



## 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
  - II) Installation du Rôle DirectAccess
  - III) Configuration de DirectAccess
    - 1) Configuration générale
    - 2) Configuration des paramètres des clients distant
    - 3) Configuration du serveur d'accès à distance
    - 4) Configuration des ressources internet disponible à distance
  - IV) Configuration du serveur ISP
  - V) Configuration du client
- 

## 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 :

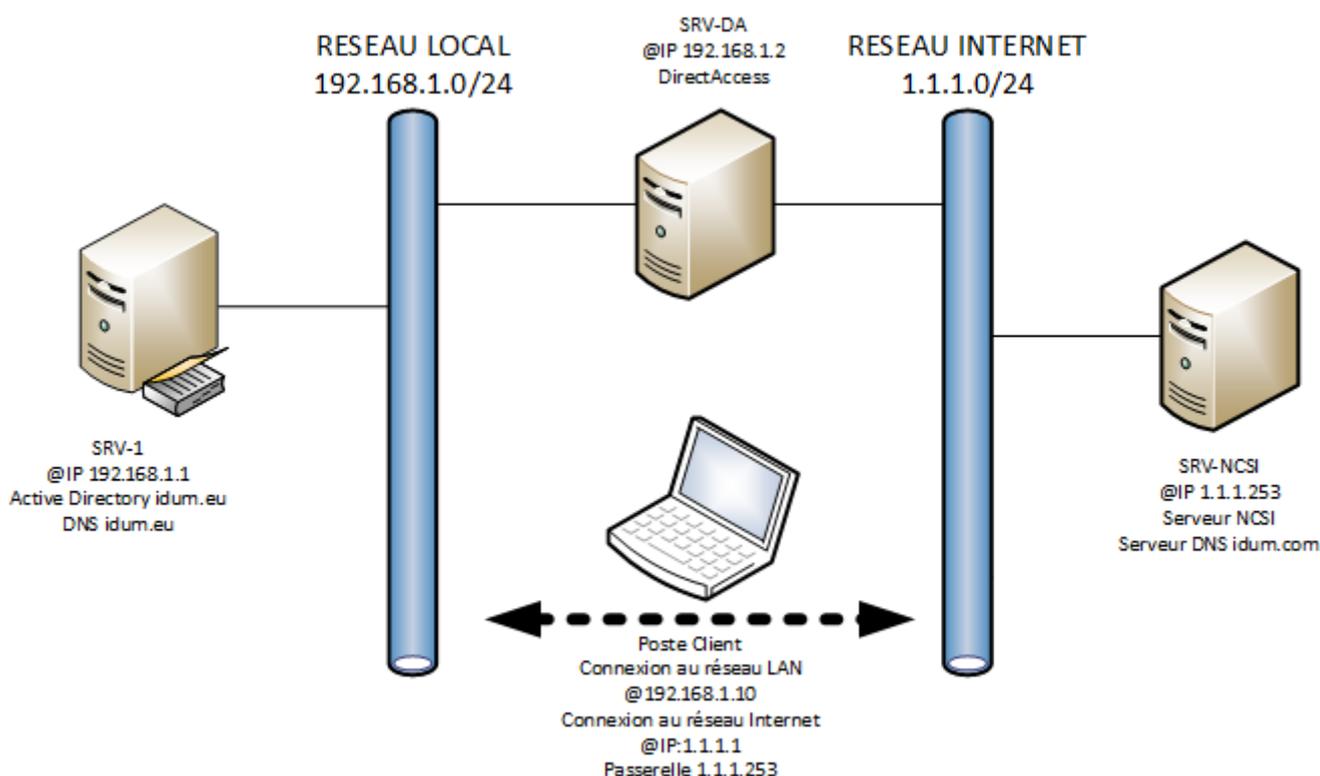
Notre labo est hors ligne, c'est à dire qu'il n'a pas accès à Internet, dans cet article pour que le client initie la connexion DirectAccess, la détection de l'accès Internet est nécessaire (Vous savez la petite icône en bas à droite à côté de l'heure !). Nous allons donc mettre en place un petit serveur 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 à 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**".

DÉMARRAGE  
RAPIDE

NOUVEAUTÉS

EN SAVOIR PLUS

# 1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

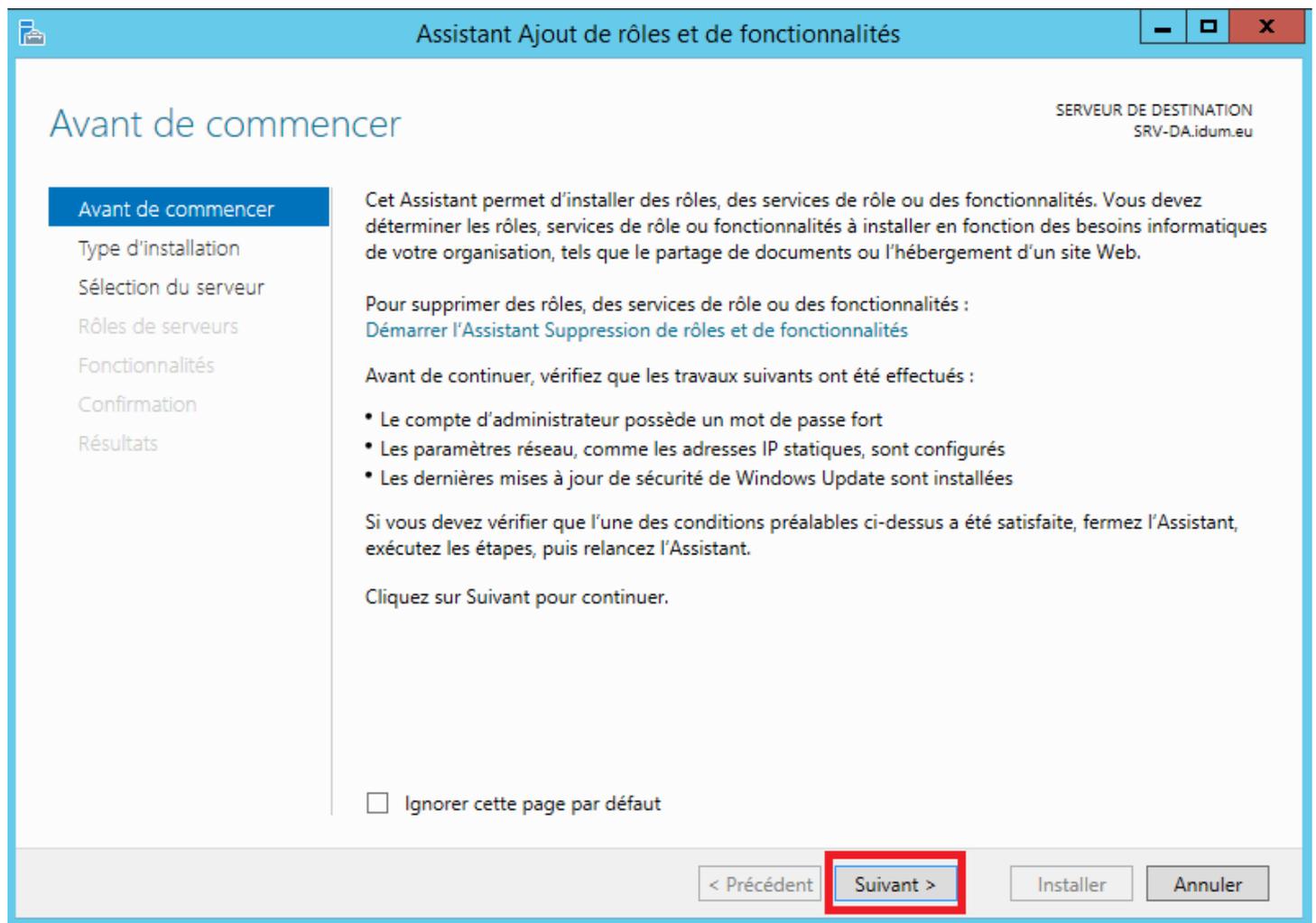
3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

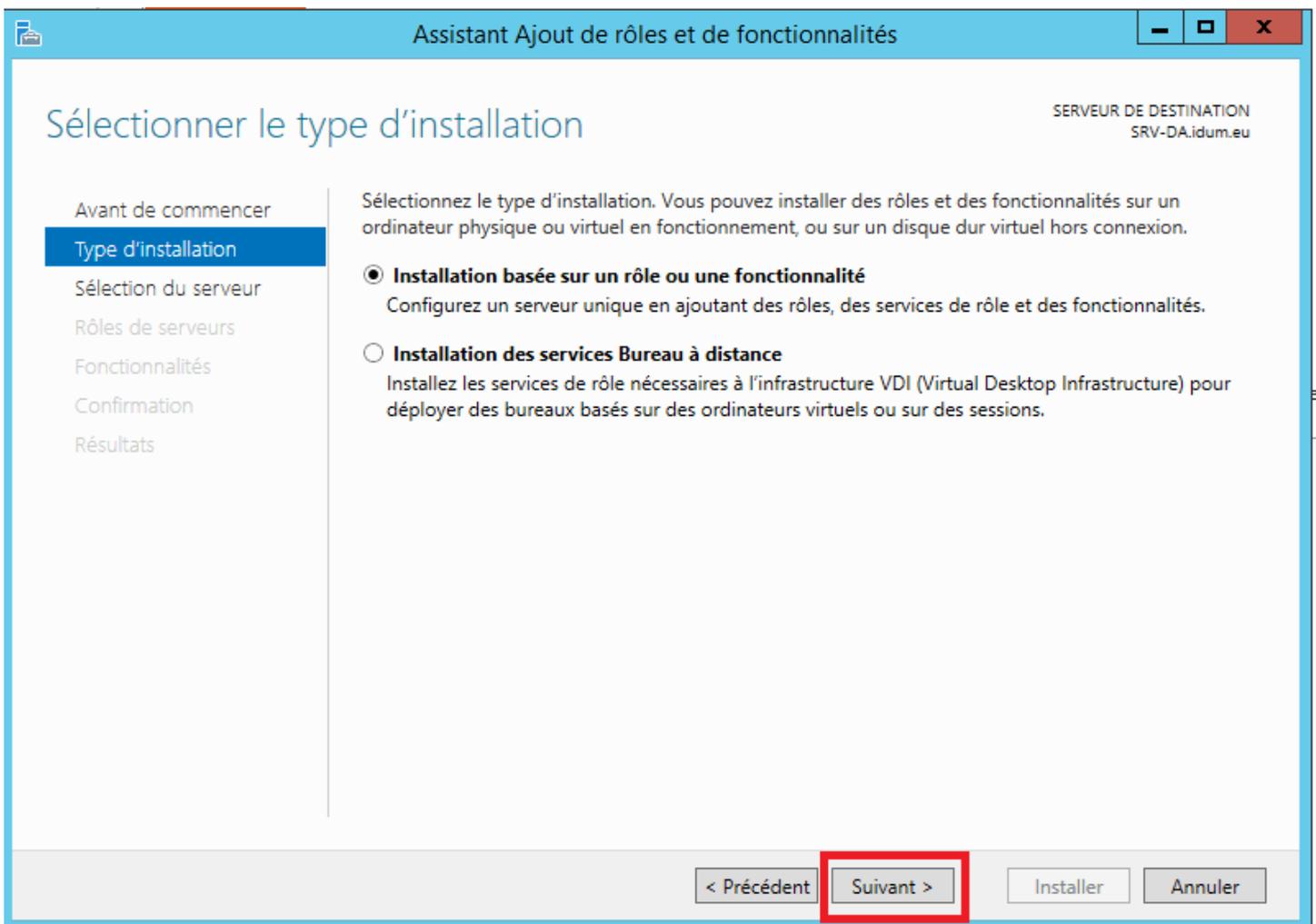
5 Connecter ce serveur aux services de cloud computing

Masquer

- Cliquez sur "**Suivant**".



- Cliquez sur "**Suivant**".



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

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER LE SERVEUR DE DESTINATION  
SRV-DA.idum.eu

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

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

Sélectionner un serveur du pool de serveurs  
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

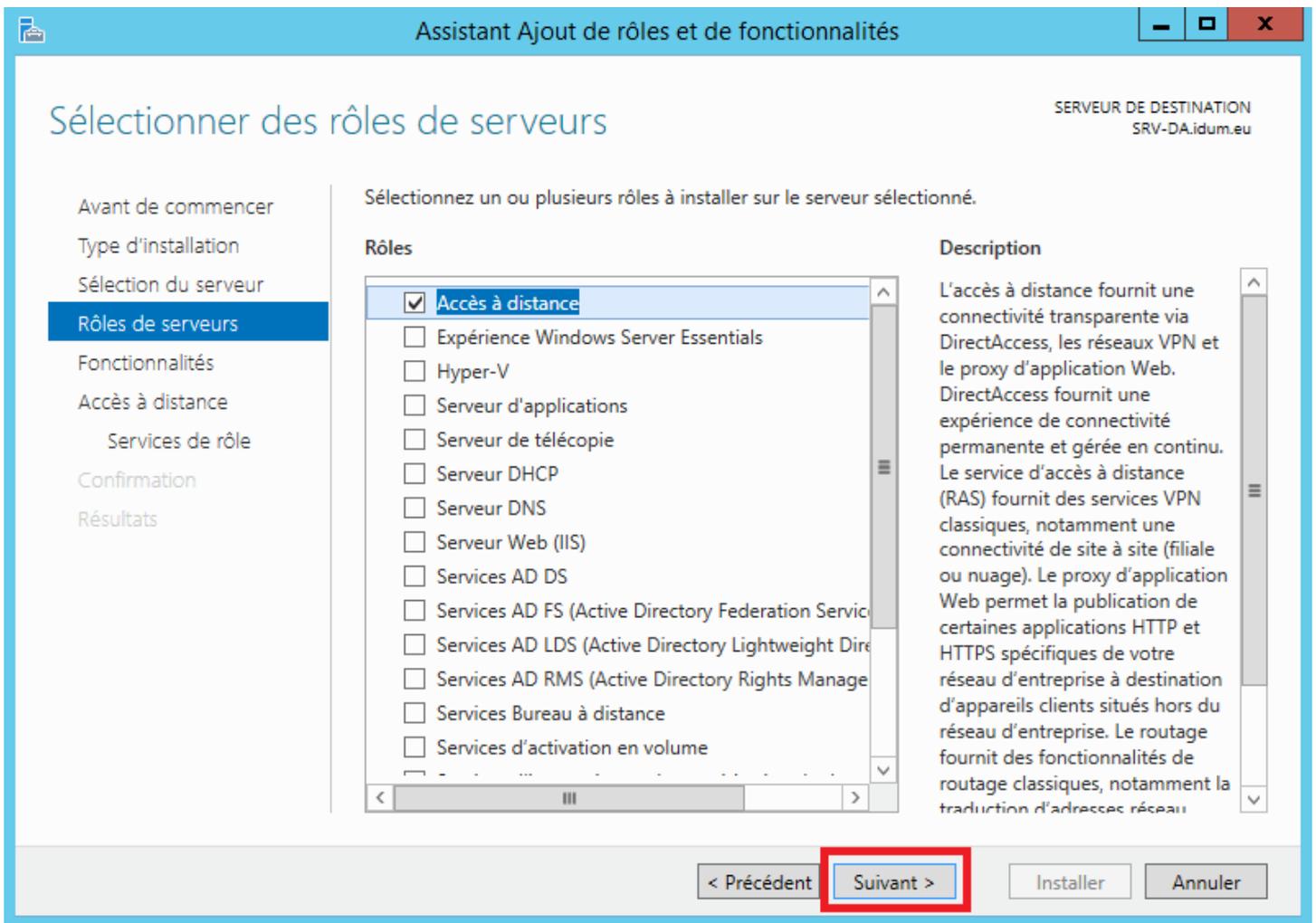
Nom	Adresse IP	Systeme d'exploitation
SRV-DA.idum.eu	1.1.1.1,192.168....	Microsoft Windows Server 2012 R2 Standard

1 ordinateur(s) trouvé(s)

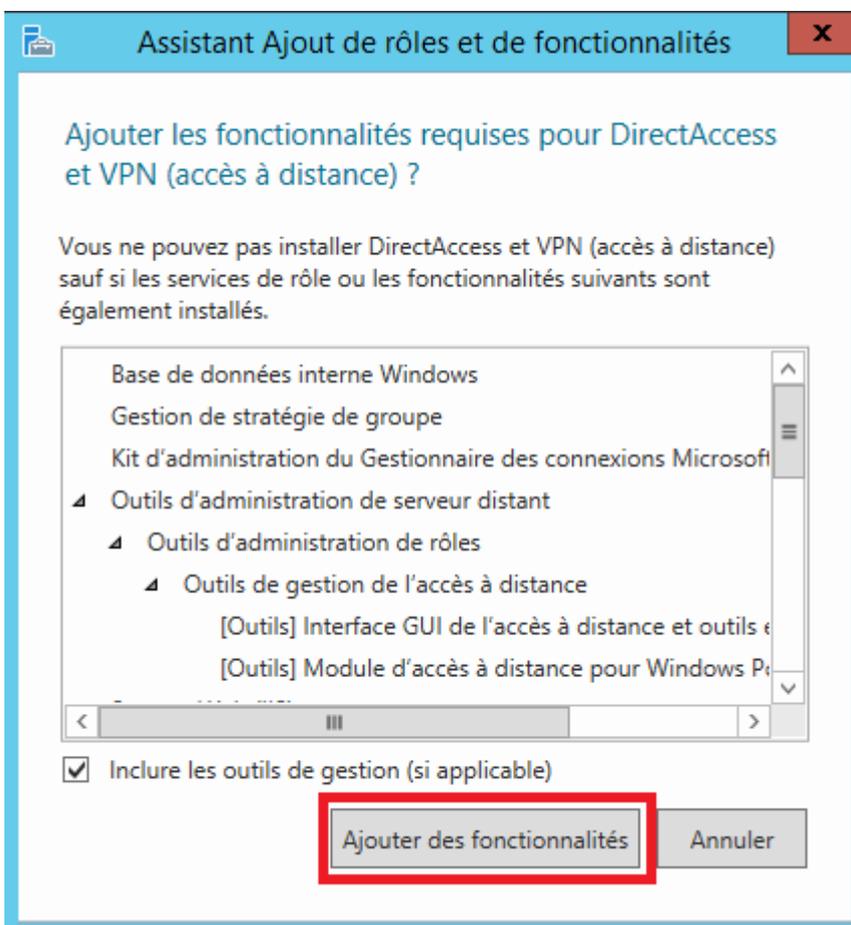
Cette page présente les serveurs qui exécutent Windows Server 2012 et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

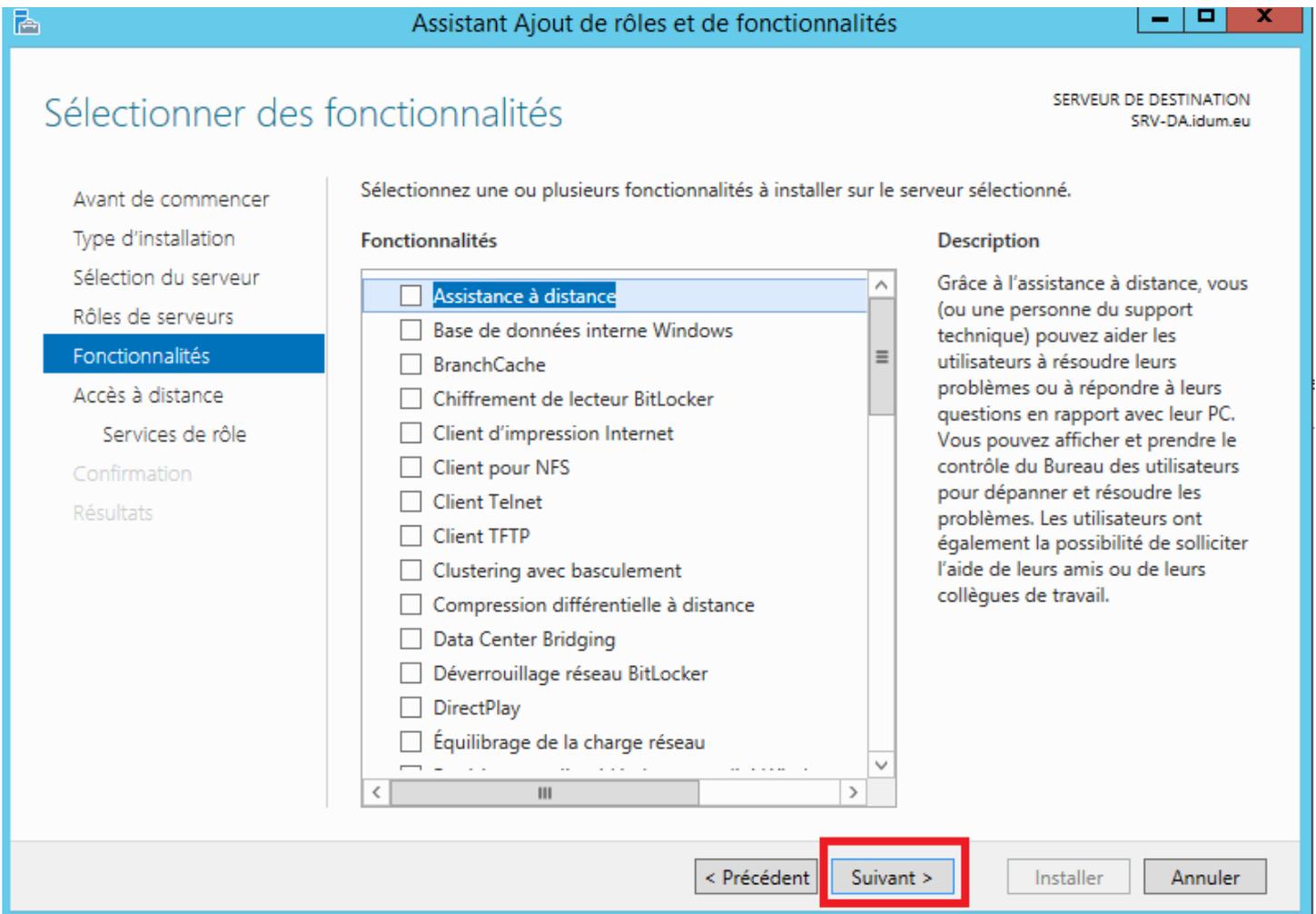
- Cochez "**Accès à distance**" et Cliquez sur "**Suivant**".



