
Pratique - Serveur DNS sous Windows Server 2019

BTS SIO - Bloc 2 - SISR - Administration des systèmes et des réseaux

1. Serveur DNS	3
1.1. Les fondamentaux de DNS	3
1.2. Installez le rôle Serveur DNS	4
1.3. Gérez le service DNS	6
1.4. Mettez en place votre première zone directe	10
1.5. Découvrez les autres types d'enregistrements	14
1.6. Mettez en oeuvre votre première zone inversée	15
1.8. En résumé	20

1. Serveur DNS

1.1. Les fondamentaux de DNS

DNS est l'abréviation de **Domain Name Service/System**. Il s'agit d'un protocole qui permet d'associer un nom à une adresse IP.

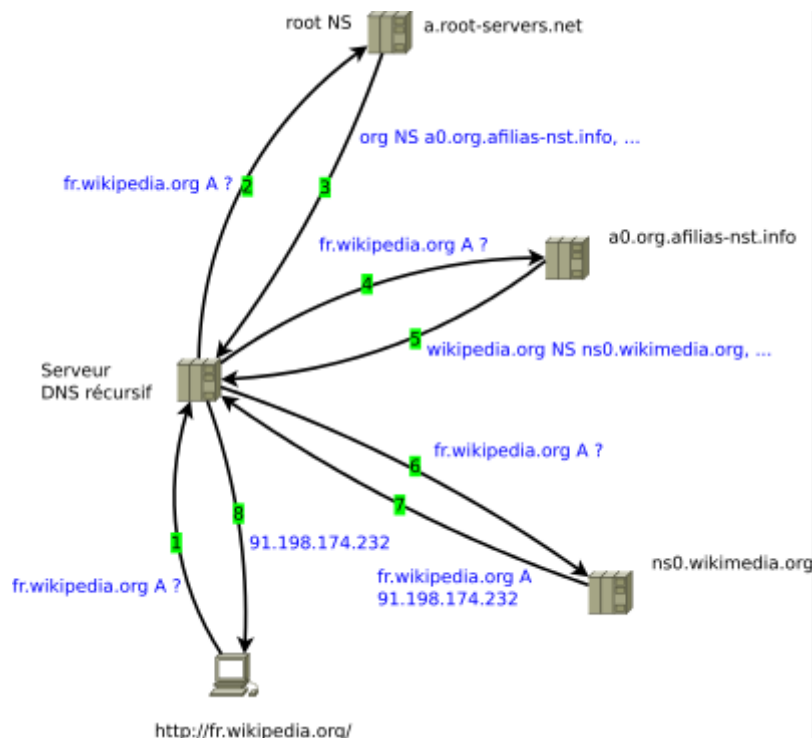
Un client (souvent le navigateur web) envoie une demande pour connaître l'adresse IP du serveur web correspondant à l'adresse que vous avez entrée.

Par exemple, si vous allez sur **www.exemple.com**, votre navigateur doit demander quelle est l'adresse IP du serveur nommé **www** dans la zone DNS **exemple.com**.

Pour cela, il va envoyer une requête au serveur DNS configuré sur votre poste, et faire une demande de **type A** concernant **www.exemple.com**. Si votre serveur DNS **ne connaît pas** la réponse, il va alors se tourner vers un autre serveur DNS (souvent ce sera l'un des serveurs racines (Root Servers) gérant les enregistrements de la zone ".").

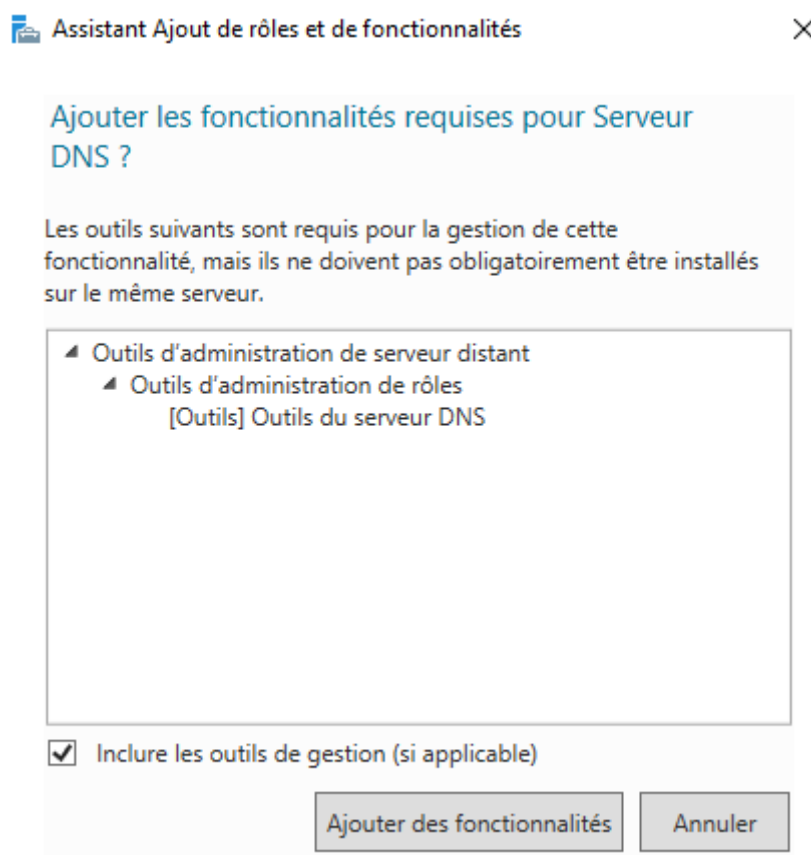
Dans cette zone particulière sont référencés les serveurs des zones **".com"**, **".fr"**, et d'une manière plus générale **".extension du nom de domaine"**.

