



Domaine Name System (DNS)

Le 3/02/2021

PARIS Jean

MAILLARD Rémy

Sommaire

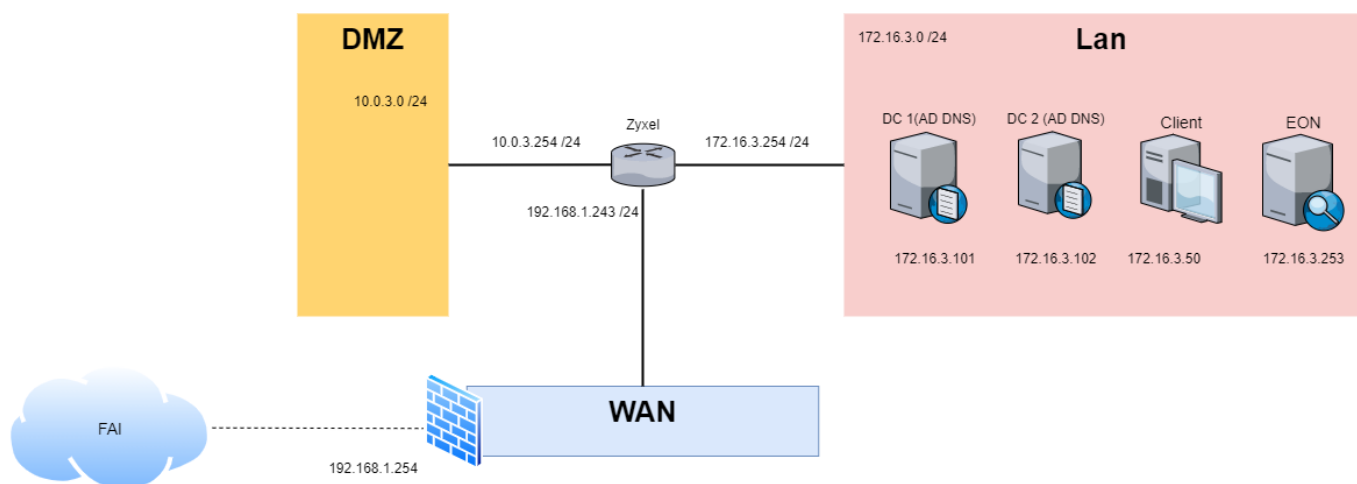
Explication

Test

Table des matières

Visio de l'infrastructure (mission 3)	2
I] DNS :.....	3
Le rôle principal du DNS :	3
L'intérêt de mettre en place le service DNS	3
II] Installation / Configuration	4
Installation :	4
Configuration :	5
Redondance DNS	5
Redirection DNS :	11
III] Tests	14

Visio de l'infrastructure (mission 3)



I] DNS :

Le rôle principal du DNS :

Le DNS est un service permettant de faire de la « résolution de noms » : traduire une adresse ip en nom de domaine. Quand on fait une recherche comme google par exemple, on cherche par le biais du nom de domaine google.com et non par son adresse IP car cela est plus facile pour l'être humain d'utiliser des mots et de laisser un service faire le lien : google.com = X.X.X.X

L'intérêt de mettre en place le service DNS

Les différents intérêts :

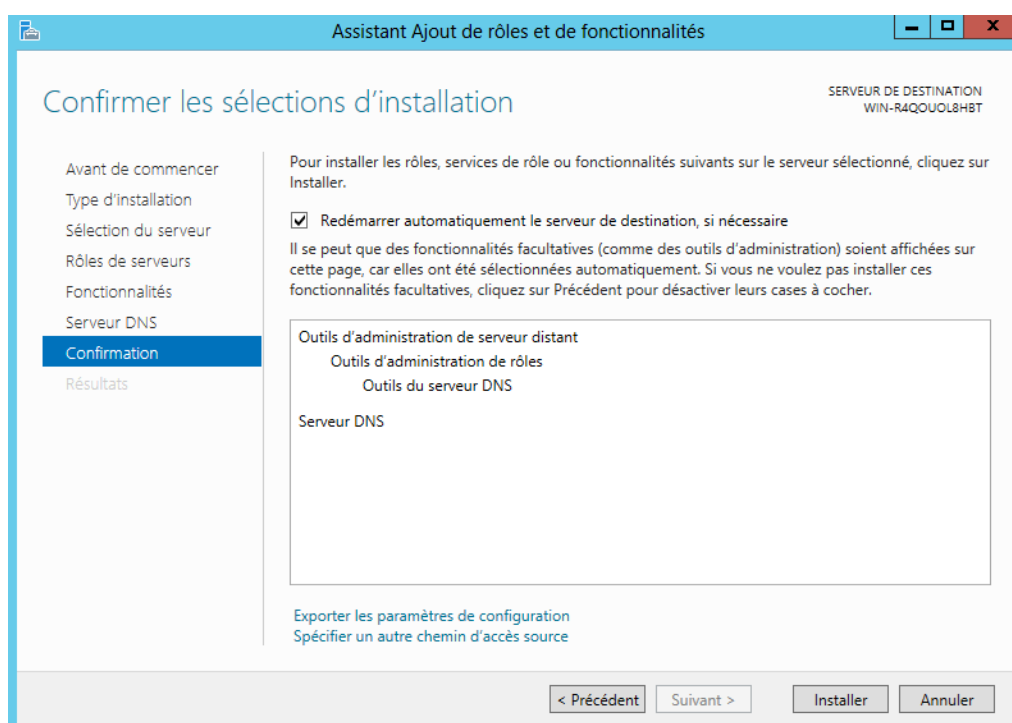
- Il est un des piliers dans une architecture réseau, beaucoup de services s'appuient sur lui comme Active Directory et bien d'autres
- Proposer un service de résolution de noms (présenté juste au dessus)
- Sécuriser un réseau