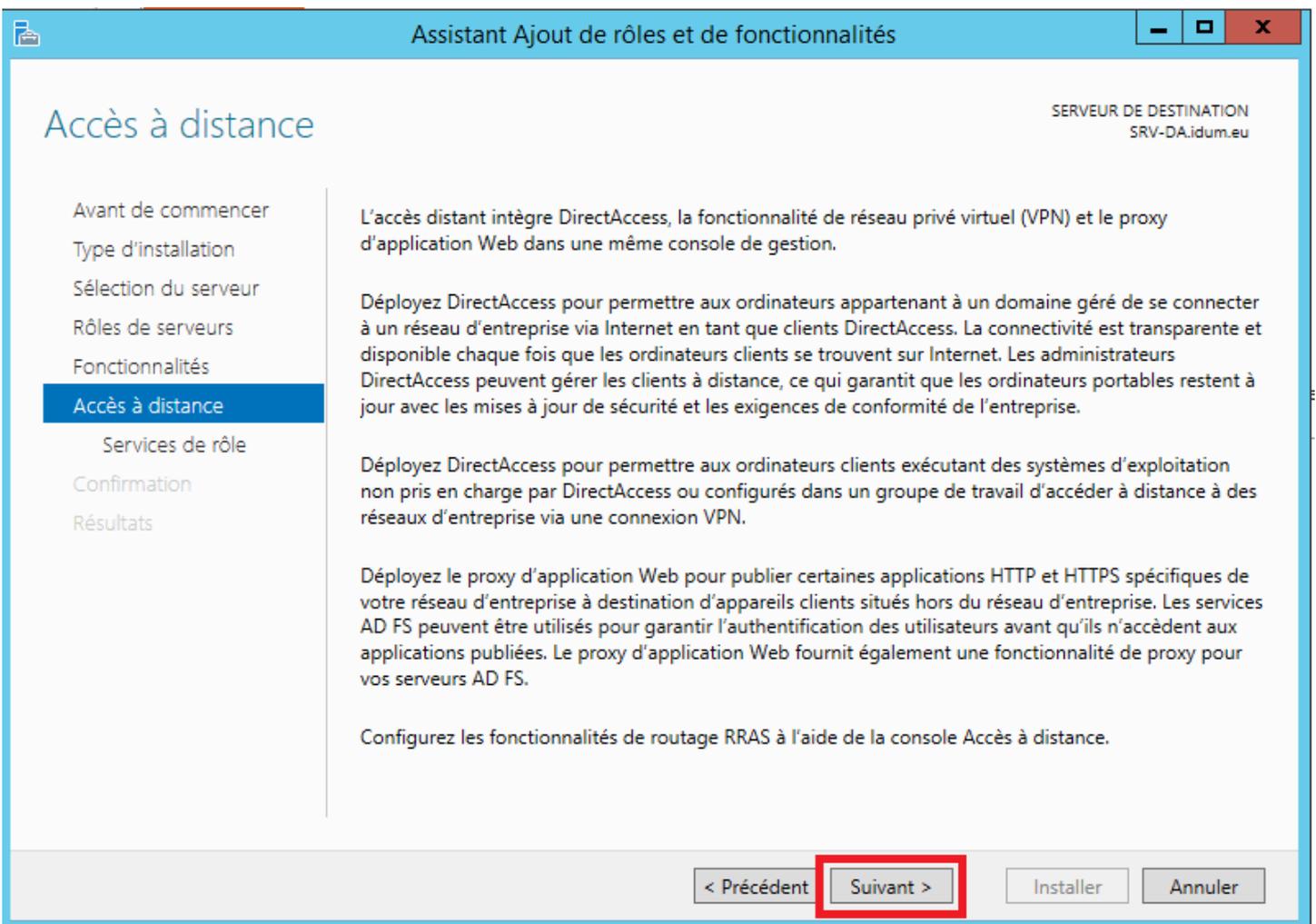
- Cliquez sur "**Ajouter des fonctionnalités**".



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



- Cliquez sur "**Suivant**".



- Cliquez sur "**Suivant**".

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION  
SRV-DA.idum.eu

## Rôle Web Server (IIS)

Avant de commencer  
Type d'installation  
Sélection du serveur  
Rôles de serveurs  
Fonctionnalités  
Accès à distance  
Services de rôle  
**Rôle Web Server (IIS)**  
Services de rôle  
Confirmation  
Résultats

Les serveurs Web sont des ordinateurs qui vous permettent de partager des informations sur l'Internet, des intranets ou des extranets. Le rôle Web Server comprend Internet Information Services (IIS) 8.5 avec un sécurité, du diagnostic et de l'administration améliorés, un plate-forme Web unifiée qui intègre IIS 8.5, ASP.NET, ainsi que Windows Communication Foundation.

À noter :

- L'utilisation du Gestionnaire de ressources système Windows (WSRM) permet d'assurer un service équitable si le Web sert du trafic, particulièrement lorsque plusieurs rôles sont présents sur cet ordinateur.
- L'installation par défaut du rôle de Web Server (IIS) comprend l'installation des services de rôles qui vous permettent de servir du contenu statique, d'effectuer de légères personnalisations (telles que les documents par défaut et les erreurs HTTP), de surveiller et de journaliser l'activité du serveur, et de configurer la compression du contenu statique.

[Plus d'informations sur Web Server IIS](#)

< Précédent **Suivant >** Installer Annuler

- Cliquez sur "**Suivant**".

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES SERVICES DE RÔLE

SERVEUR DE DESTINATION  
SRV-DA.idum.eu

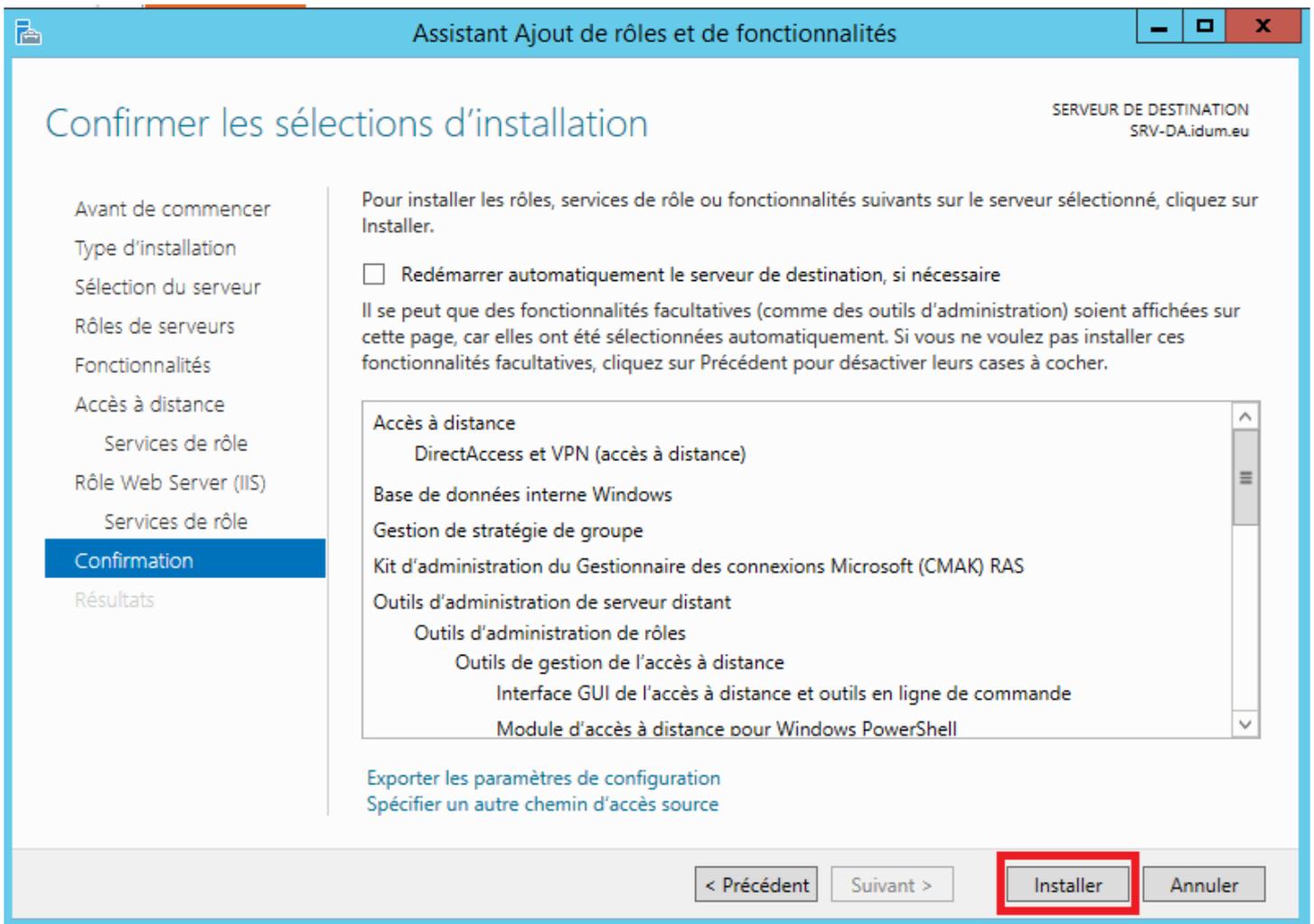
Avant de commencer  
Type d'installation  
Sélection du serveur  
Rôles de serveurs  
Fonctionnalités  
Accès à distance  
Services de rôle  
Rôle Web Server (IIS)  
**Services de rôle**  
Confirmation  
Résultats

Sélectionner les services de rôle à installer pour Serveur Web (IIS)

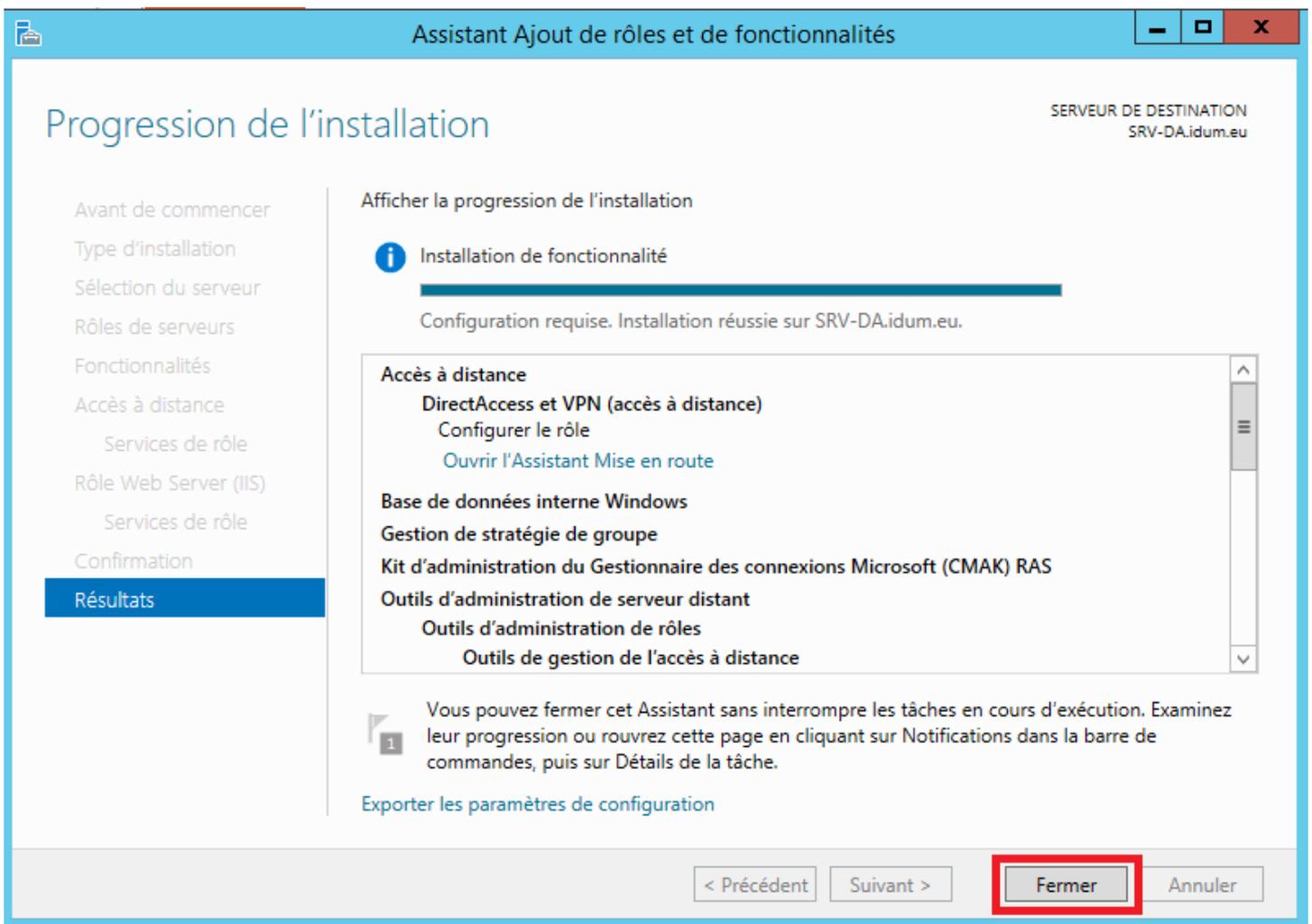
Services de rôle	Description
<input checked="" type="checkbox"/> Serveur Web	Le serveur Web fournit une prise en charge pour les site Web HTML et une prise en charge facultative pour les extensions ASP.NET, ASP et Serveur Web. Vous pouvez utiliser le serveur Web pour héberger un site Web interne ou externe ou pour fournir aux développeur un environnement pour créer des applications basées sur le Web.
<input checked="" type="checkbox"/> Fonctionnalités HTTP communes	
<input checked="" type="checkbox"/> Contenu statique	
<input checked="" type="checkbox"/> Document par défaut	
<input checked="" type="checkbox"/> Erreurs HTTP	
<input checked="" type="checkbox"/> Exploration de répertoire	
<input type="checkbox"/> Publication WebDAV	
<input type="checkbox"/> Redirection HTTP	
<input checked="" type="checkbox"/> Intégrité et diagnostics	
<input checked="" type="checkbox"/> Journalisation HTTP	
<input type="checkbox"/> Journal ODBC	
<input type="checkbox"/> Journalisation personnalisée	
<input type="checkbox"/> Observateur de demandes	
<input type="checkbox"/> Outils de journalisation	

< Précédent **Suivant >** Installer Annuler

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



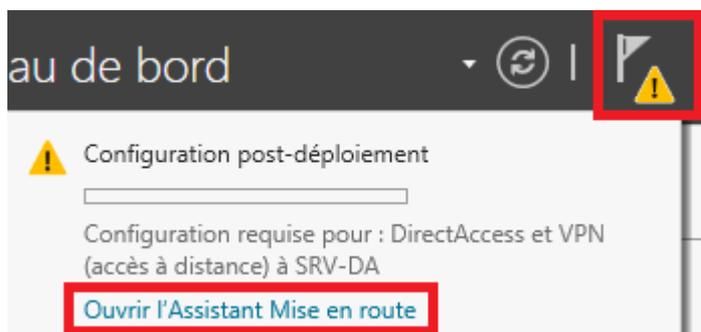
- Une fois terminée, cliquez sur "**Fermer**".



## 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**".

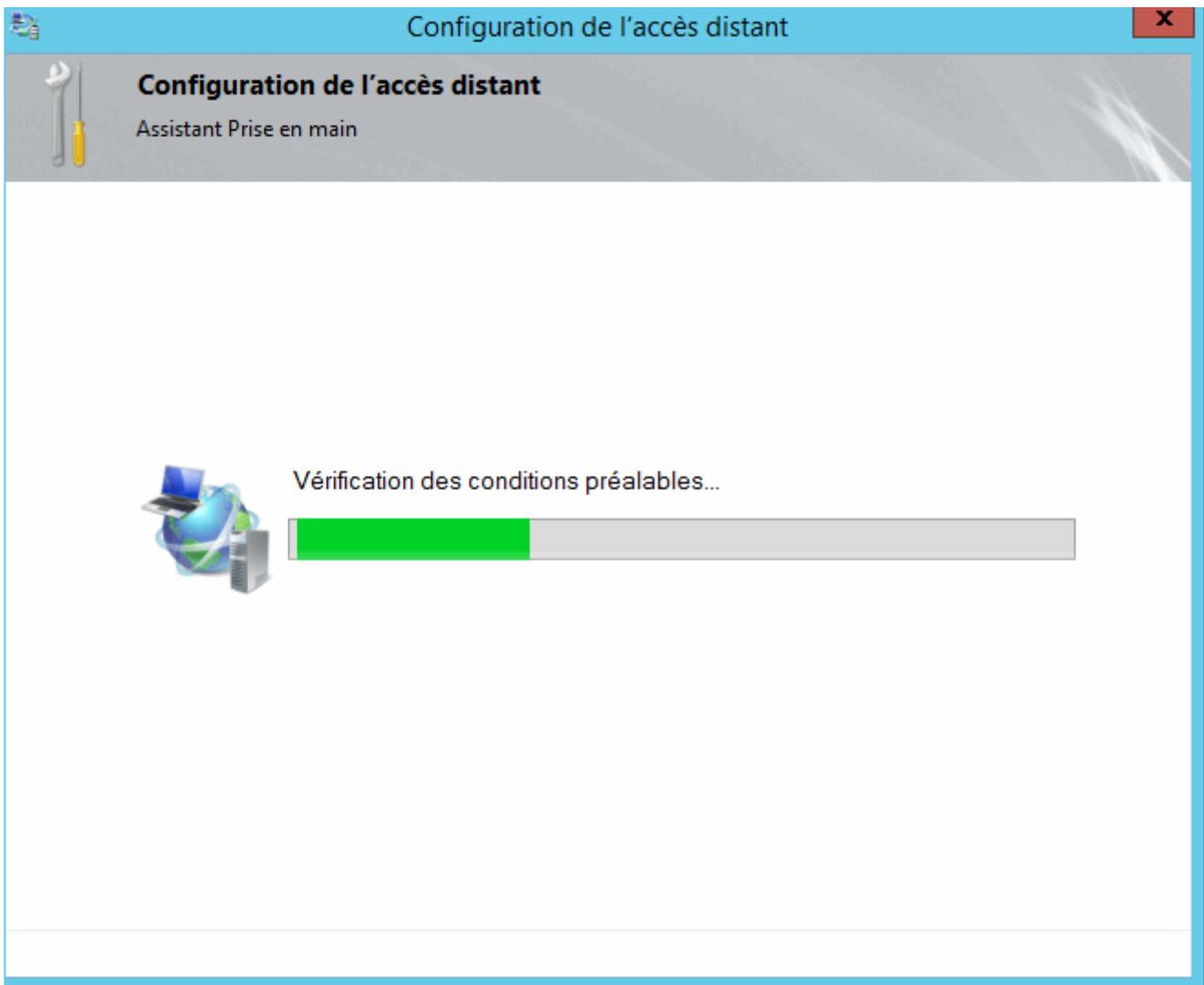
Configuration de l'accès distant

**Configuration de l'accès distant**  
Assistant Prise en main

Bienvenue dans l'accès à distance  
Utilisez les options de cette page pour configurer DirectAccess et une connexion VPN.

