

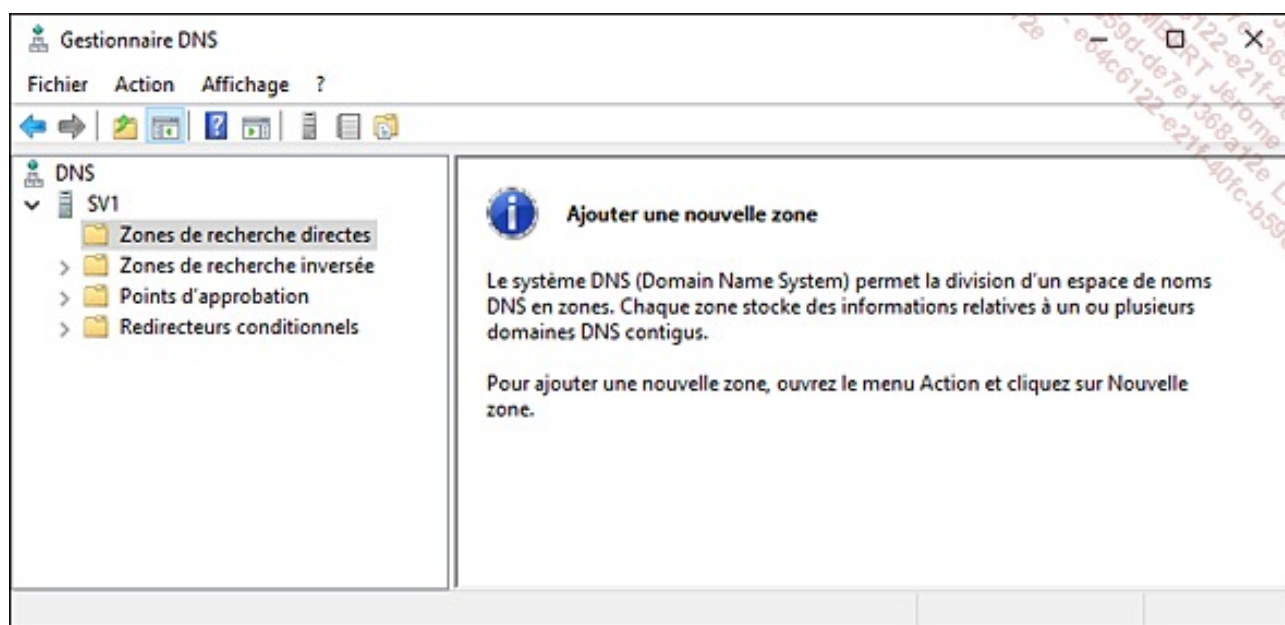
# Gestion des zones DNS

Une zone DNS est une portion du nom de domaine dont le responsable est le serveur DNS qui a autorité sur la zone. Ce dernier gère la zone et ses différents enregistrements.

## 1. Création d'une zone de recherche directe secondaire

Les zones de recherche directe prennent en charge la résolution des noms d'hôtes en adresses IP. La création d'une zone nécessite l'appartenance de l'opérateur au groupe Administrateurs.

- ➔ Sur SV1, ouvrez la console DNS.
- ➔ Déroulez **SV1** puis **Zones de recherche directes**.



- ➔ Effectuez un clic droit sur le dossier **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.

Trois types de zones peuvent être créés :

- ▾ **Zone primaire** : le serveur peut modifier les enregistrements de sa zone, il a des accès en lecture et en écriture aux enregistrements.

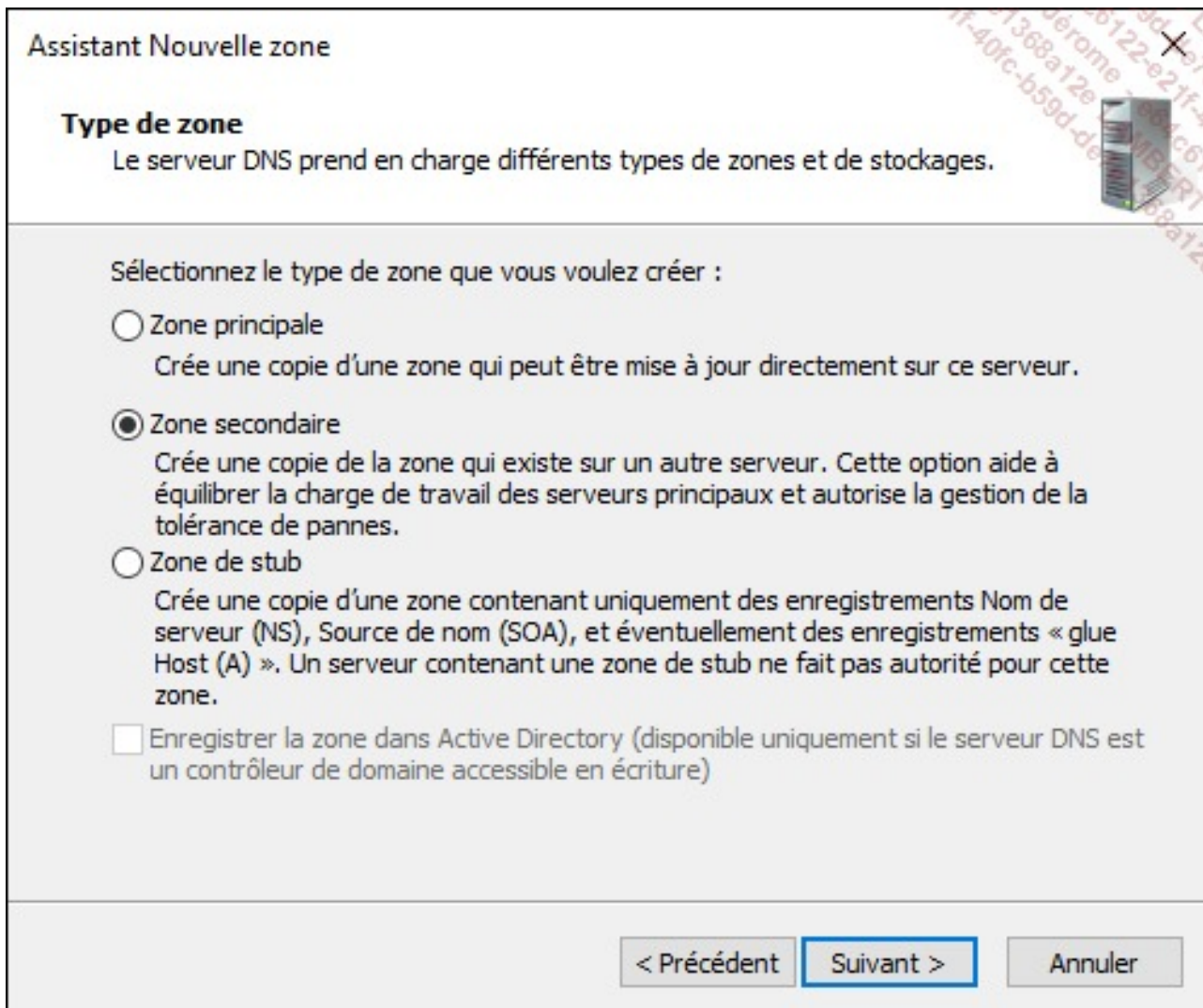
- ✓ **Zone secondaire** : ce type de zone est une copie d'une zone primaire. Le serveur ne peut pas modifier les enregistrements contenus dans la zone. Son but est de répondre aux requêtes faites par les clients.
- ✓ **Zone de stub** : la zone contient uniquement les enregistrements SOA, NS et A des serveurs DNS responsables de la zone.