II] Installation / Configuration

Installation :

Tuto expliquant l'installation du service DNS sur un Windows server :

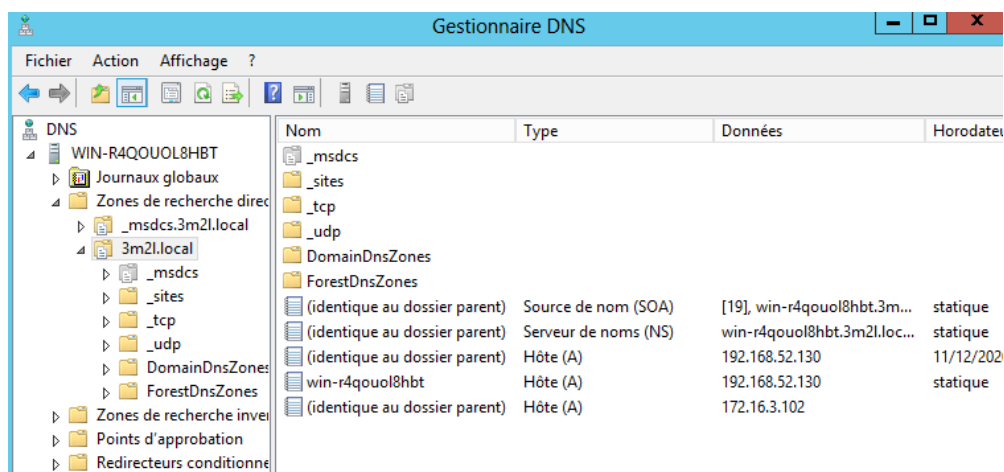
<http://www.lesysadmin.com/windows-server-2012-installer-un-serveur-contrôleur-de-domaine-active-directory-et-configurer-un-serveur-dns-sous-windows-server-2012/>



Configuration :

Une fois la création du domaine effectuée nous allons pouvoir rajouter nos enregistrements (A) dans le gestionnaire DNS. Des exemples d'enregistrements :

- L'enregistrement **A** permet de lier un hôte avec son adresse ipv4
- L'enregistrement **AAAA** permet de lier un hôte avec son adresse ipv6
- L'enregistrement **CNAME** permet de faire un alias
- L'enregistrement **MX** permet de mettre un nom de domaine à un serveur de messagerie