- **Déployer DirectAccess et VPN (recommandé)**  
Configurer DirectAccess et le réseau privé virtuel (VPN) sur le serveur et activer les ordinateurs clients DirectAccess. Autoriser les ordinateurs clients distants non pris en charge pour DirectAccess à se connecter sur le réseau privé virtuel.
- **Déployer DirectAccess uniquement**  
Configurer DirectAccess sur le serveur et activer les ordinateurs clients DirectAccess.
- **Déployer VPN uniquement**  
Configurer VPN à l'aide de la console Routage et accès à distance. Les ordinateurs clients distants peuvent se connecter sur le réseau privé virtuel et plusieurs sites peuvent être connectés au moyen de connexions VPN de site à site. VPN peut être utilisé par les clients non pris en charge pour DirectAccess.

- 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**".

Configuration de l'accès distant

### Installation du serveur d'accès à distance

Configurez les paramètres DirectAccess et VPN.

Sélectionnez la topologie de réseau du serveur.

Périphère

Derrière un périphérique de périphère (avec deux cartes réseau)

Derrière un périphérique de périphère (avec une carte réseau unique)

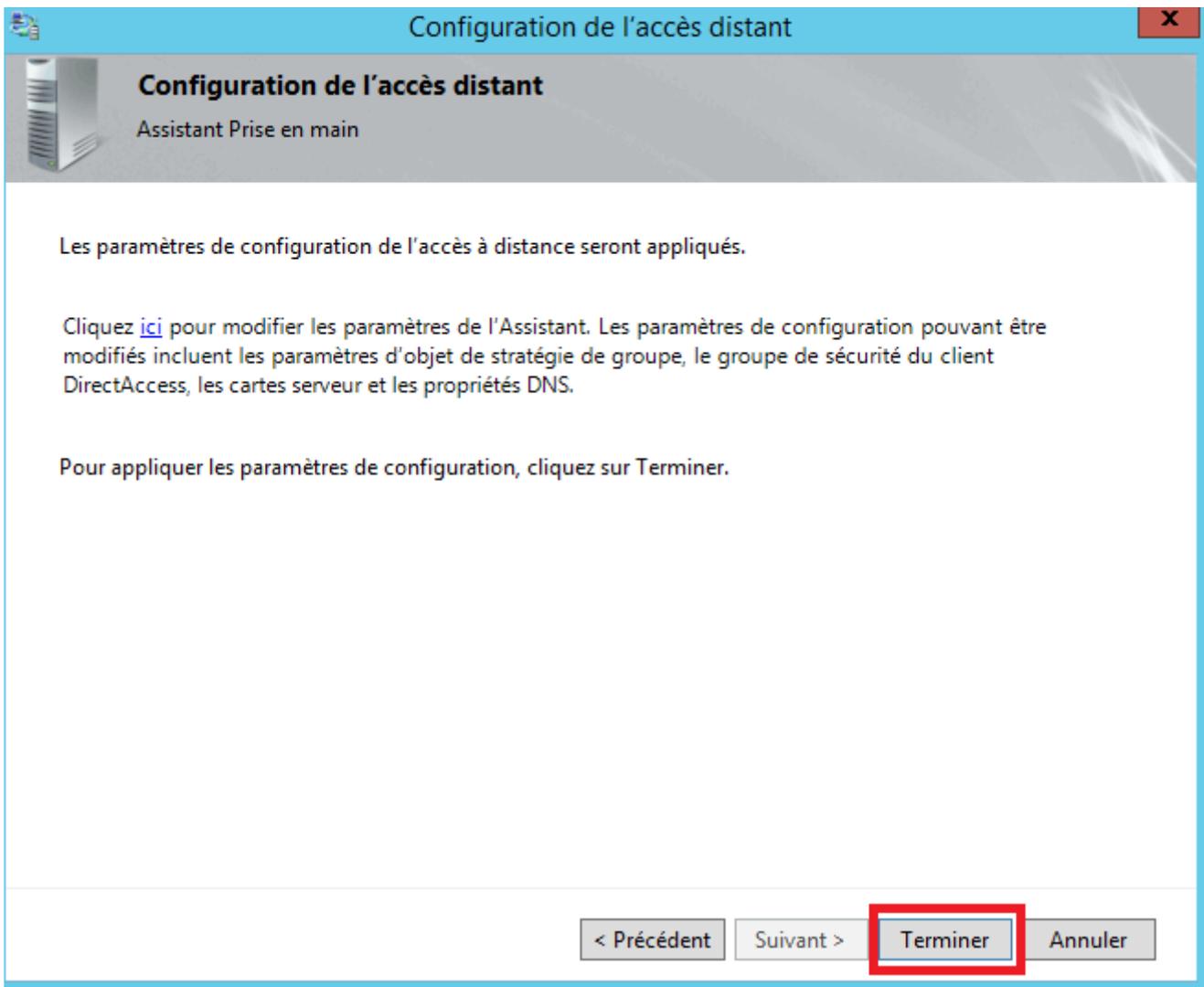
Dans cette topologie, le serveur Accès distant est déployé en périphérie du réseau d'entreprise interne et configuré avec deux cartes. Une carte est connectée au réseau interne, l'autre à Internet.

Tapez le nom public ou l'adresse IPv4 utilisé par les clients pour se connecter au serveur d'accès à distance :

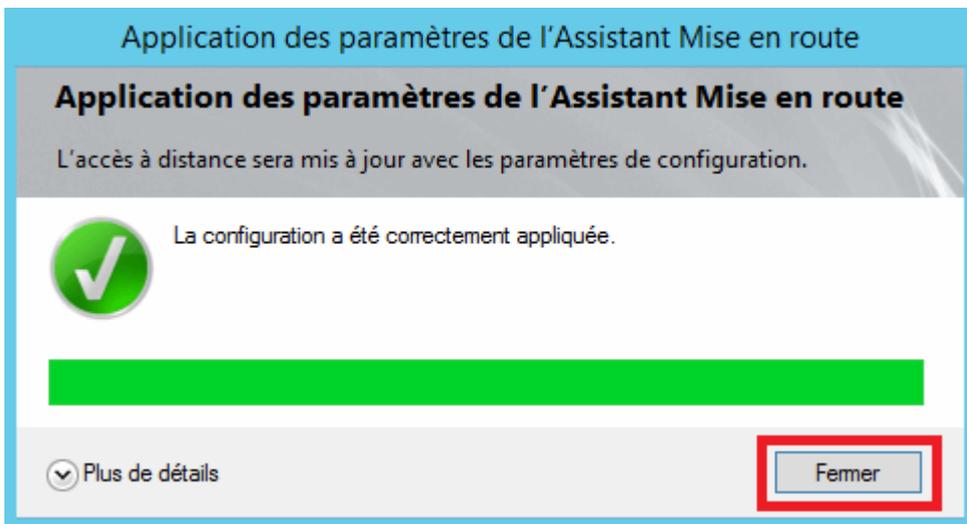
da.idum.com

< Précédent **Suivant >** Terminer Annuler

- 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**".

# Étape 1

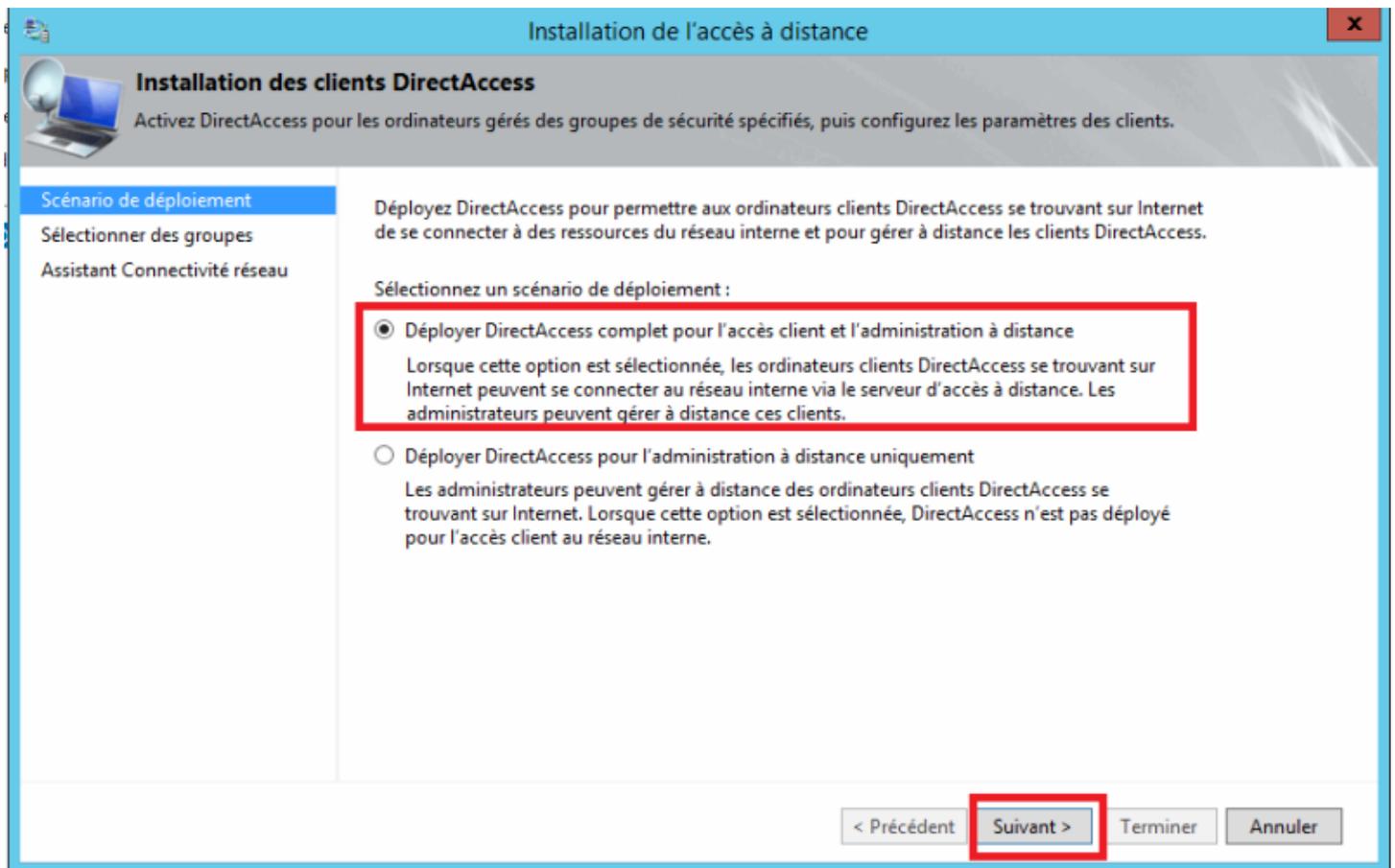
**Clients distants**



Identifiez les ordinateurs clients qui seront activés pour DirectAccess.

**Modifier...**

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



Installation de l'accès à distance

**Installation des clients DirectAccess**  
Activez DirectAccess pour les ordinateurs gérés des groupes de sécurité spécifiés, puis configurez les paramètres des clients.

Scénario de déploiement

Sélectionner des groupes

Assistant Connectivité réseau

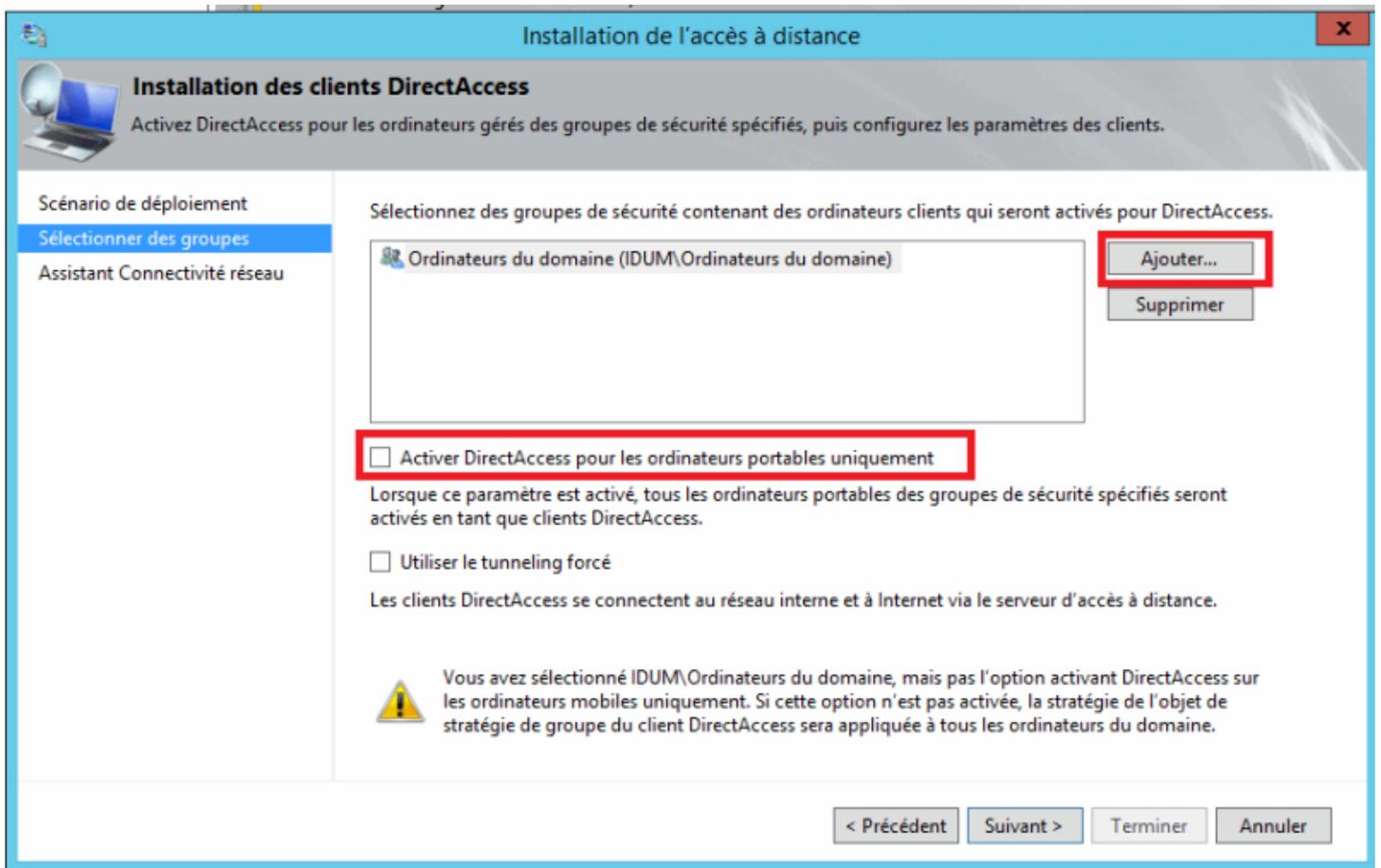
Déployez DirectAccess pour permettre aux ordinateurs clients DirectAccess se trouvant sur Internet de se connecter à des ressources du réseau interne et pour gérer à distance les clients DirectAccess.

Sélectionnez un scénario de déploiement :

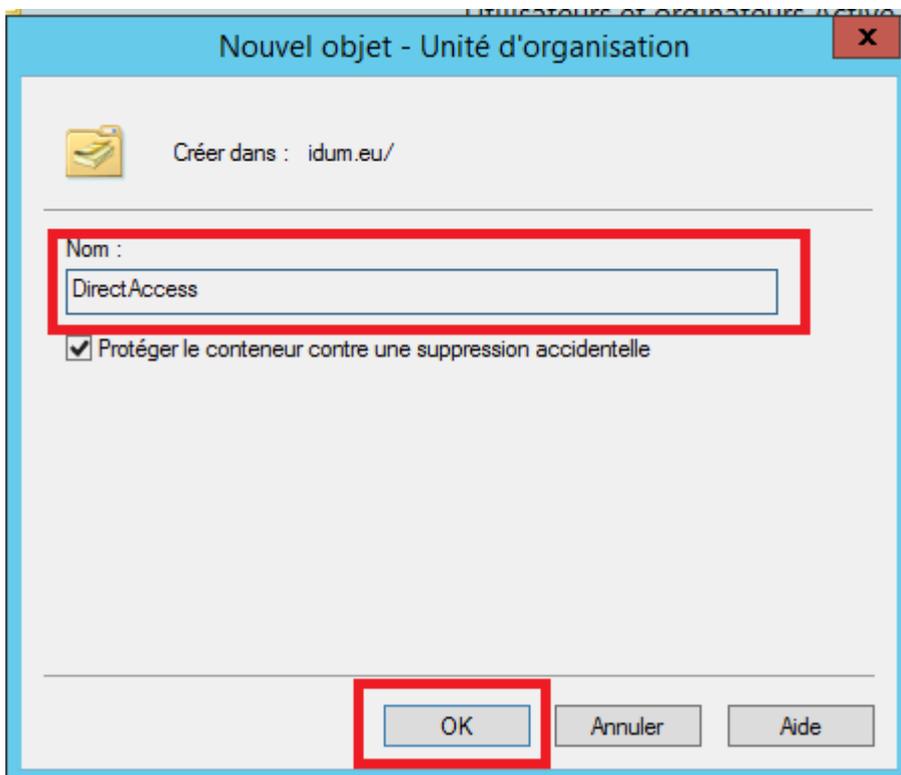
- Déployer DirectAccess complet pour l'accès client et l'administration à distance  
Lorsque cette option est sélectionnée, les ordinateurs clients DirectAccess se trouvant sur Internet peuvent se connecter au réseau interne via le serveur d'accès à distance. Les administrateurs peuvent gérer à distance ces clients.
- Déployer DirectAccess pour l'administration à distance uniquement  
Les administrateurs peuvent gérer à distance des ordinateurs clients DirectAccess se trouvant sur Internet. Lorsque cette option est sélectionnée, DirectAccess n'est pas déployé pour l'accès client au réseau interne.

< Précédent **Suivant >** Terminer Annuler

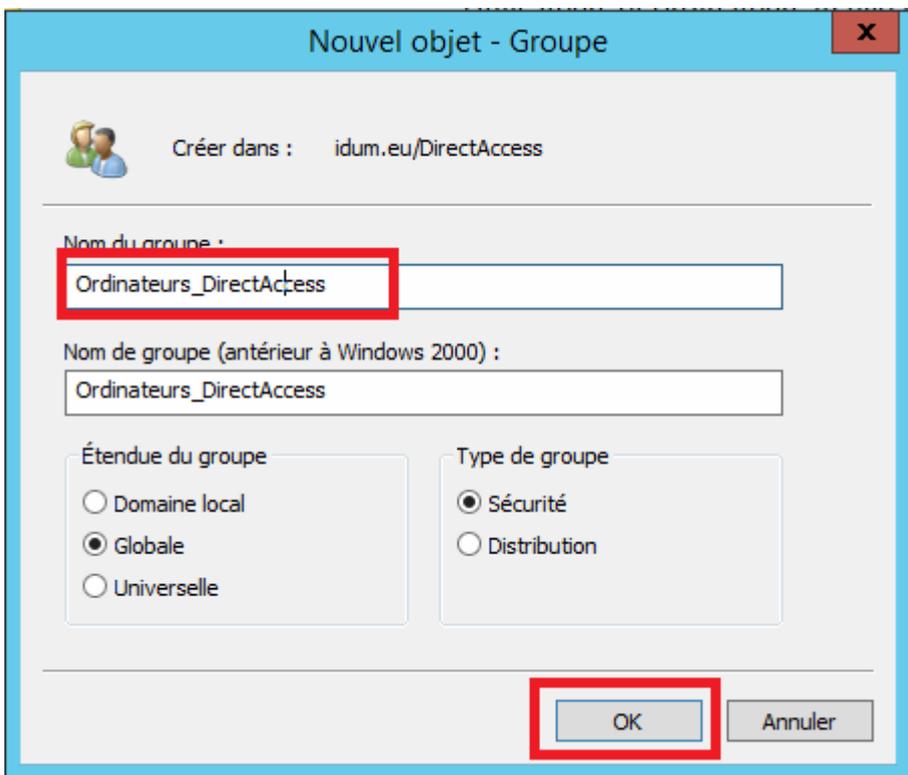
- Par défaut, l'assistant de configuration nous propose de déployer DirectAccess sur tous les ordinateurs du domaine, dans notre exemple, nous allons créer un groupe d'ordinateur spécial pour les clients DirectAccess.



