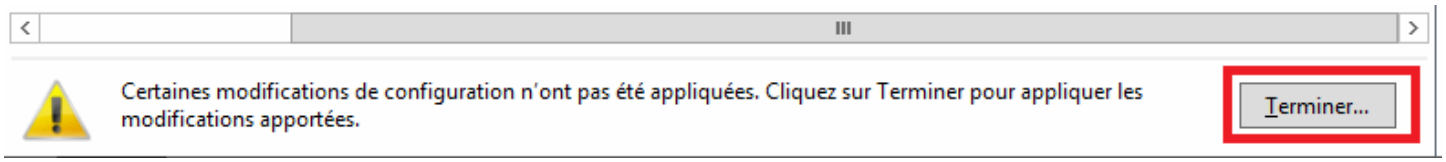
- Il est possible d'ajouter des URL de serveur d'administration, dans notre cas, nous n'allons rien ajouter. Cliquez sur "**Suivant**".



- Voilà la configuration est terminée, il ne reste plus qu'à enregistrer les paramètres et les appliquer.



- Cliquez sur **"Terminer"**.



- Fermez la fenêtre.

IV) Configuration du serveur ISP

Le serveur ISP, en plus d'héberger le service NCSI, va servir de serveur DNS au client nomade sur le réseau Internet.

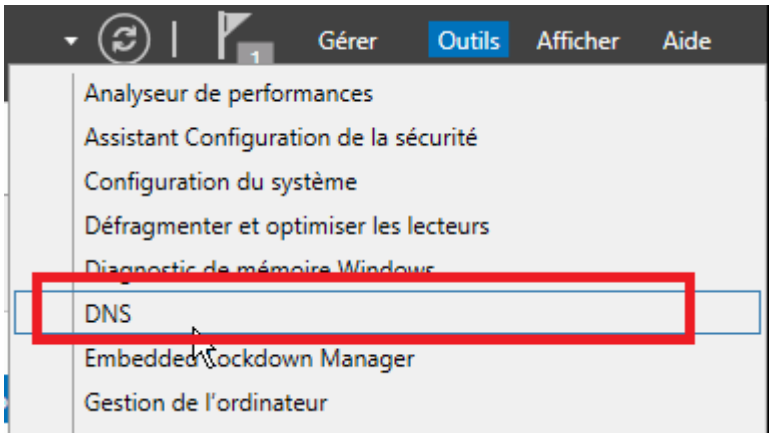
Comme nous l'avons dit précédemment, notre labo est hors ligne, c'est à dire qu'il n'a pas accès à Internet. Pour faire fonctionner DirectAccess, le poste client doit détecter une connexion à Internet pour lancer la connexion.
Nous allons faire croire à notre machine cliente qu'elle a bien accès à Internet en installant un serveur Microsoft NCSI. NCSI est le système mis en place par Microsoft pour détecter l'accès à Internet, sur vos machines il se matérialise par le petit icone en bas à gauche. Il existe trois état :

- Une croix rouge, cela signifie que le câble réseau est déconnecté ou que la carte est désactivée.
- Un petit panneau jaune signifie que le PC à accès au réseau mais Internet n'est pas atteignable
- Un petit écran d'ordinateur seul signifie que tout est correct.

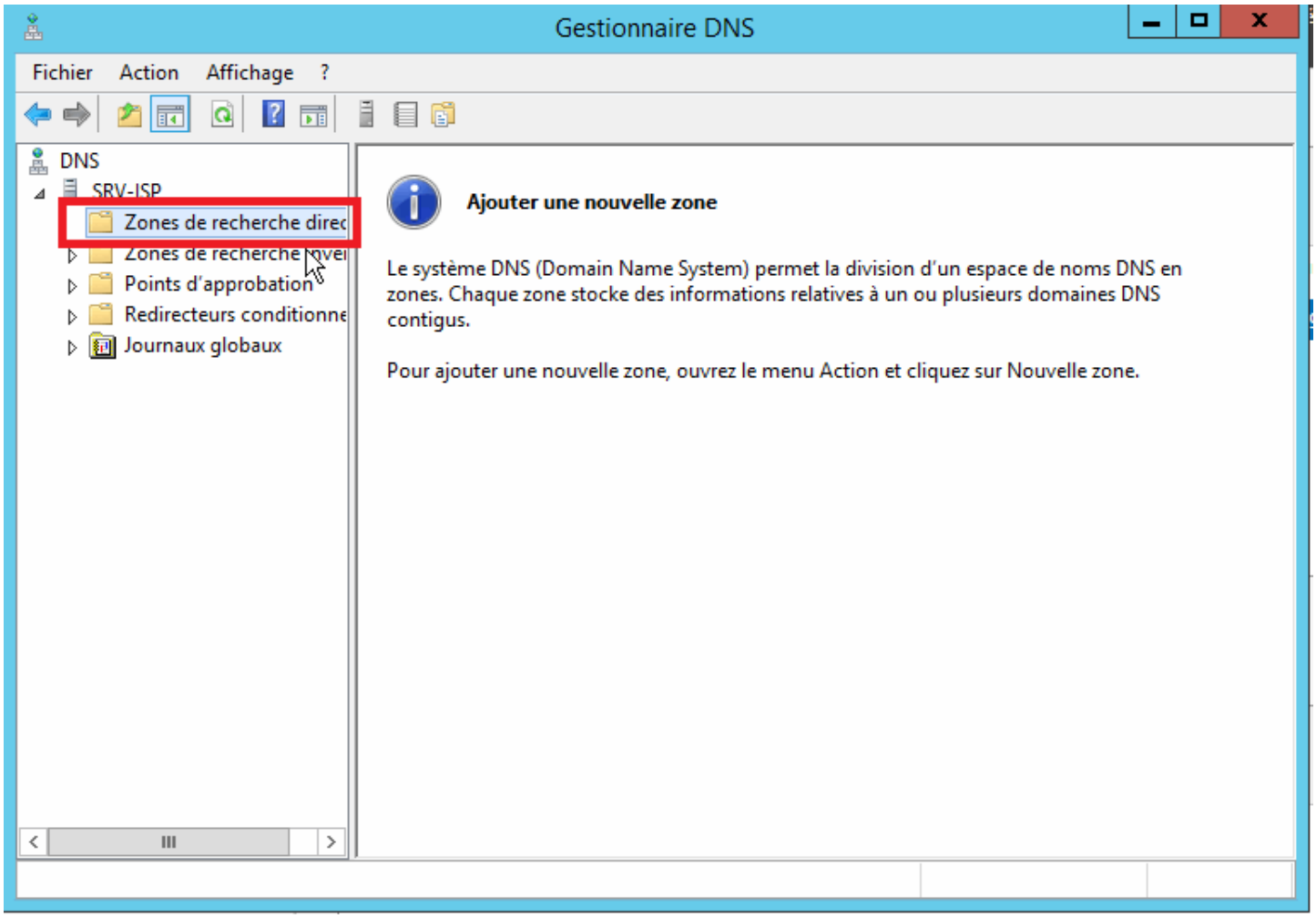
Nous allons donc mettre en place ce petit serveur NCSI. Pour ce faire, nous allons utiliser un serveur Windows 2012 R2 qui est autonome, c'est à dire non connecté au domaine.

- Nous allons installer le service DNS et le service IIS. Laisser tous les paramètres par défaut lors de l'installation.

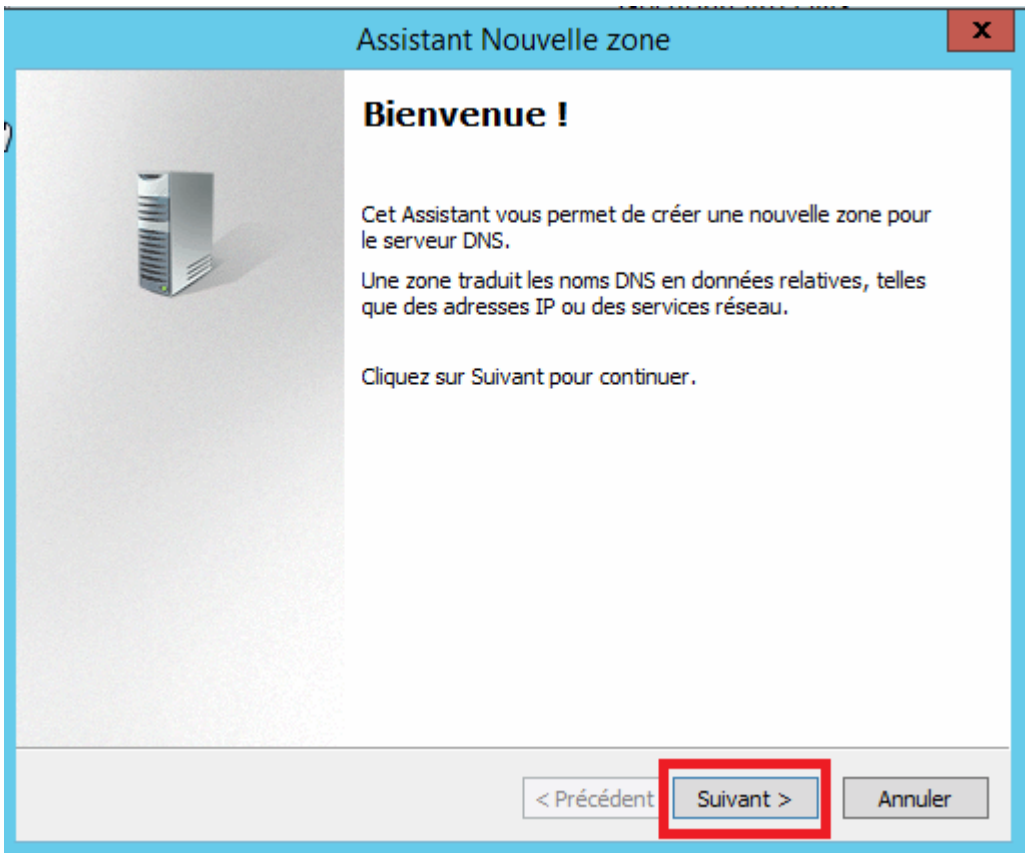
- Une fois le service DNS installé, allez dans la console de gestion. Dans le gestionnaire de serveur, cliquez sur **"Outils"**, puis sur **"DNS"**.



