

Installation du DNS Primaire

Procédure d'Implémentation de l'Infrastructure DNS Primaire et Secondaire

Objectif

L'objectif principal de cette procédure est de guider la mise en œuvre d'une architecture de résolution de noms de domaine (DNS) robuste et hautement disponible, en déployant un serveur **DNS Primaire** et un serveur **DNS Secondaire**. Cette redondance est essentielle pour garantir la continuité des services et la fiabilité de la résolution de noms pour le domaine d'entreprise.

La procédure vise spécifiquement à :

- Installer le rôle de service **DNS** sur deux serveurs distincts : le serveur **Primaire (Maître)** nommé ARES et le serveur **Secondaire (Esclave)** nommé APHRODITE.
- Configurer la **Zone Primaire** (bts.local) sur le serveur ARES, incluant les zones de recherche directe et inversée.
- Mettre en place la **Zone Secondaire** sur le serveur APHRODITE et établir le mécanisme de **transfert de zone** (zone transfer) depuis ARES.
- Assurer la bonne synchronisation des enregistrements DNS (SOA, NS, A) entre le serveur Primaire et le serveur Secondaire.
- Configurer les paramètres réseau (adresses IP statiques, masques, passerelles, serveurs DNS préférés) sur chaque serveur conformément au plan d'adressage établi pour l'infrastructure.

Contexte de la Réalisation

Rôle du DNS dans l'Infrastructure

Le **DNS (Domain Name System)** est un service fondamental de l'infrastructure informatique, responsable de la traduction des noms de domaine (ex: serveur.bts.local) en adresses IP (172.20.0.x) et inversement. La disponibilité et la performance du DNS sont critiques pour l'authentification des utilisateurs, le bon fonctionnement des applications et la connectivité réseau.

Architecture Redondante

Cette réalisation s'inscrit dans un projet visant à éliminer tout point de défaillance unique (Single Point of Failure). L'architecture est donc construite autour de deux serveurs Windows Server dédiés :

- **DNS Primaire (Maître) :**
 - Nom : ARES
 - Adresse IP : 172.20.0.10
 - Rôle : Détient la copie principale et modifiable de la zone de domaine (bts.local).
- **DNS Secondaire (Esclave) :**
 - Nom : APHRODITE
 - Adresse IP : 172.20.0.14
 - Rôle : Détient une copie en lecture seule de la zone, qu'il maintient à jour via des requêtes de transfert de zone régulières auprès du serveur Primaire.

Le déploiement de cette structure garantit qu'en cas de panne ou de maintenance du serveur primaire (ARES), le serveur secondaire (APHRODITE) puisse continuer à répondre aux requêtes de résolution de noms des clients, assurant ainsi la **continuité des opérations**.

Nom Machine : ARES

Rôles : DNS

Adresse IP : 172.20.0.10

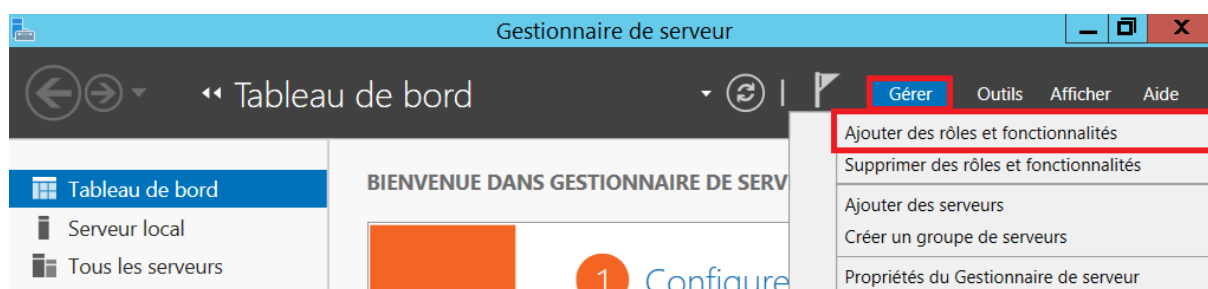
Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 172.20.0.1

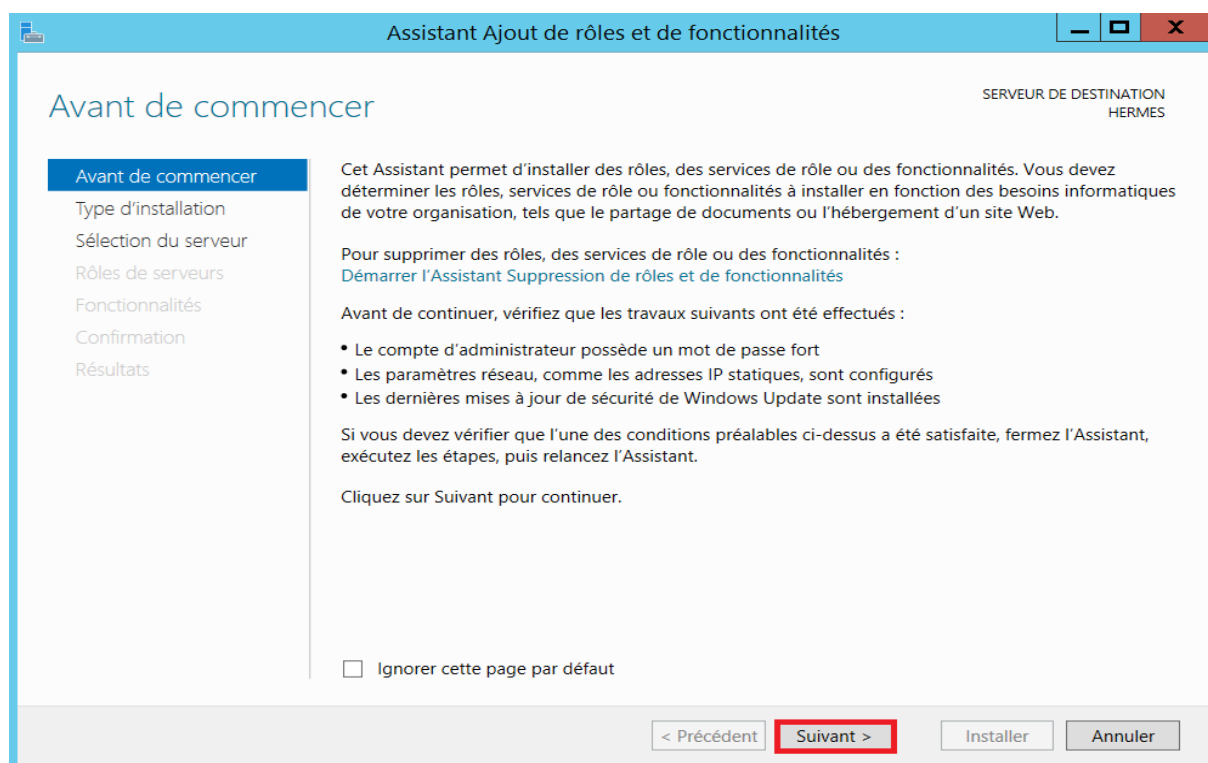
Serveur DNS préféré : 172.20.0.13

Installation du rôle DNS

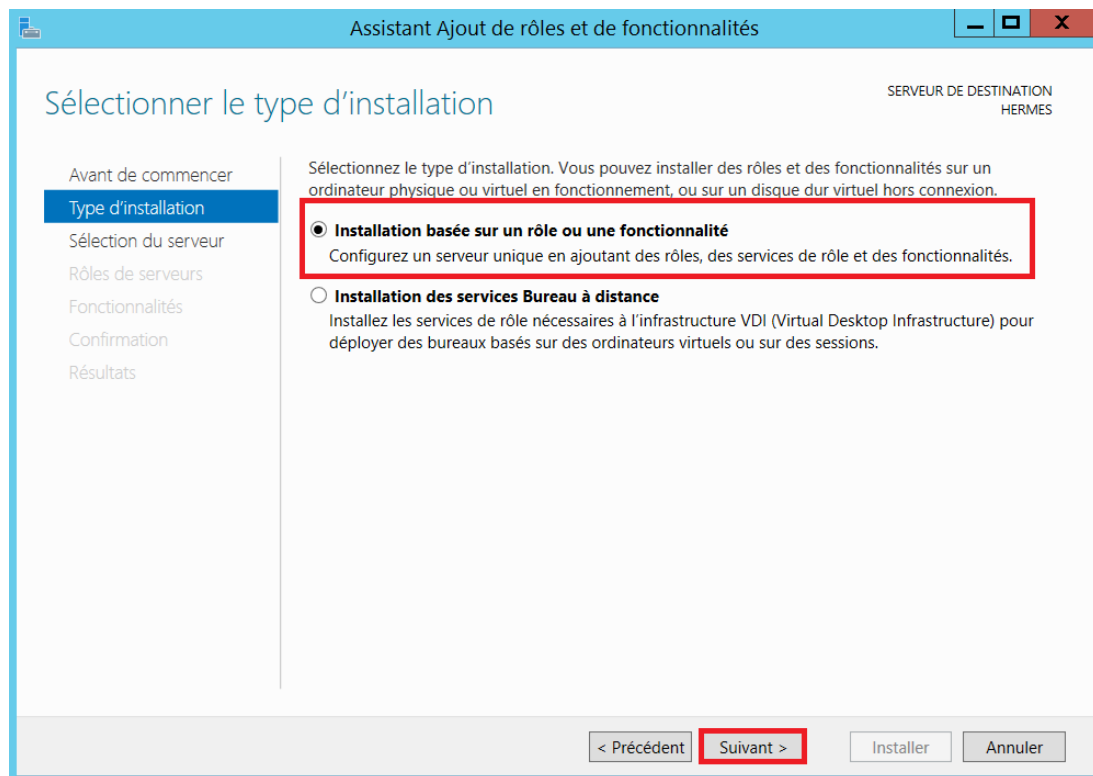
- Depuis le Gestionnaire de serveur, cliquer sur **gérer** puis «**Ajouter des rôles et des fonctionnalités**»



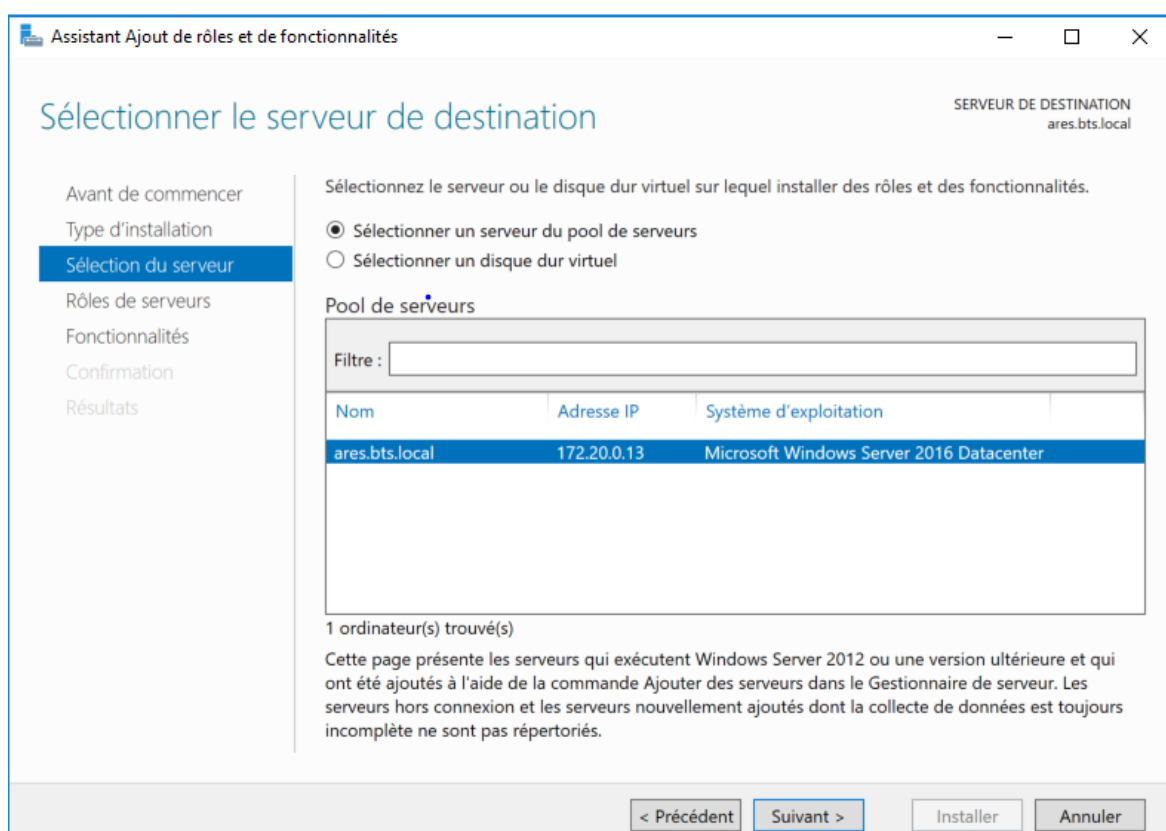
- Sur l'Assistant Ajout de rôles et de fonctionnalités, passer l'introduction avec **suivant**.