Sélectionnez **Zone secondaire** puis cliquez sur **Suivant**.



Il est impossible de cocher l'enregistrement de la zone dans AD car le serveur n'est pas contrôleur de domaine.



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.

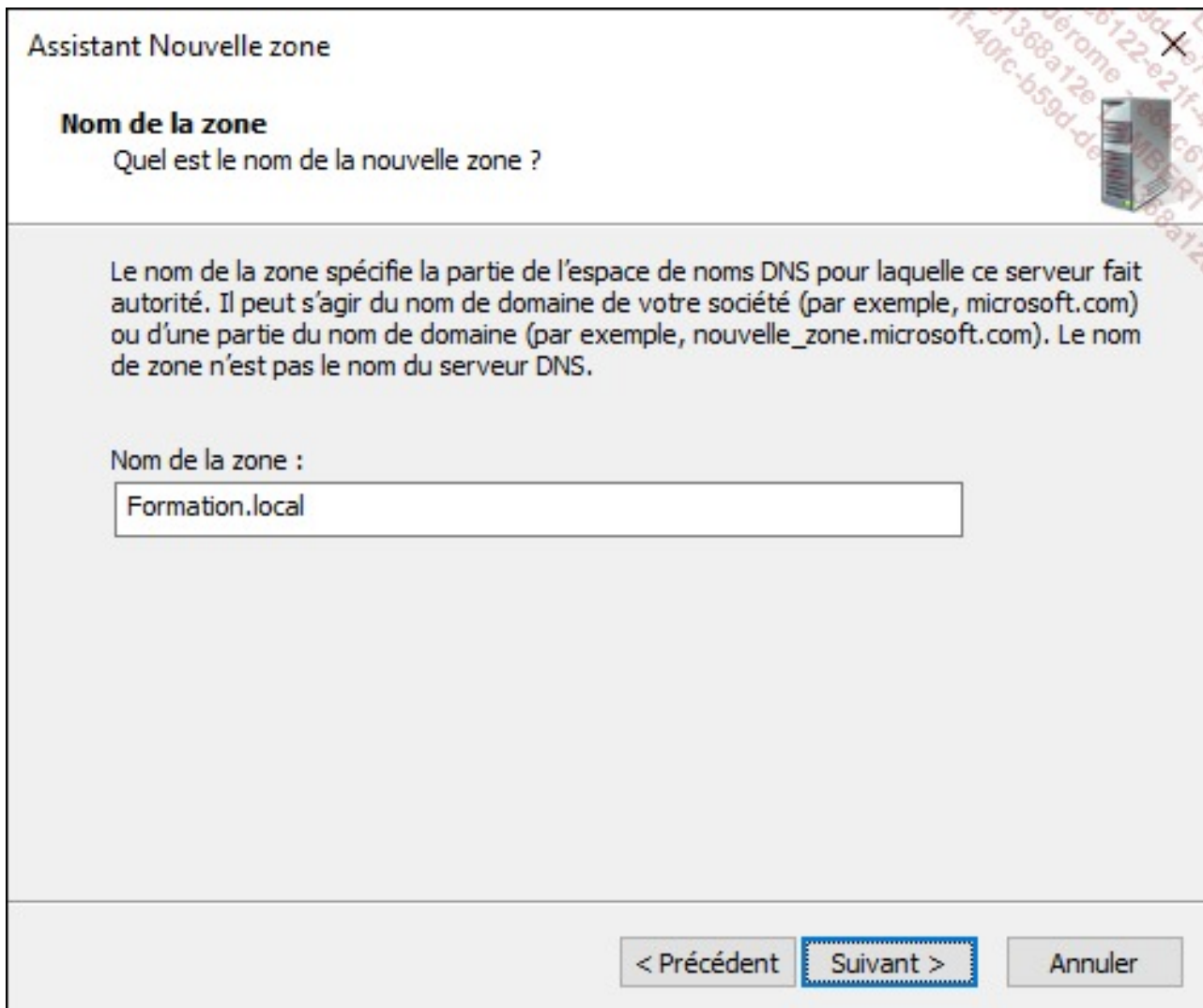
☒ Zone secondaire  
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.

☐ 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

➔ Saisissez **Formation.local** dans le champ **Nom de la zone**.



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 :

Formation.local

< Précédent   Suivant >   Annuler

- ➔ Saisissez dans le champ du serveur maître l'adresse IP du serveur AD1 (192.168.1.90) et validez en appuyant sur la touche [Entrée].

Le serveur maître est le serveur qui a un accès en écriture sur la zone, contrairement à la zone secondaire qui, elle, a un accès en lecture.

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 po...		
✓ 192.168.1.90	<Tentative de ré...	OK

Supprimer

Monter

Descendre

< Précédent Suivant > Annuler

→ Cliquez sur **Suivant** lorsque la résolution du nom est terminée.