Alors votre serveur interrogera en retour le serveur de nom de la zone **".com"** à la recherche du serveur DNS de la zone **".com"**, et la mécanique recommencera à la recherche de la zone **exemple.com** qui renverra, à ce moment-là, l'enregistrement **A** correspondant au champ **www** de sa zone : vous devriez avoir l'IP 93.184.216.34.



1.2. Installez le rôle Serveur DNS

Maintenant, je vous propose d'**installer le rôle DNS** sur un serveur Windows. Pour cela, comme vous le savez, rendez-vous sur le **gestionnaire de serveur** et ajoutez un rôle. À la sélection du rôle, Microsoft vous propose comme pour le DHCP, des fonctionnalités obligatoires :



Ensuite, vous avez des informations sur ce rôle, qui vous présentent le fonctionnement général (avec le lien au DHCP) et une configuration possible, préconisée par Microsoft, à savoir l'intégration à l'active Directory. Cela permet de bénéficier du **mécanisme de réplication de l'AD** pour simplifier la réplication des zones sur les serveurs AD (qui se doivent d'avoir le rôle Serveur DNS pour fonctionner) :

Serveur DNS

SERVEUR DE DESTINATION
SRVDHCPPAR01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

Confirmation

Résultats

Le système DNS (Domain Name System) fournit une méthode standard d'association de noms à des adresses Internet numériques. Cela permet aux utilisateurs de référencer les ordinateurs du réseau en utilisant des noms faciles à retenir au lieu de longues séries de chiffres. En outre, le système DNS intègre un espace de noms hiérarchique, ce qui permet que chaque nom d'hôte soit unique sur un réseau local ou étendu. Les services DNS Windows peuvent être intégrés aux services DHCP (Dynamic Host Configuration Protocol) sur Windows. Il n'est ainsi plus nécessaire d'ajouter des enregistrements DNS lorsque des ordinateurs sont ajoutés au réseau.

Éléments à noter :

- L'intégration du serveur DNS aux services de domaine Active Directory réplique les données DNS et d'autres données du service d'annuaire, ce qui facilite la gestion DNS.
- Les services de domaine Active Directory nécessitent l'installation d'un serveur DNS sur le réseau. Si vous installez un contrôleur de domaine, vous pouvez aussi installer le rôle serveur DNS avec l'Assistant Installation des services de domaine Active Directory, en sélectionnant le rôle Services de domaine Active Directory.

< Précédent

Suivant >

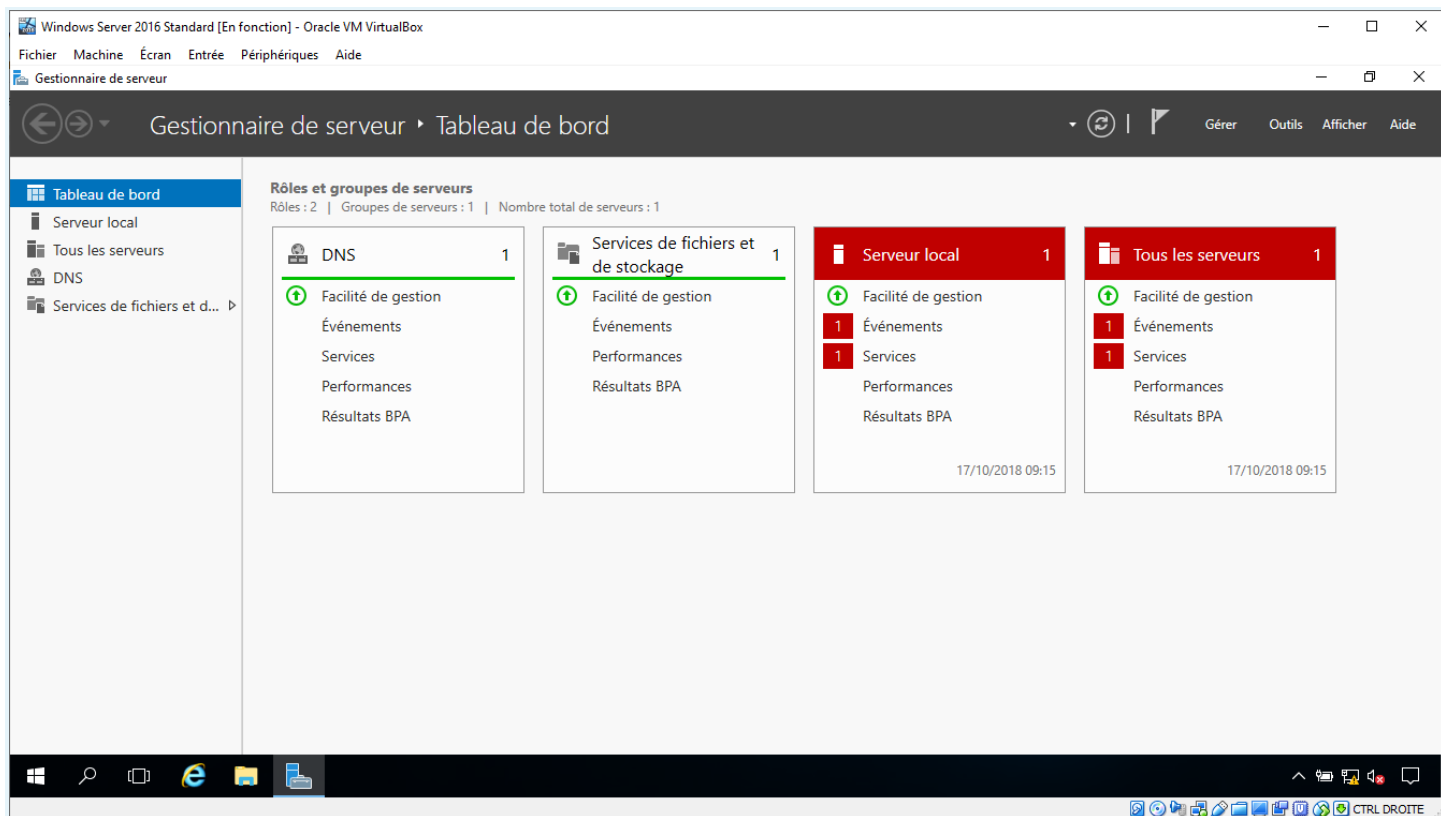
Installer

Annuler

Informations sur le rôle Serveur DNS de l'assistant d'installation

Validez les informations finales et lancez l'installation en cliquant sur **"Installer"**.