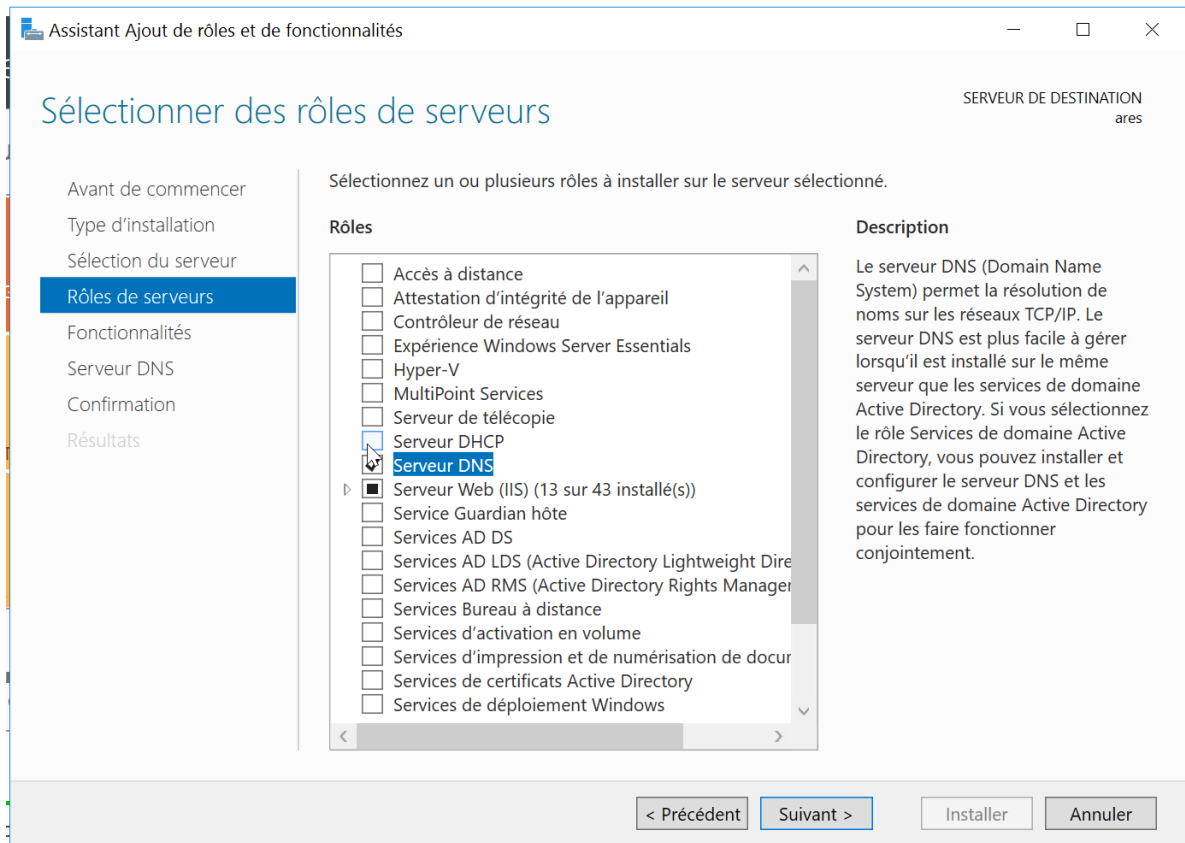
- Sélectionné le type **d'installation basée sur un rôle ou une fonctionnalité**.



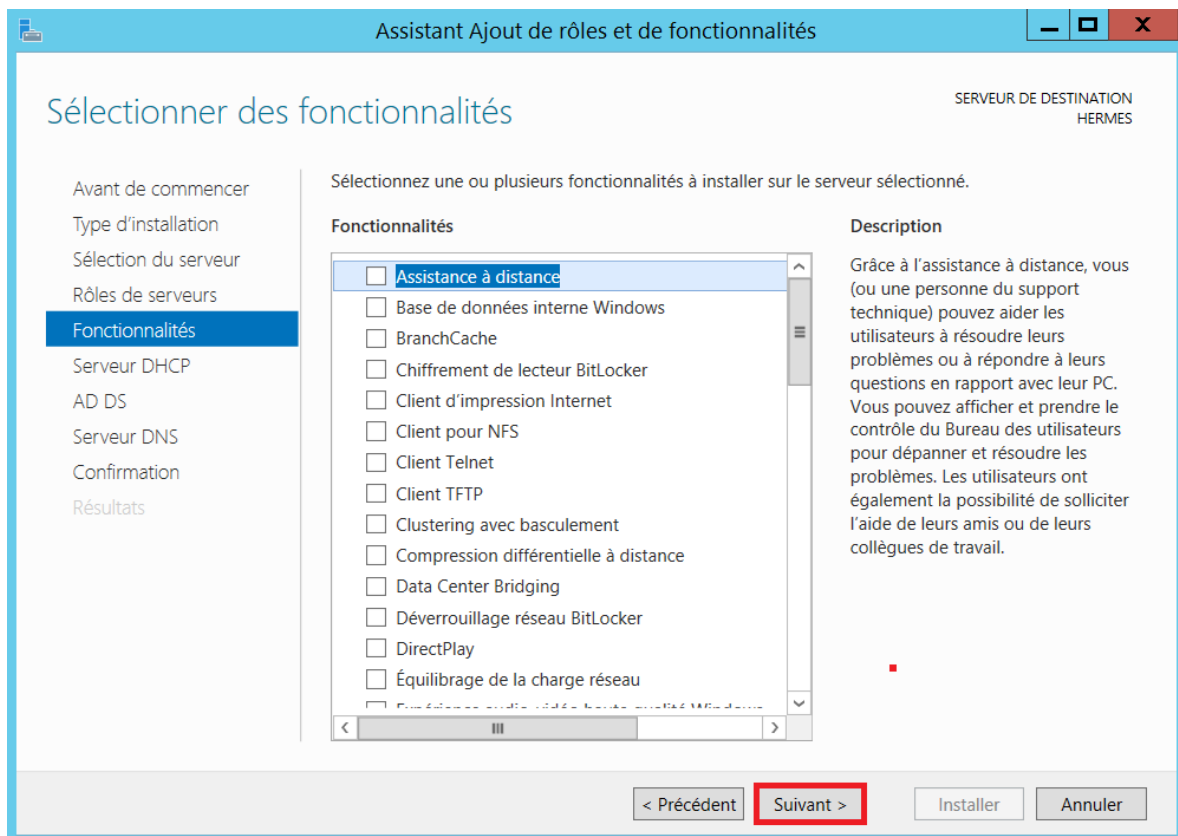
- Sélectionner son serveur pool pour installer les rôles et suivant.



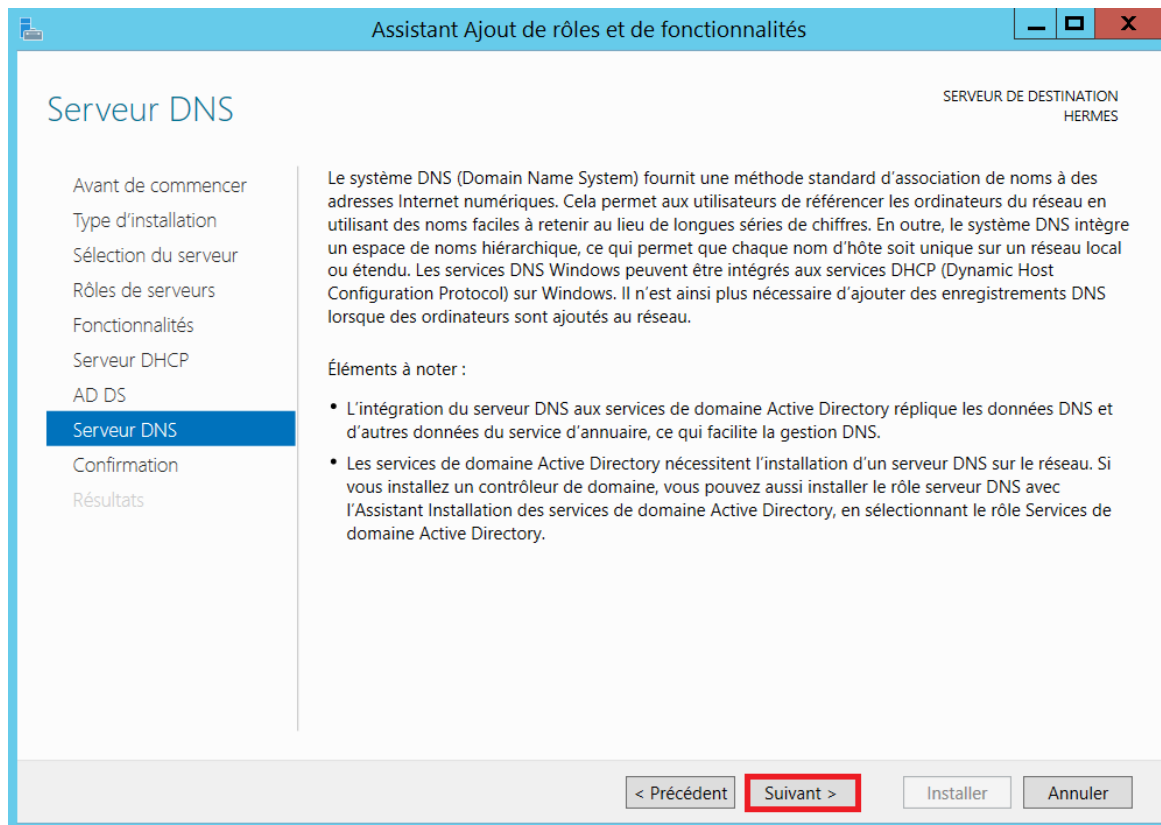
- Sélectionner les rôles **DNS** puis suivant.