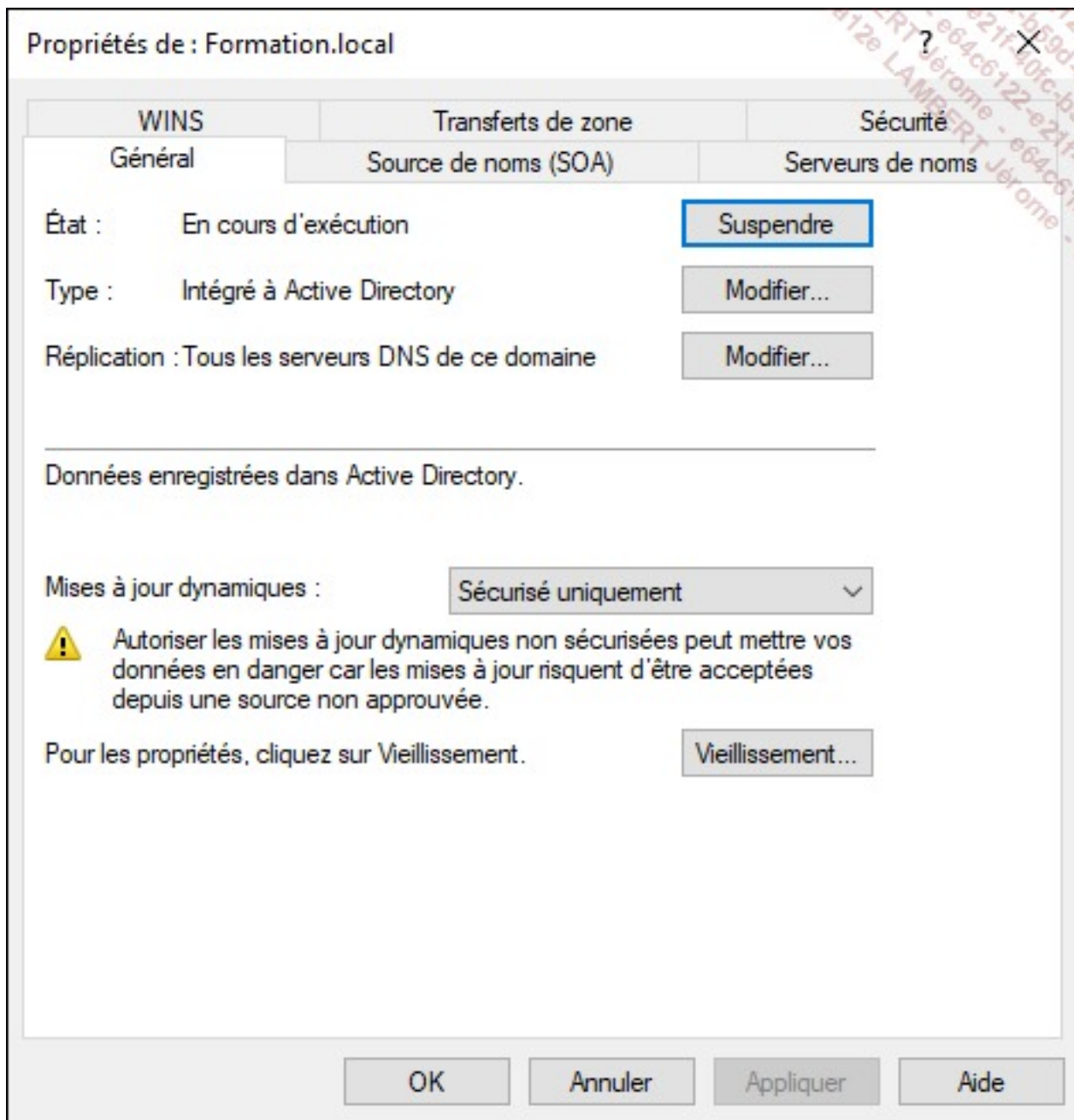
→ Cliquez sur **Terminer**.

Un message avertit qu'il est impossible de charger la zone. Ce message est dû au transfert de zone non configuré. Deux types de réplication avec DNS sont possibles :

- ✓ **La réplication avec AD** : ce type de réplication est utilisé pour les zones intégrées à AD. La réplication s'effectue en même temps que la réplication Active Directory.
- ✓ **La réplication avec le transfert de zone** : pour les zones qui ne sont pas intégrées à Active Directory, le transfert de zone est utilisé. Contrairement aux zones intégrées à AD, ce type de réplication nécessite une configuration.

→ Sur AD1 lancez la console DNS.

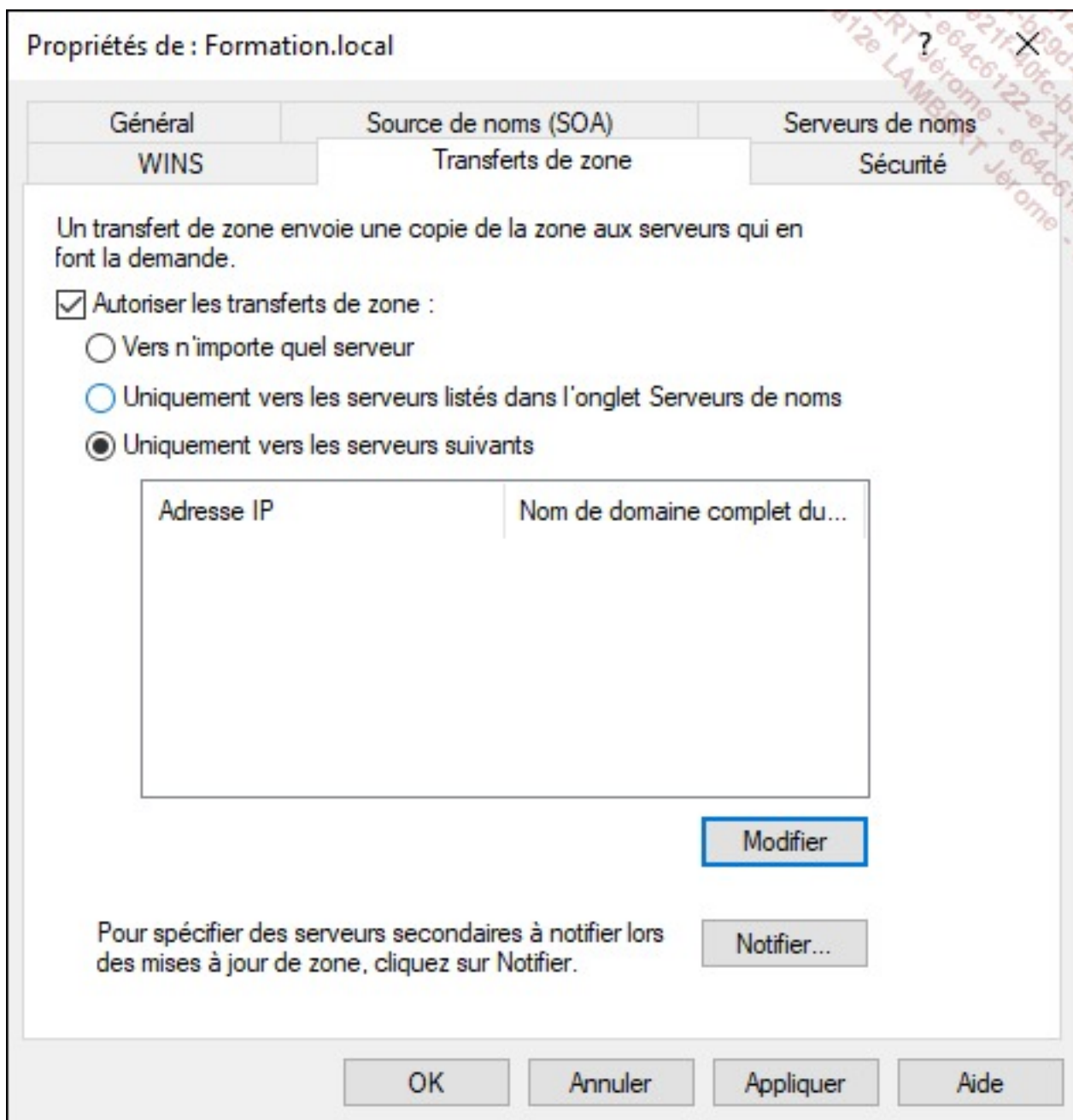
➔ Effectuez un clic droit sur la zone puis sélectionnez **Propriétés**.