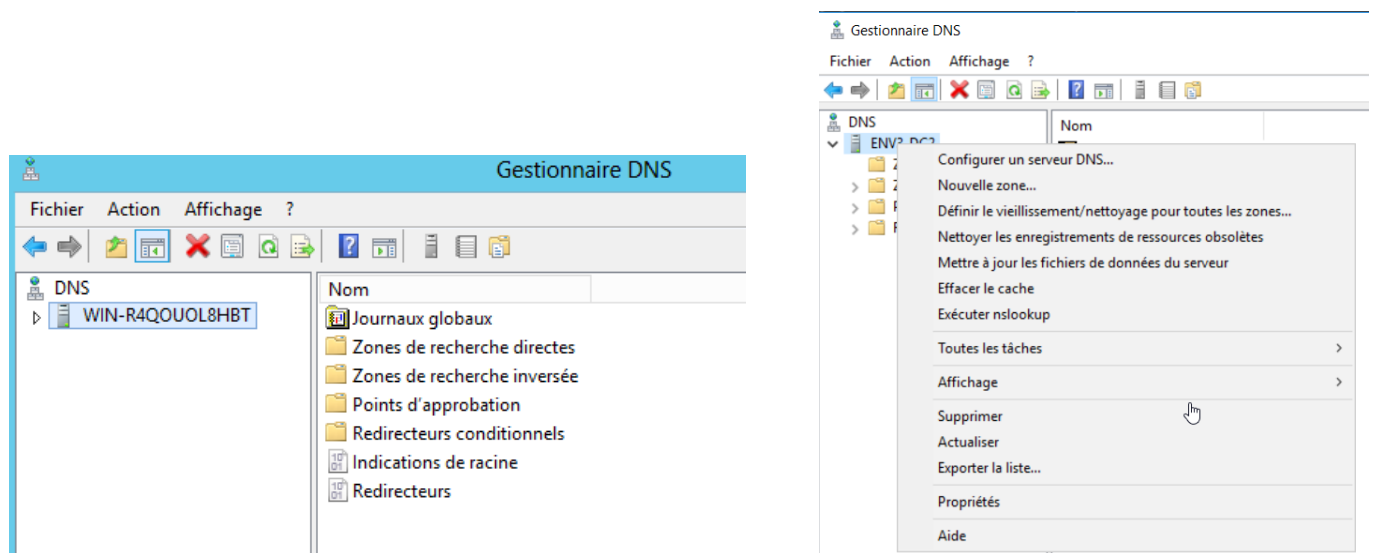
The screenshot shows the 'Gestionnaire DNS' window. The left pane displays the tree structure under 'DNS' > 'WIN-R4QOUOL8HBT' > 'Zones de recherche directes' > '3m2l.local'. The right pane shows the list of DNS records for this zone.

Nom	Type	Données	Horodatage
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[19], win-r4qouol8hbt.3m...	statique
(identique au dossier parent)	Serveur de noms (NS)	win-r4qouol8hbt.3m2l.loc...	statique
(identique au dossier parent)	Hôte (A)	192.168.52.130	11/12/2020
win-r4qouol8hbt	Hôte (A)	192.168.52.130	statique
(identique au dossier parent)	Hôte (A)	172.16.3.102	

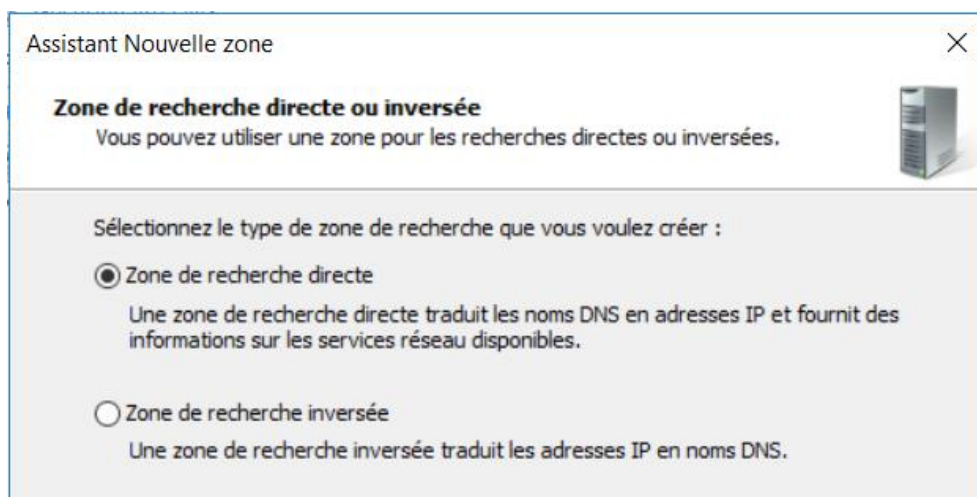
Redondance DNS

L'intérêt de redonder notre DNS sur notre DC2 est que celui-ci aura une copie de la zone primaire se trouvant sur le DC1. Ainsi comme il a une zone secondaire il ne pourra pas modifier la zone mais il pourra quand même faire de la résolution de noms.

Après avoir installé le service DNS sur le DC2 on rajoute dans notre zone directe, une nouvelle zone secondaire.



On rajoute dans la zone de recherche directe car on veut traduire les noms de domaine en @IP et non l'inverse comme le propose la zone de recherche inversée. Ex : `www.google.com` → @ip



Comme énoncé auparavant, on va rajouter une zone secondaire car on veut une copie d'une zone déjà existante se trouvant sur le DC1 en 172.16.3.101

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)

On indique le nom de la zone vers laquelle le DC2 doit pointer → 3m2l.local qui est notre nom de domaine racine et le serveur DNS maître → DC1(172.16.3.101) pour que le DC2 comprenne ce qu'il doit transférer et à qui.