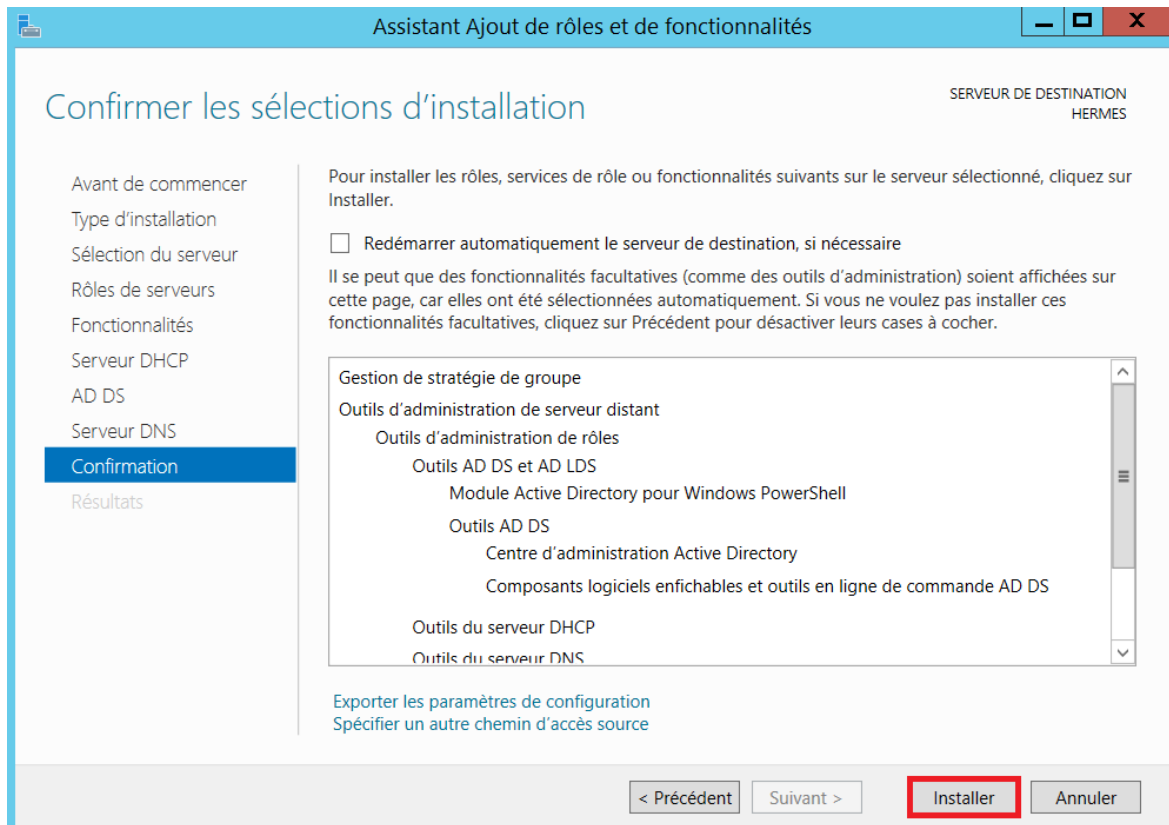
- Ne pas sélectionner de fonctionnalités et suivant.



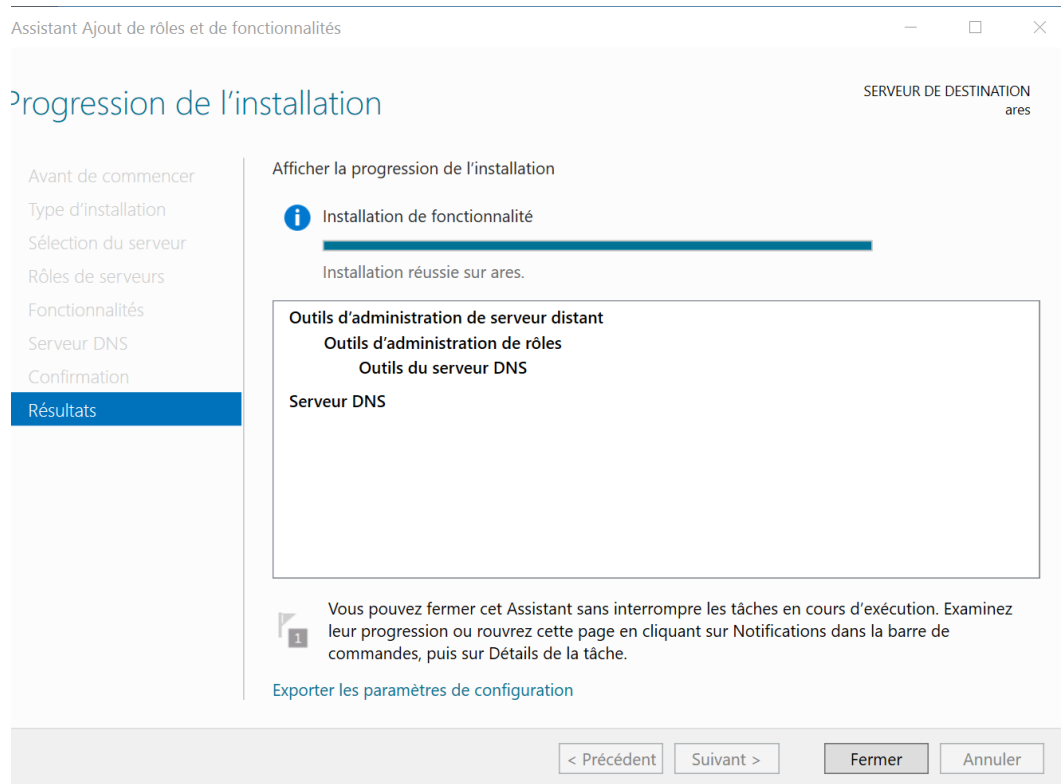
- Passer les explications du DNS et **suivant**.



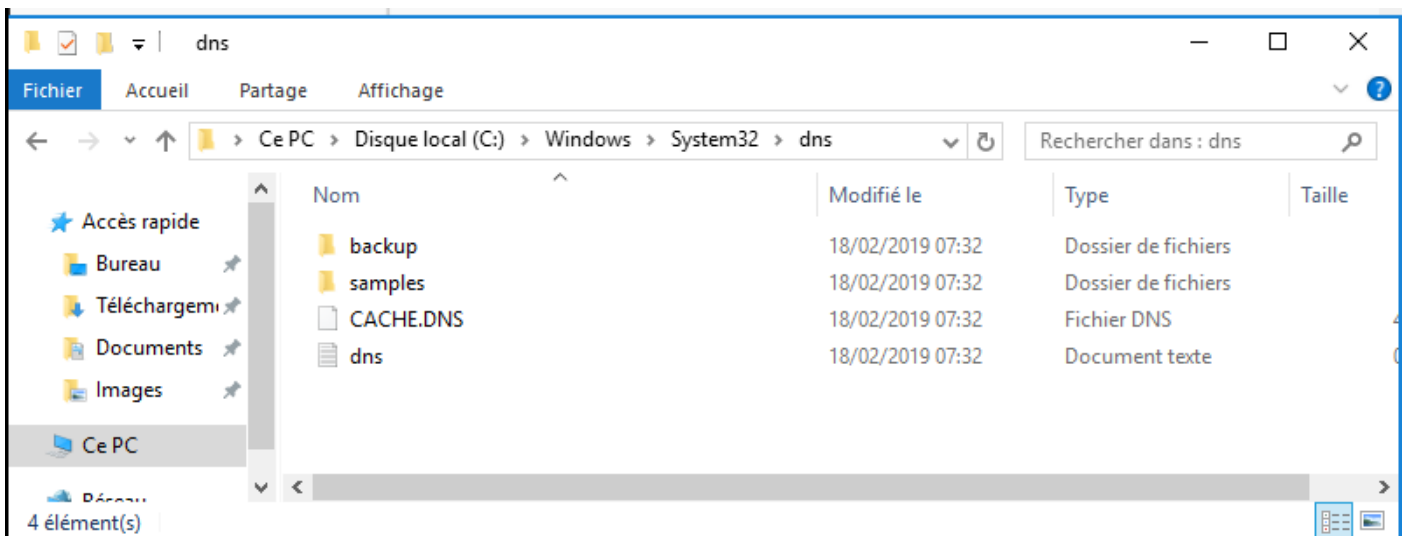
- Confirmer l'installation en cliquant sur **installer**.



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



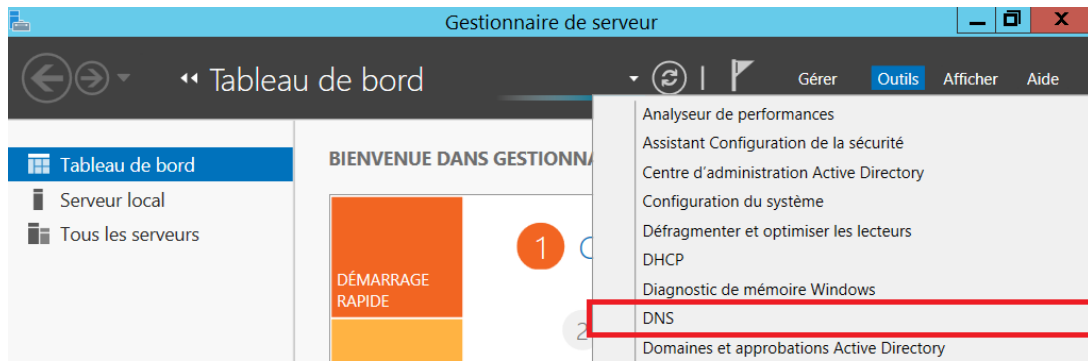
Après l'installation du service DNS, un répertoire **Dns** va être créé dans **c:\windows\system32** ce répertoire va stocker les bases DNS ainsi que le fichier cache qui répertorie les 13 serveurs root



Configuration DNS

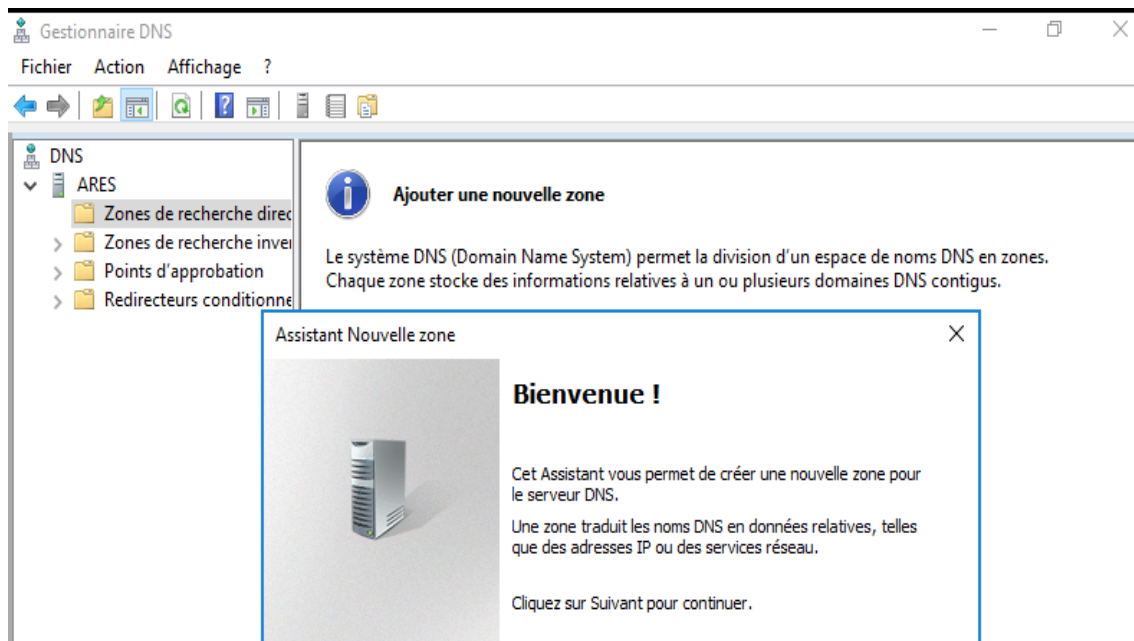
Création de la zone de recherche directe :

- Gestionnaire de serveur → Outils → DNS.