➔ Cliquez sur l'onglet **Transferts de zone**.

➔ Cochez la case **Autoriser les transferts de zone** puis sélectionnez le bouton radio **Uniquement vers les serveurs suivants**.





→ Cliquez sur le bouton **Modifier** et saisissez l'adresse IP du serveur maître (SV1, 192.168.1.92).

**Autoriser les transferts de zone**

Zone DNS :

Formation.local

Adresses IP des serveurs secondaires :

Adresse IP	Nom de domaine compl...	Validé
<Cliquez ici pour ajo...		
192.168.1.92	SV1	Le serveur ayant cette ...

Supprimer

Monter

Descendre

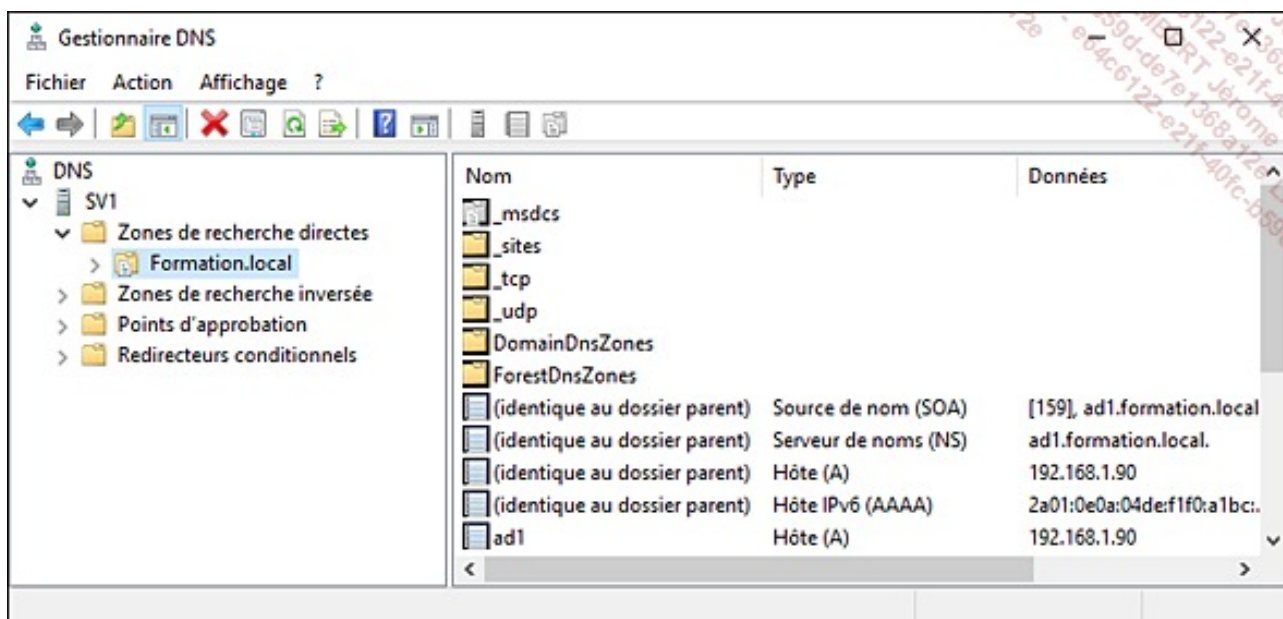
Le nom de domaine complet du serveur n'est pas disponible si les entrées et les zones de recherche inversée appropriées ne sont pas configurées.

OK Annuler

→ Cliquez deux fois sur **OK** pour valider et fermer les fenêtres.

Au bout de quelques minutes, le transfert de zone est terminé.

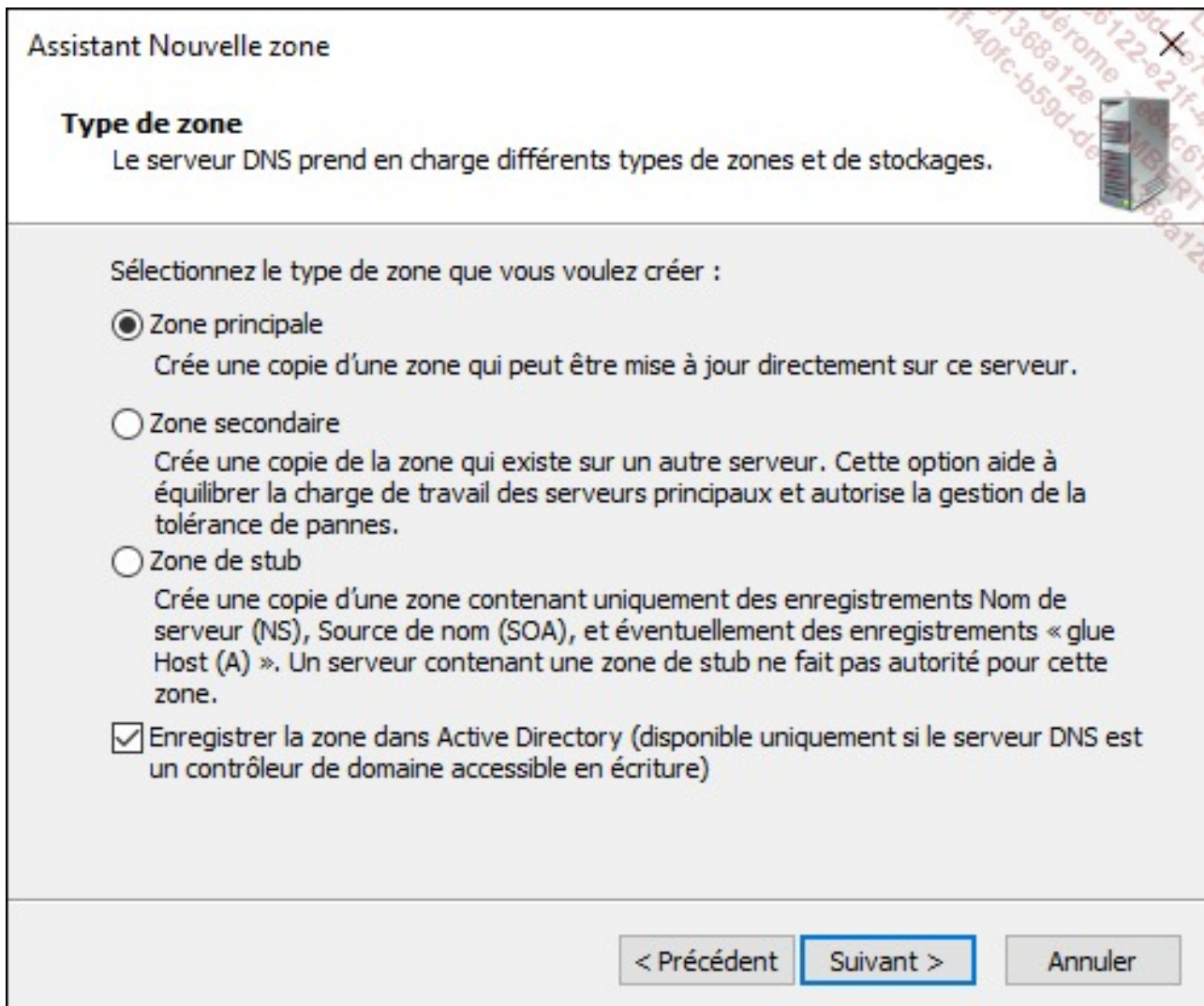




## 2. Création d'une zone de recherche directe principale

La zone Forms.msft doit être créée sur AD1 pour être intégrée à AD.