Cette fois, il n'est pas nécessaire de redémarrer. Cette étape dépend des rôles et vous serez averti par les notifications sur le tableau de bord si un redémarrage est nécessaire.



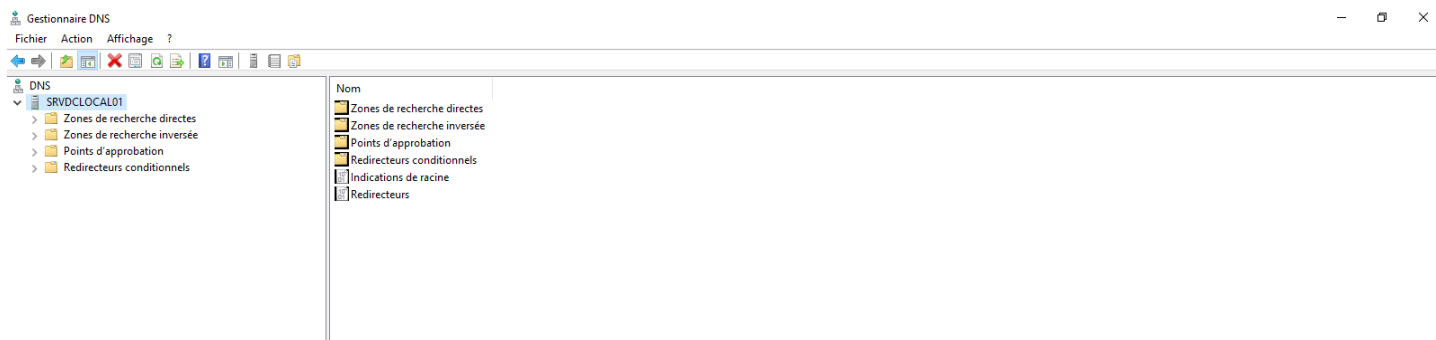
Si vous allez sur le tableau de bord de votre serveur, vous pourrez noter à quel point le nommage est **primordial** ! J'ai volontairement laissé le nom que j'ai positionné sur le serveur lors de l'installation du rôle DHCP, voyez la confusion possible pour l'administrateur :



Il ne semble pas logique de ne pas avoir un nom ne reflétant pas le rôle du serveur. Attention toutefois, si votre serveur est accessible de l'extérieur de votre réseau, le fait de connaître, via son nom, son rôle, est une information critique. Entre les mains d'un pirate informatique, cela permet d'accélérer les recherches de vecteurs d'attaque. Il conviendra de correctement configurer le DNS pour éviter de faire fuiter de telles informations.

1.3. Gérez le service DNS

Tout comme le gestionnaire DHCP, il existe le gestionnaire DNS. Cette console dédiée à l'administration du rôle DNS permet de **créer les différentes zones** nécessaires au fonctionnement du DNS.



La maîtrise des noms est un domaine souvent pris à la légère. Rappelez-vous que 100 % des requêtes vers Internet passent par le DNS.

Avant de créer votre première zone directe, il faut savoir comment un serveur DNS fonctionne : à chaque requête d'un client, la réponse va être mise en cache localement. Ce cache permettra à votre serveur, après avoir récupéré l'adresse IP du serveur `www.exemple.com`, de répondre plus rapidement sans avoir à relancer une requête récursive aux serveurs "root", ainsi qu'au serveur de la zone "exemple.com". Ce cache doit être géré.

Pourquoi ce cache doit-il être géré ?

Eh bien, tout simplement pour éviter de garder en mémoire l'association **www.exemple.com vers l'IP 93.184.216.34**.

Eh oui, si l'administrateur de ce serveur décide de changer d'adresse IP, il serait dommage de ne plus pouvoir accéder à www.exemple.com.

Attention donc à régler le cache à une valeur ni trop faible, ni trop forte.