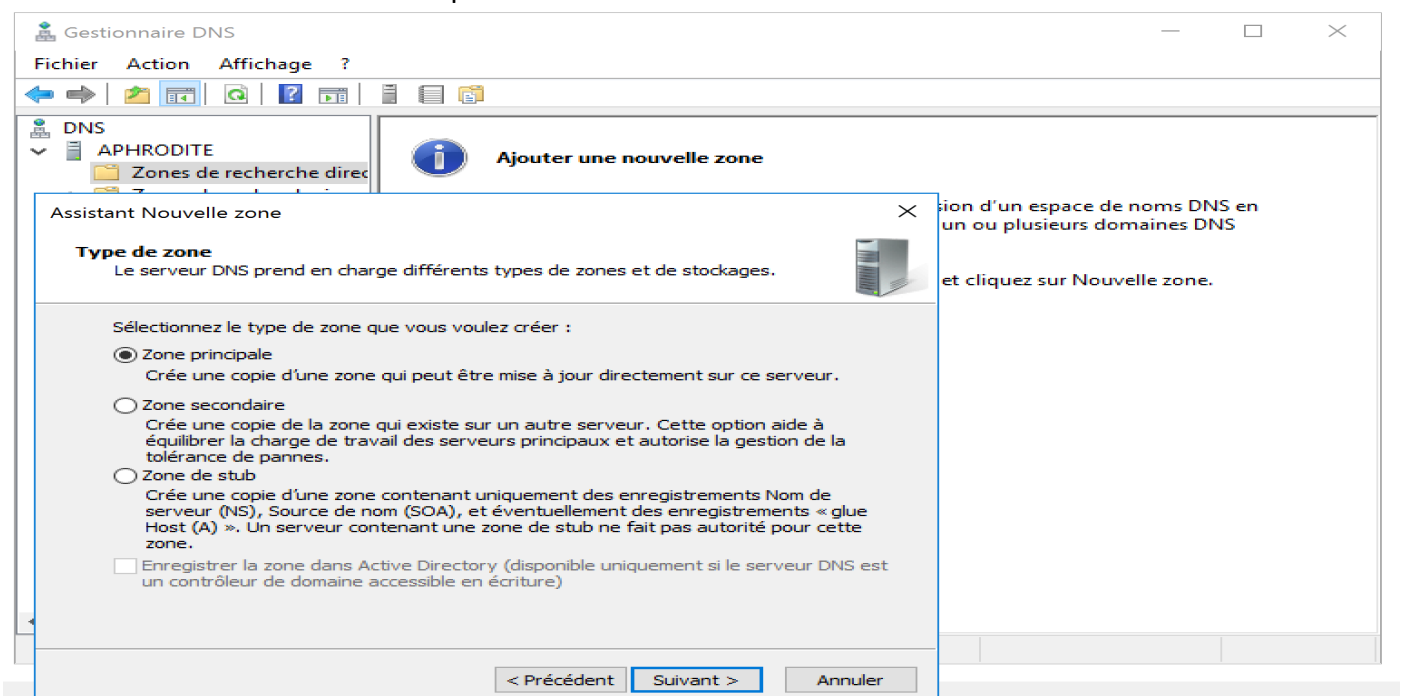


Nouvelle Zone Directe :

- Clic droit sur Zones de recherche directe → Nouvelle zones...



Faites le choix en cochant la zone primaire



Indiquez bts.local comme nom de la zone dns

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 :

< Précédent Suivant > Annuler

Assistant Nouvelle zone

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.

< Précédent Suivant > Annuler

Autorisez les mise à jour dynamiques

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

Cliquez sur terminer pour finir la configuration

Assistant Nouvelle zone

Fin de l'Assistant Nouvelle zone

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

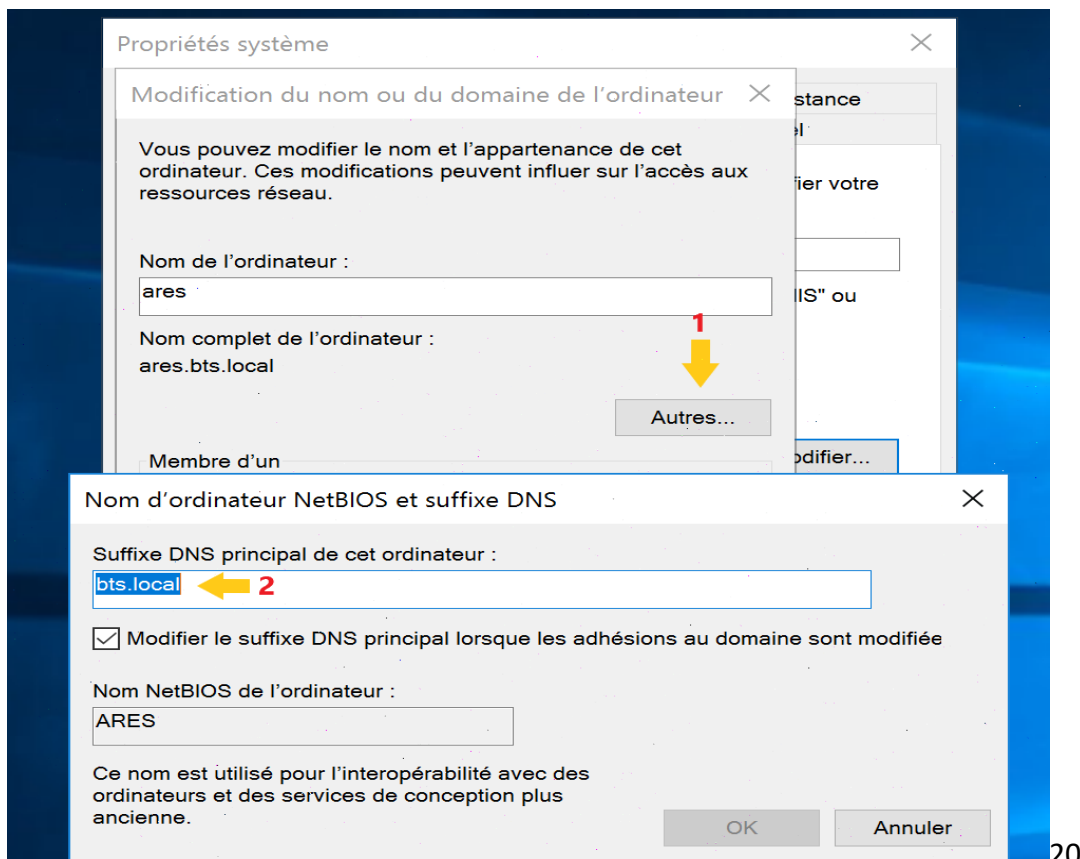
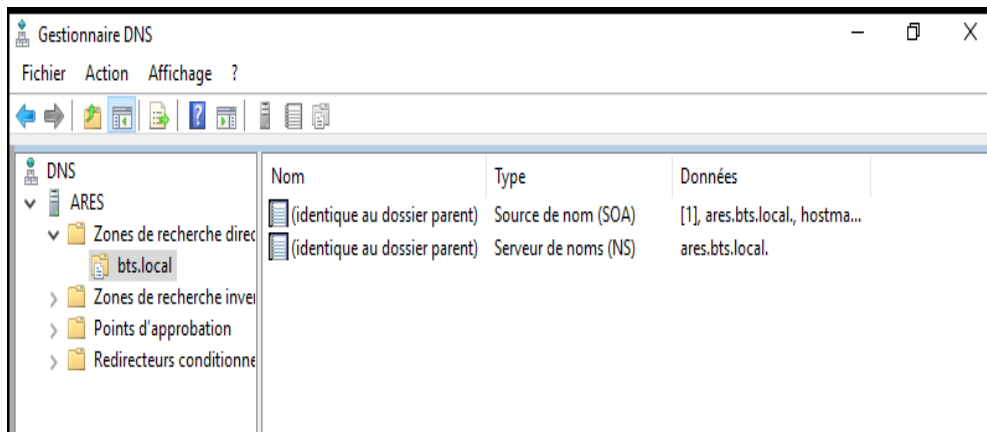
Nom : bts.local
 Type : Zone principale standard
 Type de recherche : Directe
 Nom de fichier : bts.local.dns

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

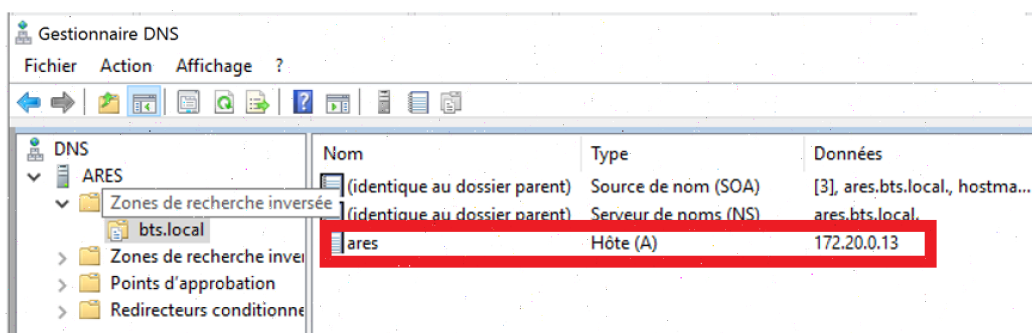
< Précédent **Terminer** Annuler

En développant la zone directe bts.local on remarque qu'il existe 2 types d'enregistrement SOA et NS mais il manque un enregistrement de type A qui correspond au server Ares. Pour faire apparaître cet enregistrement il faut renseigner le suffixe dns en mettant le nom de cette zone (bts.local)



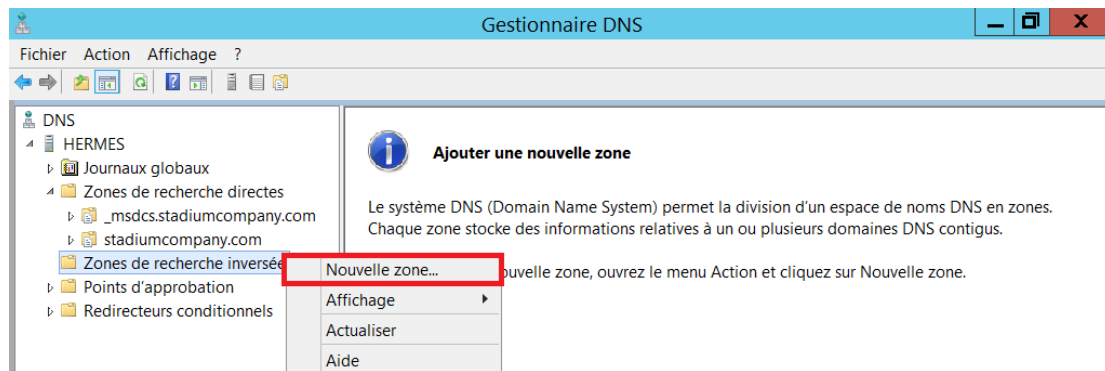
20

Une fois le suffixe dns renseigné redémarrer la machine, vous vérifiez l'existence de l'enregistrement de type A

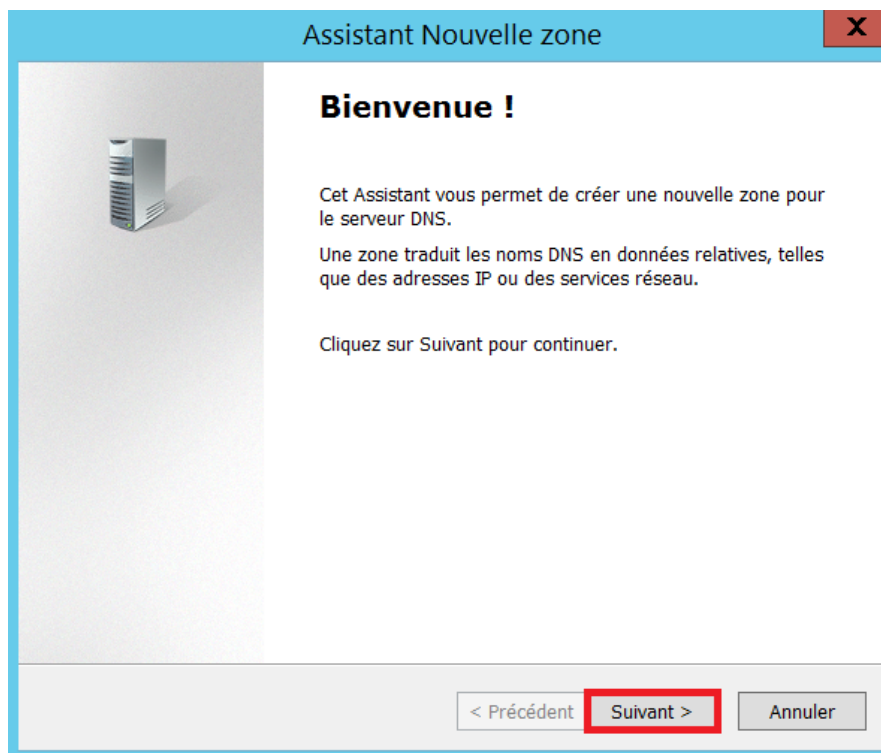


Nouvelle Zone inversé :