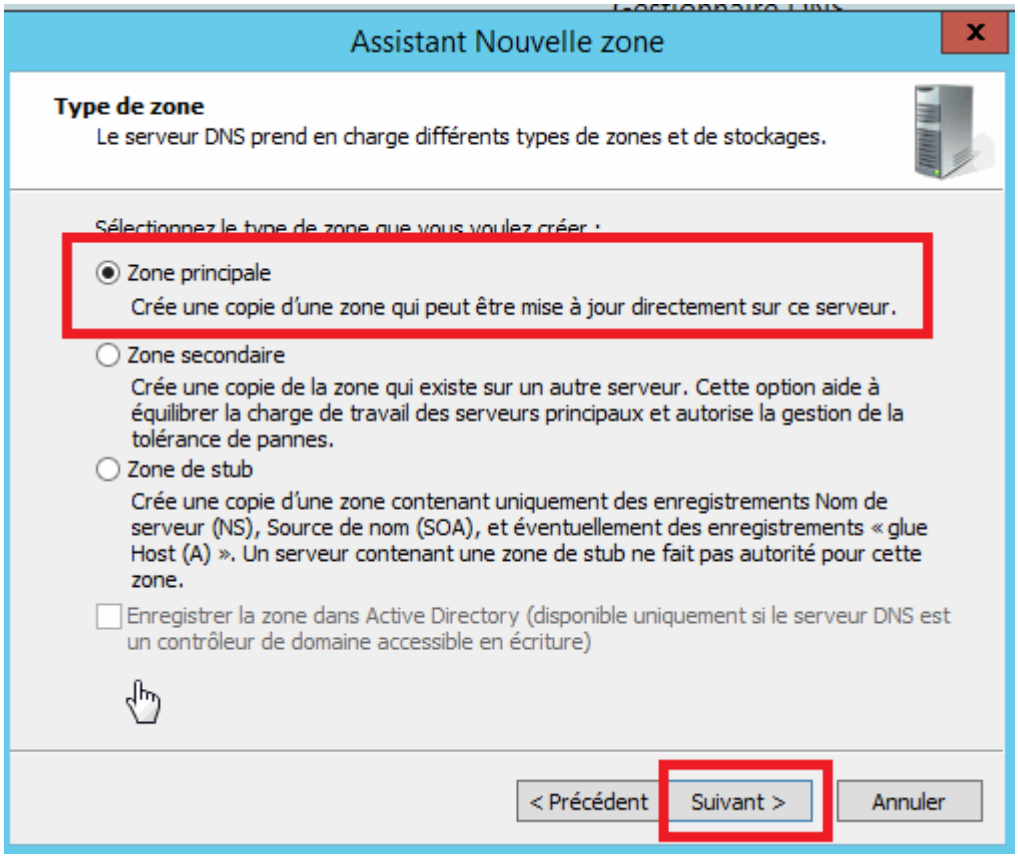
- Créez une nouvelle zone de recherche directe.



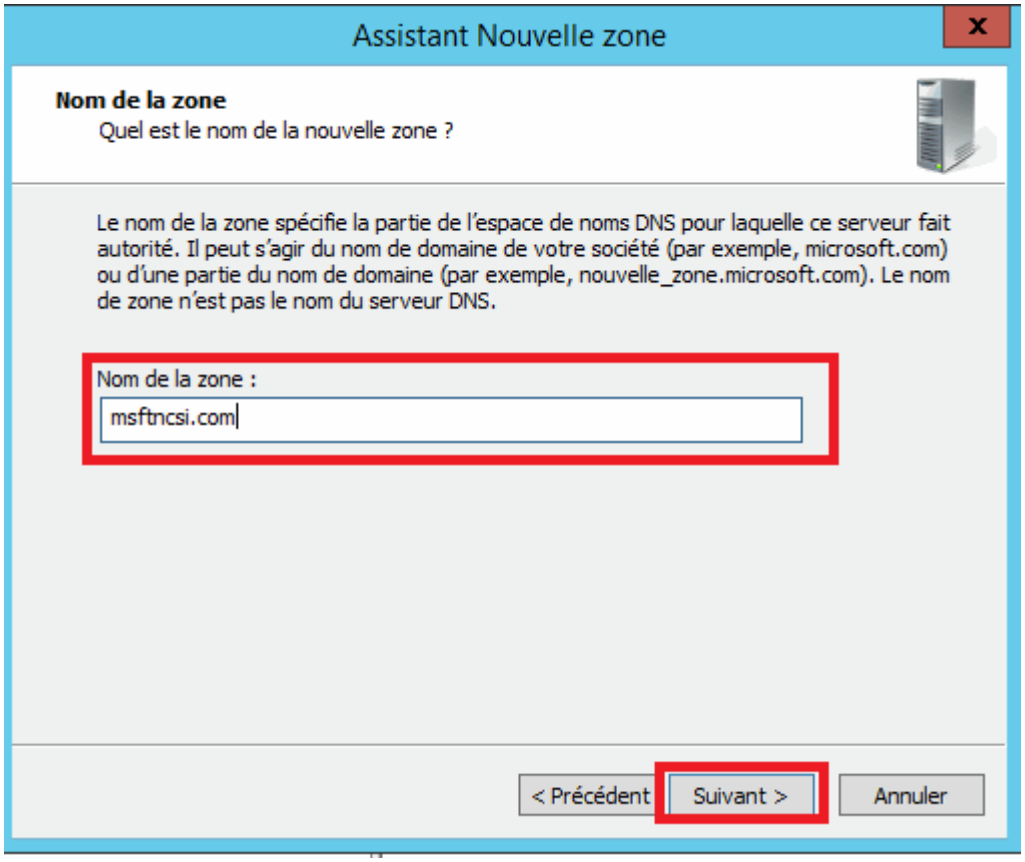
- Cliquez sur suivant pour lancer la création de la zone.



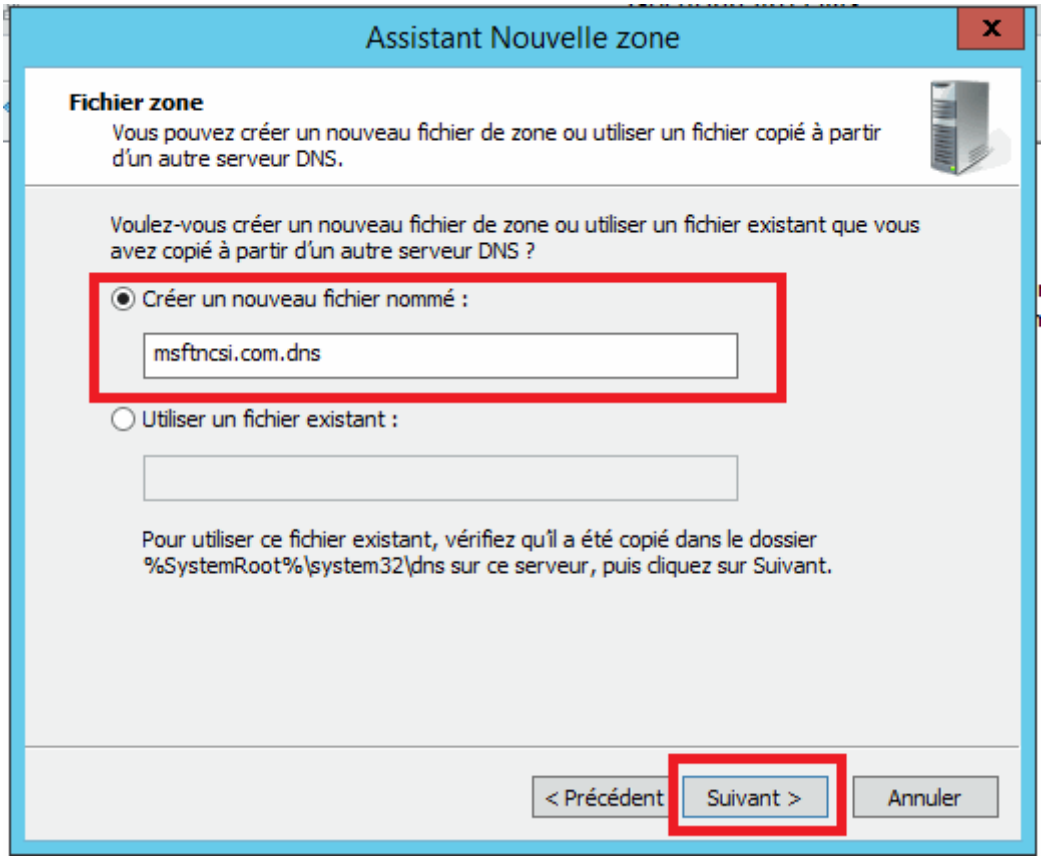
- Nous allons créer une zone principale.