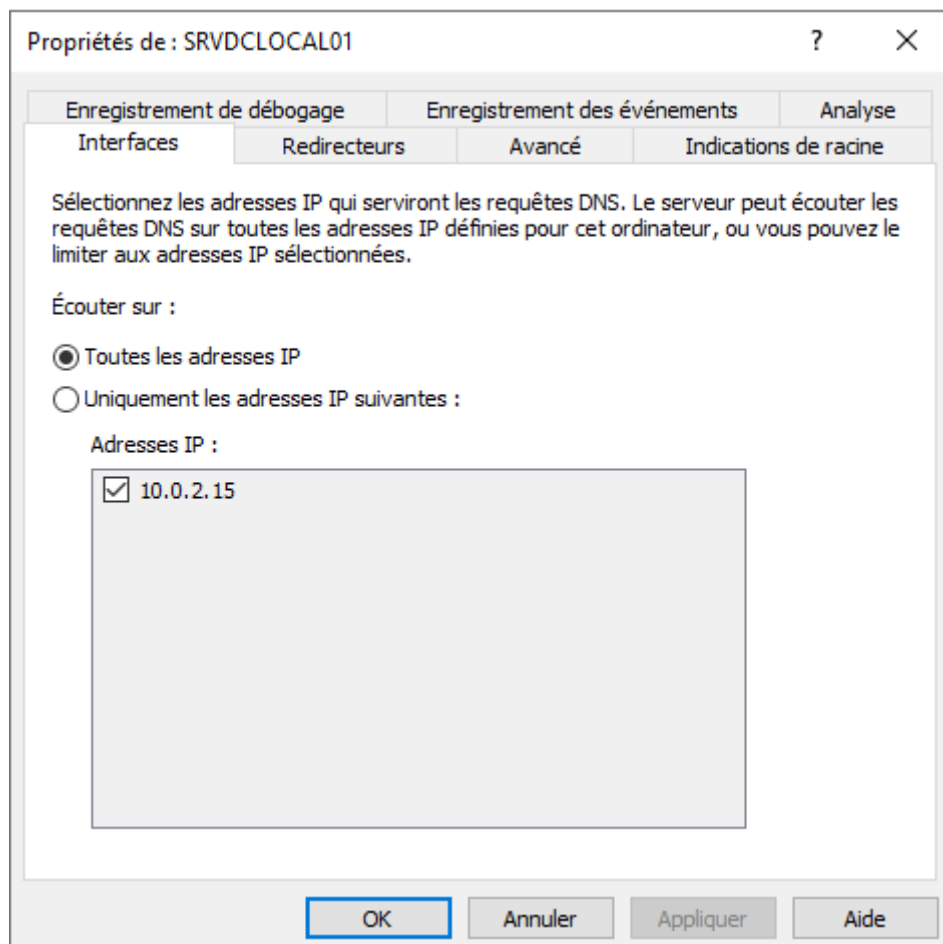
Par défaut, cette valeur est d'une journée (24h) pour les réponses positives (une adresse IP au moins existe pour un nom qualifié) et de 15 minutes pour les réponses négatives. Pour afficher ces informations, ouvrez PowerShell et tapez la commande `Get-DnsServerCache` :

```
Administrateur : Windows PowerShell
PS C:\Program Files> get-dnsservercache

MaxTTL                : 1.00:00:00
MaxNegativeTTL         : 00:15:00
MaxKBSize              : 0
EnablePollutionProtection : True
LockingPercent         : 100
StoreEmptyAuthenticationResponse : True
IgnorePolicies         : False

PS C:\Program Files>
```

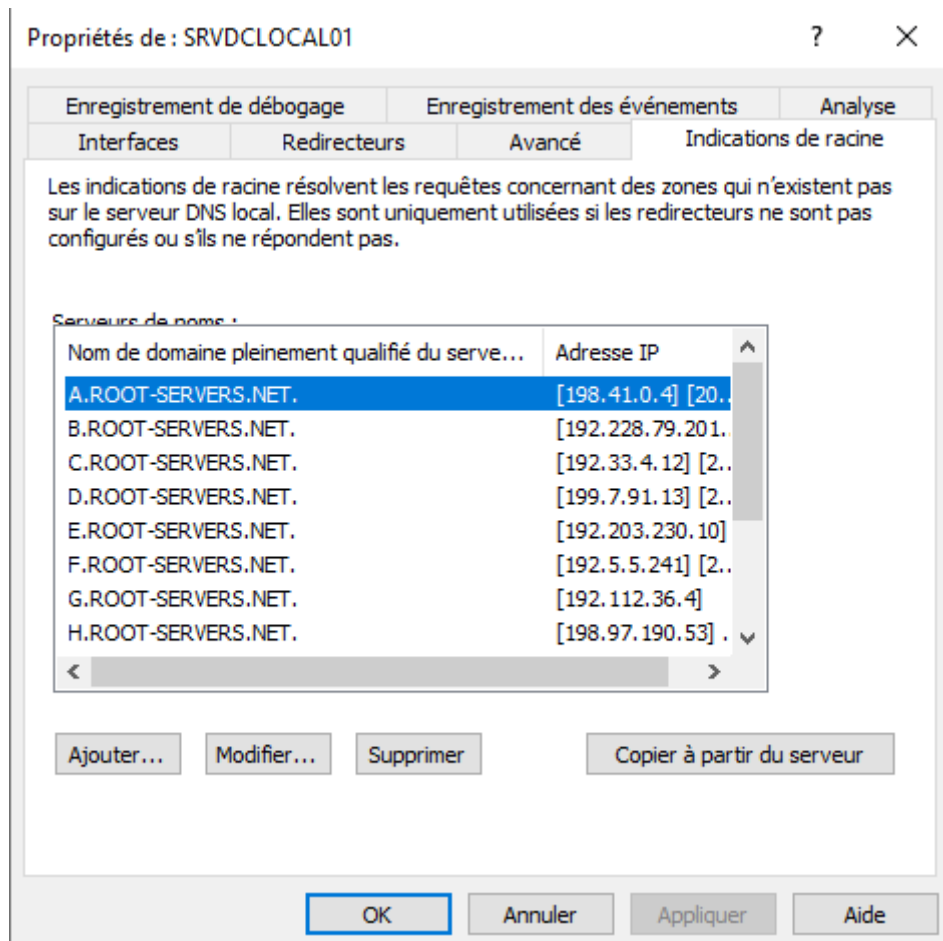
Enfin, vous allez vous assurer que le rôle DNS est correctement configuré. Dans le gestionnaire DNS, avec un clic droit sur le nom du serveur, choisissez "**propriétés**" :



Sur quelle interface écoute le service DNS ?