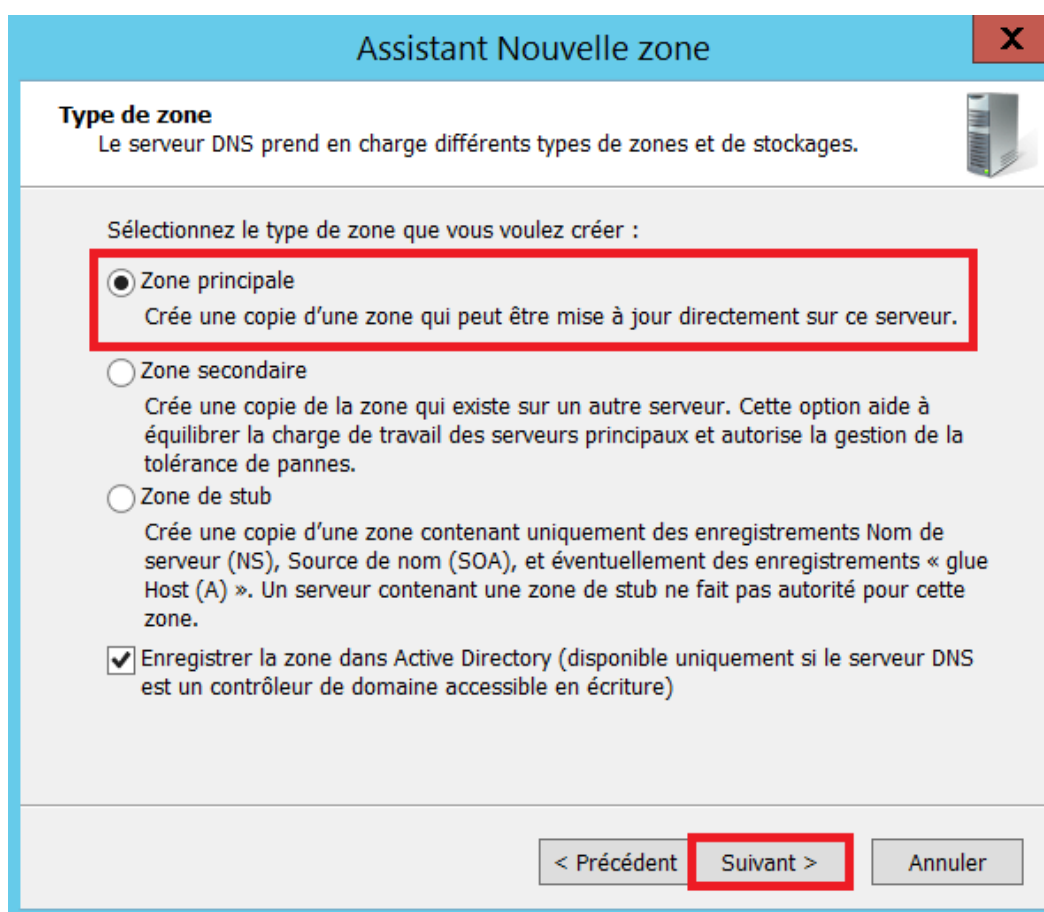
- Clic droit sur Zones de recherche inversée → Nouvelle zones...



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



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



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

Assistant Nouvelle zone

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

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

☒ Zone de recherche inversée IPv4

☐ Zone de recherche inversée IPv6

< Précédent Suivant > Annuler

Sélectionné « **L'ID réseau 172.20.0.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 « **autoriser que les mises à jour dynamiques sécurisées et no securisées** », faire **suivant**.

Assistant Nouvelle zone

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

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

☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

☒ **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées**
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

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

< Précédent **Suivant >** Annuler

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

Assistant Nouvelle zone

Fin de l'Assistant Nouvelle zone

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

Nom :	0.20.172.in-addr.arpa
Type :	Serveur principal intégré à Active Directory
Type de recherche :	Inversée

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent **Terminer** Annuler

Maintenant on va vérifier que les bases de données DNS sont créés dans **c:\windows\system32**

Disque local (C:) > Windows > System32 > dns

Nom	Modifié le	Type	Taille
backup	18/02/2019 07:32	Dossier de fichiers	
samples	18/02/2019 07:32	Dossier de fichiers	
0.20.172.in-addr.arpa.dns	18/02/2019 10:27	Fichier DNS	1 Ko
bts.local.dns	18/02/2019 10:25	Fichier DNS	1 Ko
CACHE.DNS	18/02/2019 07:32	Fichier DNS	4 Ko
dns	18/02/2019 07:32	Document texte	0 Ko
TrustAnchors.dns	18/02/2019 07:43	Fichier DNS	1 Ko

Installation du DNS Secondaire

Nom Machine : Aphrodite

Rôles : DNS

Adresse IP : 172.20.0.14

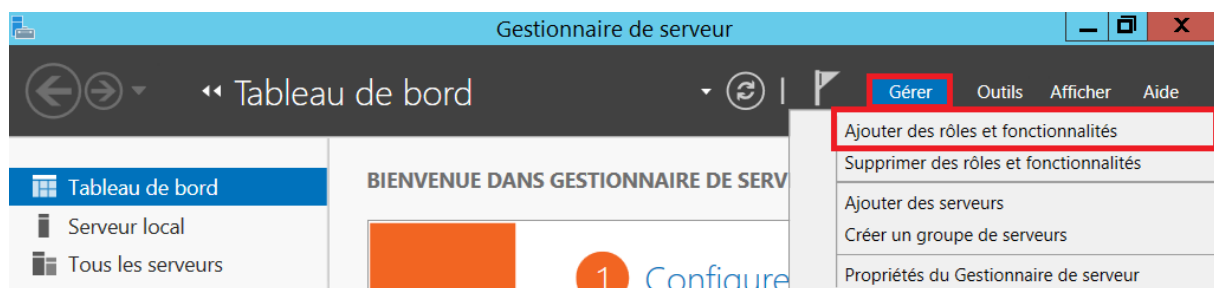
Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 172.20.0.14

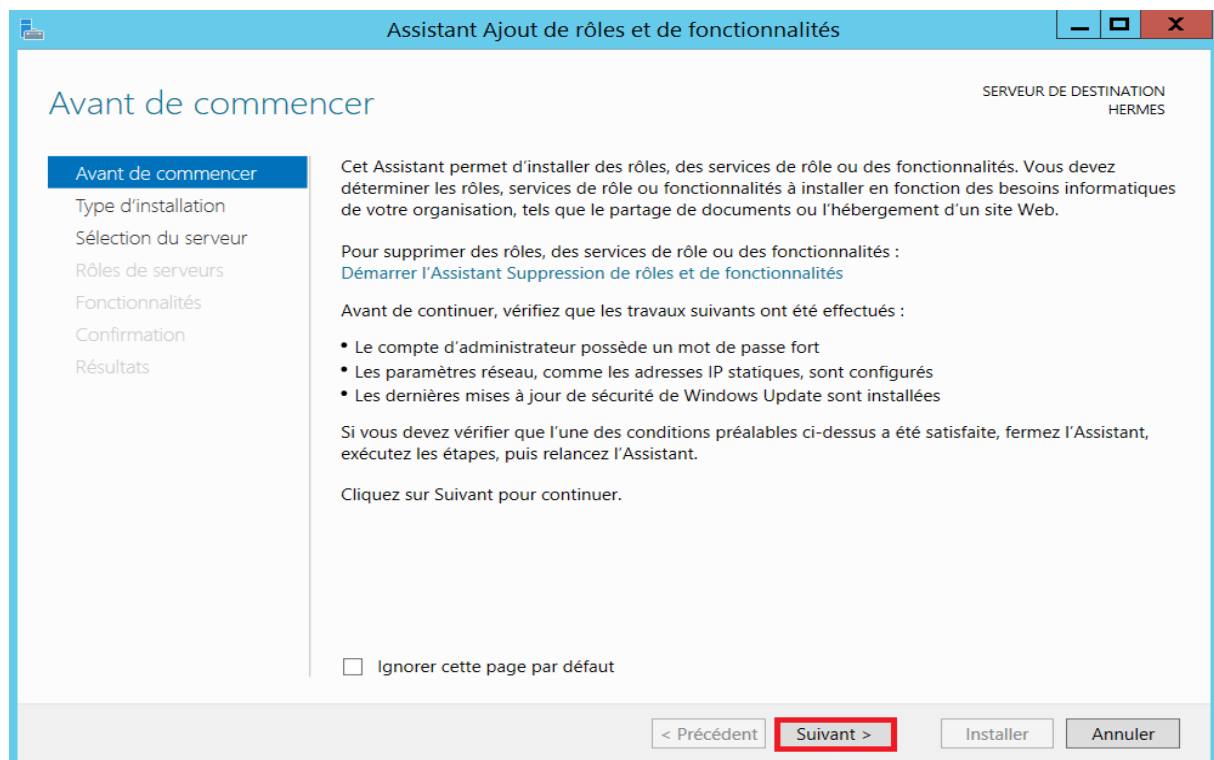
Serveur DNS préféré : 172.20.0.13

Installation du rôle DNS

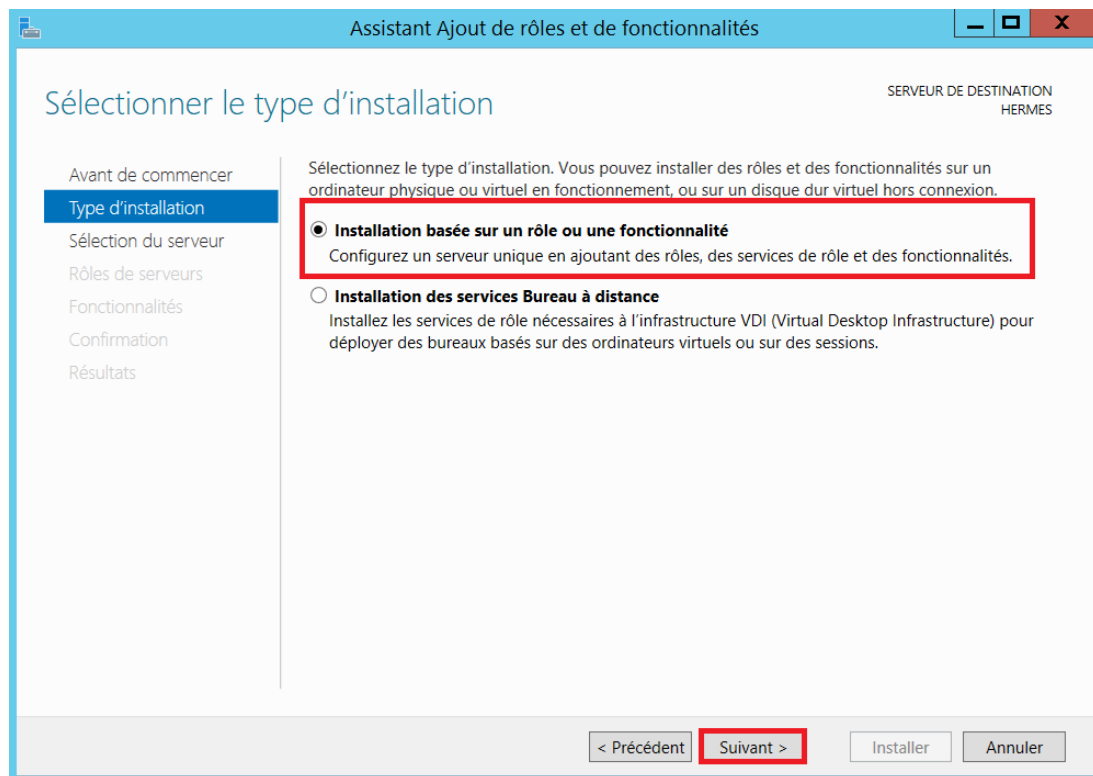
- Depuis le Gestionnaire de serveur, cliquer sur **gérer** puis «**Ajouter des rôles et des fonctionnalités**»