- ➔ Lancez la console DNS sur AD1.
- ➔ Déroulez **AD1** puis **Zones de recherche directes**.
- ➔ Effectuez un clic droit sur le dossier **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.
- ➔ Laissez les paramètres par défaut dans le type de zone.



**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

La réplication de la zone peut se faire sur tous les serveurs DNS du domaine Formation.local ou sur les serveurs DNS de la forêt Formation.local.



Laissez la réplication sur **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : Formation.local** et cliquez sur **Suivant**.

Assistant Nouvelle zone

### Étendue de la zone de réplication de Active Directory

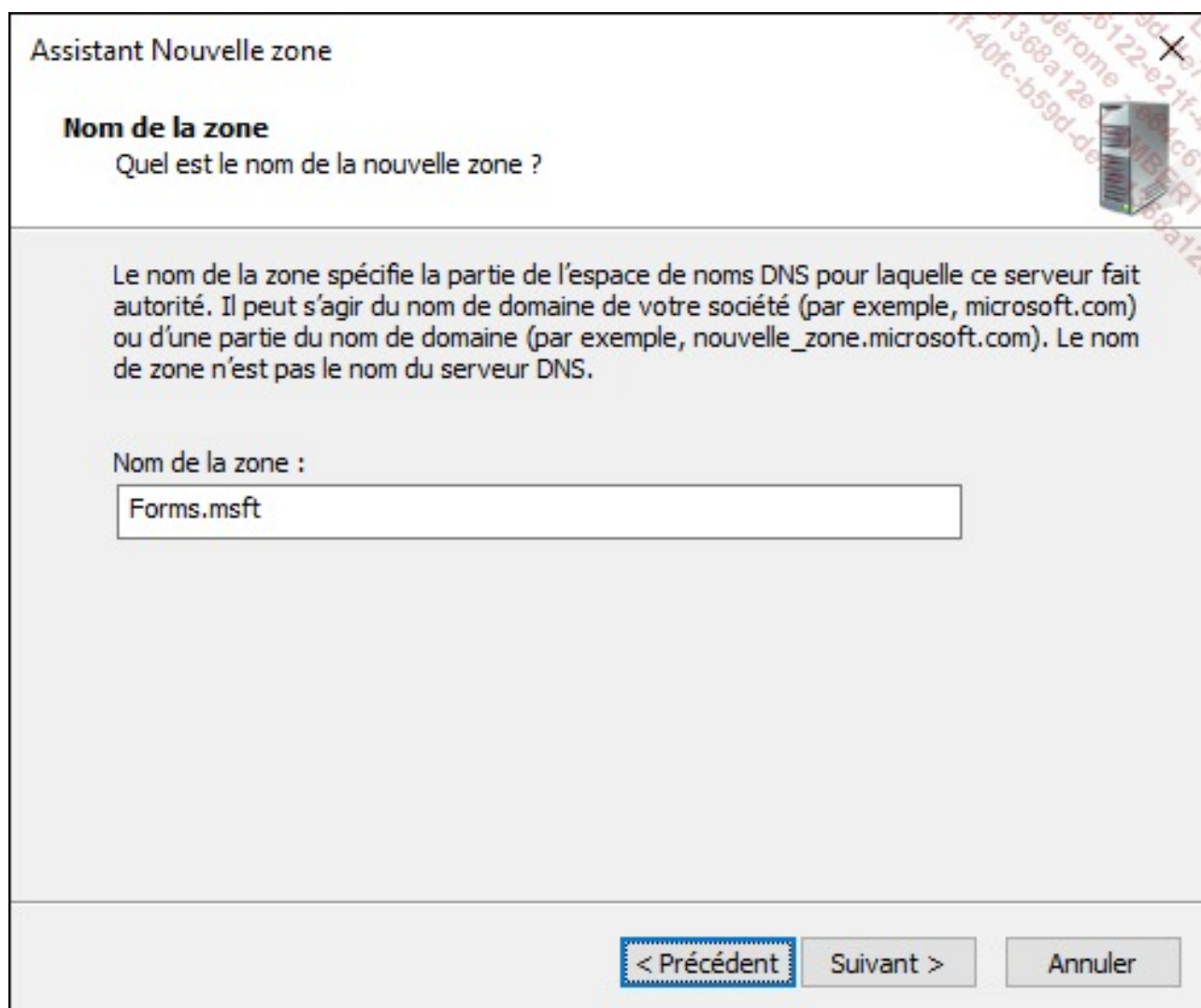
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

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

- ☐ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : Formation.local
- ☒ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : Formation.local
- ☐ Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : Formation.local
- ☐ Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

< Précédent   **Suivant >**   Annuler

➔ Saisissez **Forms.msft** dans le champ **Nom de la zone**.



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.

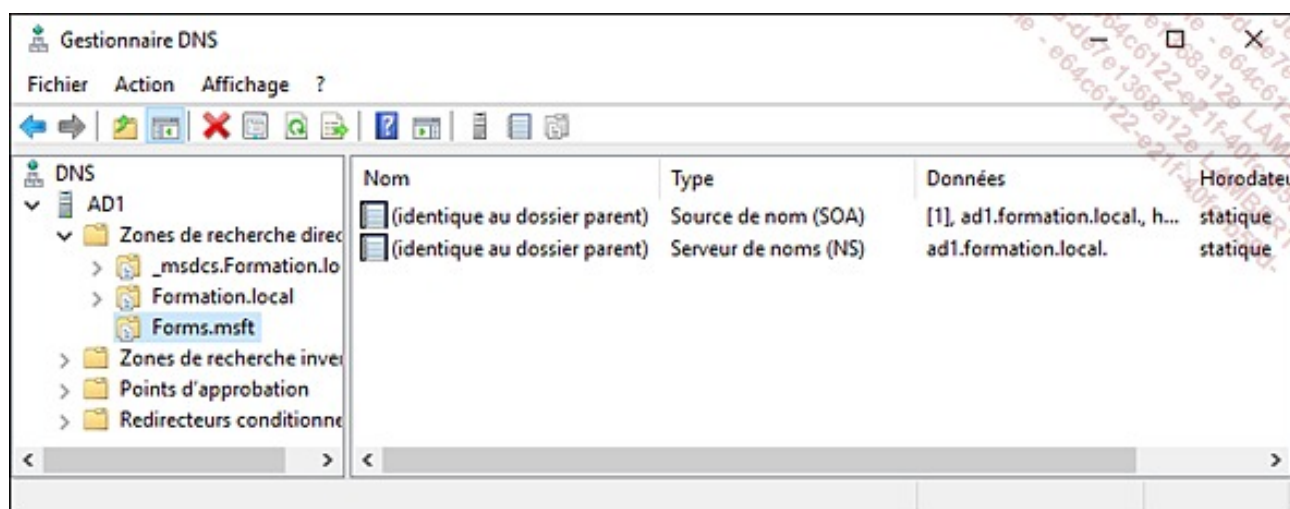
Nom de la zone :