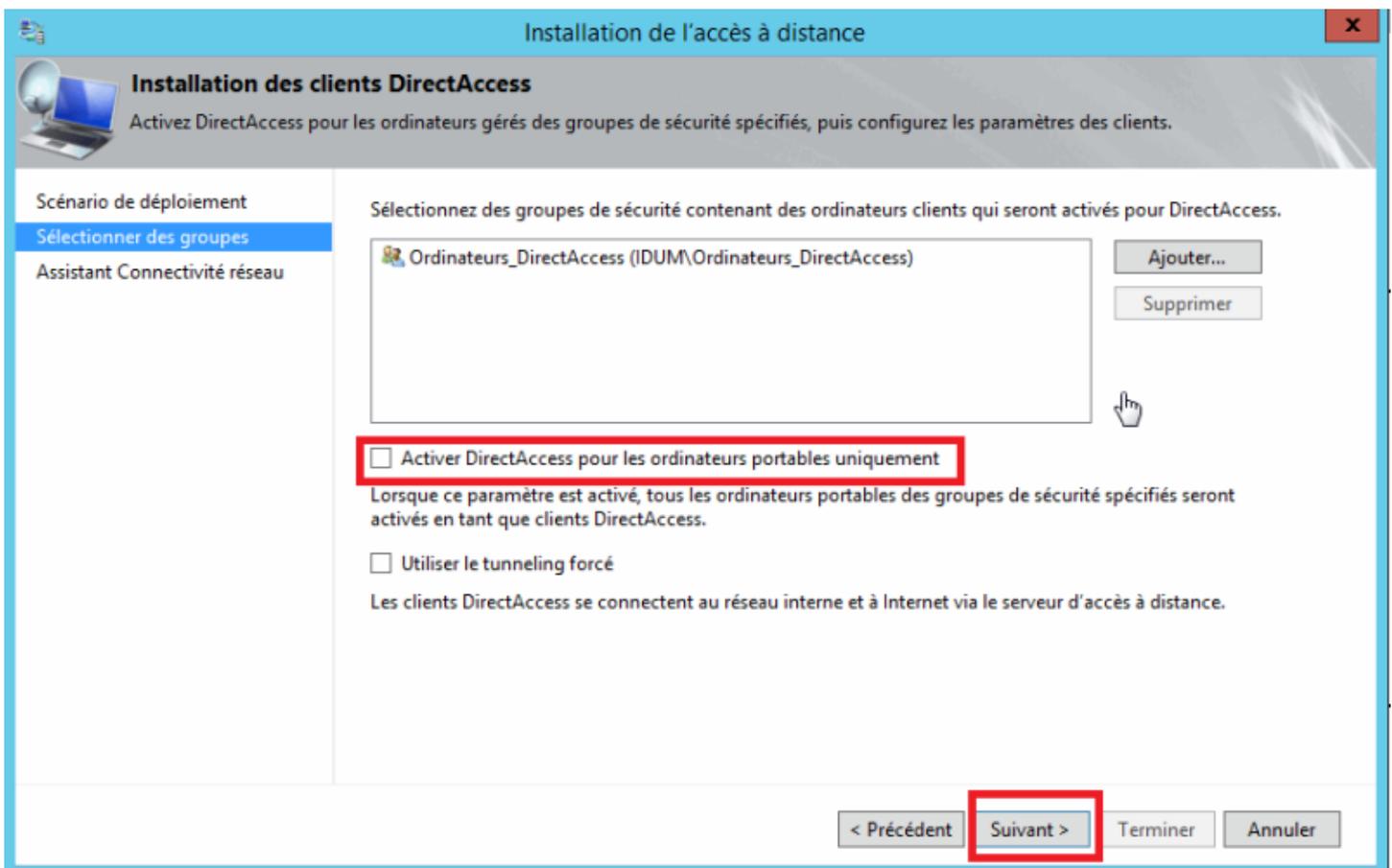
- Sur l'ActiveDirectory, créez une OU (Unité organisationnelle) et créez un groupe dans cette OU. Dans l'outil "**Utilisateurs et ordinateurs du domaine**", faites un clic droit sur le domaine et sélectionnez "**nouveau**" puis "**Unité d'organisation**". Nommez-la comme vous voulez.



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

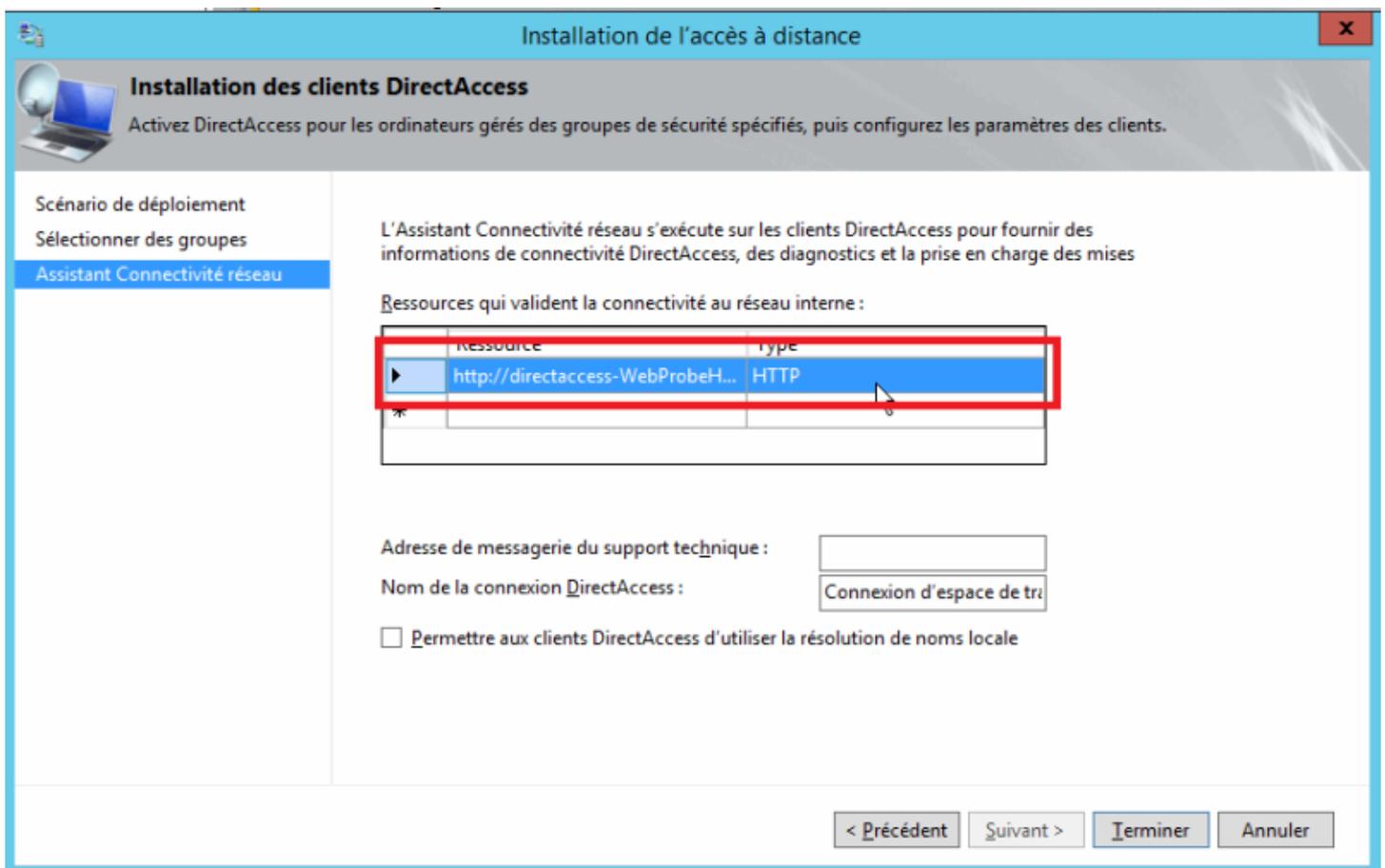


- Revenons à l'assistant de configuration, sélectionnez "**Ajouter**" et entrer le nom de votre groupe. En passant, décocher l'option "**Activez DirectAccess pour les ordinateurs portables uniquement**".

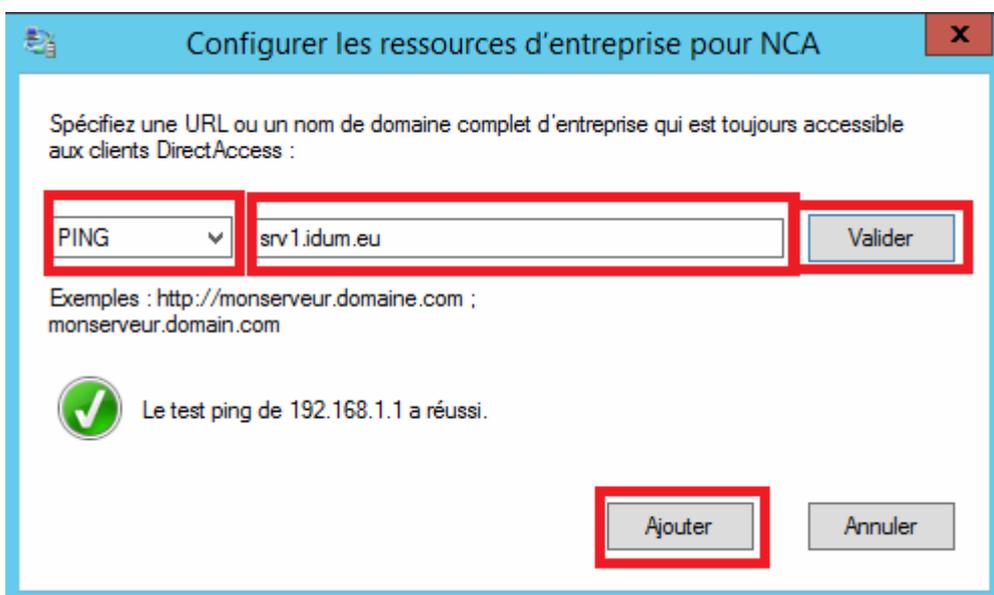


L'assistant de connectivité réseau c'est le protocole de test pour savoir si l'ordinateur se trouve dans le LAN ou bien s'il est hors du réseau local. Pour notre démonstration, nous allons faire un ping vers le serveur ActiveDirectory, à savoir srv1.idum.eu.

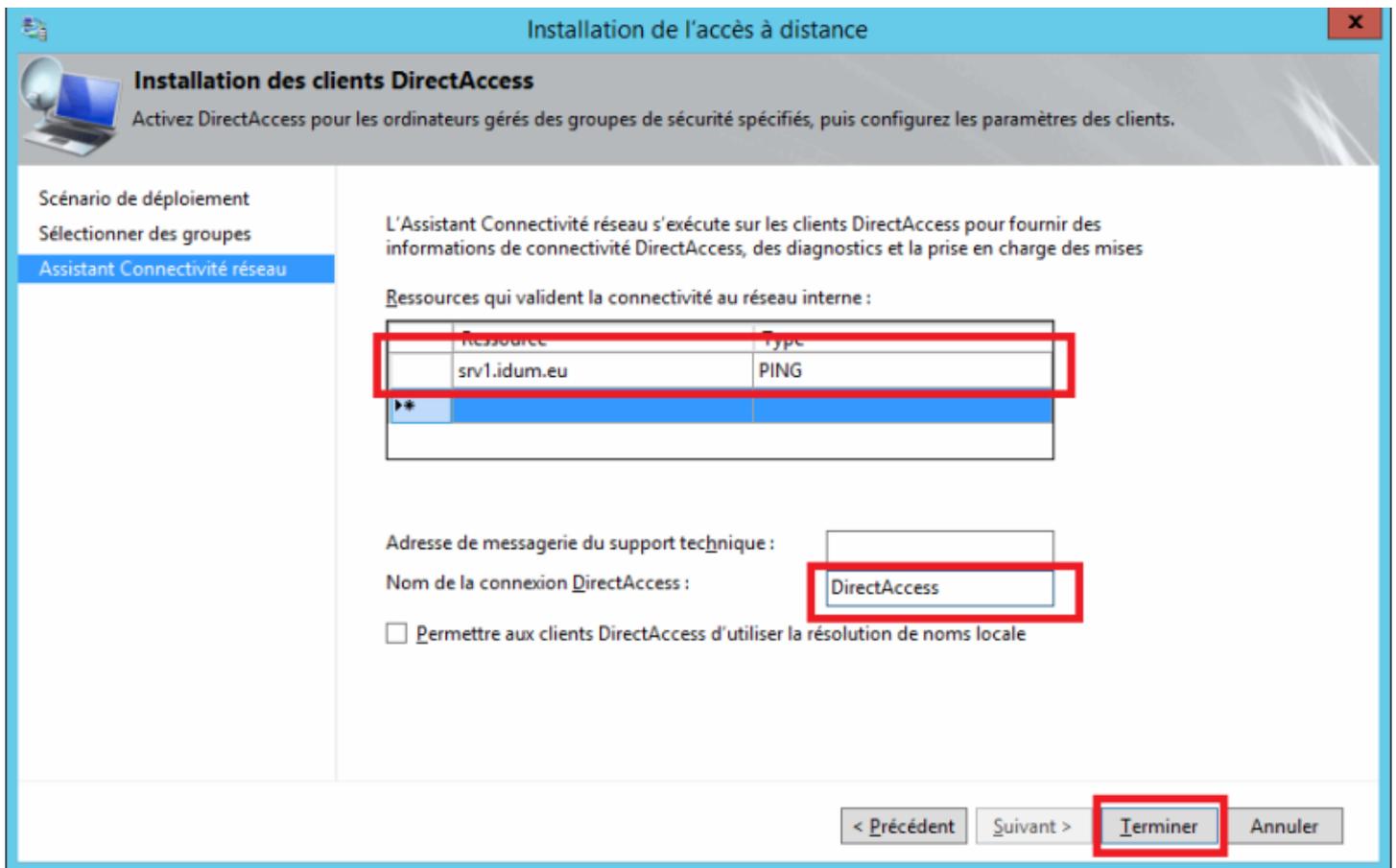
- Faites un clic droit sur la ligne déjà proposé et cliquez sur "**Supprimer**". Faîte un clic droit sur la ligne vide et cliquez sur "**Nouveau**".



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



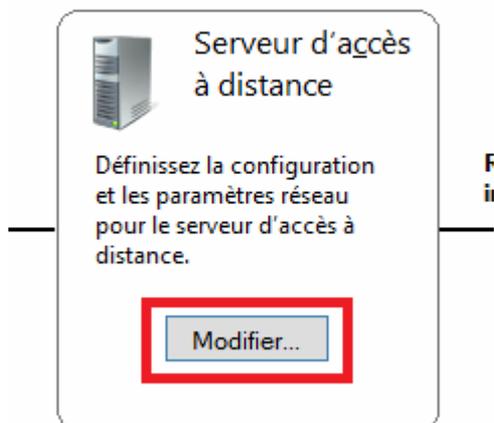
- Dans "**Nom de la connexion**" entrer le nom que vous souhaitez voir apparaître sur le client.



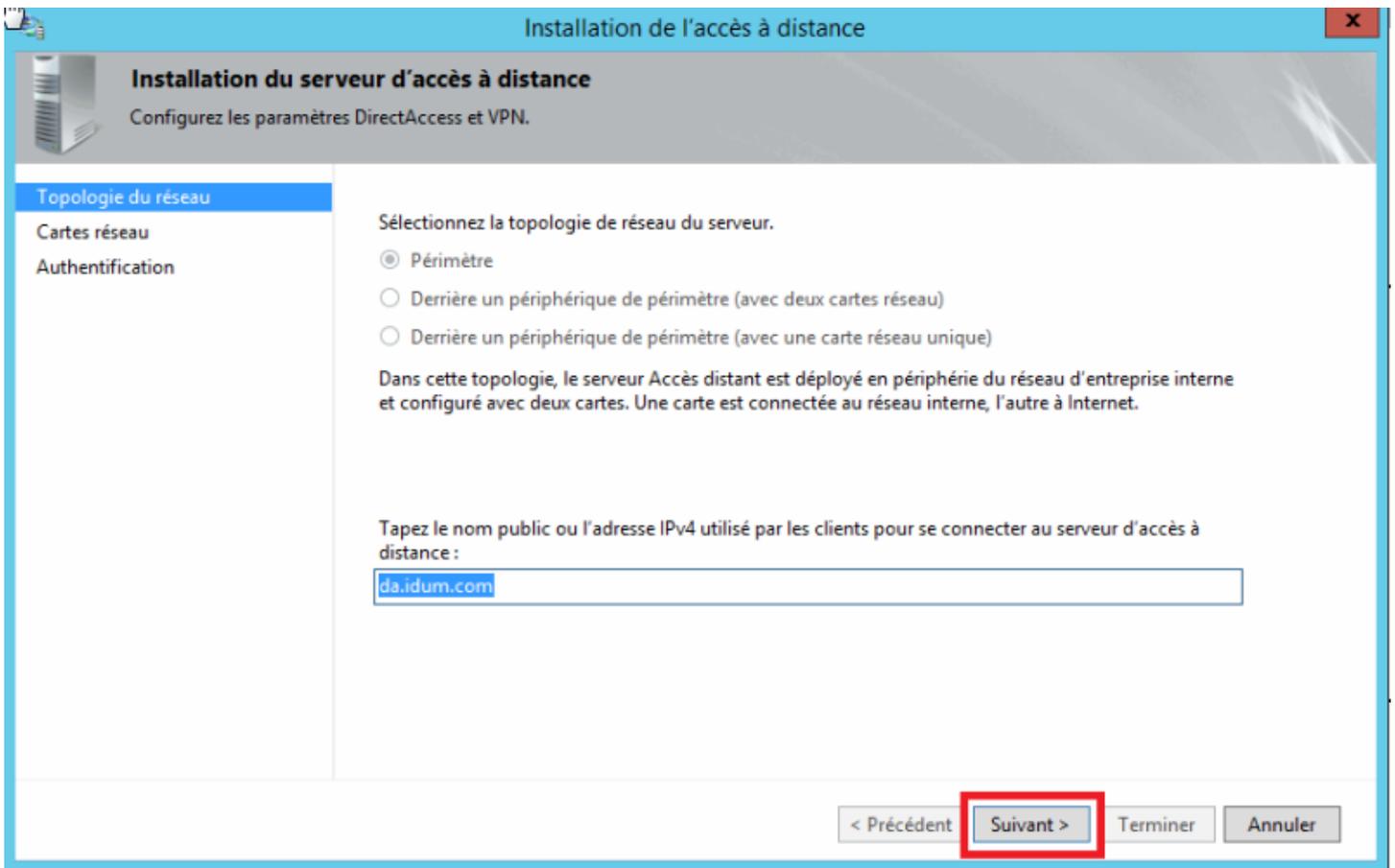
### 3) Configuration du serveur d'accès à distance