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

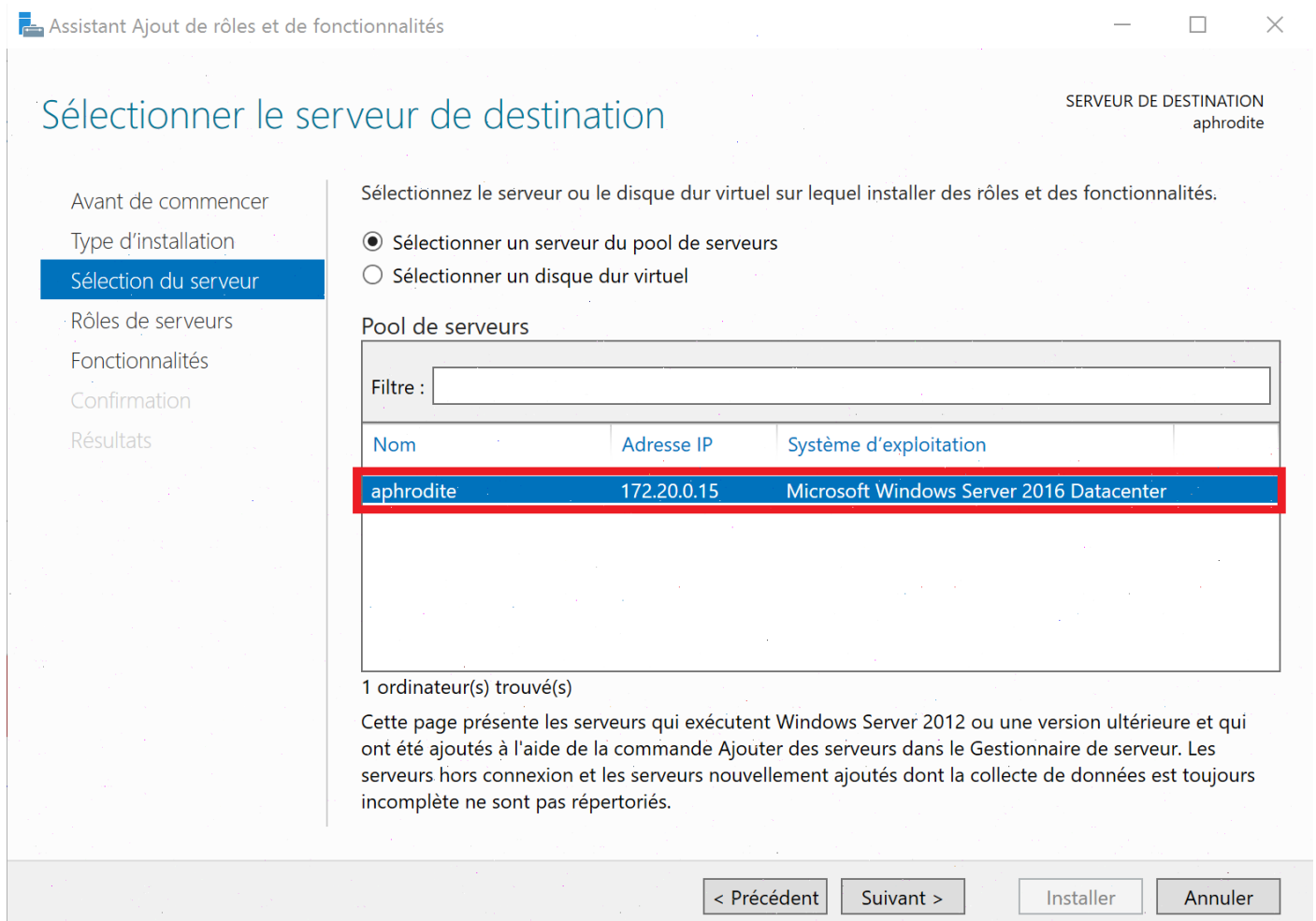


- Sélectionné le type d'installation basée sur un rôle ou une fonctionnalité.

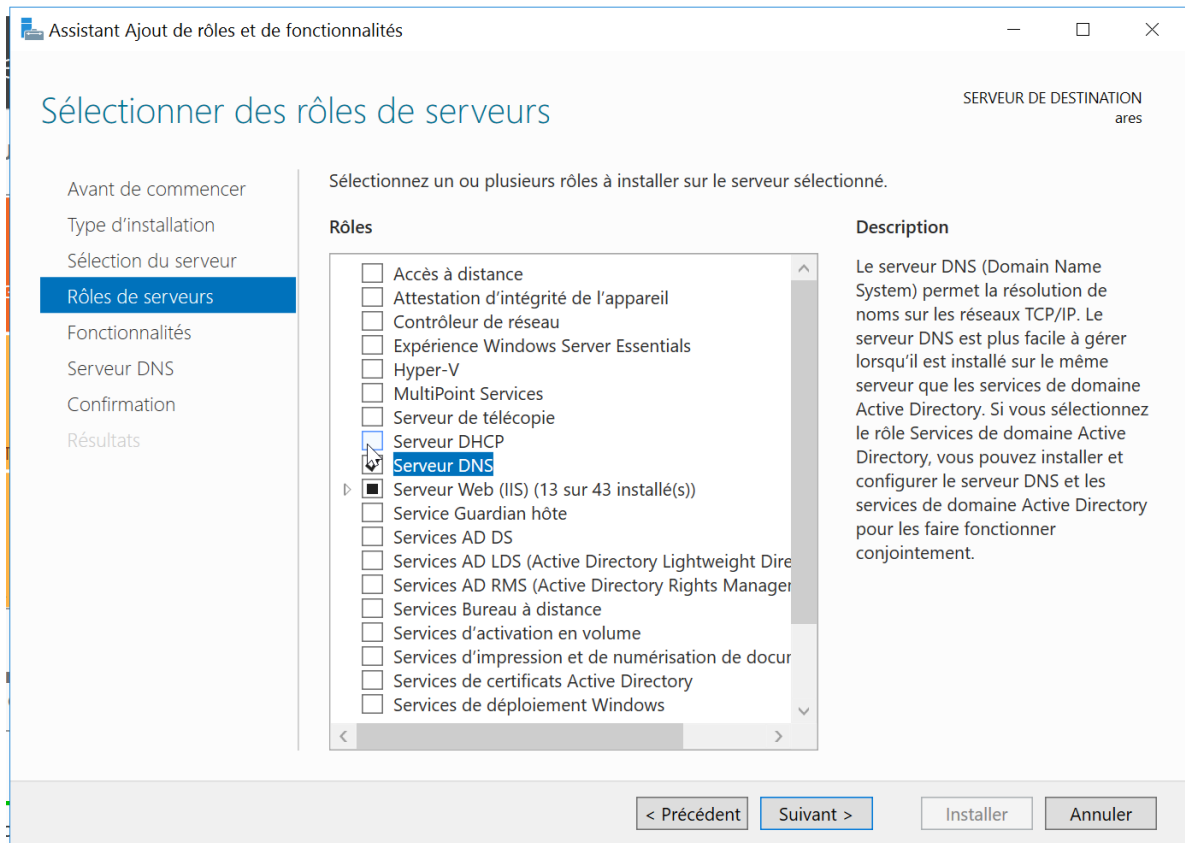


- Sélectionner son serveur pool pour installer les rôles et suivant.