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 :

3m2l.local

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 :

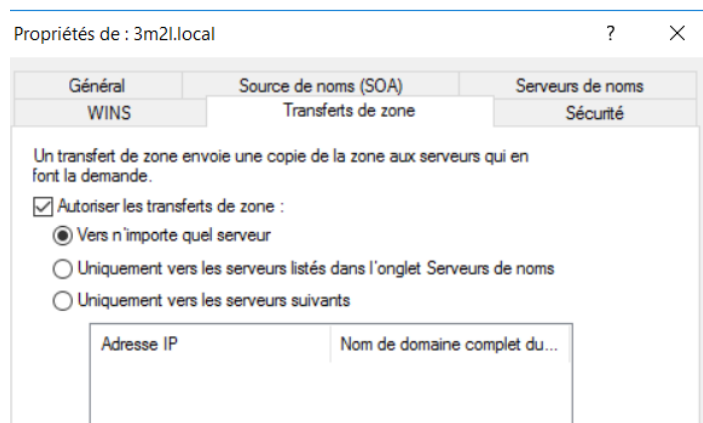
Adresse IP	Nom de domaine ...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
✓ 172.16.3.101	<Tentative de ré...	OK

Supprimer

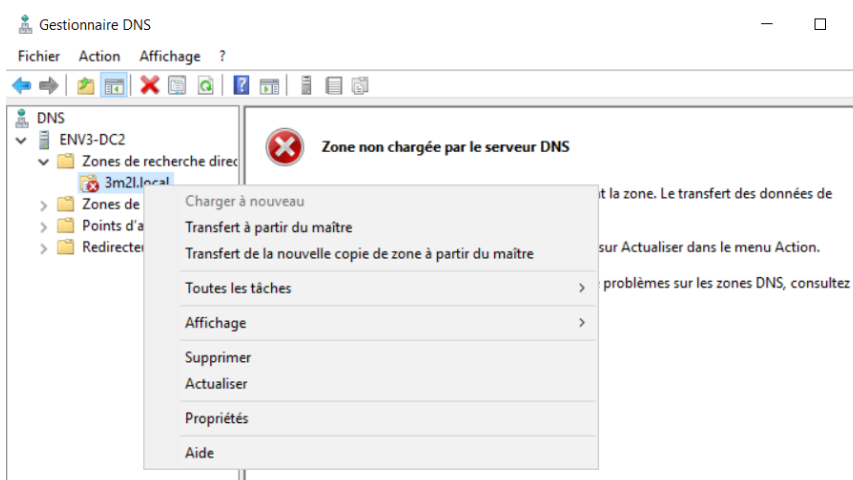
Monter

Descendre

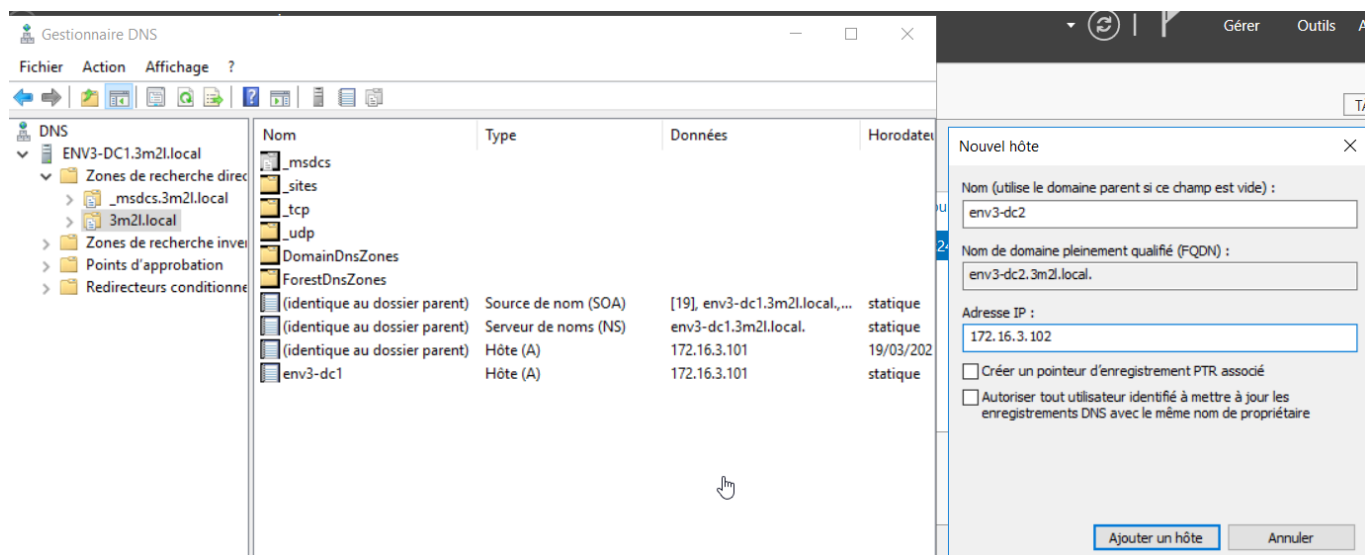
Une fois la zone créée, pour la récupérer depuis le maître il faut d'abord autoriser le transfert de zone. On peut choisir entre tous les serveurs présents sur le réseau ou les serveurs spécifiques qu'il faudra renseigner dans ce même onglet ou dans l'onglet serveurs de noms.