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

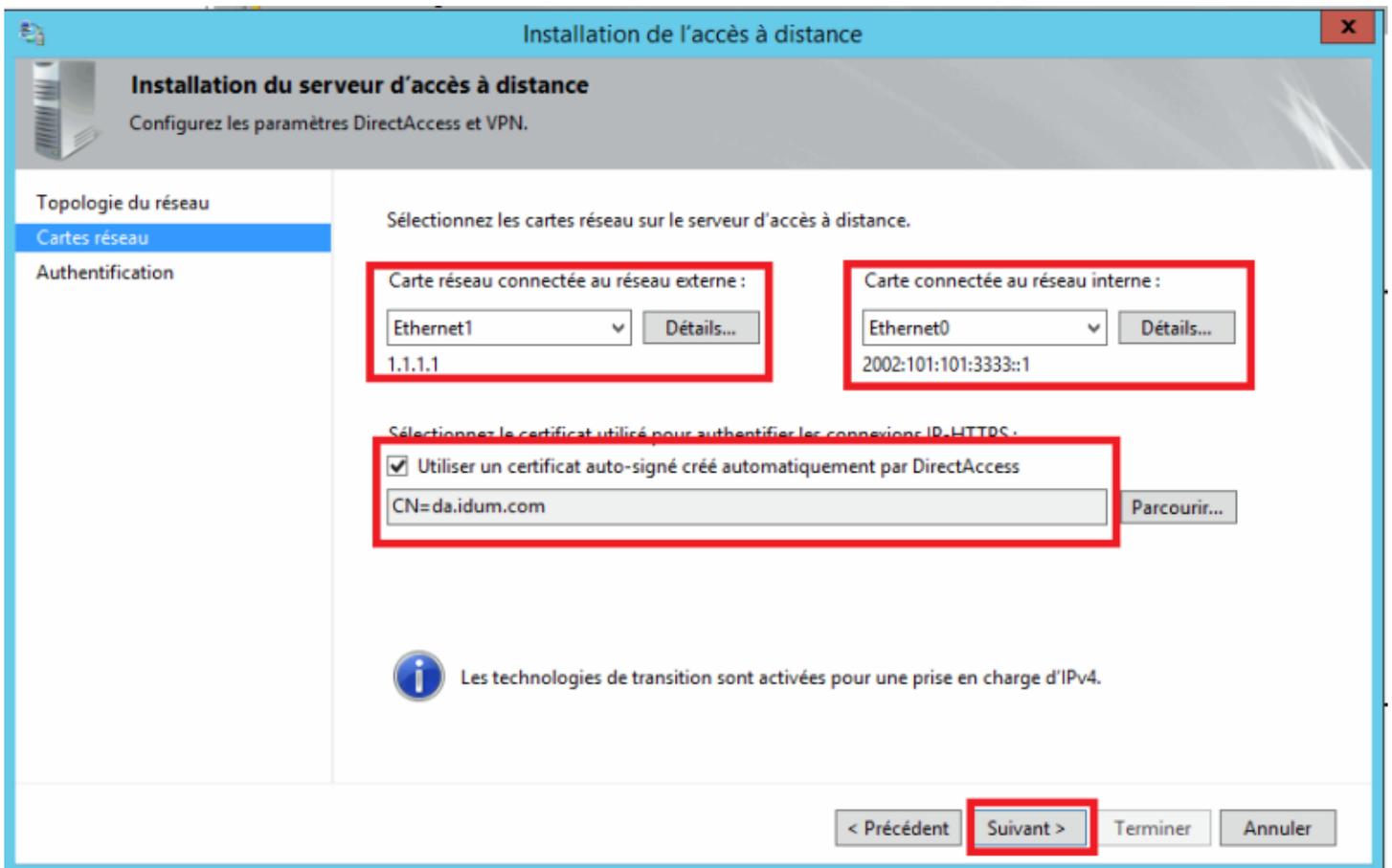
#### Étape 2



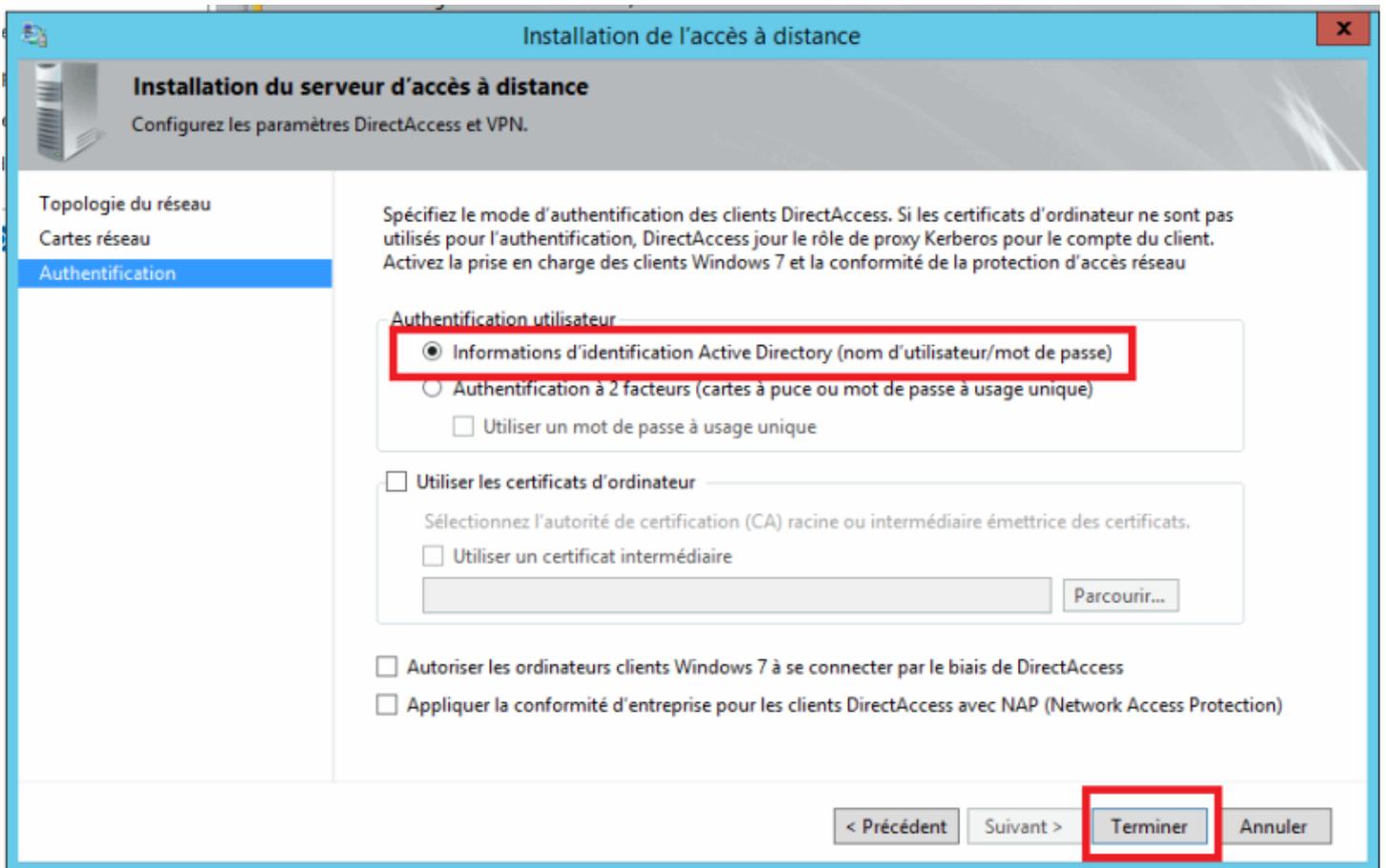
- Vous retrouvez ici le paramètre défini avant, ne modifiez rien et cliquez sur "**Suivant**".



- 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**".



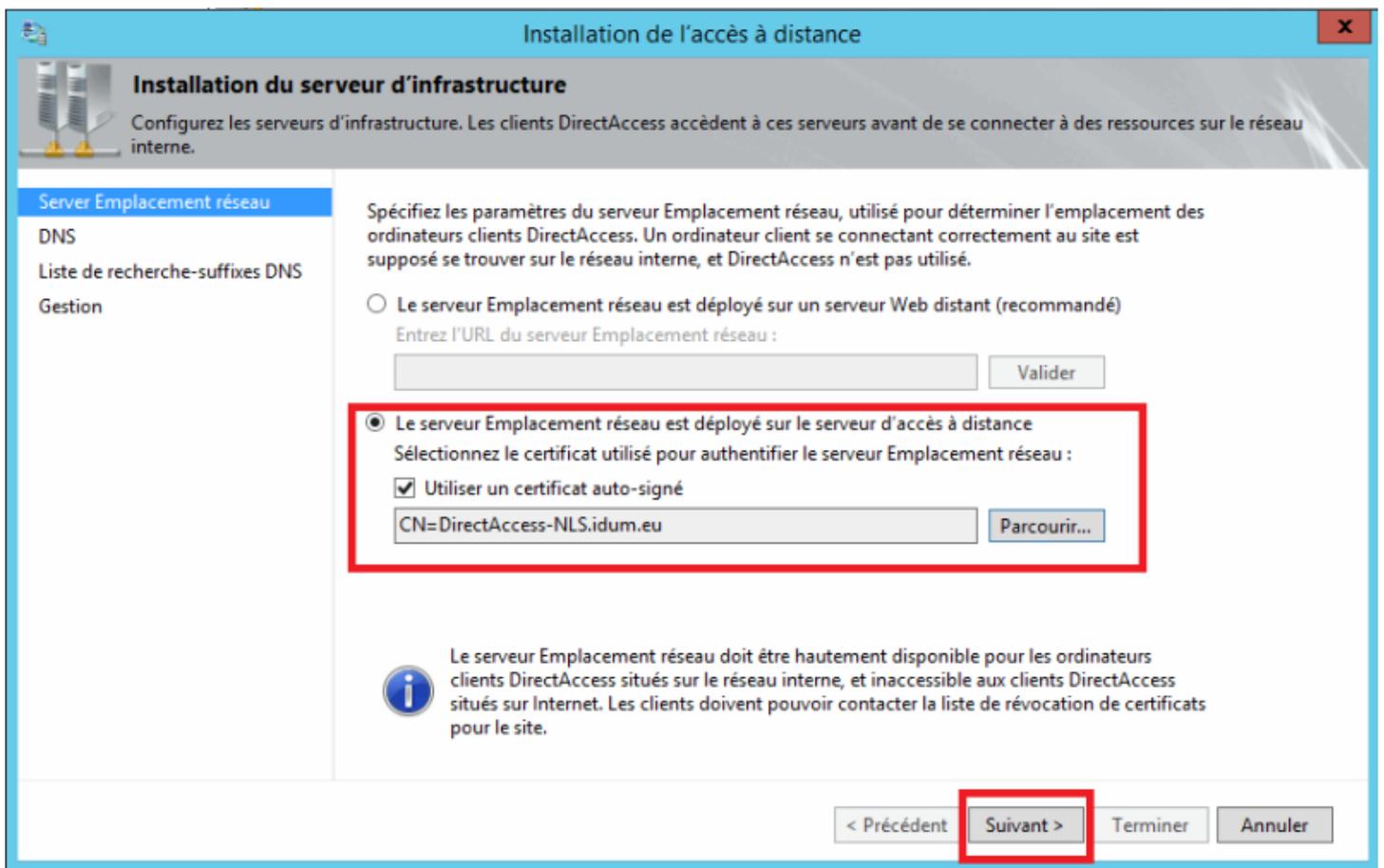
## 4) Configuration des ressources internet disponible à distance

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

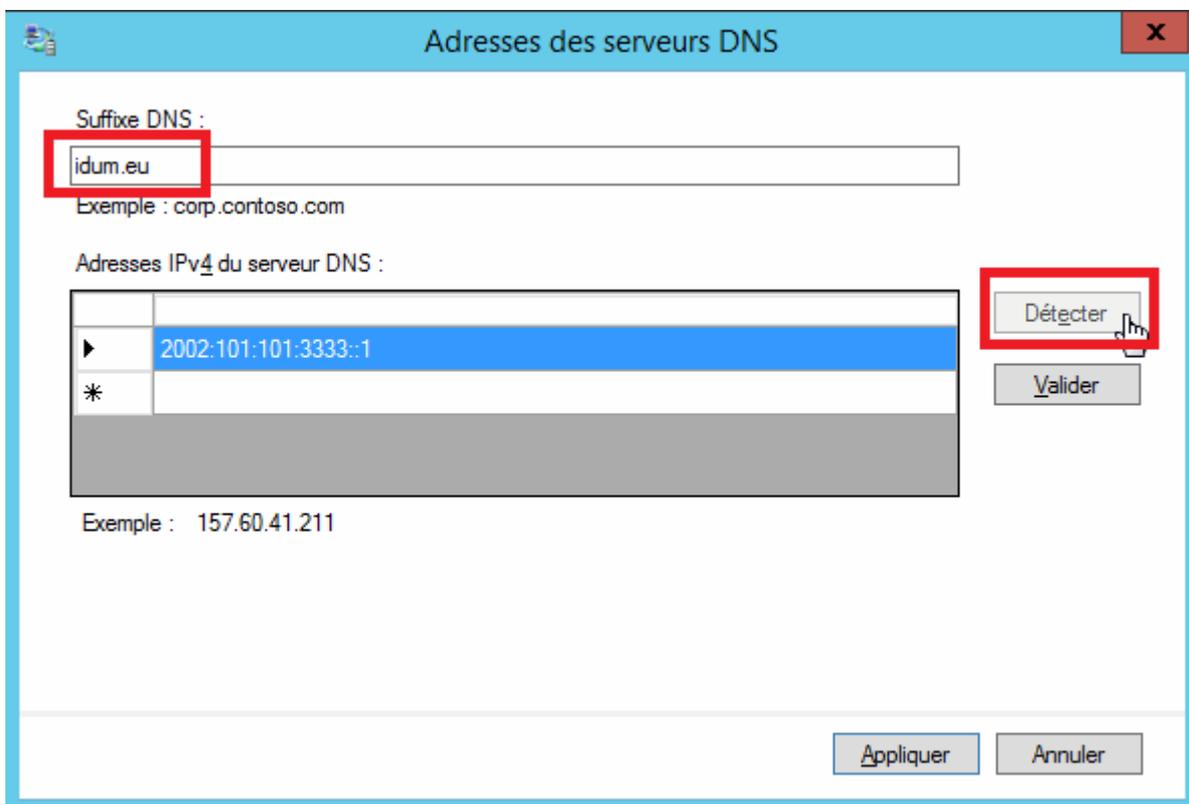
### Étape 3



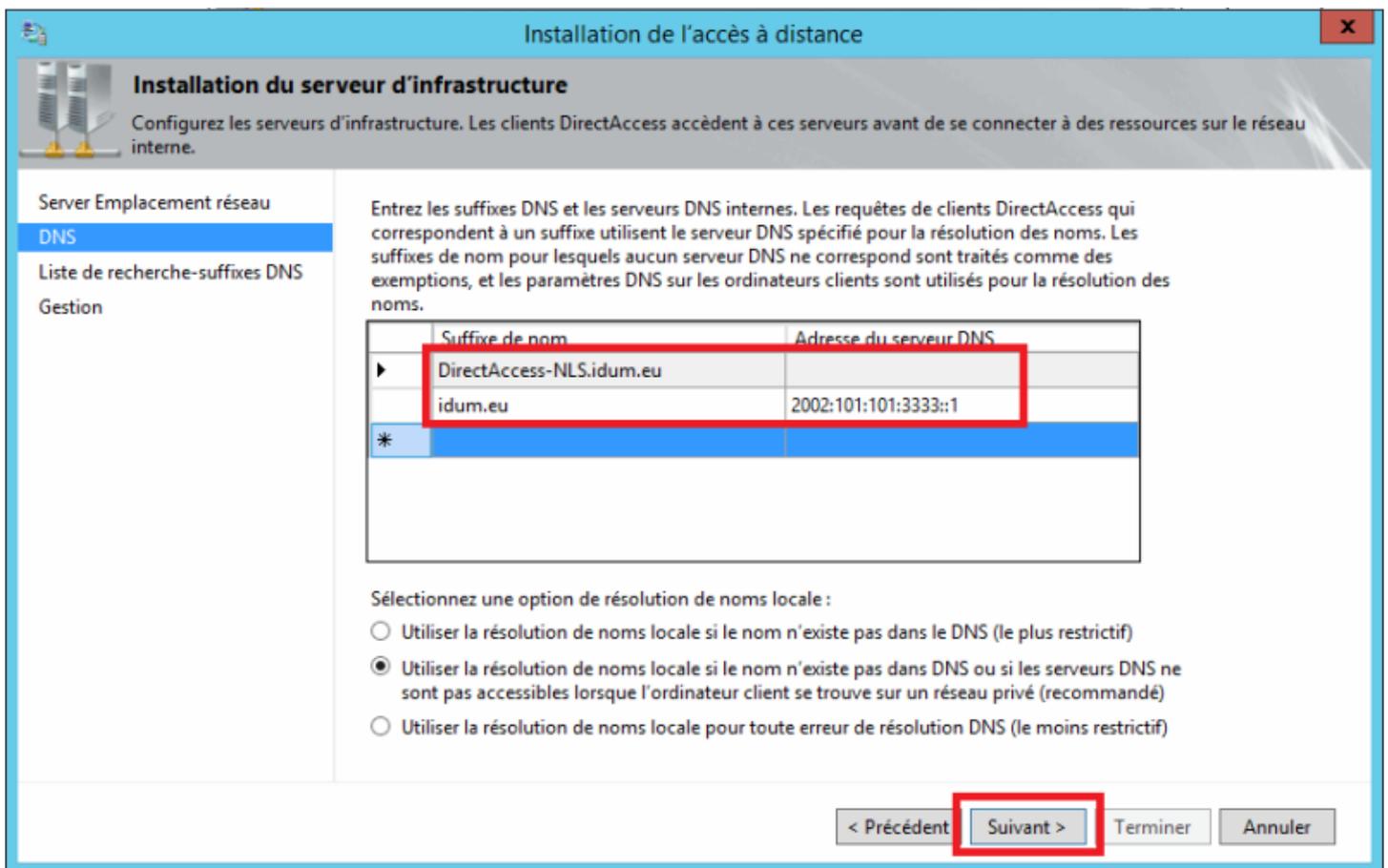
- Le serveur d'emplacement réseau, permet aussi au client de s'assurer qu'il se trouve sur le réseau local.