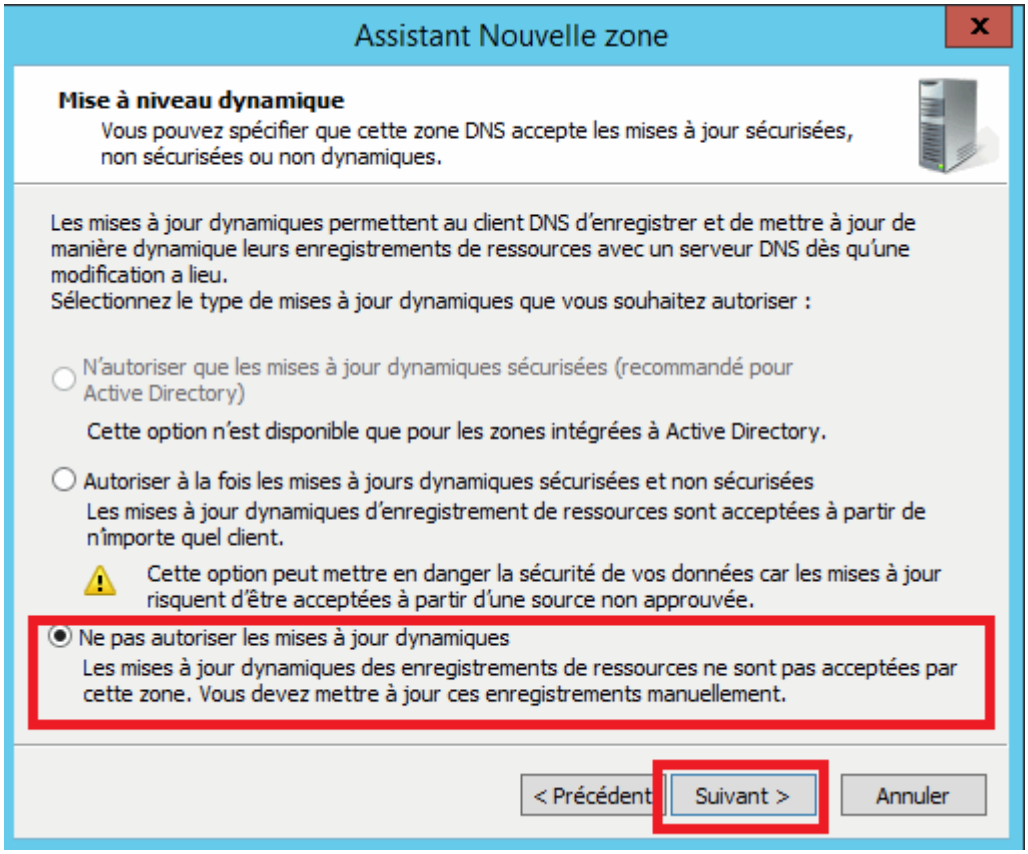
- Nommez cette zone msftncsi.com.



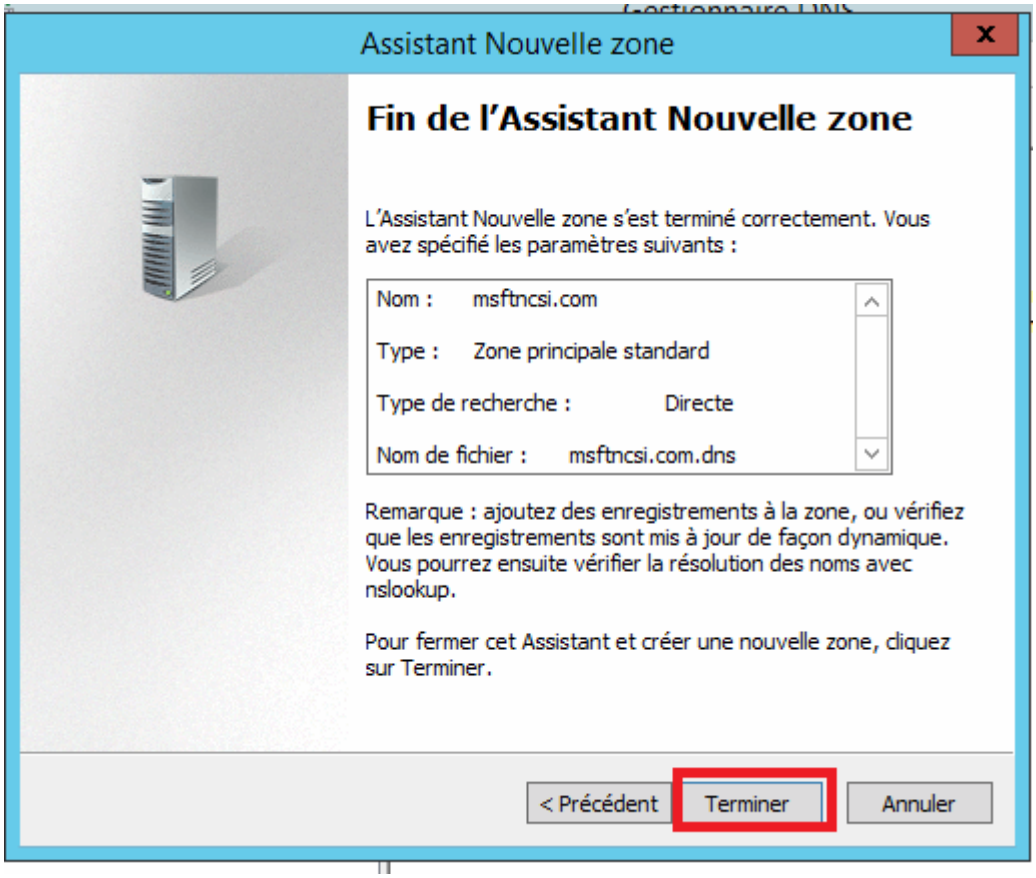
- Laissez tel quel le nom du fichier de zone.



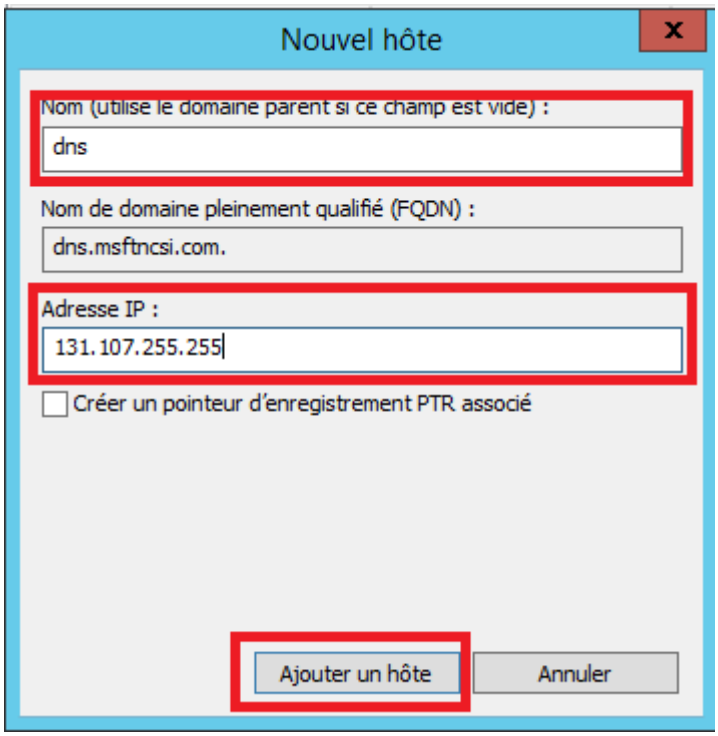
- Etant donné que le serveur n'est pas dans un domaine, nous n'allons pas autoriser les mises à jour dynamiques.



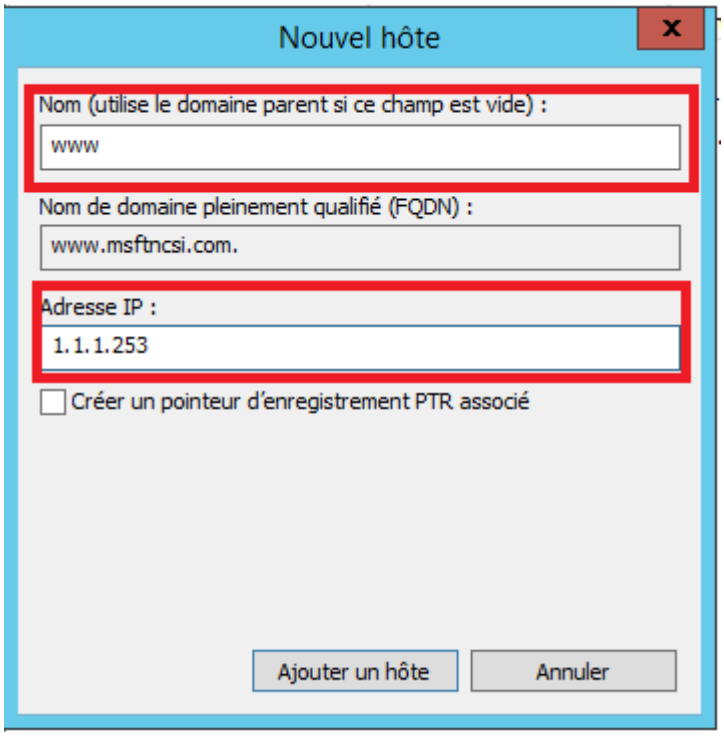
- Cliquez sur "**Terminer**". Et voilà, la zone msftncsi.com est maintenant active.