Par défaut, il écoutera les requêtes DNS sur toutes les interfaces. Si vous avez un réseau d'administration, il peut être intéressant de ne pas écouter les requêtes sur ce réseau. Je vous propose donc de sélectionner uniquement **l'IP fixe** que vous avez configurée sur votre serveur.

Dirigez-vous sur l'onglet Indication de racine. Allez vérifier que votre serveur connaît les serveurs racines. Ce seront les serveurs qui seront contactés pour identifier une réponse à **www.exemple.com** par exemple.



Serveurs racines connus de votre serveur DNS

Ouvrez, sur votre serveur, une invite de commande (un *Shell*). Tapez la commande `nslookup - 10.0.2.15` (où 10.0.2.15 est l'adresse IP de l'interface réseau de votre serveur). Vous entrez alors dans un client DNS interactif, en lien avec votre serveur ! Testez **www.exemple.com** :

```
nslookup - 10.0.2.15
Serveur par défaut : UnKnown
> www.exemple.com
Serveur : UnKnown
Réponse ne faisant pas autorité :
Nom : www.exemple.com
Adresses : 2606:2800:220:1:248:1893:25c8:1946
          93.184.216.34
```

Comme votre serveur n'est pas le gestionnaire de la zone **exemple.com**, il interroge récursivement les serveurs racines, puis le serveur DNS de la zone **exemple.com**. La réponse que votre serveur vous fournit ne fait pas autorité, car votre serveur la tient d'un autre serveur 😊.

Comment avoir des réponses faisant autorité ?

En disposant d'une zone DNS ; ça tombe bien, c'est ce que vous allez mettre en place !

1.4. Mettez en place votre première zone directe

Une **zone directe** permet d'associer un nom à une adresse IP, c'est bien plus simple pour nous, humains, de se rappeler d'un nom ; surtout qu'une adresse IP peut changer avec le temps, comme par exemple, lors d'un changement de fournisseur d'accès.

La première étape consiste à choisir un nom de domaine. Je vous propose de prendre une zone privée.

Prenez le cas suivant : suite à la configuration du DHCP, la direction de BTS SIO S.A. vous demande de trouver un moyen de nommer les différents équipements et services sur le réseau. Le directeur en a marre de devoir taper l'adresse IP 10.0.2.10 pour accéder à l'intranet. Vous allez donc créer une zone directe pour le domaine "**bts-sio.cci**" et y placer un enregistrement **A** faisant pointer intranet.bts-sio.cci vers 10.0.2.10. Ainsi votre directeur pourra tranquillement taper **https://intranet.bts-sio.cci** au lieu de l'adresse IP, mission réussie !

Pour cela, vous disposez (encore) d'un assistant. Faites un clic droit sur le nom du serveur DNS dans le gestionnaire DNS, puis sélectionnez "**Configurer un serveur DNS**" ; après l'écran de bienvenue, vous devriez avoir l'écran suivant :

Le premier choix est parfait, c'est ce que vous voulez faire. Validez ce choix par "**Suivant**". Sur l'écran suivant, une question étrange est posée : est-ce que vous allez gérer la zone via ce serveur DNS, ou est-ce que votre zone est gérée par un serveur d'un fournisseur de service ?

Emplacement du serveur principal

Vous pouvez choisir où s'effectue la maintenance de vos données DNS pour vos ressources réseau.



Quel serveur DNS assure la maintenance de votre zone de recherche directe principale ?

- ☒ Ce serveur assure la maintenance de la zone
Cet Assistant vous aidera à créer une zone de recherche directe principale.
- ☐ Un fournisseur de services Internet gère la zone, et une copie secondaire en lecture seule réside sur ce serveur
Cet Assistant vous aidera à créer une zone de recherche directe secondaire.

< Précédent

Suivant >

Annuler


Comme vous êtes en train de créer une zone privée, ce sera votre serveur qui assurera la maintenance de la zone. Ensuite le nom de la zone : il s'agit de **"bts-sio.cci"** dans le cas présent. Puis la création du fichier de zone (et son emplacement sur votre serveur). Arrive ensuite la question des mises à jour dynamiques.

Cette option est à prendre avec des pincettes, car elle permet à un client de mettre à jour des enregistrements. Mal configurée, cette option permettrait à un utilisateur malveillant de changer vos enregistrements pour les envoyer vers l'adresse IP d'un serveur qu'il gère, et pourrait mener à une campagne de fuite d'informations... Attention donc !

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

Ensuite, il vous est proposé de configurer des redirecteurs. Ce sont des serveurs DNS souvent publics qui interrogent les serveurs racines. Vous pourriez par exemple utiliser **one.one.one.one** (1.1.1.1) qui est un serveur DNS public de ce type, ou **google-public-dns-a.google.com** (8.8.8.8). Le premier est un service de **Cloudflare**, le second, de **Google**. Si vous entrez une adresse IP d'un serveur ne permettant pas ce fonctionnement, l'assistant vous le fera remarquer via l'icône à côté de l'adresse IP :

Redirecteurs

Les redirecteurs sont des serveurs DNS vers lesquels ce serveur envoie les requêtes auxquelles il ne peut pas répondre.



Ce serveur DNS doit-il rediriger des requêtes ?

☒ Oui, il doit rediriger les requêtes vers les serveurs DNS ayant les adresses IP suivantes :

Adresse IP	Nom de domaine complet du serveur
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>	
1.1.1.1	one.one.one.one
8.8.8.8	google-public-dns-a.google.com

Supprimer

Monter

Descendre

☐ Non, il ne doit pas rediriger les requêtes

Si ce serveur n'est pas configuré pour utiliser des redirecteurs, il peut toujours résoudre des noms en utilisant des serveurs de noms racines.

< Précédent

Suivant >

Annuler

Je vous propose de ne pas en configurer (ou de laisser tel que, avec 1.1.1.1 et 8.8.8.8).