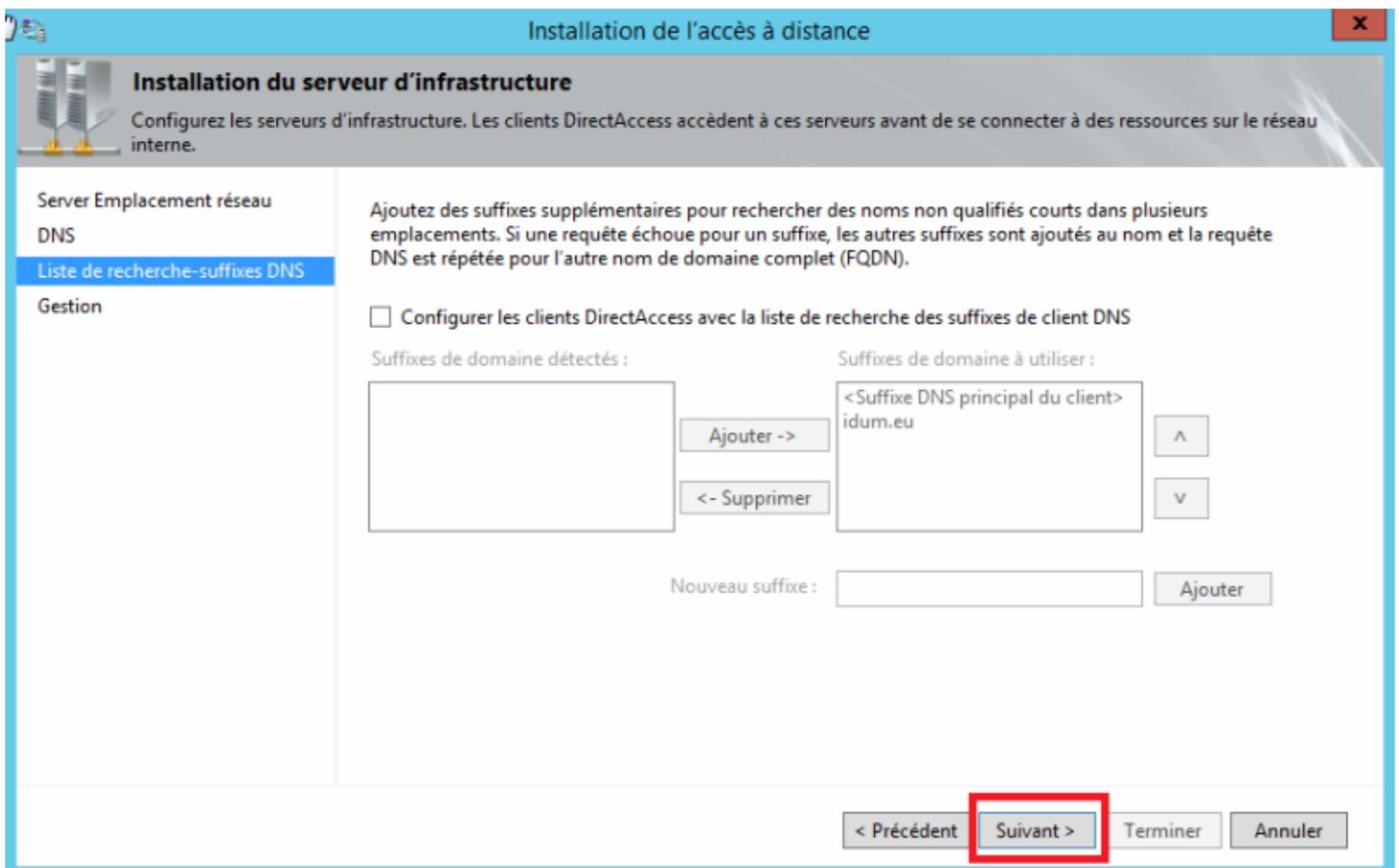
- Le client, une fois connecté en DirectAccess au réseau local, va utiliser le serveur DNS du domaine, on va ajouter le domaine idum.eu et cliquer sur détecter pour qu'il ajoute automatiquement l'adresse du DNS. L'adresse IPV6 du serveur doit s'afficher comme ici :



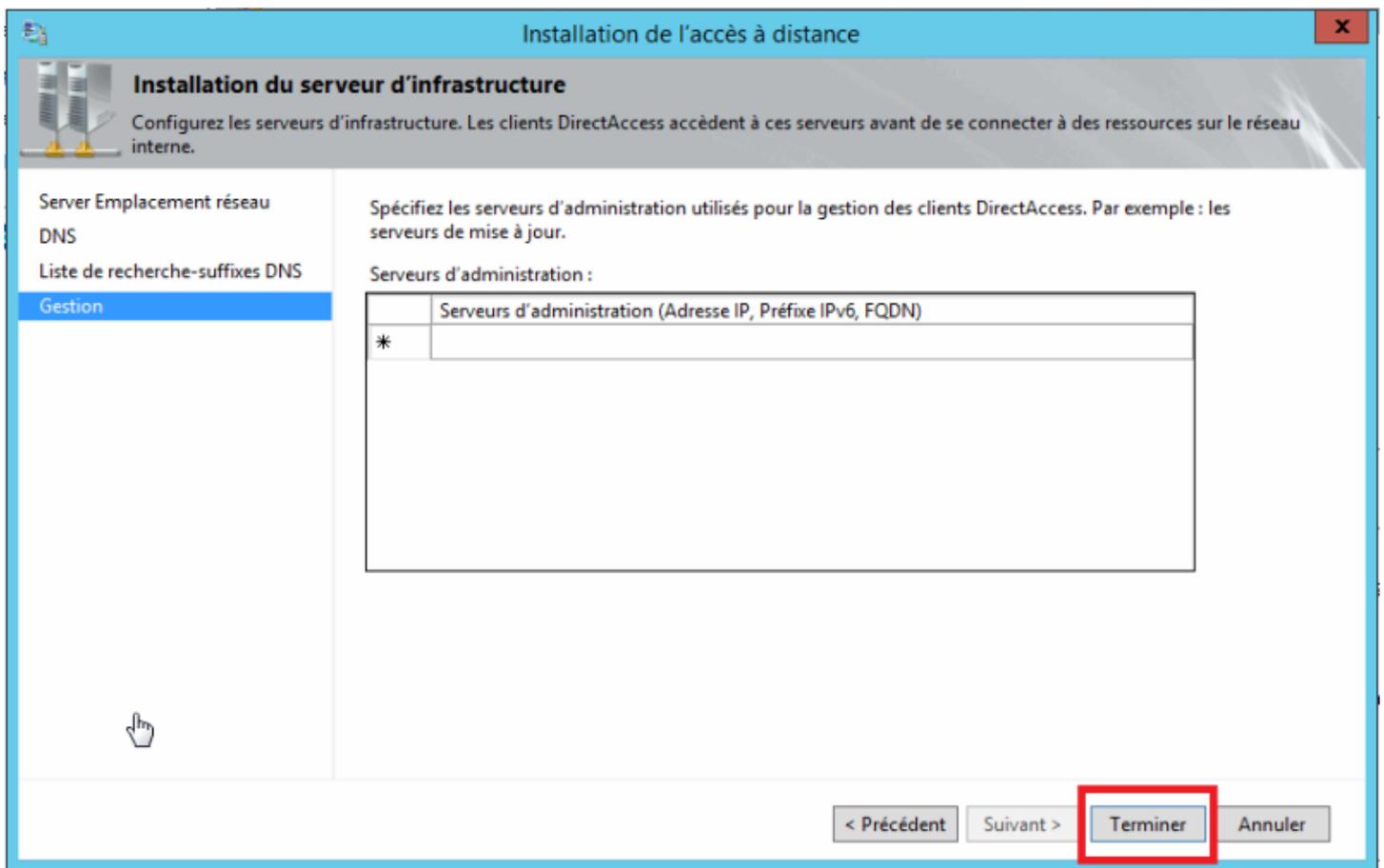
- Par défaut, on va signifier au client, que le DNS local va résoudre la zone idum.eu.



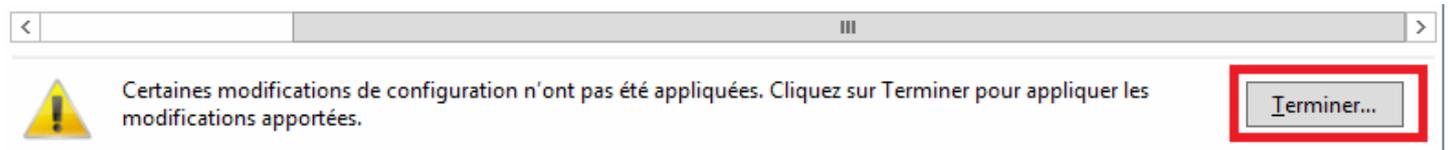
- Il est possible d'ajouter des URL de serveur d'administration, dans notre cas, nous n'allons rien ajouter. Cliquez sur "**Suivant**".



- 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 icône 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 a 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.

DÉMARRAGE  
RAPIDE

NOUVEAUTÉS

EN SAVOIR PLUS

## 1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

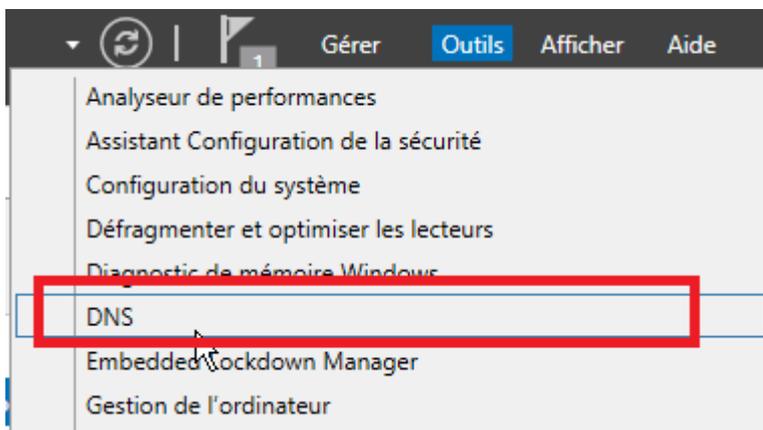
3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

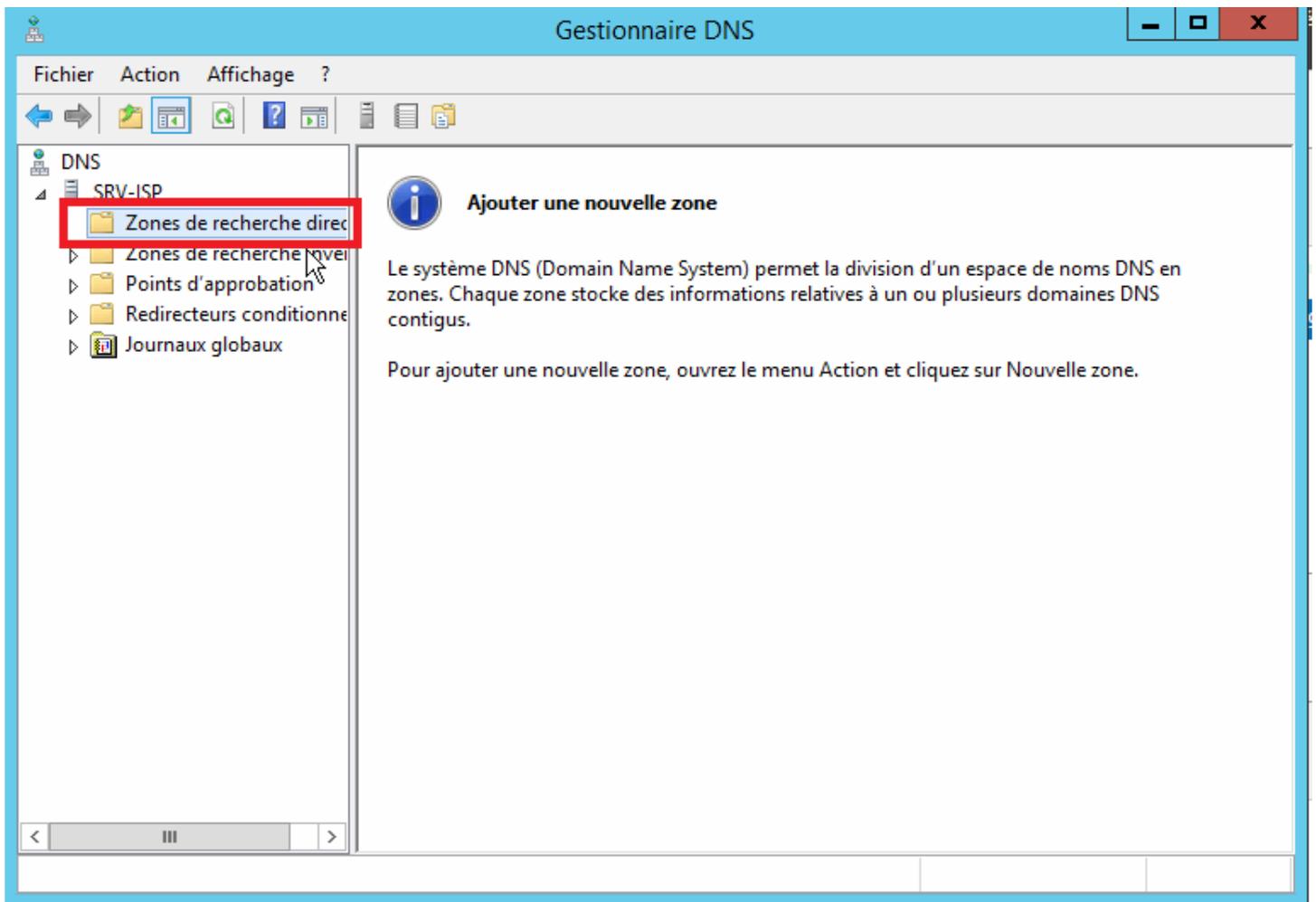
5 Connecter ce serveur aux services de cloud computing

Masquer

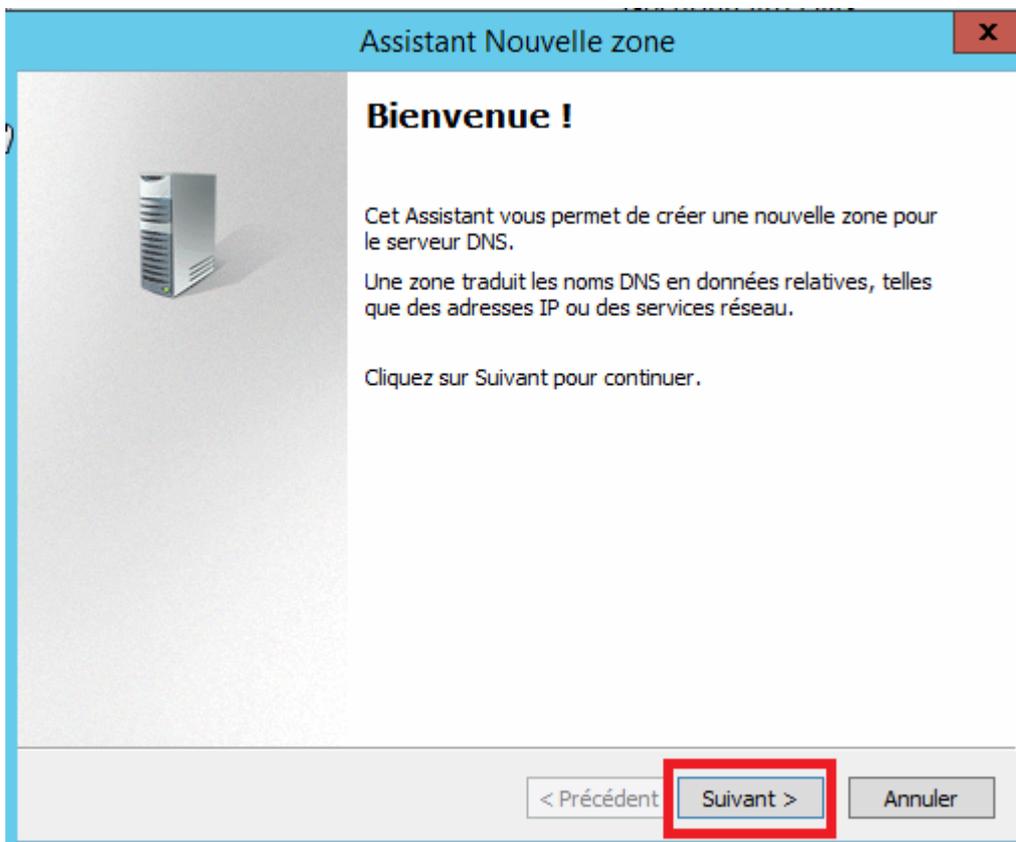
- Une fois le service DNS installé, allez dans la console de gestion. Dans le gestionnaire de serveur, cliquez sur "**Outils**", puis sur "**DNS**".



- Créez une nouvelle zone de recherche directe.



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



- Nous allons créer une zone principale.

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

- Nommez cette zone msftncsi.com.

Assistant Nouvelle zone

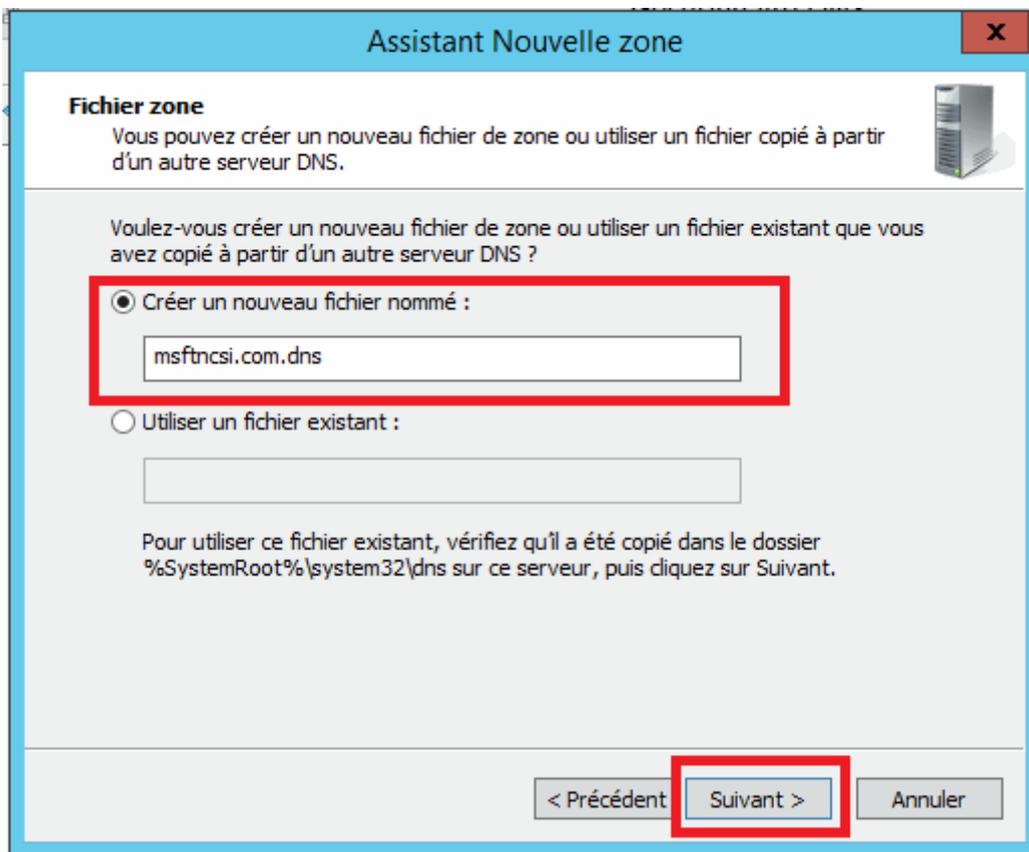
**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

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

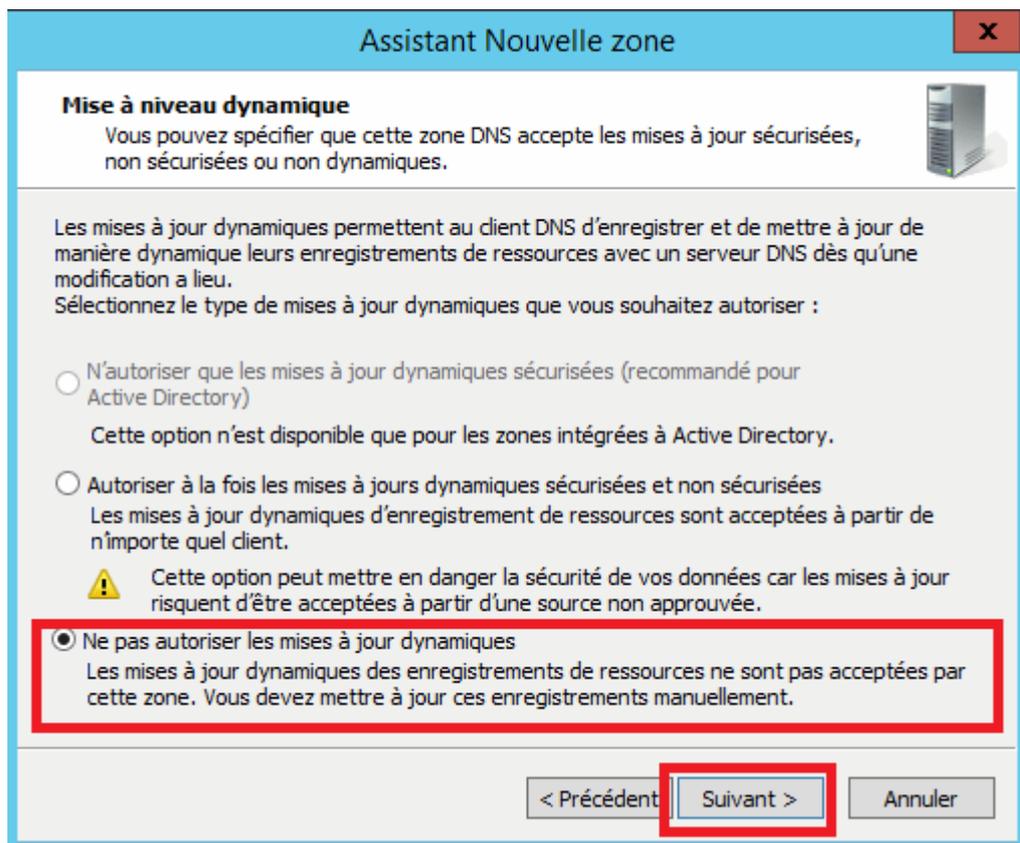
Nom de la zone :  
msftncsi.com

< Précédent   **Suivant >**   Annuler

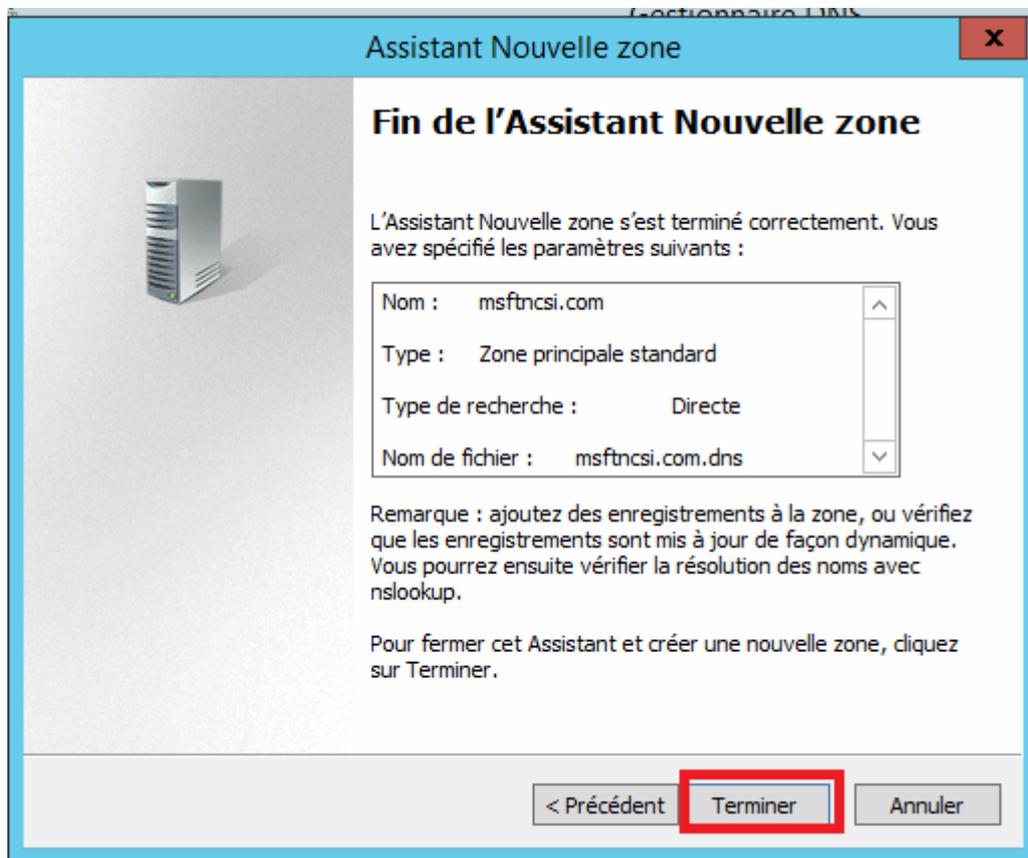
- Laissez tel quel le nom du fichier de zone.