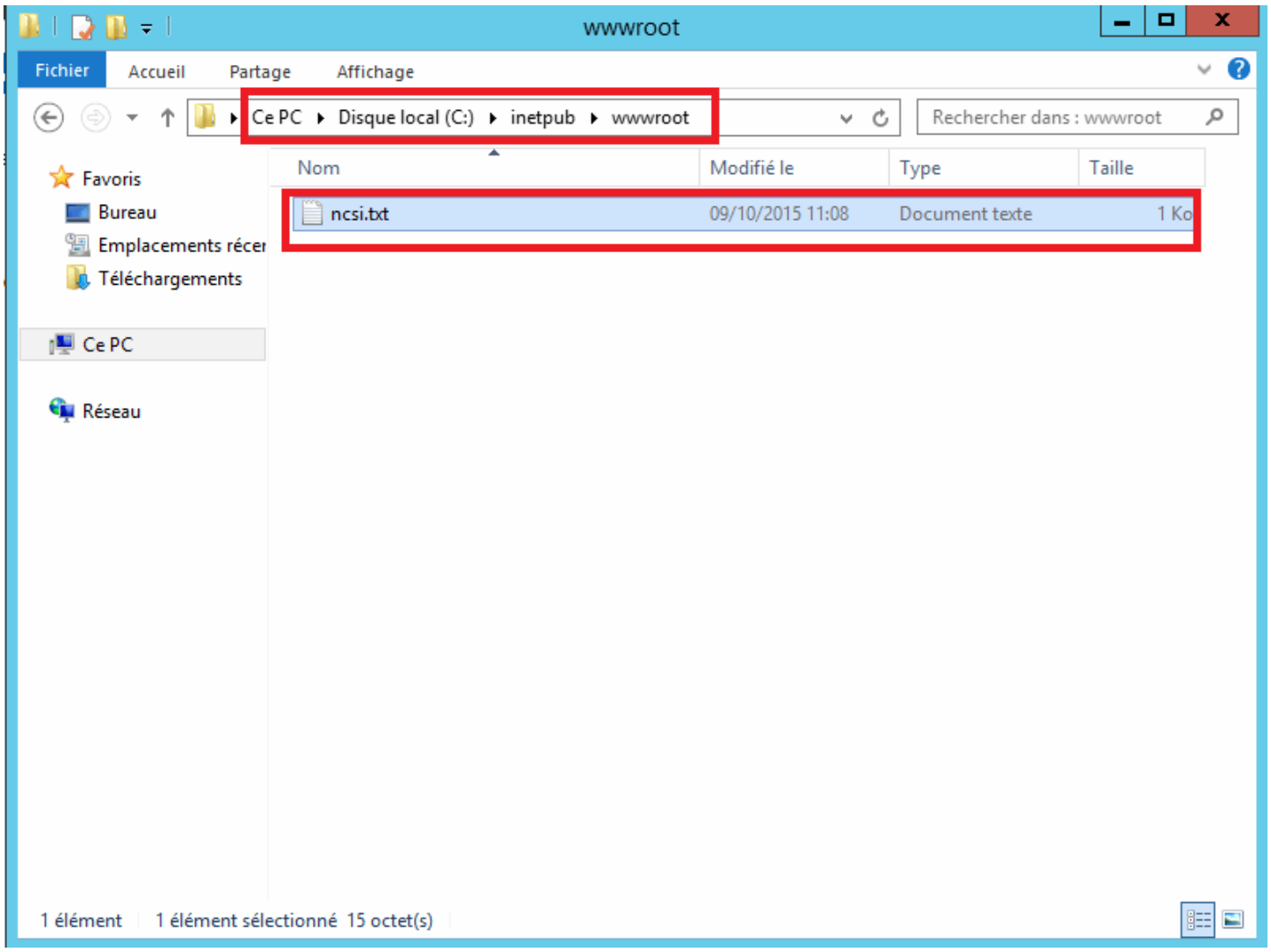
- Nous allons maintenant créer deux enregistrements DNS A. Le premier est l'enregistrement dns.msftncsi.com avec comme valeur "**131.107.255.255**".



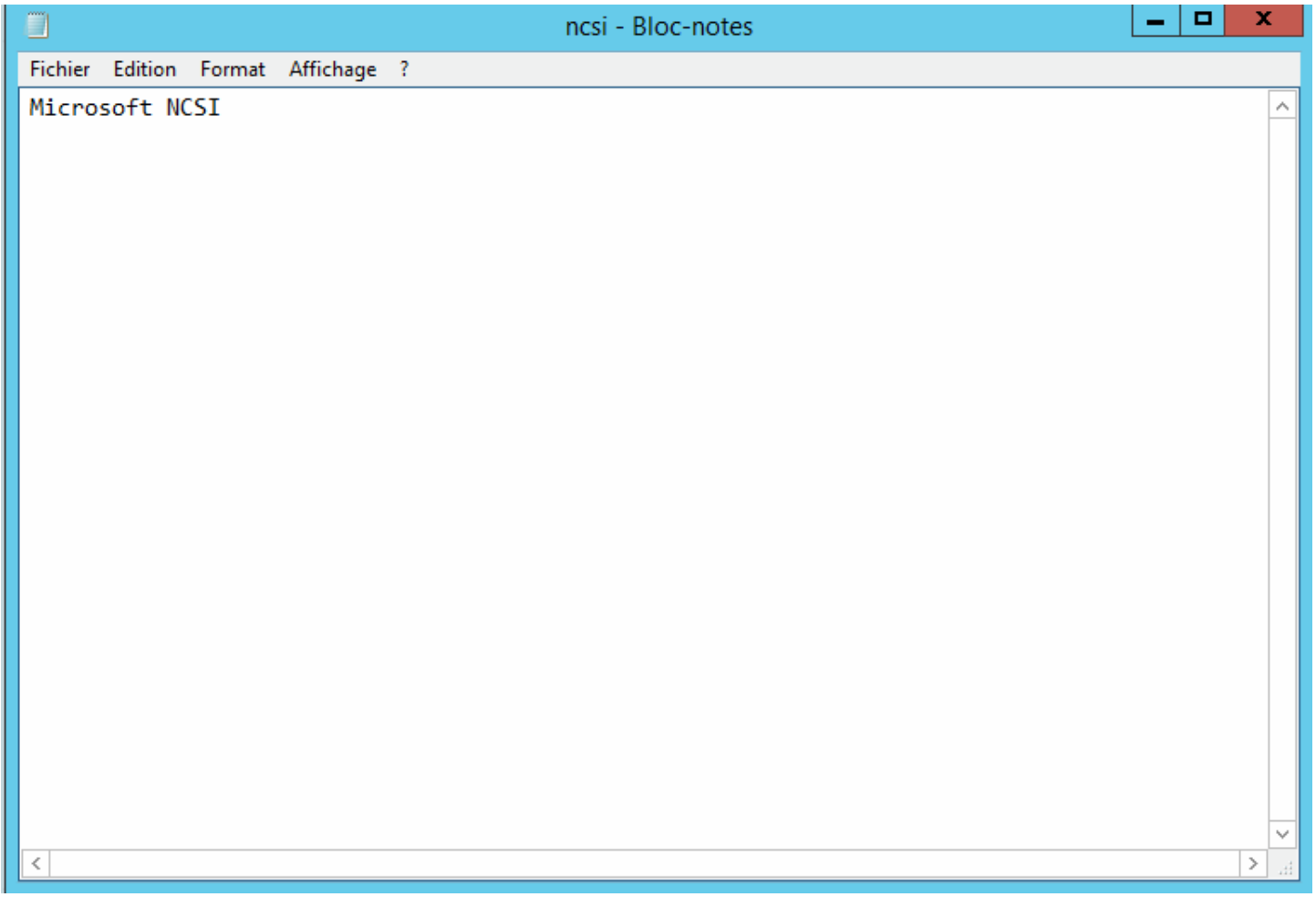
- Le second est www.msftncsi.com avec comme valeur l'adresse IP de votre serveur qui simule l'accès à Internet, ici "**1.1.1.253**".



- Voilà pour la partie DNS. Pour la partie Web, rien de plus simple, créer un fichier txt nommé ncsi.txt dans le répertoire root de votre serveur web IIS, normalement **"c :\inetpub\wwwroot"**.