Forms.msft

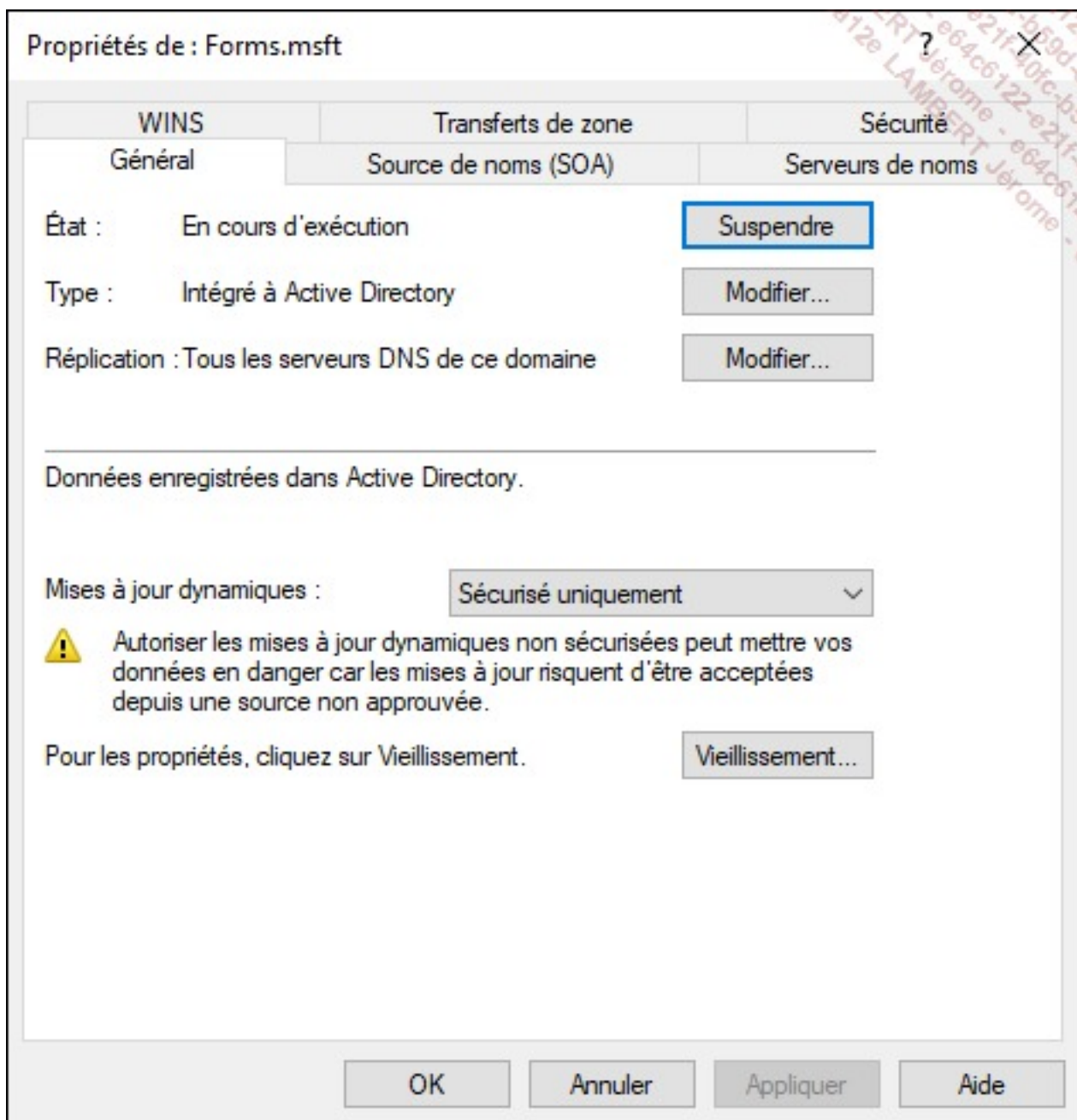
< Précédent   Suivant >   Annuler

- ➔ Laissez le choix par défaut dans la fenêtre **N'autoriser que les mises à jour dynamiques sécurisées** (recommandé pour Active Directory) puis cliquez sur **Next**.

La zone est maintenant présente dans la console DNS.



Dans les propriétés de celle-ci, on peut voir qu'elle est bien intégrée à AD.



Le serveur DNS peut maintenant résoudre des noms du domaine Forms.msft.

### 3. Création d'une zone de recherche inversée

L'ajout d'une zone de recherche inversée dans DNS est semblable sous de nombreux aspects à la création d'une zone de recherche directe. Elle permet la résolution d'adresses



IP en noms de postes.

La zone de recherche inversée est un sous-domaine du domaine in-addr.arpa. Les recherches pour les domaines IPv4 et IPv6 (ip6.arpa) sont prises en charge.

Le nom est construit avec l'adresse réseau. Ainsi le nom de la zone est créé en effectuant une inversion de l'ordre des octets de l'adresse IP, suivie de in-addr.arpa ou ip6.arpa.

Si l'ID réseau est 192.168.1, le nom de la zone de recherche inversée est alors 1.168.192.in-addr.arpa. L'outil de ligne de commande dnscmd permet également la création de zone.

- ➔ Lancez la console DNS sur AD1.
- ➔ Déroulez **AD1** puis **Zones de recherche inversée**.
- ➔ Effectuez un clic droit sur le dossier **Zones de recherche inversée** puis sélectionnez **Nouvelle zone**.
- ➔ Laissez le choix par défaut dans le type de zone (**Enregistrer la zone dans Active Directory**).



**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

➔ Laissez le choix par défaut dans la fenêtre **Étendue de la zone de réplcation de Active Directory**.

L'adresse IP du serveur est 192.168.1.90 et le masque de sous-réseau est 255.255.255.0. L'ID réseau est donc sur 3 octets soit 192.168.1.

➔ Saisissez 192.168.1 dans le champ **ID réseau**.

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 :

192 .168 .1 .