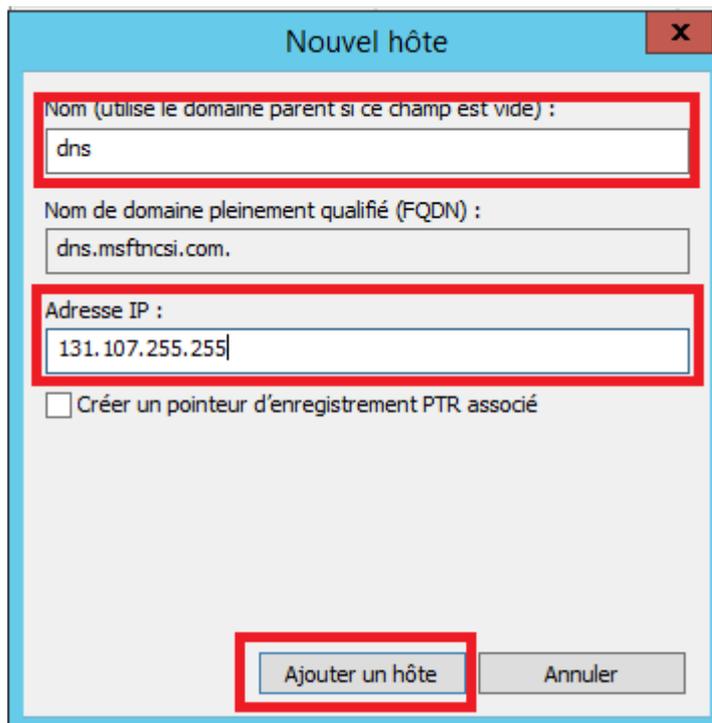
- Etant donné que le serveur n'est pas dans un domaine, nous n'allons pas autoriser les mises à jour dynamiques.



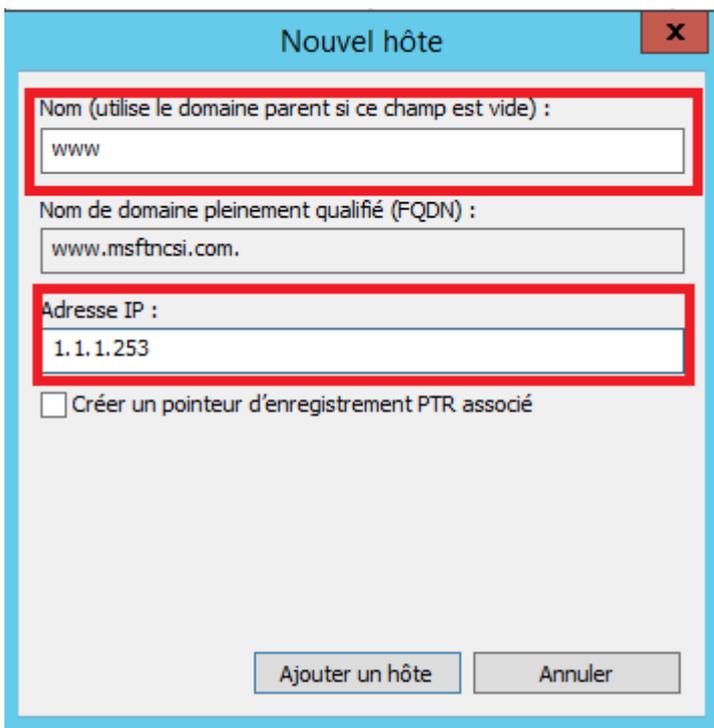
- Cliquez sur "Terminer". Et voilà, la zone msftncsi.com est maintenant active.



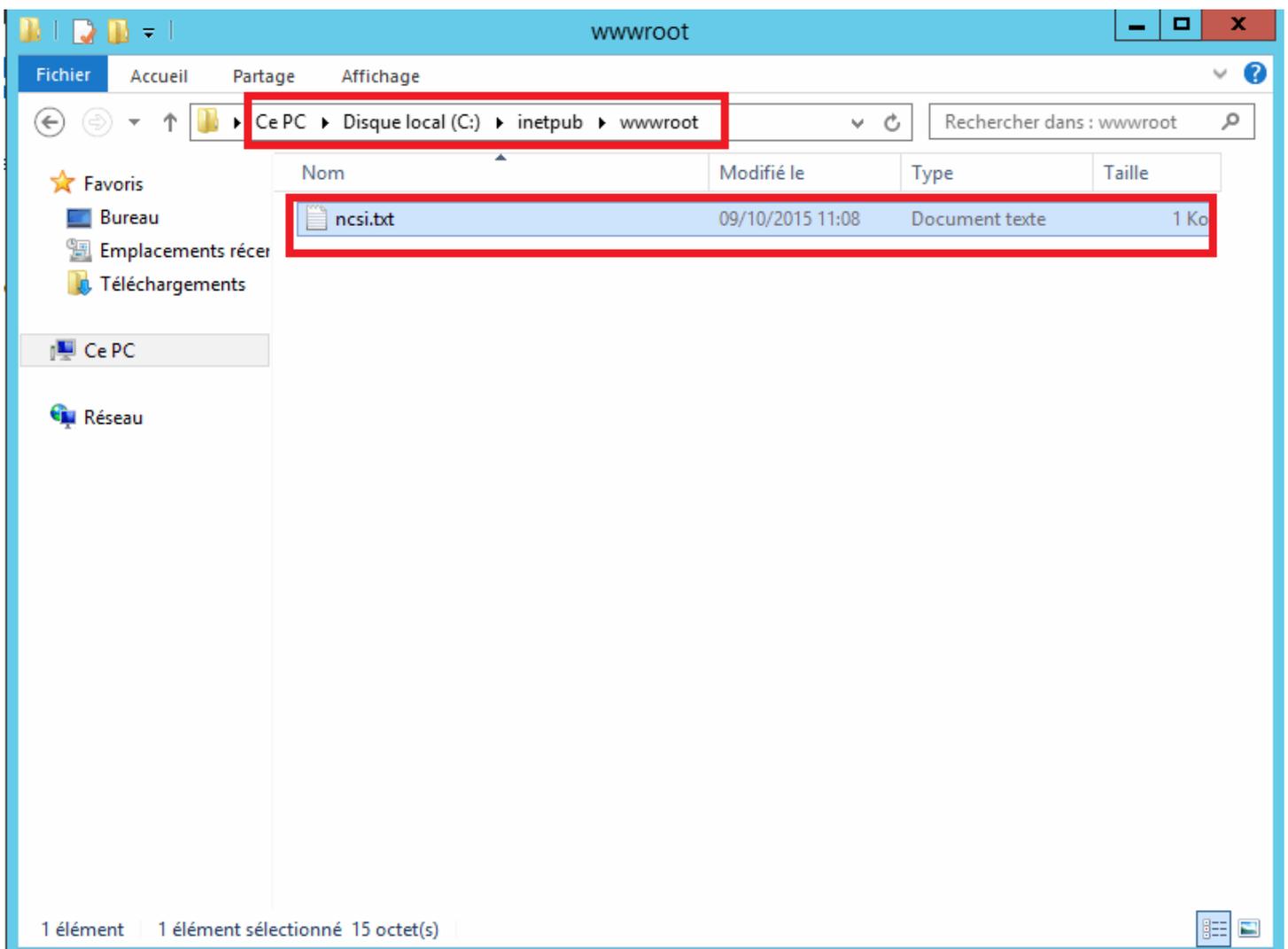
- Nous allons maintenant créer deux enregistrements DNS A. Le premier est l'enregistrement dns.msftncsi.com avec comme valeur "131.107.255.255".



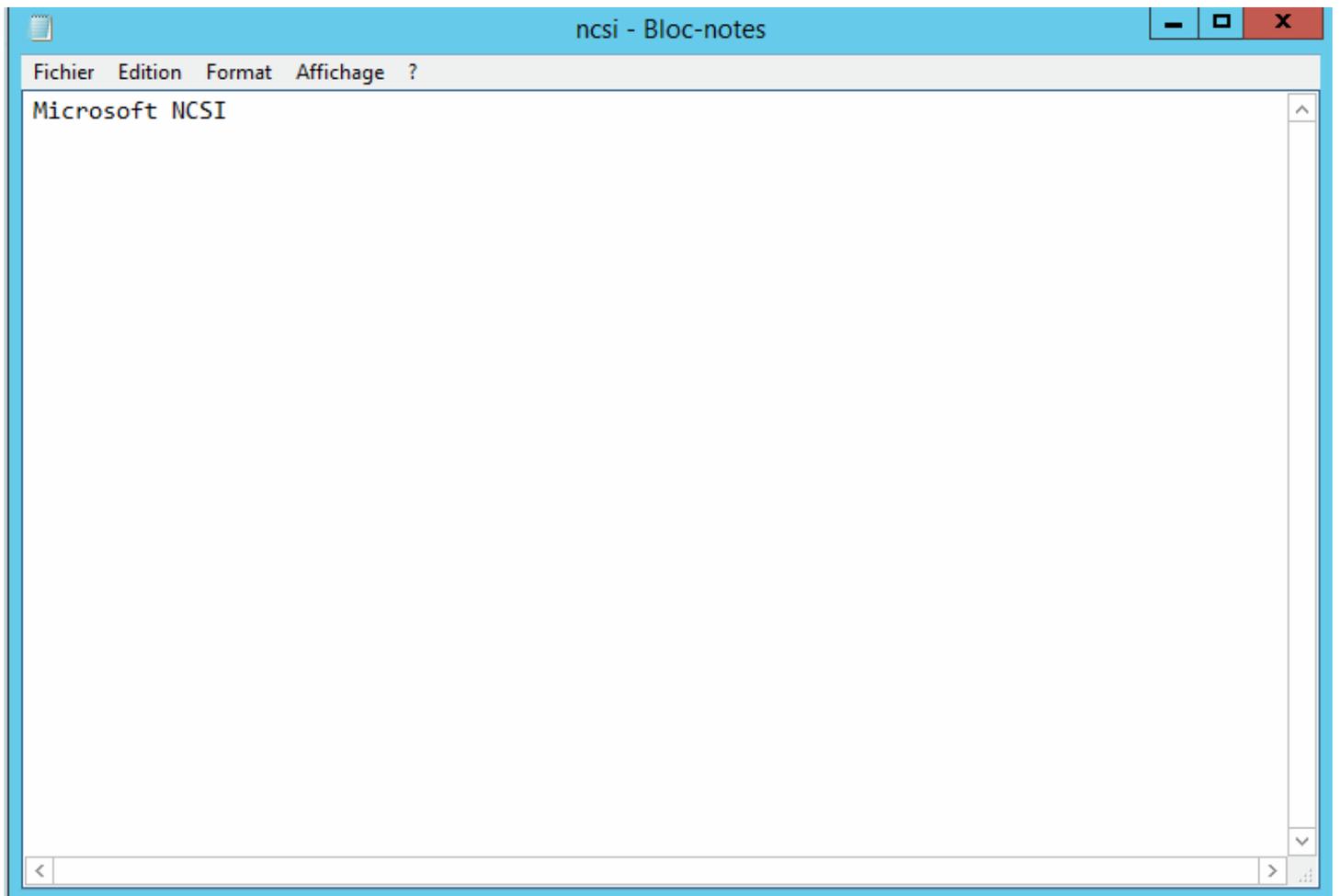
- Le second est www.msftncsi.com avec comme valeur l'adresse IP de votre serveur qui simule l'accès à Internet, ici "1.1.1.253".



- 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".



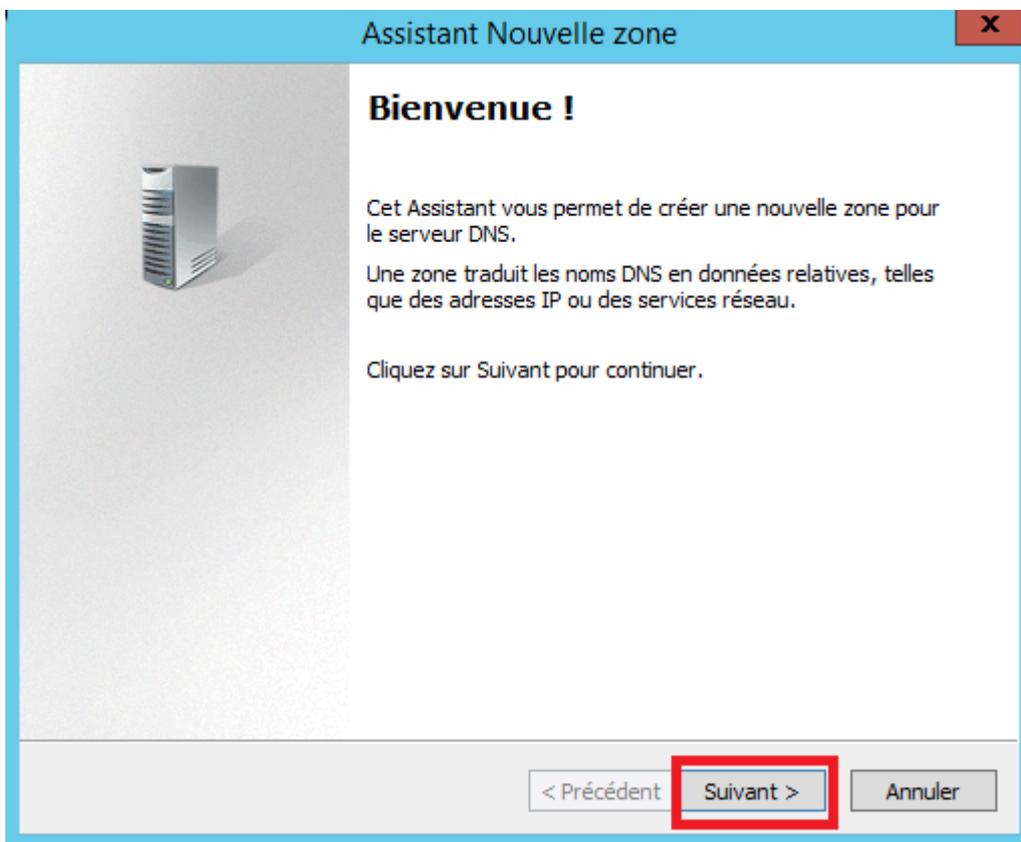
- A l'intérieur de ce fichier, entrer le texte "Microsoft NCSI" sans retour à la ligne.



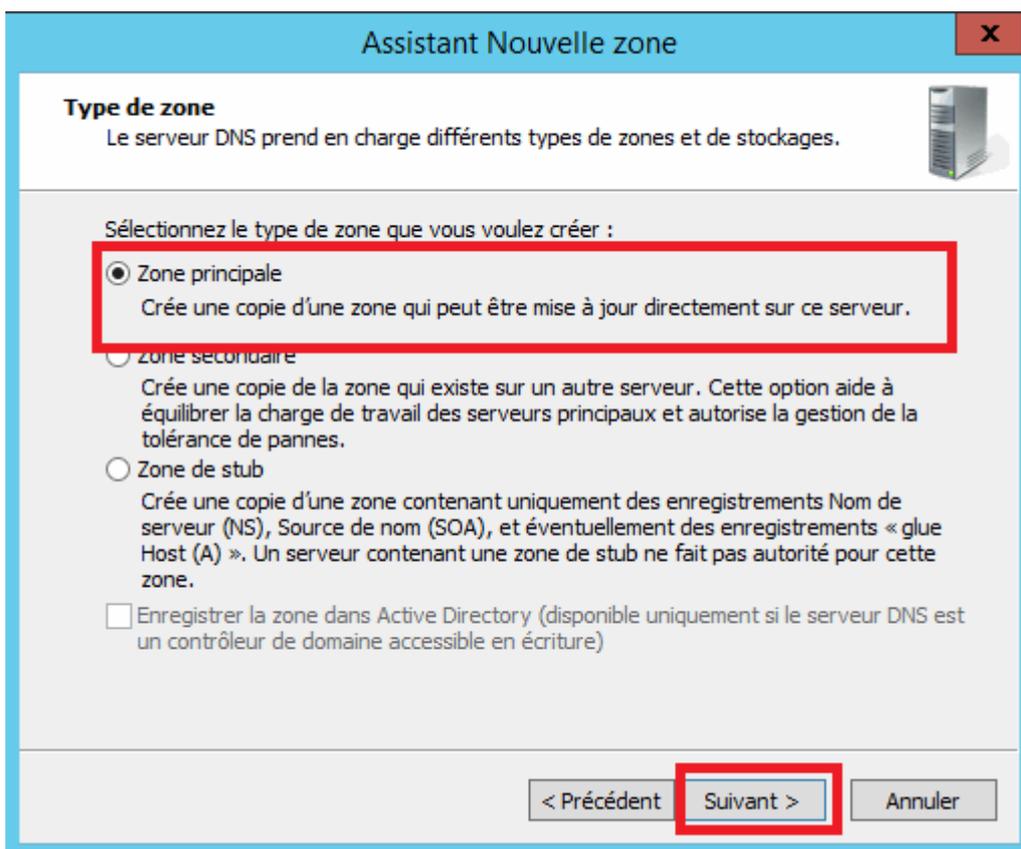
Maintenant que le serveur NCSI est prêt. Pour tester l'accès à Internet, le client va d'abord faire une requête DNS sur [dns.msftncsi.com](https://dns.msftncsi.com) et ensuite il va télécharger le contenu de la page à l'adresse [www.msftncsi.com](https://www.msftncsi.com). Toutes les réponses attendues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

Il nous reste à créer la zone [idum.com](https://idum.com) et créer l'enregistrement [da.idum.com](https://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.

**Assistant Nouvelle zone** X

---

**Nom de la zone**  
Quel est le nom de la nouvelle zone ? 

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

Nom de la zone :

- Laissez le nom de fichier de zone par défaut.