Attention toutefois, il convient de maîtriser les flux au mieux, car les requêtes DNS permettent de savoir qui consulte quel site Internet et à quel moment, attention donc au respect de la vie privée !

Votre zone est créée, allez voir maintenant son contenu, en cliquant sur **Terminer** puis en dépliant **Zones de recherche directes** :

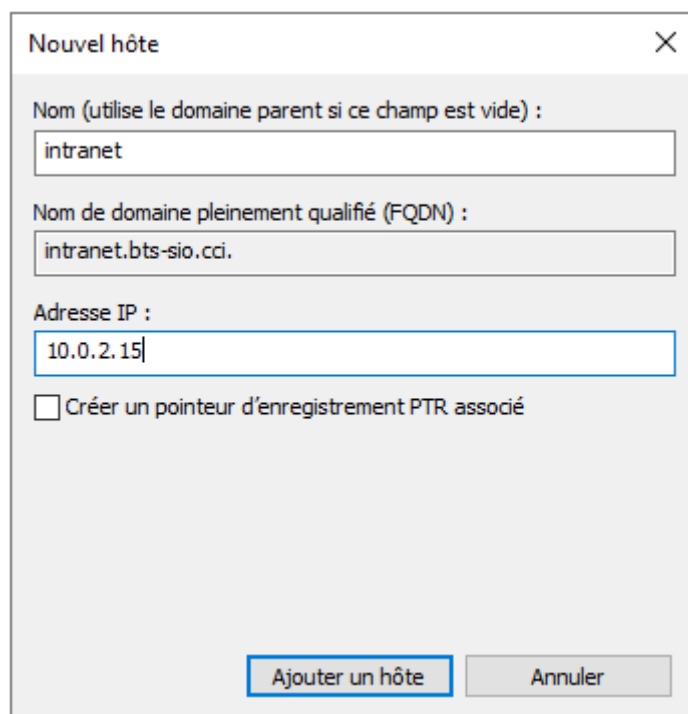
Gestionnaire DNS
Fichier Action Affichage ?

DNS
SRVDCLOCAL01
Zones de recherche directes
bts-sio.cci
Zones de recherche inversée
Points d'approbation
Redirecteurs conditionnels

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[6], srvdclocal01., hostmaster.
(identique au dossier parent)	Serveur de noms (NS)	srvdclocal01.

Votre zone ne contient que **deux enregistrements** qui permettent d'identifier le serveur faisant autorité (SOA), et le serveur de noms (NS). Il serait intéressant de créer votre enregistrement intranet demandé par la direction. Pour cela, un clic droit dans la fenêtre de droite (ou sur le nom de la zone) et sélectionnez **nouvel hôte A ou AAAA**. Les

enregistrements A sont pour les IPv4 et les AAAA pour les IPv6. Entrez **le nom de l'hôte** au sein de la zone ("intranet" donc) et **l'adresse IP** associée :



Vous avez ici la possibilité de créer un **PTR**, vous verrez cela dans la section suivante; ne cochez pas cette case et validez via **"Ajouter un hôte"**. Vous remarquerez le champ (non modifiable) du nom de domaine pleinement qualifié (*fully qualified domain name - FQDN*), il comporte un "point" à la fin qui représente la zone racine (root), suivi de l'extension "cci" puis du domaine "bts-sio". Le nom qualifié de l'intranet est donc *"intranet.bts-sio.cci"*

Pour vérifier que votre enregistrement est correctement créé, relancez une invite de commande et tapez la commande `nslookup intranet.bts-sio.cci 10.0.2.15` pour demander de quelle adresse IP dispose l'hôte *"intranet.bts-sio.cci"* au serveur 10.0.2.15 :

```
>nslookup intranet.bts-sio.cci 10.0.2.15
Serveur : Unknown
Address: 10.0.2.15

Nom : intranet.bts-sio.cci
Address: 10.0.2.10
```

Voilà, vous savez créer des enregistrements A sur une zone directe ! Vous allez pouvoir nommer tous vos équipements ou serveurs avec des noms et arrêter d'utiliser les adresses IP.

1.5. Découvrez les autres types d'enregistrements

Avant de passer à la zone inversée, je vous propose de voir quelques éléments supplémentaires. Le DNS permet de répondre à une requête d'un client, le type A permet de demander une adresse IP à partir d'un nom, mais de nombreux autres types sont disponibles, comme NS qui permet de connaître le serveur de noms. Sous Windows, vous pouvez effectuer des requêtes sur différents types avec l'option `set type=XXX`, où XXX est le type demandé.

Un autre type est le SOA (Start Of Authority), permettant de savoir quel serveur fait autorité sur une zone.

```
>nslookup - 10.0.2.15
Serveur par défaut : UnKnown
Address: 10.0.2.15

>set type=SOA
>bts-sio.cci
Serveur : UnKnown
Address: 10.0.2.15
bts-sio.cci
primary name server = srvclocal01
responsible mail addr = hostmaster
serial = 3
refresh = 900 (15 mins)
retry = 600 (10 mins)
expire = 86400 (1 day)
default TTL = 3600 (1 hour)

>set type=NS
>bts-sio.cci
Serveur : UnKnown
Address: 10.0.2.15

bts-sio.cci nameserver = srvclocal01
```

Un autre type est le **CNAME** qui permet d'associer un nom à un nom.