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 :

1.168.192.in-addr.arpa

< Précédent   Suivant >   Annuler

- La zone est intégrée à AD. Autorisez uniquement les mises à jour dynamiques sécurisées (recommandé pour Active Directory).

La zone apparaît dans la console.

## 4. Création d'une zone GlobalNames

Une des opérations les plus courantes sur les réseaux informatiques est la résolution de noms. Outre les noms DNS, on trouve également la résolution de noms NetBIOS. Ce dernier n'est pas composé du nom du domaine mais d'un simple nom en une partie (exemple : **POSTE01**). Dans certains cas, il est nécessaire de déployer un serveur WINS (*Windows Internet Naming Service*), alternative à DNS. WINS et NetBIOS ne

prennent pas en charge le protocole IPv6. Ils sont donc appelés à disparaître progressivement.

Depuis Windows Server 2008, il est possible de créer une zone spéciale nommée GlobalNames dans le serveur DNS. Avec cette dernière, on peut faire résoudre des noms en une partie par le serveur DNS.

Néanmoins, la zone GlobalNames n'a pas pour fonction de remplacer totalement le service WINS. En effet, la zone ne doit servir qu'à résoudre des noms statiques (les serveurs les plus utilisés...) ; les enregistrements inscrits de manière dynamique doivent continuer à être traités par le serveur WINS.

- ➔ Sur AD1, ouvrez la console DNS.
- ➔ Déroulez **AD1** puis **Zones de recherche directes**.
- ➔ Effectuez un clic droit sur le dossier **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.
- ➔ La zone créée est une zone principale intégrée à AD. Laissez le choix par défaut dans la fenêtre **Type de zone**.
- ➔ Sélectionnez l'option **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : Formation.local** puis cliquez sur **Suivant**.

Assistant Nouvelle zone

### Étendue de la zone de réplication de Active Directory

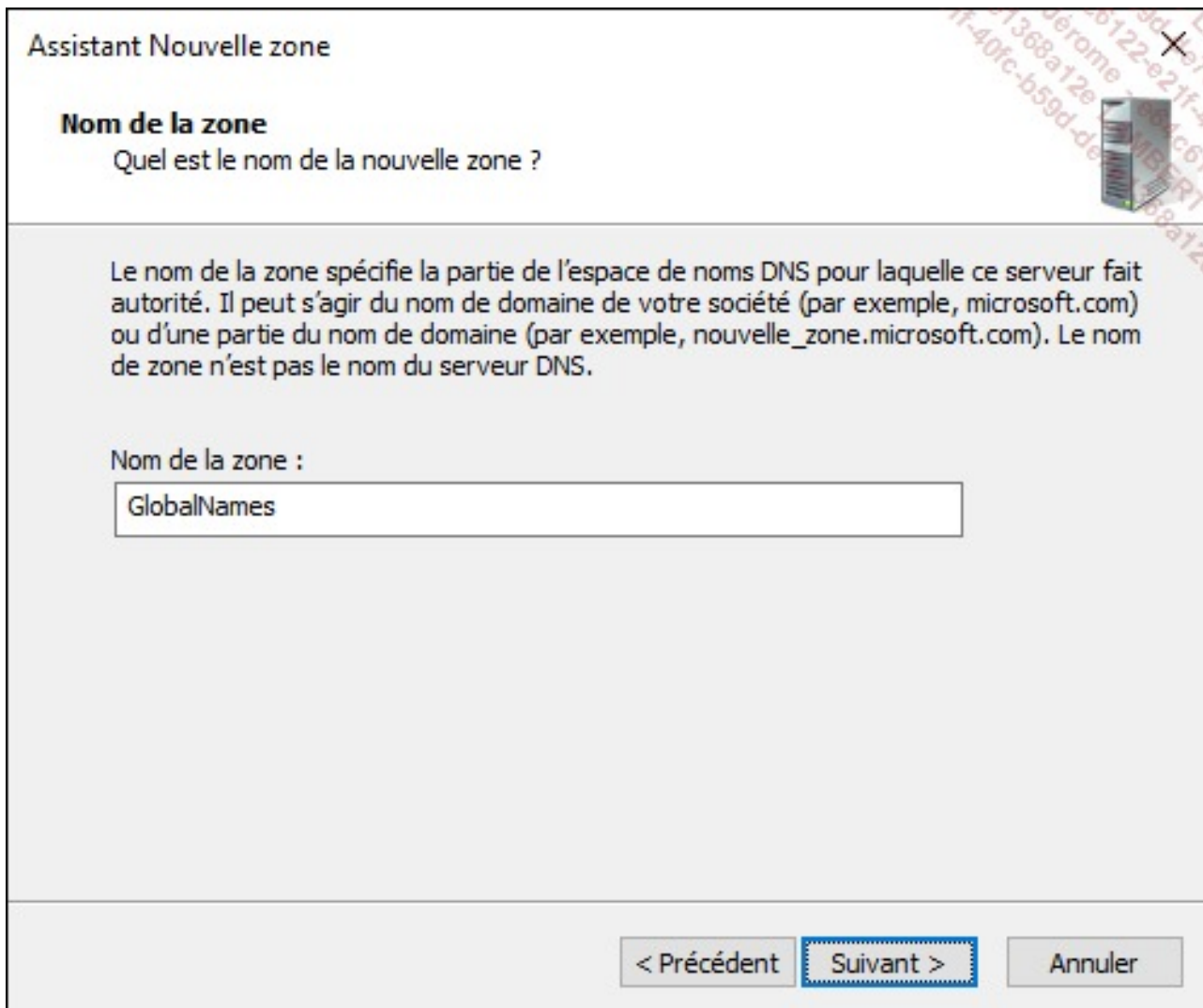
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

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

- ☒ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : Formation.local
- ☐ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : Formation.local
- ☐ Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : Formation.local
- ☐ Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

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

➔ Saisissez **GlobalNames** dans le champ **Nom de la zone**.



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 :

GlobalNames

< Précédent   Suivant >   Annuler

Les enregistrements sont créés par l'administrateur, aucune mise à jour dynamique n'est nécessaire.



Sélectionnez le bouton radio correspondant au choix **Ne pas autoriser les mises 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.