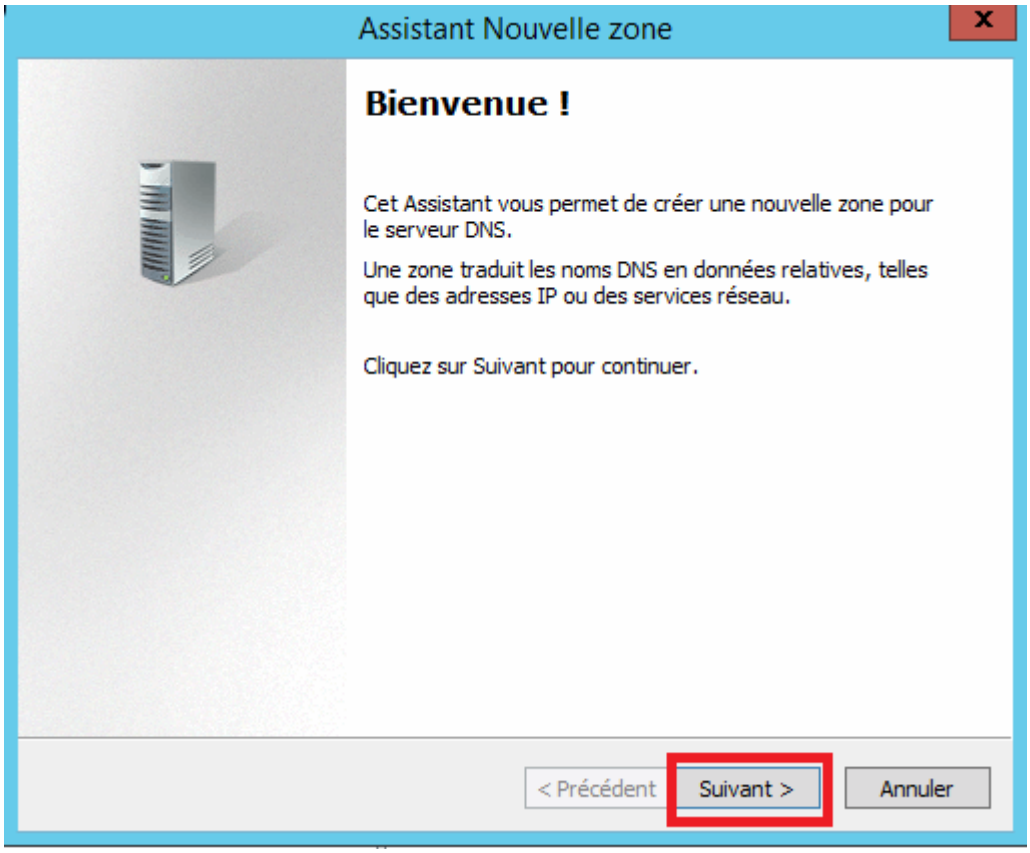
- A l'intérieur de ce fichier, entrer le texte "Microsft NCSI" sans retour à la ligne.



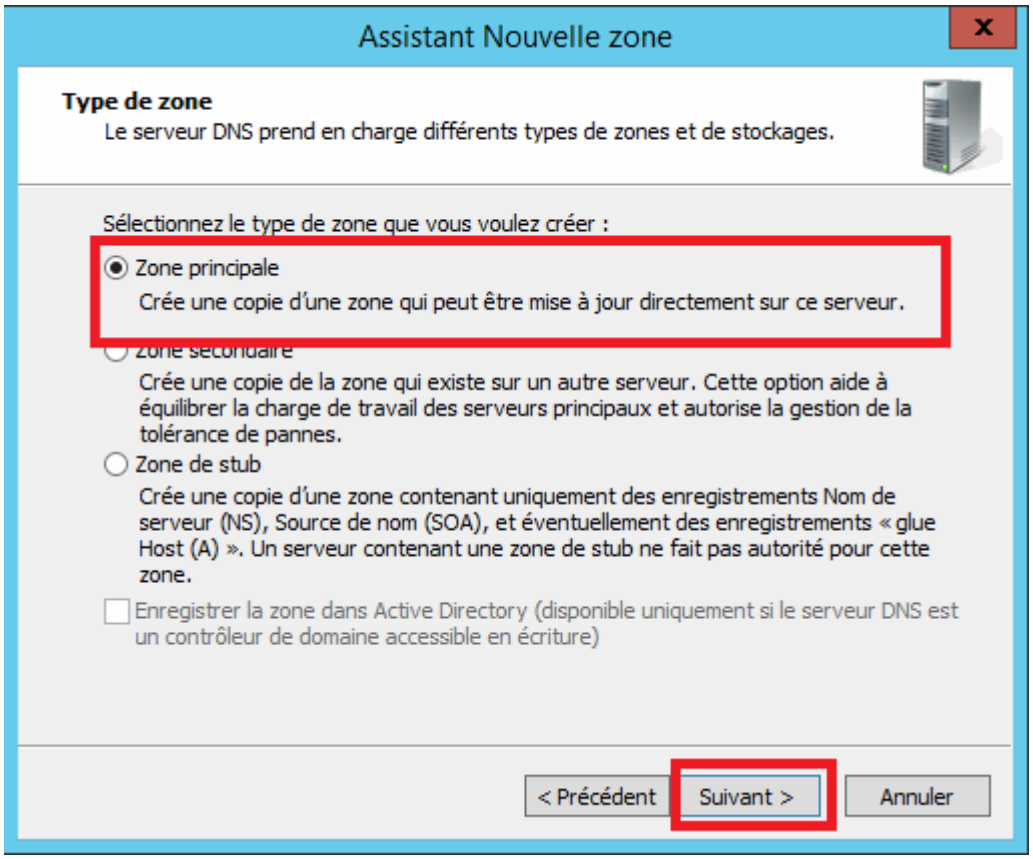
Maintenant que le serveur NCSI est prêt. Pour tester l'accès à Internet, le client va d'abord faire une requête DNS sur dns.msftncsi.com et ensuite il va télécharger le contenues de la page à l'adresse www.msftncsi.com. Toutes les réponses attendues par ces requêtes sont contenu dans la base de registre de Windows.

Il nous reste à créer la zone Idum.com et créer l'enregistrement da.idum.com.

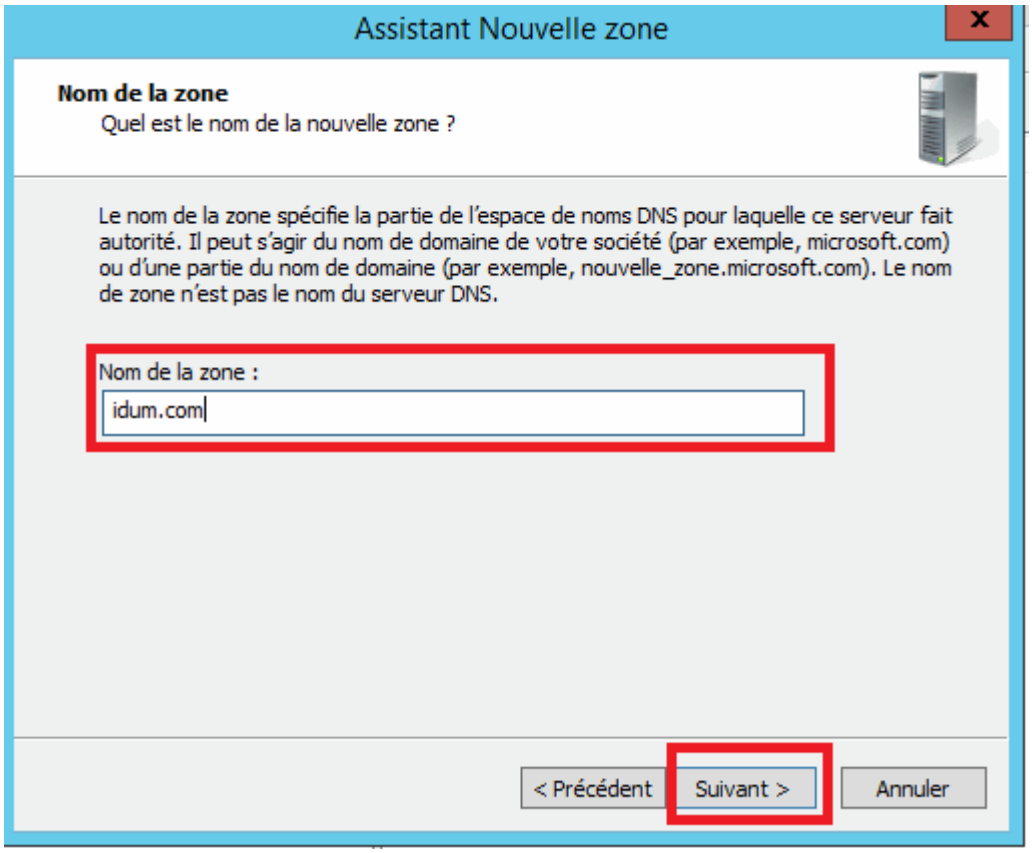
- Dans le gestionnaire DNS, faites un clic droit sur zone de recherche directe et choisissez nouvelle zone.
- Cliquez sur suivant pour lancer la création de la zone.



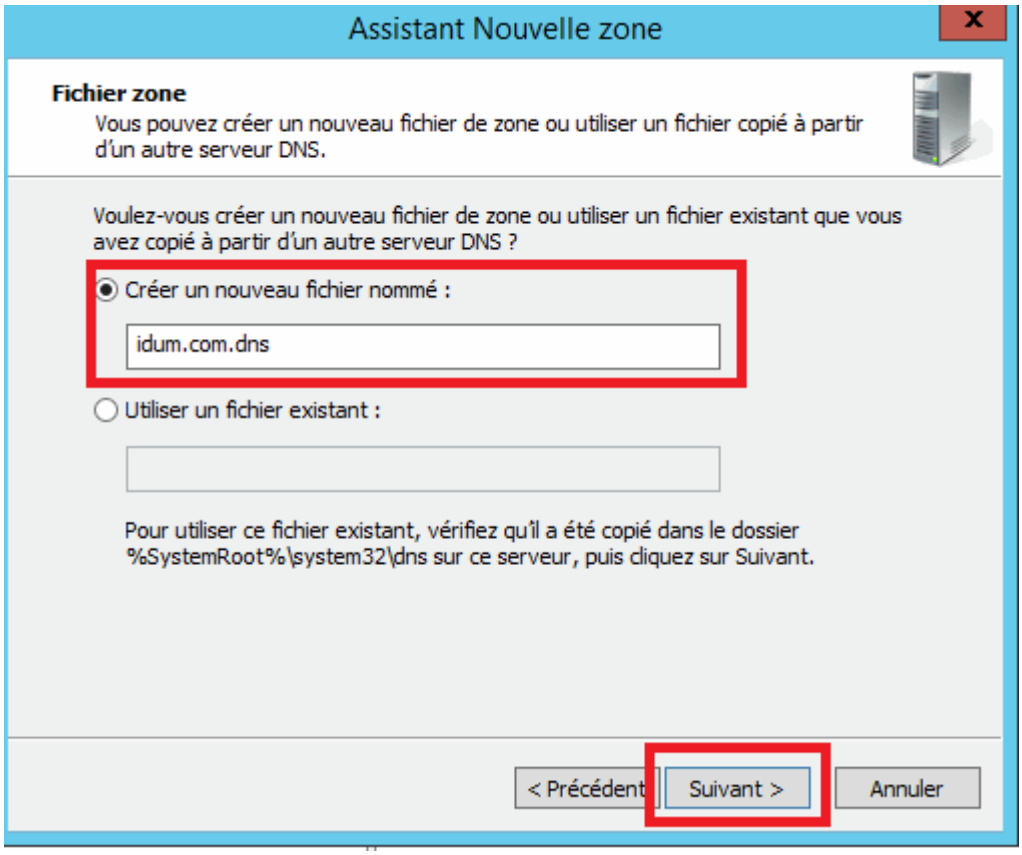
- Nous allons créer une zone principale.