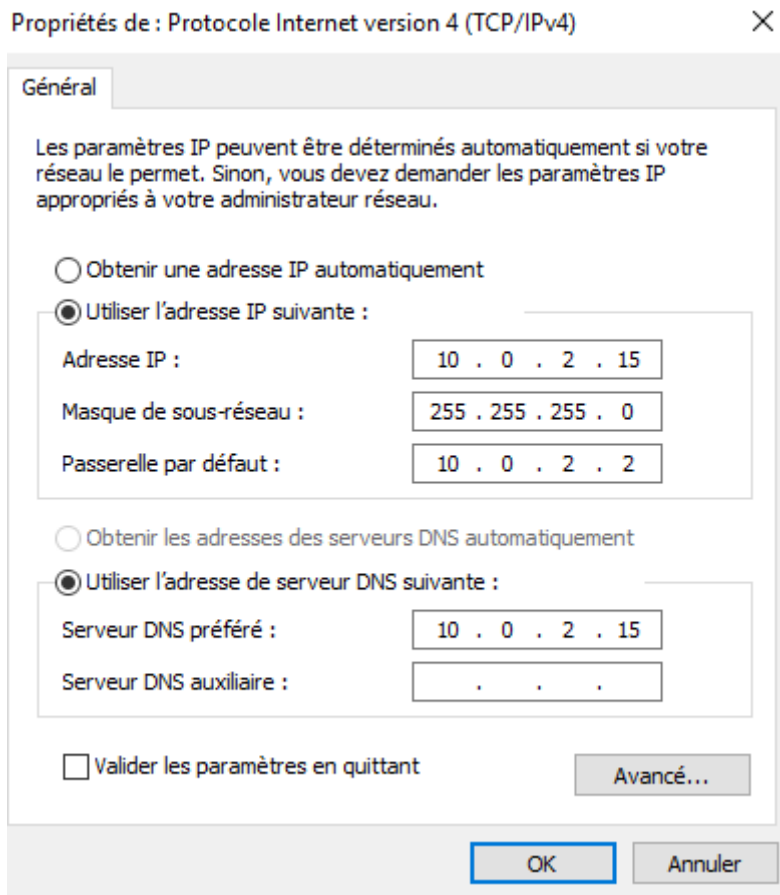
Cela peut être pratique pour donner un nom à un serveur en pointant sur le nom du service. Par exemple, cela peut être intéressant d'avoir un nom différent pour administrer l'intranet, mais il peut être long de taper "intranet.bts-sio.cci" lorsque l'on administre ce service. Alors un **CNAME** "int.bts-sio.cci" pointant sur intranet.bts-sio.cci permet de résoudre ce problème :

```
>set type=CNAME
>int.bts-sio.cci
Serveur : UnKnown
Address: 10.0.2.15
int.bts-sio.cci canonical name = intranet
```

Il existe de nombreux types, les plus connus étant **NS**, **SOA**, **A**, **AAAA**, **CNAME**, **TXT**, **MX** (Mail eXchange pour les serveurs de messagerie). La méthode à mettre en œuvre est la même, quel que soit le type.

1.6. Mettez en oeuvre votre première zone inversée

Maintenant que vous disposez d'une zone directe, ne serait-ce pas intéressant de créer une zone inversée ? C'est une association d'une **adresse IP à un nom**, en somme l'inverse de la zone directe. Cela permet de confirmer que le nom choisi dans une zone directe est bien associé à l'adresse IP, et donc d'interroger un DNS sur une adresse IP, si vous changez l'adresse du serveur DNS configuré sur votre serveur DNS, ici, dans la zone Serveur DNS préféré :



Toutes les requêtes de nom seront alors envoyées à votre serveur. Ouvrez alors une invite de commande et tapez ping intranet.bts-sio.cci :

```
C:\Users\Administrateur>ping intranet.bts-sio.cci
Envoi d'une requête 'ping' sur intranet.bts-sio.cci [10.0.2.10] avec 32 octets de données :
```

```
C:\Users\Administrateur>ping 10.0.2.10
Envoi d'une requête 'ping' 10.0.2.10 avec 32 octets de données :
```

Le nom **intranet.bts-sio.cci** est bien résolu (par la zone directe) en 10.0.2.10 mais l'inverse ne se fait pas ! Il vous faut créer une zone inversée.

Pour cela, rendez-vous sur le Gestionnaire DNS et avec un clic droit sur la partie "zone inversée", sélectionnez "**Nouvelle zone**"; après l'écran d'accueil vous devriez arriver sur l'écran suivant :

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

Là encore, vous disposez de différents types de zones en fonction du niveau de maîtrise que vous souhaitez. Nous n'aborderons ici que le type principal. L'écran suivant vous propose de choisir entre IPv4 et v6.

Idem, **ici restez sur IPv4**. Ensuite, vous n'avez plus qu'à entrer l'ID de votre réseau. Il s'agit des octets de l'adresse IP représentant votre réseau et enfin, le nom du fichier de zone vous sera proposé et à nouveau la mise à jour dynamique (idem, on refusera les mises à jour dynamiques) :

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 :

10 . 0 . 2 .

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 :

2.0.10.in-addr.arpa

< Précédent

Suivant >

Annuler

Fin de l'Assistant Nouvelle zone

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

Nom : 2.0.10.in-addr.arpa

Type : Zone principale standard

Type de recherche : Inversée

Nom de fichier : 2.0.10.in-addr.arpa.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

De la même façon que pour une zone directe, vous n'avez que deux enregistrements par défaut :

DNS	Nom	Type	Données
SRVDCLOCAL01	(identique au dossier parent)	Source de nom (SOA)	[1], srvdclocal01., hostmaster.
Zones de recherche directes	(identique au dossier parent)	Serveur de noms (NS)	srvdclocal01.
bts-sio.cci			
Zones de recherche inversée			
2.0.10.in-addr.arpa			
Points d'approbation			
Redirecteurs conditionnels			