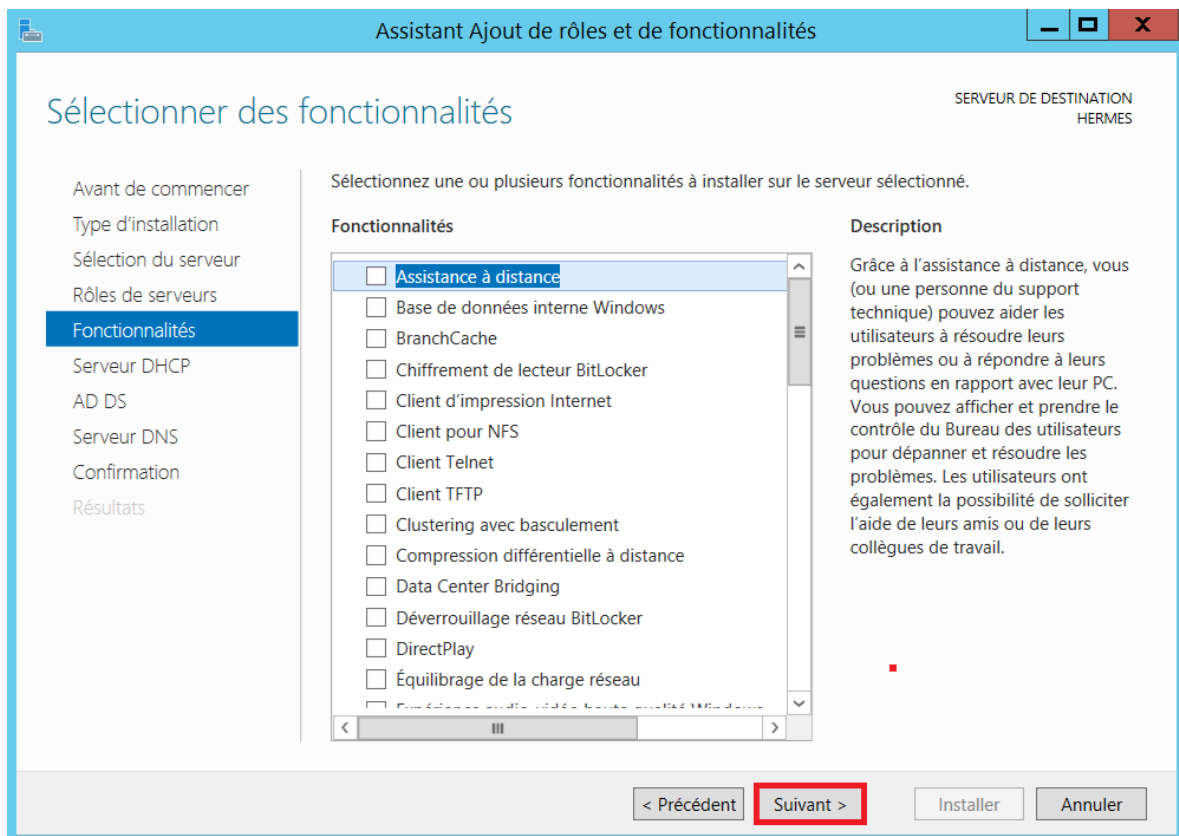
17



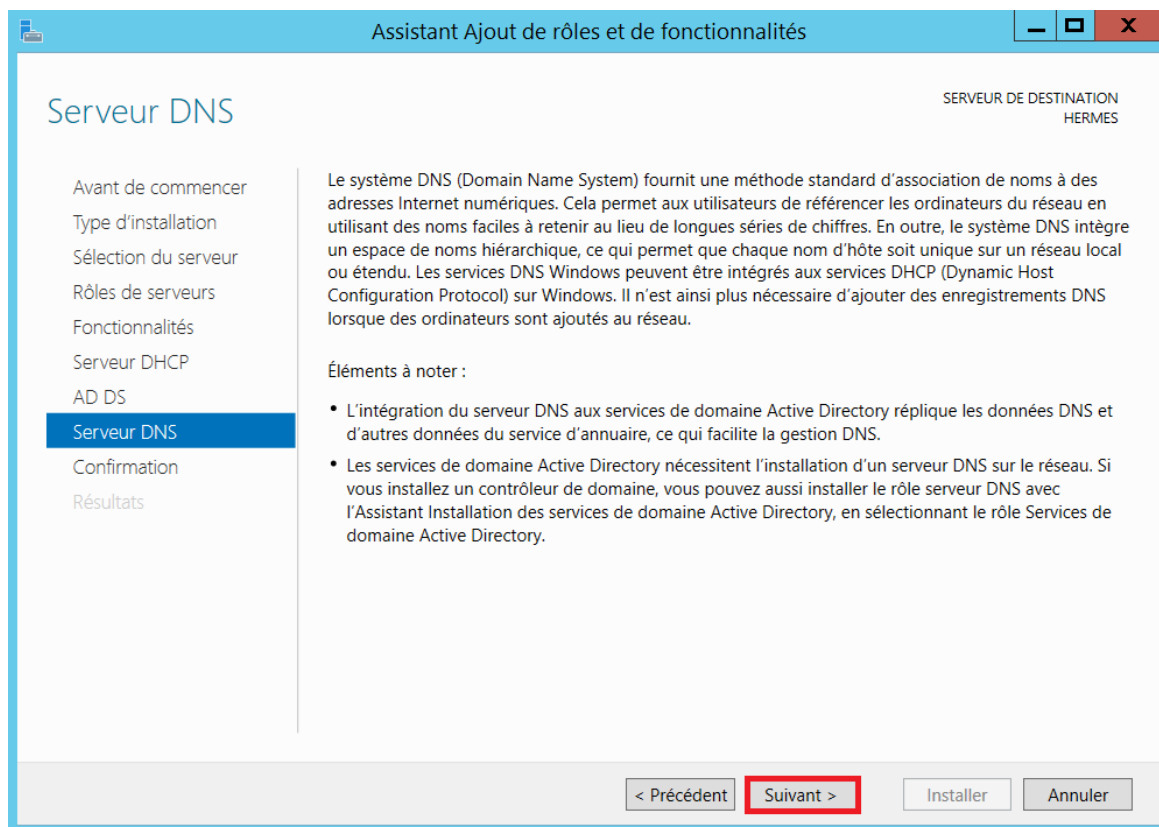
- Sélectionner les rôles **DNS** puis suivant.



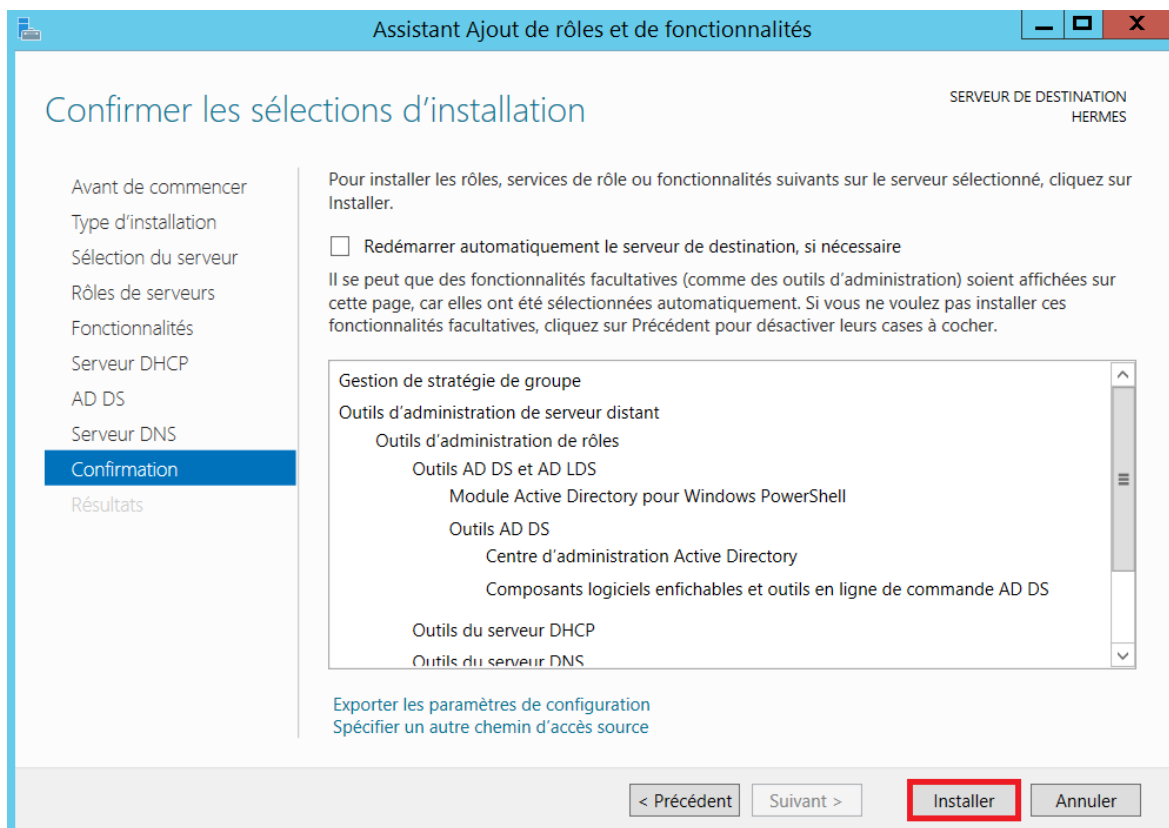
- Ne pas sélectionner de fonctionnalités et suivant.



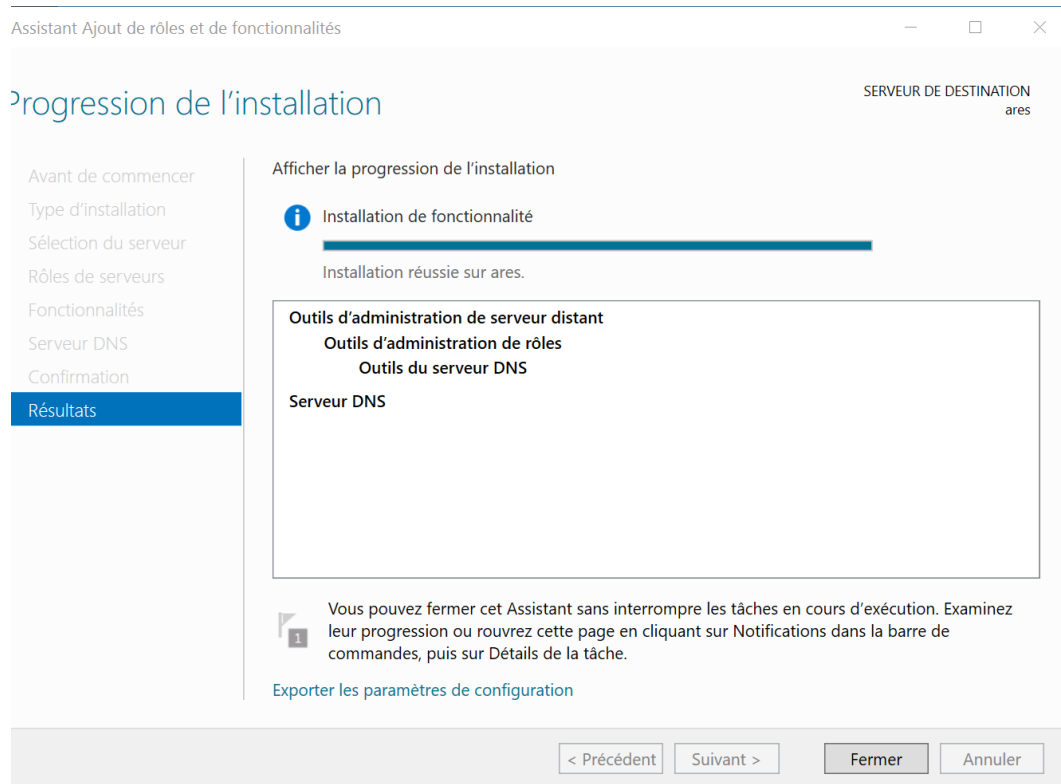
- Passer les explications du DNS et **suivant**.
- bts



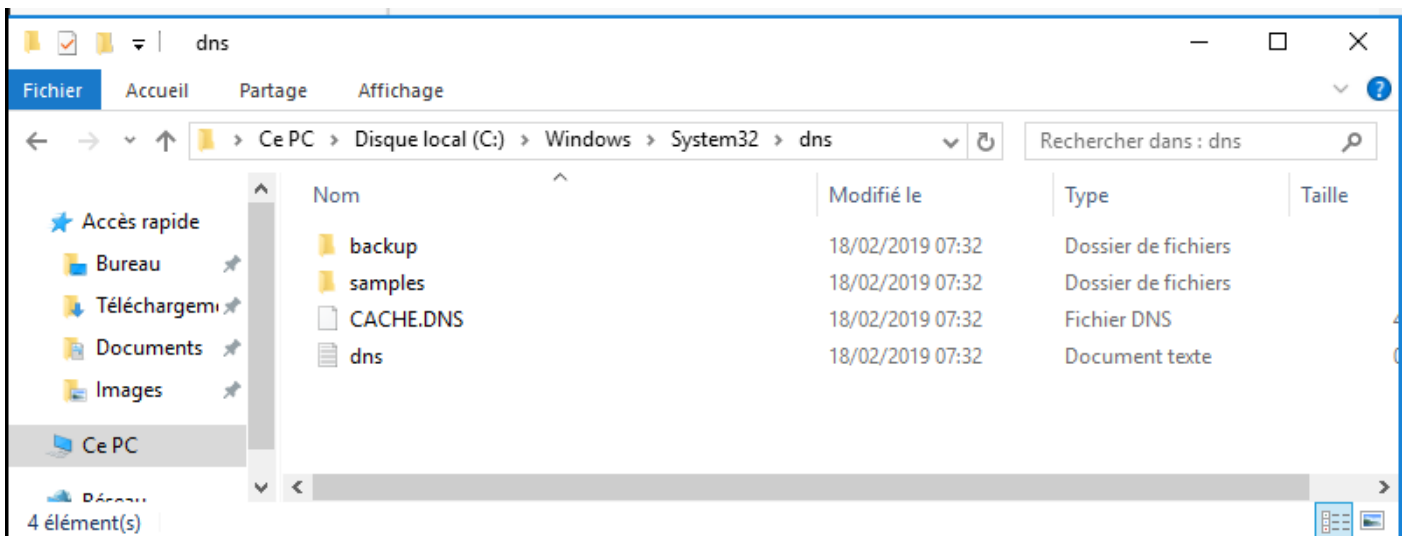
- Confirmer l'installation en cliquant sur **installer**.



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



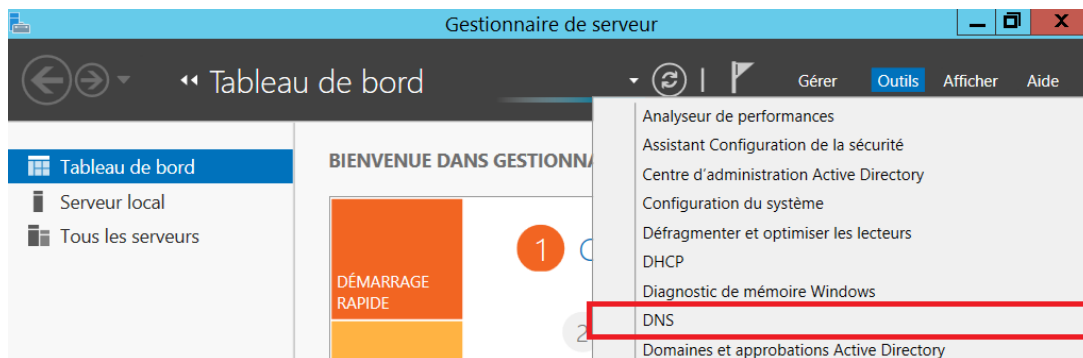
Après l'installation du service DNS, un répertoire **Dns** va être créé dans **c:\windows\system32** ce répertoire va stocker les bases DNS ainsi que le fichier cache qui répertorie les 13 serveurs root



Configuration DNS

Création de la zone de recherche directe :

- Gestionnaire de serveur → Outils → DNS.