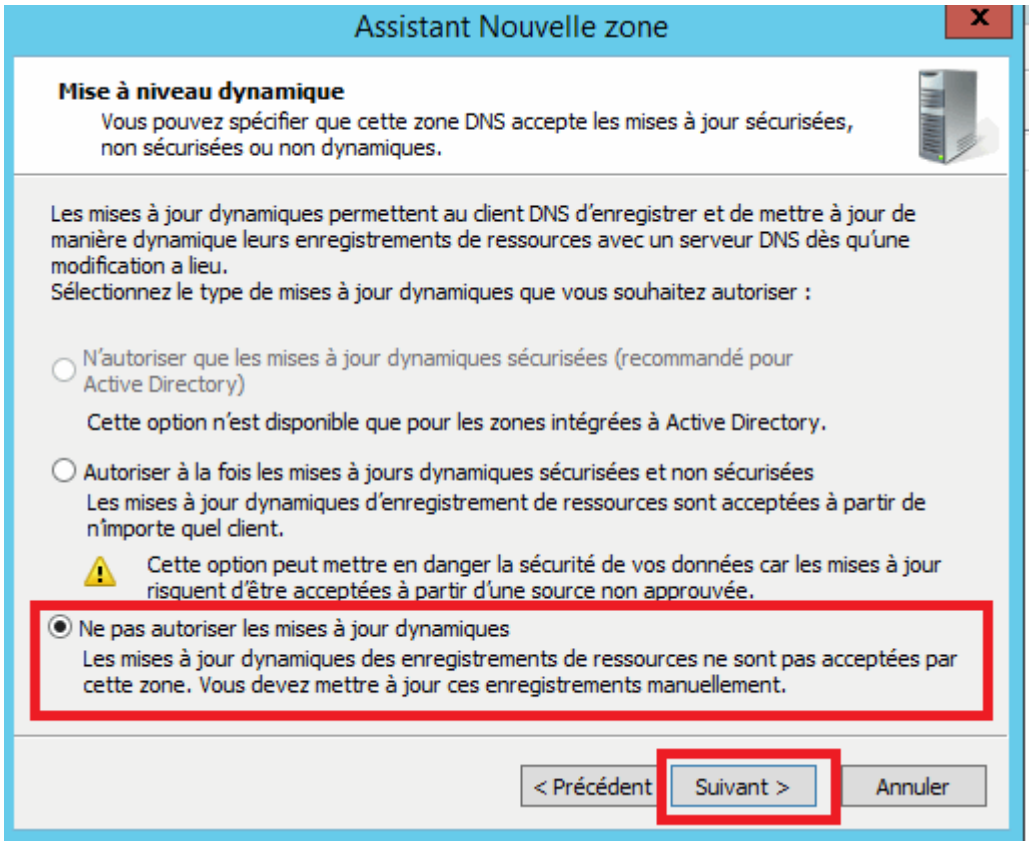
- Nommez cette zone idum.com.



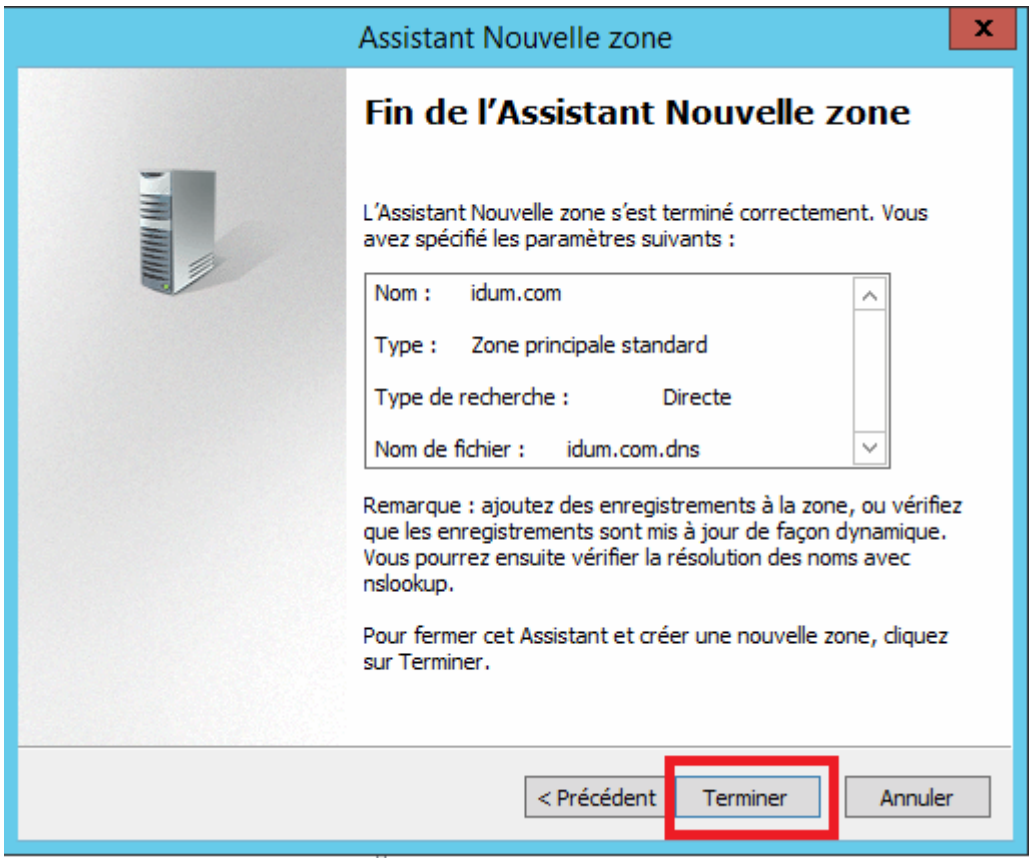
- Laissez le nom de fichier de zone par défaut.



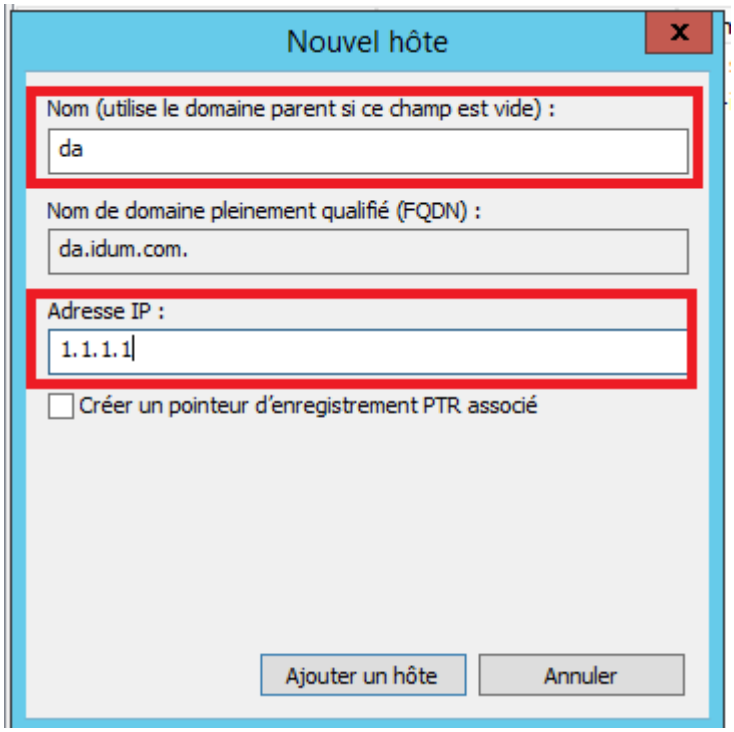
- Etant donné que le serveur n'est pas dans un domaine, nous n'allons pas autoriser les mises à jour dynamiques.



- La zone idum.com est maintenant active.