**Assistant Nouvelle zone** X

---

**Fichier zone**  
Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS. 

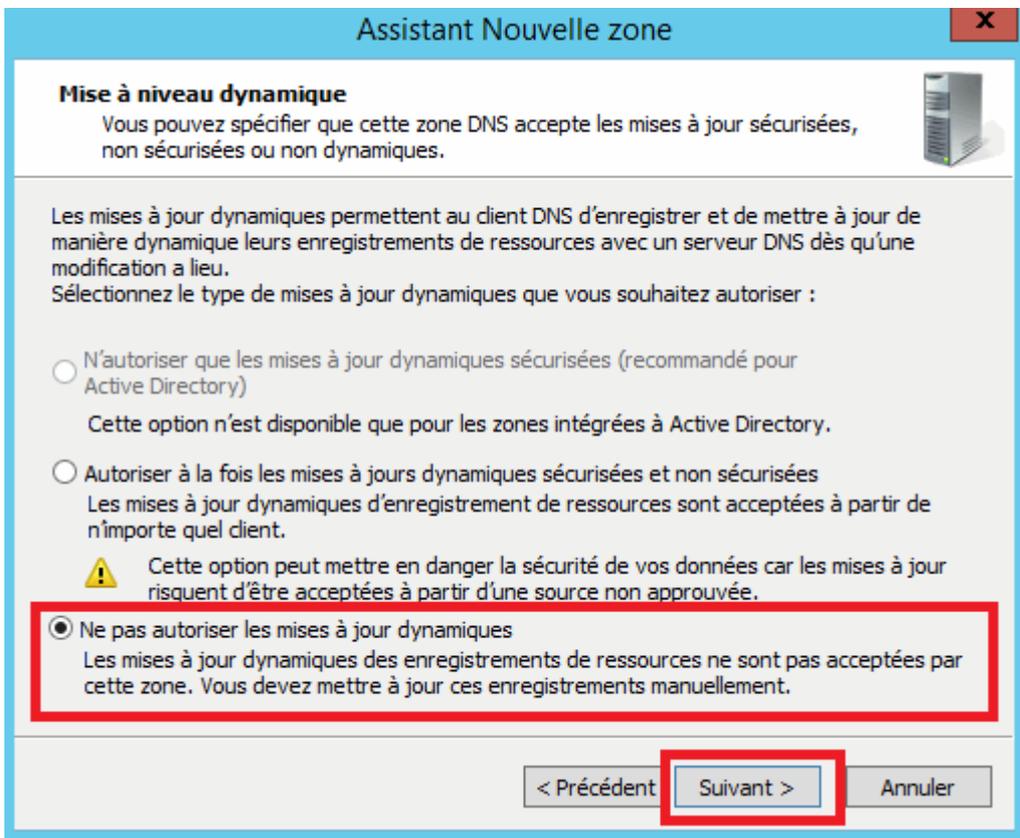
Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

Créer un nouveau fichier nommé :

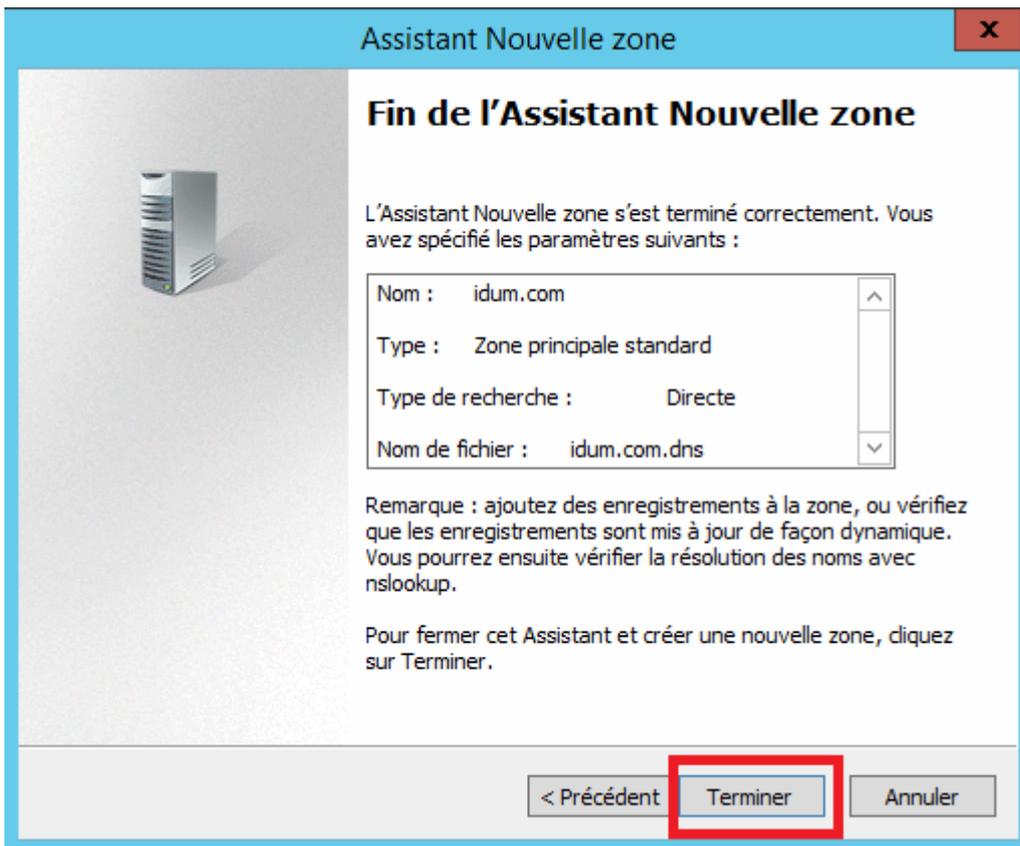
Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

- 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".

Nouvel hôte

Nom (utilisez le domaine parent si ce champ est vide) :  
da

Nom de domaine pleinement qualifié (FQDN) :  
da.idum.com.

Adresse IP :  
1.1.1.1

Créer un pointeur d'enregistrement PTR associé

Ajouter un hôte Annuler

## 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 :

Modification du nom ou du domaine de l'...

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :  
CLT1

Nom complet de l'ordinateur :  
CLT1

Autres...

Membre d'un

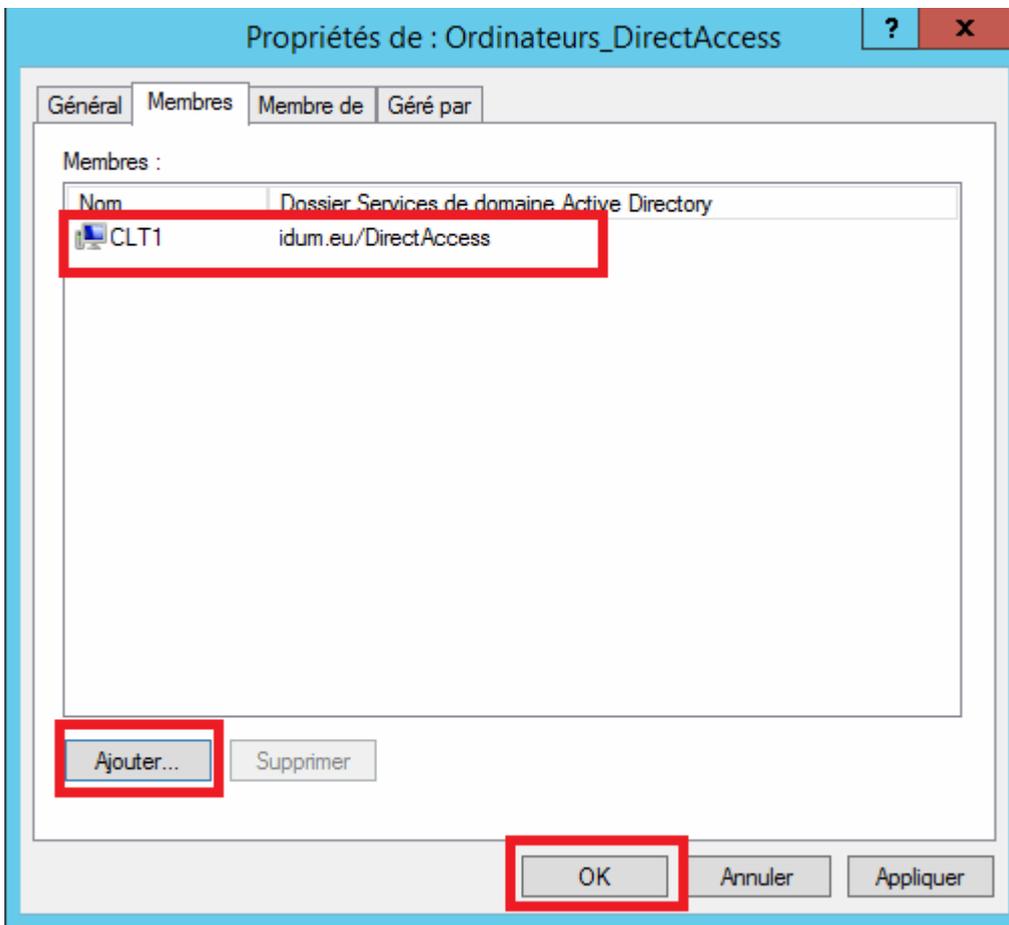
Domaine :  
idum.eu

Groupe de travail :  
WORKGROUP

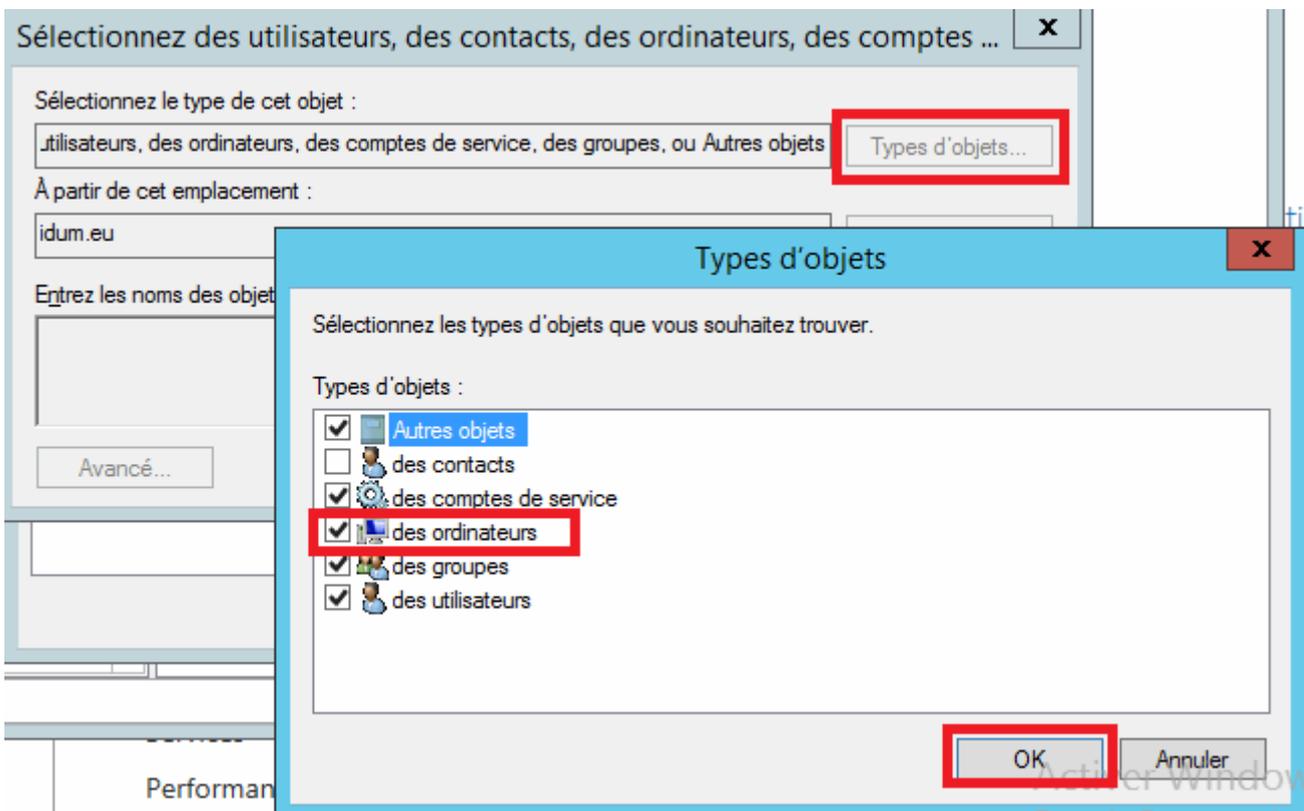
OK Annuler

- 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 sommes connectés au LAN donc DirectAccess est désactivé :

# Réseaux

Afficher les paramètres de connexion

## Connexions

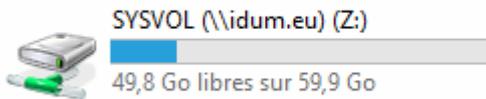
 Ethernet0  
Limité

 DirectAccess

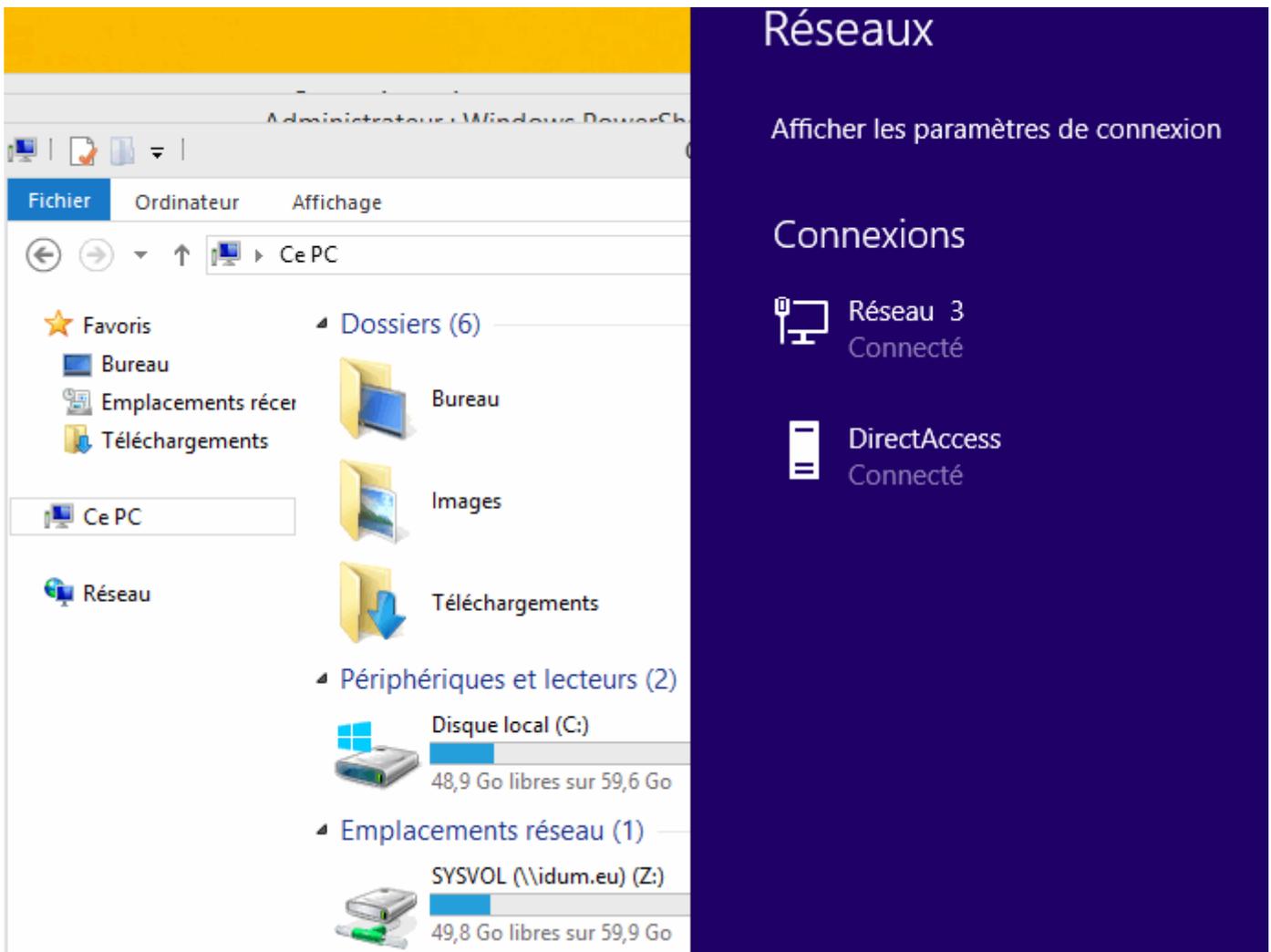
Connecté au réseau localement ou via un réseau VPN.

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

### ▲ Emplacements réseau (1)



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 sommes connectés en DirectAcces et que le lecteur réseau est accessible.



Quelques commandes pour le debugging Directaccess :

- Avec powershell :

```
Get-DAConnectionStatus
```

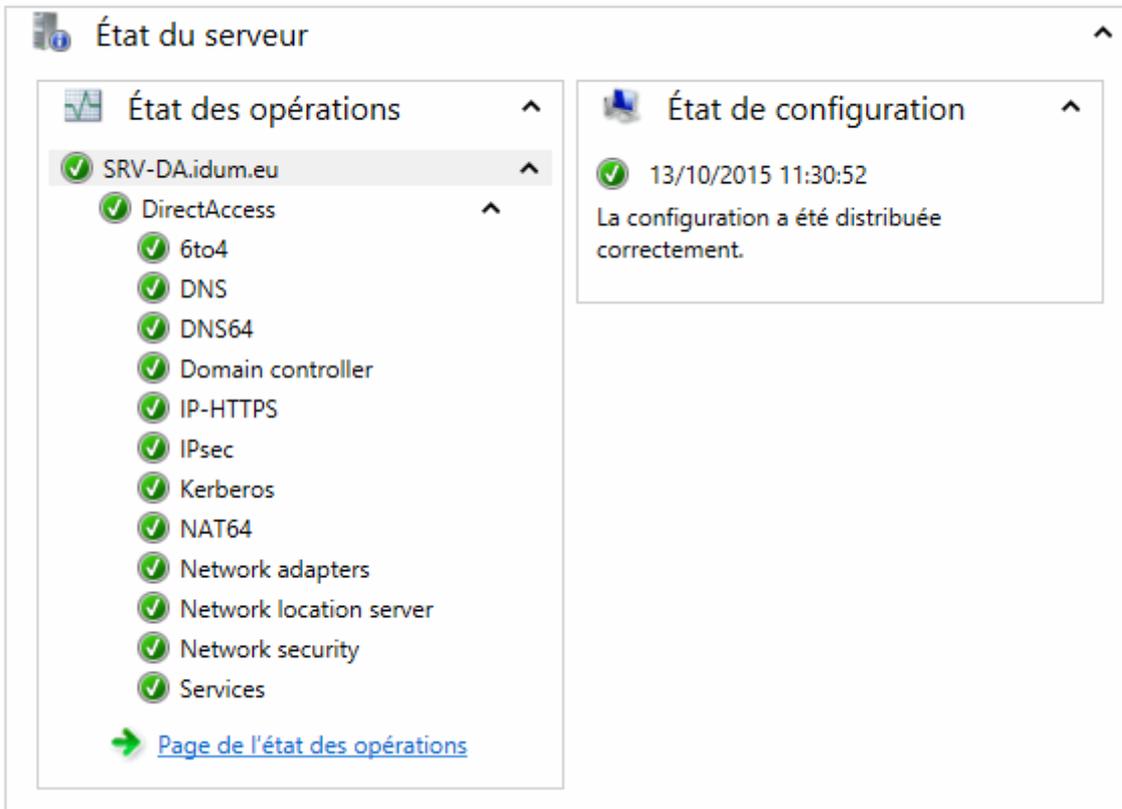
- Avec CMD :

Utilisez "**netsh**" pour gérer 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.

## Tableau de bord des accès distants



The screenshot displays a dashboard titled "État du serveur" (Server Status) with two main sections:

- État des opérations** (Operational Status): A list of services for server SRV-DA.idum.eu, all marked with green checkmarks:
  - DirectAccess
    - 6to4
    - DNS
    - DNS64
    - Domain controller
    - IP-HTTPS
    - IPsec
    - Kerberos
    - NAT64
    - Network adapters
    - Network location server
    - Network security
    - ServicesA link "Page de l'état des opérations" is provided at the bottom.
- État de configuration** (Configuration Status): Shows a timestamp "13/10/2015 11:30:52" and a message: "La configuration a été distribuée correctement." (Configuration has been distributed correctly).

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.

16 novembre 2015 -- N.SalmonA.Lebarbanchon -- article\_293.pdf



# Idum