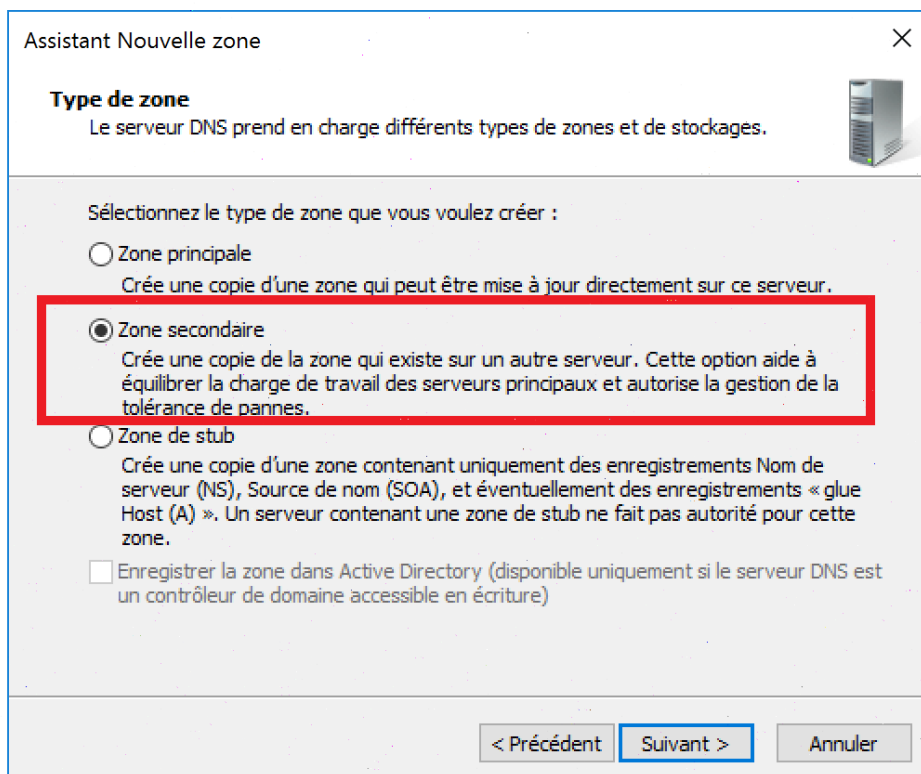


Nouvelle Zone Directe :

- Clic droit sur Zones de recherche directe → Nouvelle zones...



Indiquez Zone secondaire comme type de zone dns



Indiquez bts.local comme nom de la zone dns

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 :

< Précédent Suivant > Annuler

Indiquez l'adresse ip du serveur maitre(Ares)

Assistant Nouvelle zone

Serveurs DNS maîtres
La zone secondaire est copiée à partir d'un ou de plusieurs serveurs DNS.

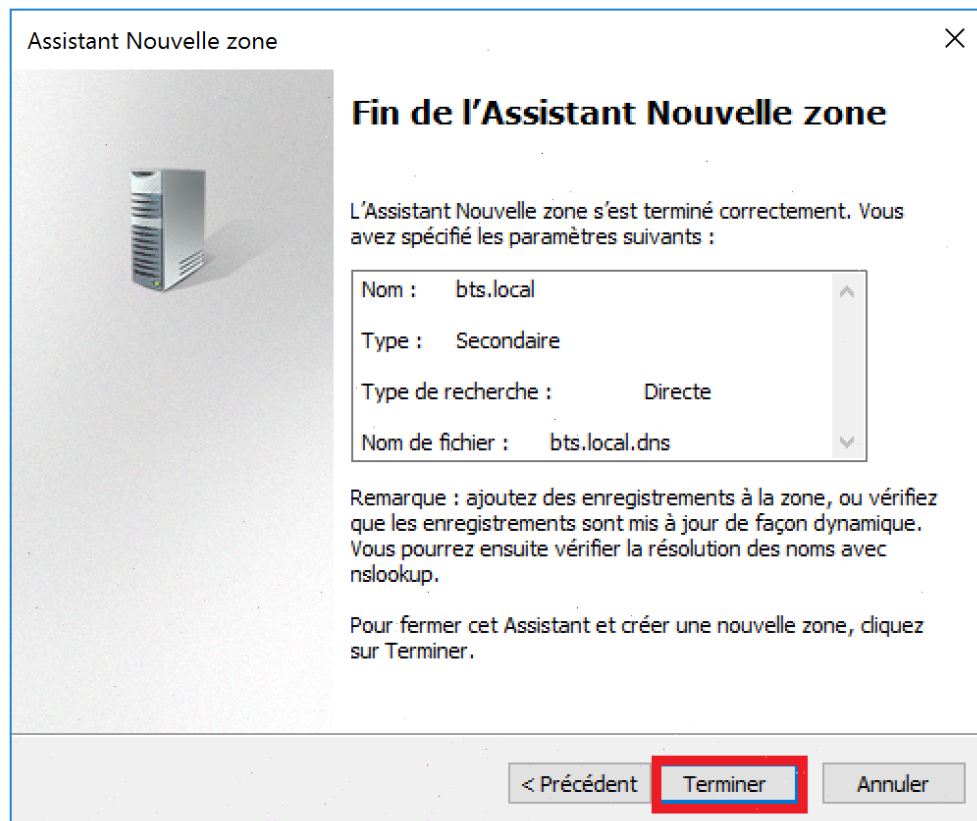
Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre indiqué.

Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
172.20.0.13	ares.bts.local	OK

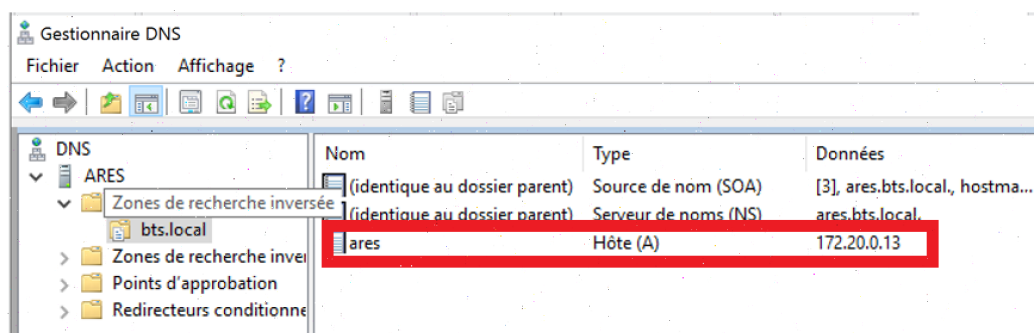
Supprimer Monter Descendre

< Précédent Suivant > Annuler



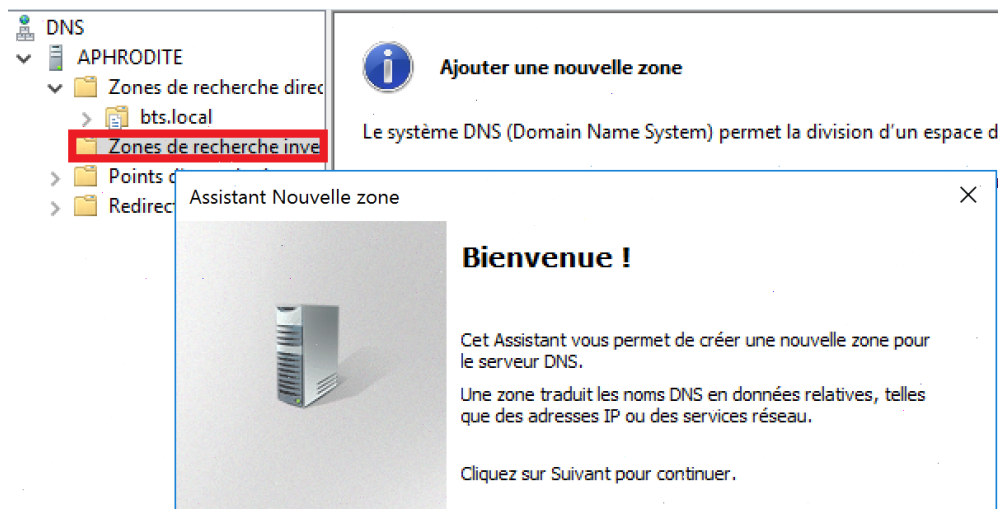
En développant la zone directe bts.local on remarque qu'il existe 2 types d'enregistrement SOA et NS mais il manque un enregistrement de type A qui correspond au server Ares. Pour faire apparaître cet enregistrement il faut renseigner le suffixe dns en mettant le nom de cette zone (bts.local)

Une fois le suffixe dns renseigné redémarrer la machine, vous vérifiez l'existence de l'enregistrement de type A

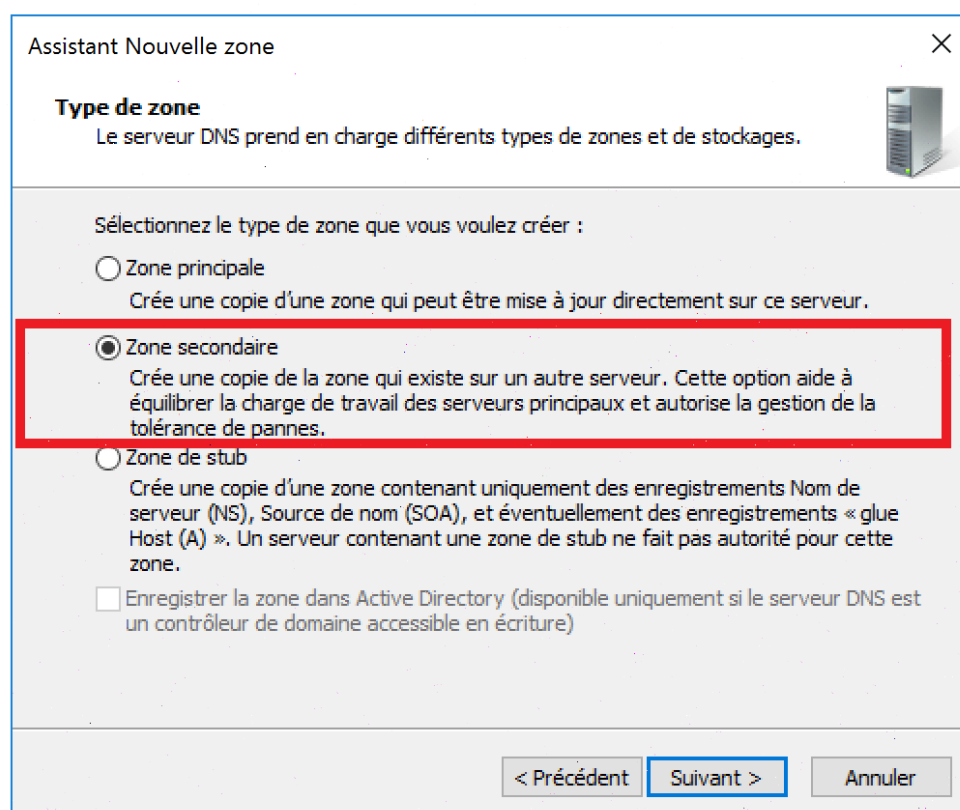


Nouvelle Zone inversé :

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



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



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

Assistant Nouvelle zone

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

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

☒ Zone de recherche inversée IPv4

☐ Zone de recherche inversée IPv6

< Précédent **Suivant >** Annuler

Sélectionné « **L'ID réseau 172.20.0.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

Assistant Nouvelle zone

Serveurs DNS maîtres

La zone secondaire est copiée à partir d'un ou de plusieurs serveurs DNS.

Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre indiqué.

Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
172.20.0.13	ares.bts.local	OK

Supprimer

Monter

Descendre

< Précédent Suivant > Annuler

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

Assistant Nouvelle zone

Fin de l'Assistant Nouvelle zone

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

Nom : 0.20.172.in-addr.arpa

Type : Serveur principal intégré à Active Directory

Type de recherche : Inversée

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent Terminer Annuler

Attention il faut autoriser le transfert de zones pour les deux zone directe et inversée sur le serveur maitre
ARES