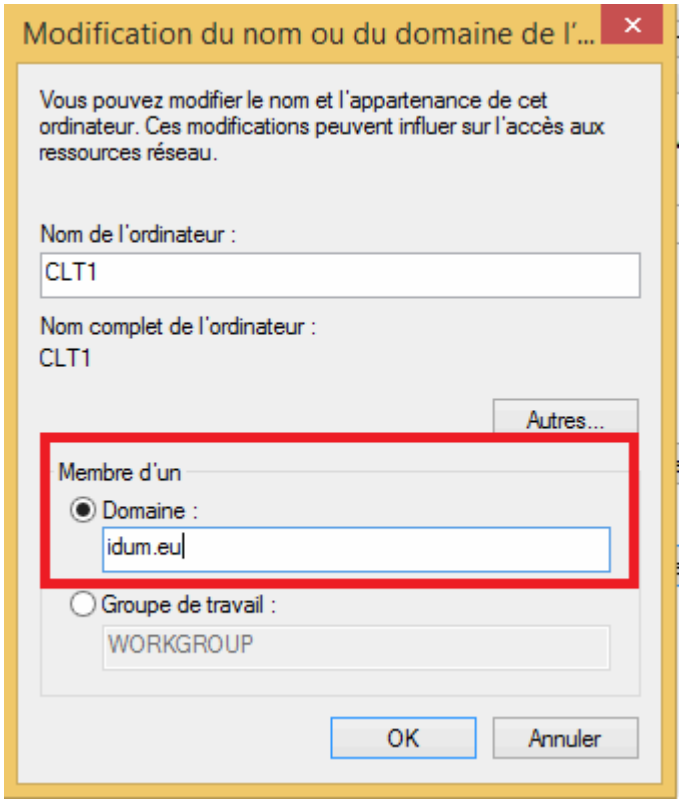
- Créez maintenant un enregistrement DNS da.idum.com avec l'adresse IP WAN du serveur DirectAccess, pour nous "**1.1.1.1**".



V) Configuration du client

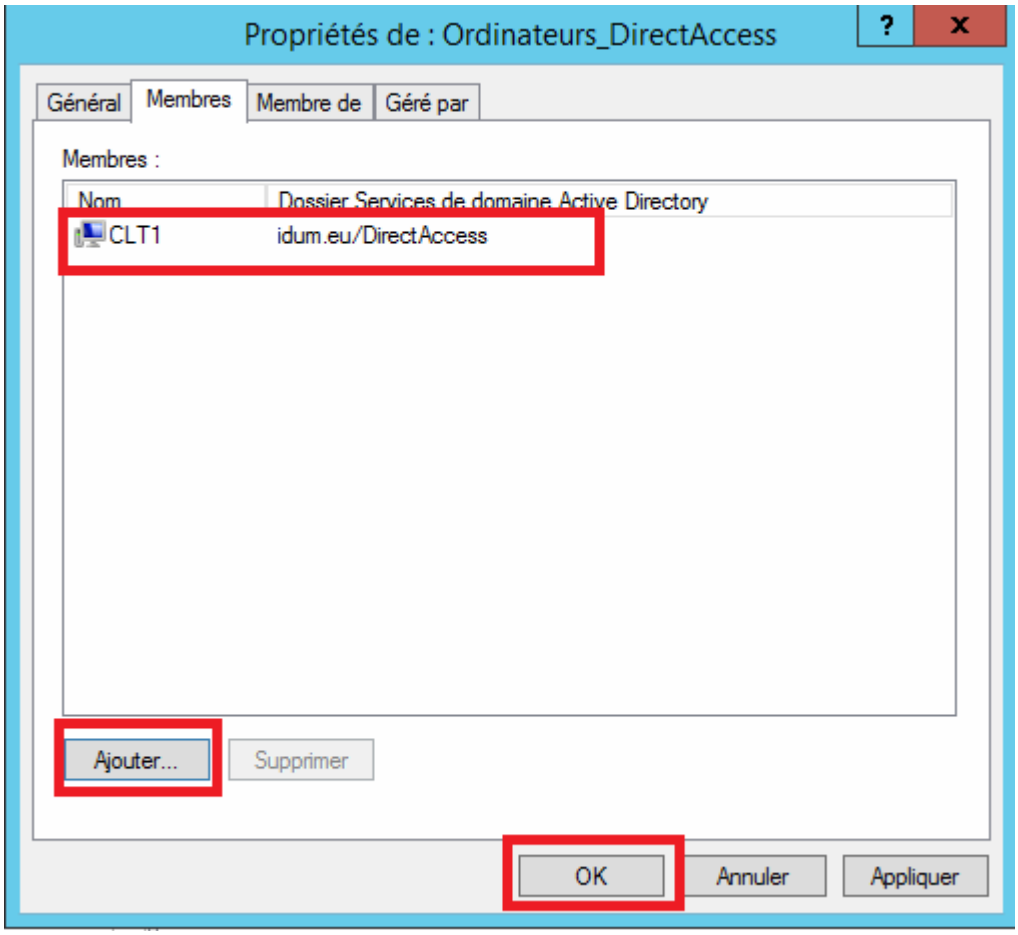
Pour fonctionner, notre client doit d'abord être connecté au réseau local pour rejoindre le domaine et appliquer les GPO liées à DirectAccess.

- Ajouter le client au domaine :

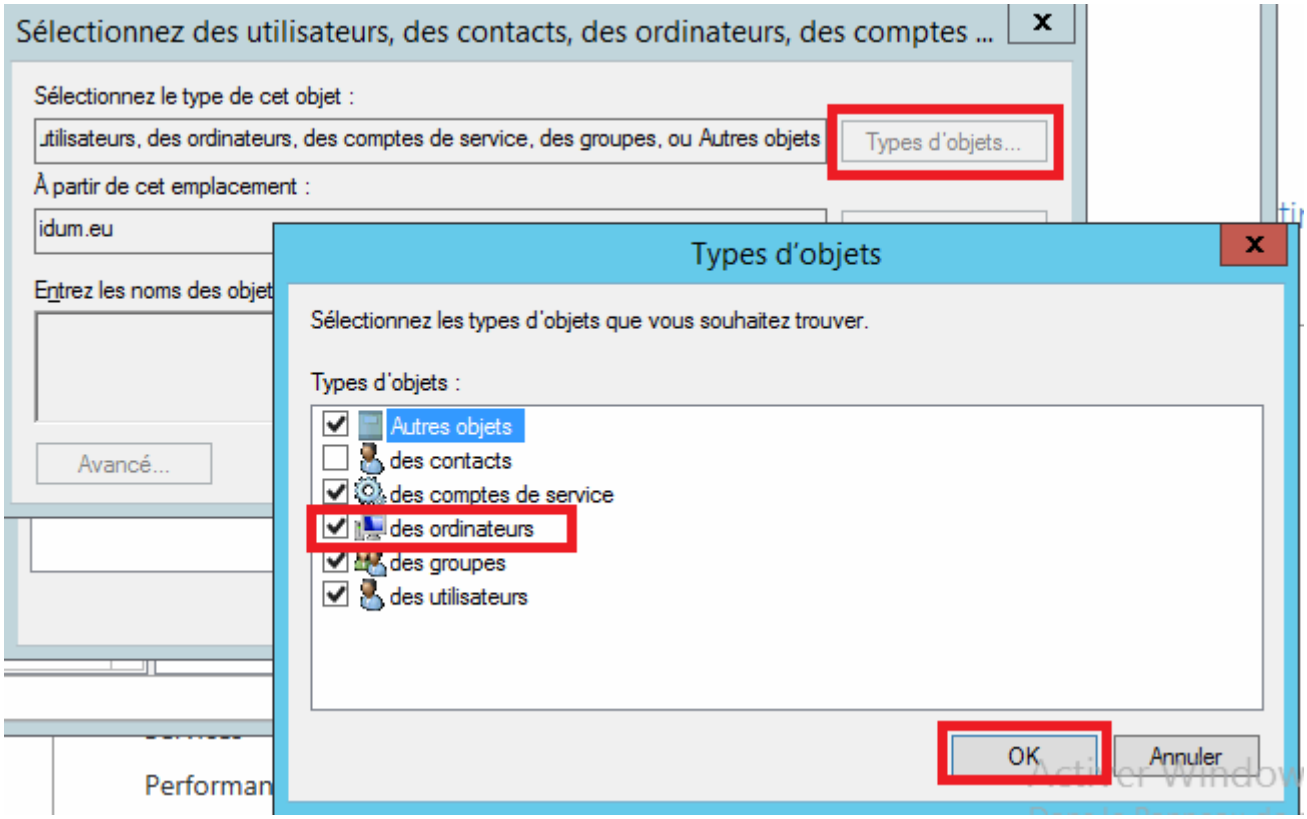


- Sur le contrôleur de domaine, pensez à ajouter votre client dans l'OU DirectAccess et dans le groupe DirectAccess.

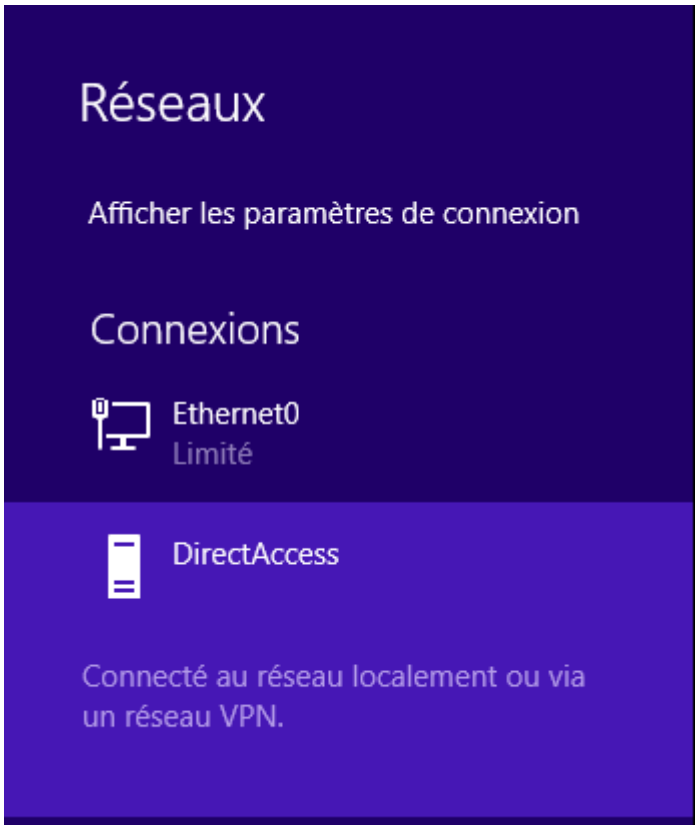
- Pour ajouter un membre au groupe DirectAccess, cliquez sur ajouter et types d'objet pour rechercher aussi les ordinateurs.