Ajoutez un enregistrement de type **PTR** pour *intranet.bts-sio.cci* (vous pouvez parcourir votre zone directe avec l'assistant de création d'enregistrement PTR pour être certain de pointer vers le bon nom !). **Entrez l'adresse IP** (enfin, juste le dernier octet) et vous obtenez votre premier enregistrement :

DNS	Nom	Type	Données
SRVDCLOCAL01	(identique au dossier parent)	Source de nom (SOA)	[1], srvdclocal01., hostmaster.
Zones de recherche directes	(identique au dossier parent)	Serveur de noms (NS)	srvdclocal01.
bts-sio.cci			
Zones de recherche inversée			
2.0.10.in-addr.arpa			
Points d'approbation			
Redirecteurs conditionnels			

Pour tester la résolution de ce type avec un ping, ajoutez -a à votre ligne de commande.

```
C:\Users\Administrateur>ping -a 10.0.2.10
Envoi d'une requête 'ping' sur intranet.bts-sio.cci [10.0.2.10] avec 32 octets de données :
```

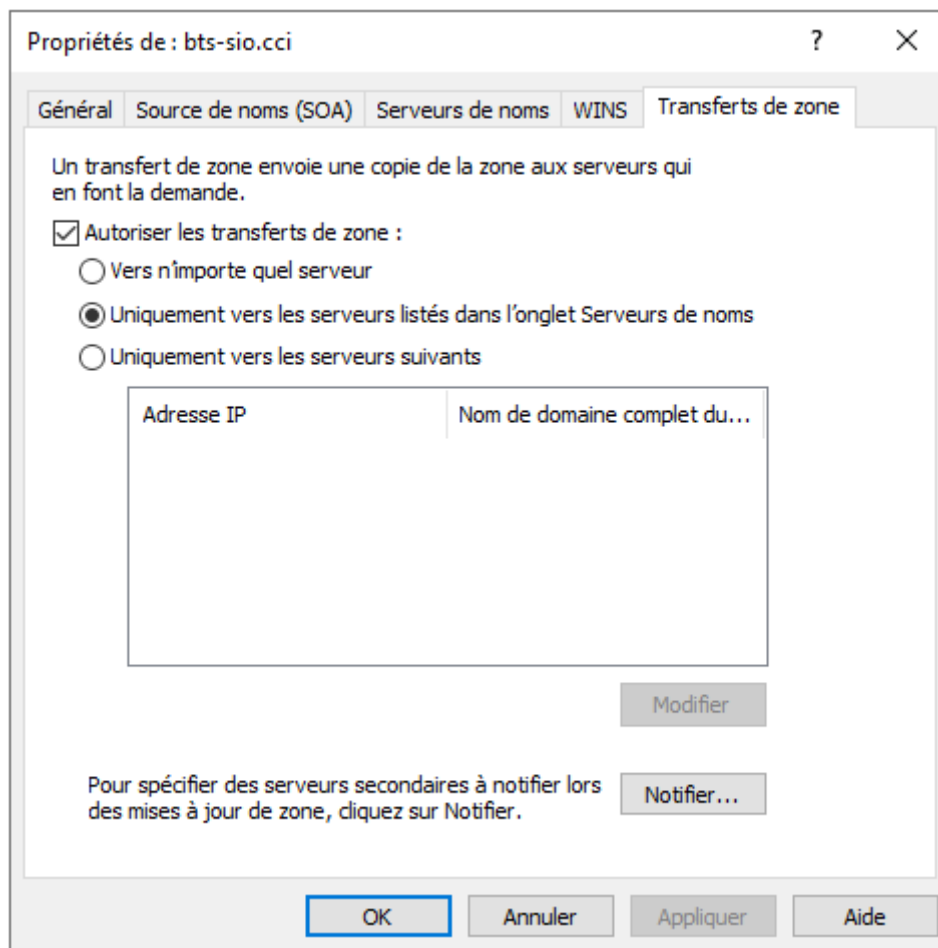
Voilà, vous avez maintenant un serveur DNS configuré pour simplifier la gestion du réseau de votre entreprise BTS-SIO S.A.

1.7. Une dernière chose

Avant de vous laisser configurer d'autres rôles, il reste quelques configurations à mettre en œuvre. La première est **le transfert de zone**. Cette fonctionnalité est intéressante dans le cas où vous avez plusieurs serveurs pour une même zone (ce qui est une bonne chose), mais peut se montrer **dangereux** si vous exposez votre serveur DNS publiquement.

Un transfert de zone contient tous les enregistrements d'une zone et permet donc de retrouver facilement toutes les adresses IP de vos équipements, un attaquant pourrait s'en servir contre vous.

Pour cela, faites un clic droit sur le nom de votre zone, allez dans l'onglet "**Transfert de zone**" et refusez les transferts, ou listez les serveurs **de confiance** que vous allez **autoriser** à récupérer vos enregistrements ! Une bonne pratique consiste également à journaliser toutes les transactions DNS, vous verrez en détail dans les cours concernant la surveillance d'un système :



Enfin, vous pouvez lancer le **BPA** de Microsoft sur ce rôle, pour vous assurer que votre configuration respecte les bonnes pratiques de Microsoft.

N'oubliez pas d'autoriser le port **UDP 53** sur votre pare-feu, sinon votre serveur DNS ne sera pas accessible sur le réseau ; rappelez-vous, vous avez activé le pare-feu pour bloquer tous les flux n'étant pas couverts par une règle de flux entrant !

1.8. En résumé

- Le rôle DNS de Windows Server permet de créer des **zones directes et inversées** ;
- Le serveur DNS permet de **résoudre des noms en adresses IP et des adresses IP en noms** ;
- Le **transfert de zone** doit être **restreint aux serveurs de confiance** uniquement ;
- Un serveur DNS s'**interroge** à l'aide de la commande **nslookup** ou via les navigateurs web (entre autres).