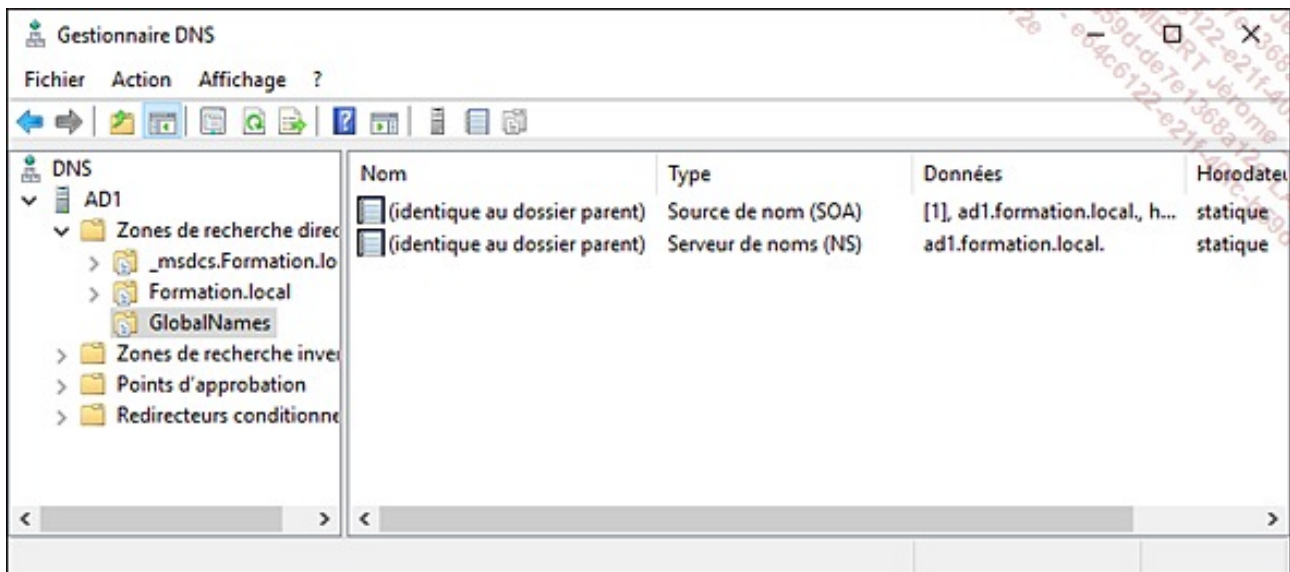
☐ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées  
 Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.  
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées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

La zone GlobalNames est maintenant présente dans la console DNS.

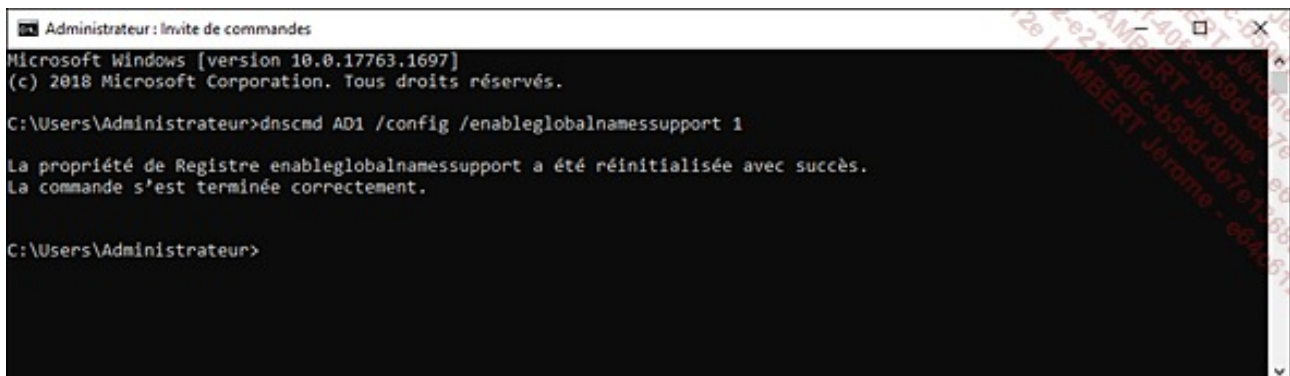


Il est à présent nécessaire d'activer la prise en charge de la zone GlobalNames.

- ➔ Ouvrez une invite de commandes DOS.
- ➔ Saisissez la commande `dnscmd AD1 /config /enableglobalnamesupport 1`



La zone GlobalNames n'est pas disponible pour la résolution de noms tant que la prise en charge de cette zone n'est pas activée de manière explicite au moyen de la commande ci-dessus sur chaque serveur DNS de référence dans la forêt.





- ➔ Effectuez un clic droit sur la zone GlobalNames puis sélectionnez **Nouvel alias (CNAME)**.
- ➔ Saisissez **SRVAD** dans le champ **Nom de l'alias** puis saisissez **ad1.formation.local** dans le champ **Nom de domaine complet (FQDN) pour l'hôte de destination**.

Nouvel enregistrement de ressource

Nom canonique (CNAME)

Nom de l'alias (utilise le domaine parent si ce champ est vide) :

SRVAD

Nom de domaine pleinement qualifié (FQDN) :

SRVAD.GlobalNames.

Nom de domaine complet (FQDN) pour l'hôte de destination :

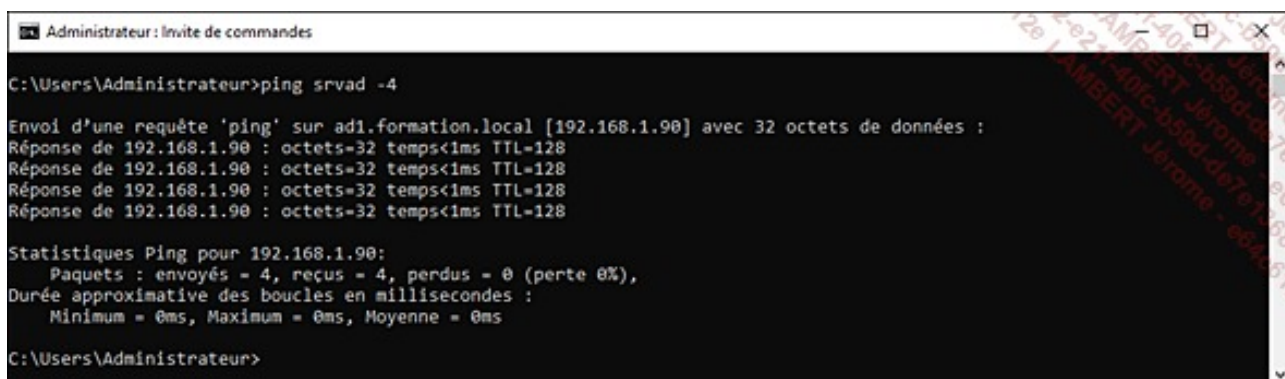
ad1.formation.local

Parcourir...

☐ Autoriser tout utilisateur identifié à mettre à jour tous les enregistrements DNS avec le même nom. Ce paramètre s'applique uniquement aux enregistrements DNS pour un nouveau nom.

OK Annuler

- ➔ Dans une invite de commandes DOS, saisissez `ping Srvad`. Le serveur **ad1.formation.local** répond.



```
Administrateur : invite de commandes

C:\Users\Administrateur>ping srvad -4

Envoi d'une requête 'ping' sur ad1.formation.local [192.168.1.90] avec 32 octets de données :
Réponse de 192.168.1.90 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.90 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.90 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.90 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.90:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

La résolution se fait correctement et le serveur nous répond.