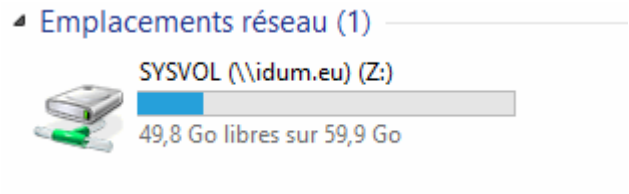
- Tapez le nom de votre client et validez le tout.



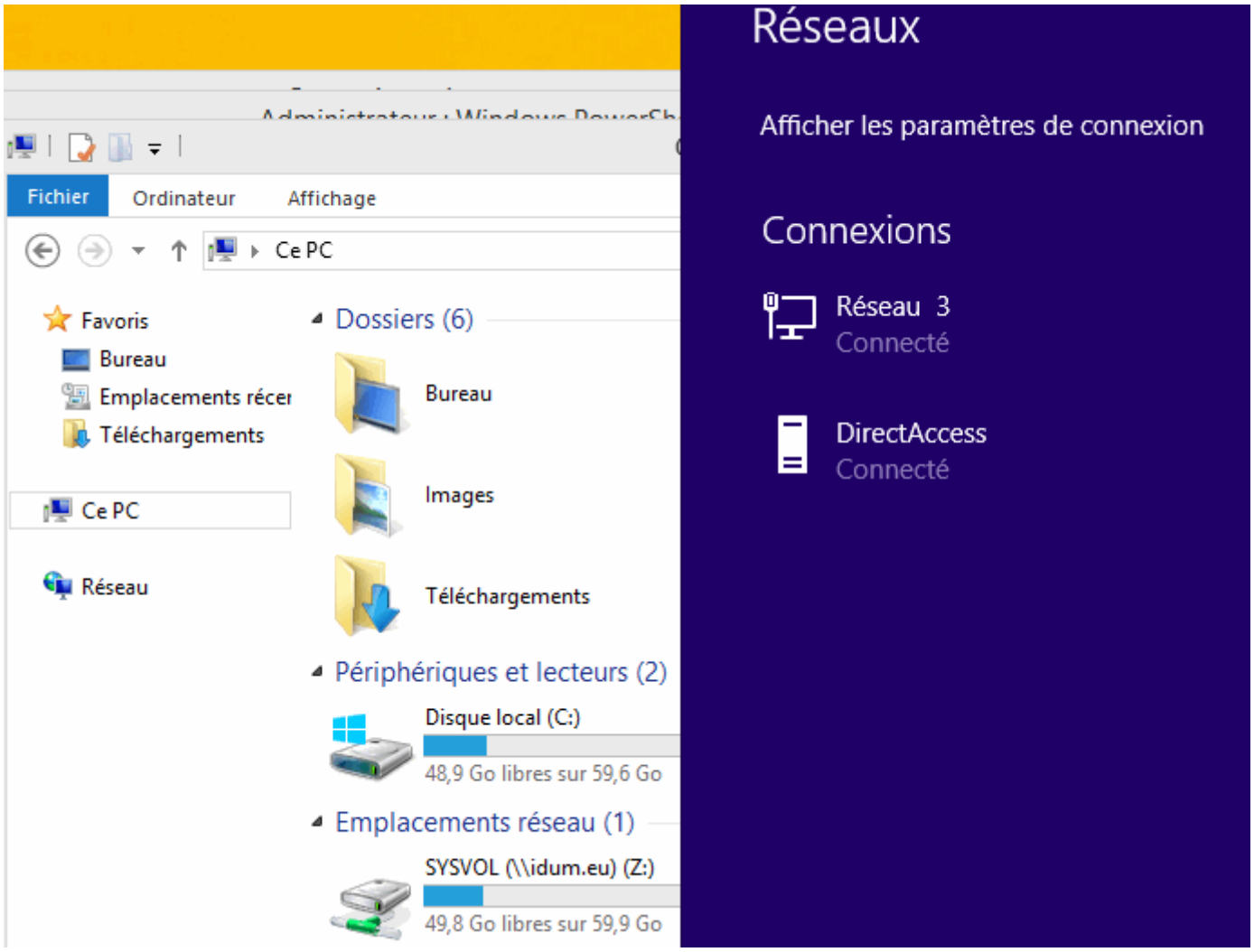
- Au niveau des serveurs, tout est correct, il n'y a plus qu'à aller voir sur le client ce qu'il se passe. Si tout est correct, une GPO a été appliquée et la connexion DirectAccess a été ajoutée au gestionnaire de connexion et nous indique que nous somme connectés au LAN donc DirectAccess est désactivé :



- Pour tester la connexion aux ressources interne, nous allons créer un lecteur réseau vers le **"sysvol"** du contrôleur du domaine idum.eu.



Pour tester maintenant la connexion à DirectAccess, il faut désactiver la carte réseau local et passer sur le réseau WAN. On voit ici que nous somme connectés en DirectAcces et que le lecteur réseau est accessible.



Quelques commandes pour le debugging Directaccess :

- Avec powershell :

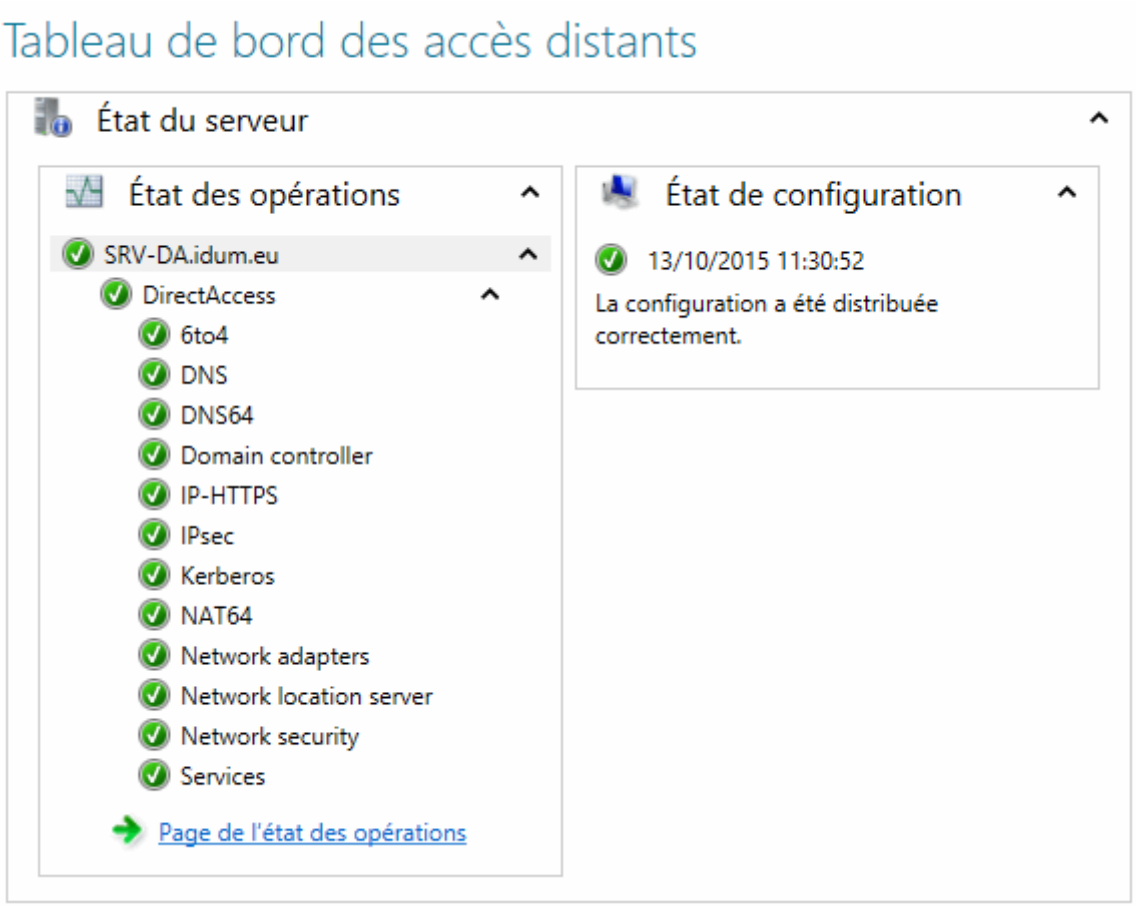
```
Get-DAConnectionStatus
```

- Avec CMD :

Utilisez **"netsh"** pour gèrer les cartes réseaux ipv4/v6.

- Notre serveur DirectAcces est en place et fonctionne.

Sur le serveur DirectAccess, dans la console, il existe un tableau de bord qui permet de voir rapidement l'état des services qui composent DirectAccess.



Des améliorations pourraient être apporté à ce service tel que la génération de certificat par une autorité de certification, la haute disponibilité des serveurs ou encore la mise en place d'un VPN standard en secours du DirectAccess.