Maintenant que notre zone secondaire est créée et qu'on a autorisé le transfert, nous pouvons transférer à partir du maître (DC1 : 172.16.3.101).



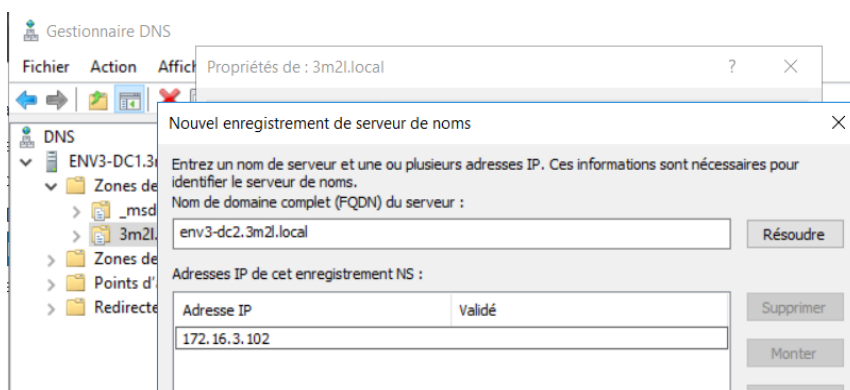
Le DC2 est maintenant capable de traduire des noms de domaine. Cependant il faut compléter la zone, on peut remarquer que l'enregistrement A et SN du DC1 est inscrit dans la zone mais qu'il manque l'enregistrement A et SN du DC2 qu'il faut donc rajouter afin de pouvoir traduire le nom de domaine env3-dc2.3m2l.local. en 172.16.3.102



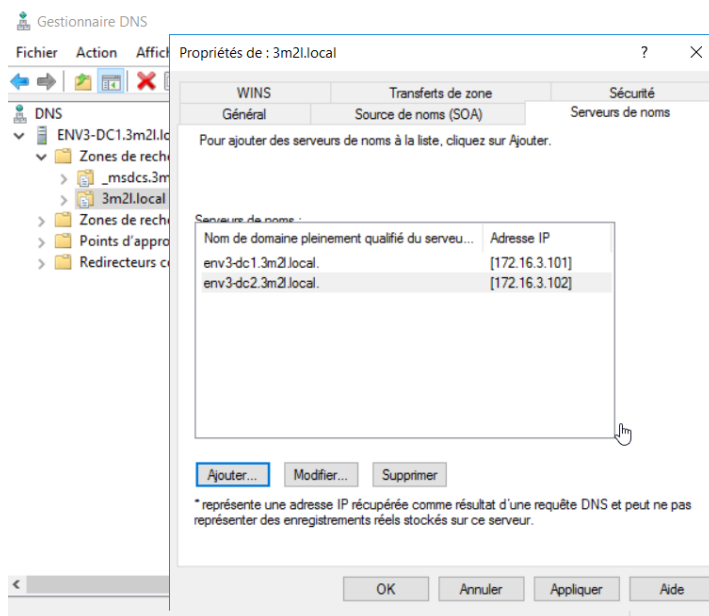
Nom	Type	Données	Horodate
(identique au dossier parent)	Source de nom (SOA)	[19], env3-dc1.3m2l.local.,...	statique
(identique au dossier parent)	Serveur de noms (NS)	env3-dc1.3m2l.local.	statique
(identique au dossier parent)	Hôte (A)	172.16.3.101	19/03/202
env3-dc1	Hôte (A)	172.16.3.101	statique

L'enregistrement A (@ipV4) du DC2 est maintenant implanté dans la zone. La résolution de nom du DC2 est possible.

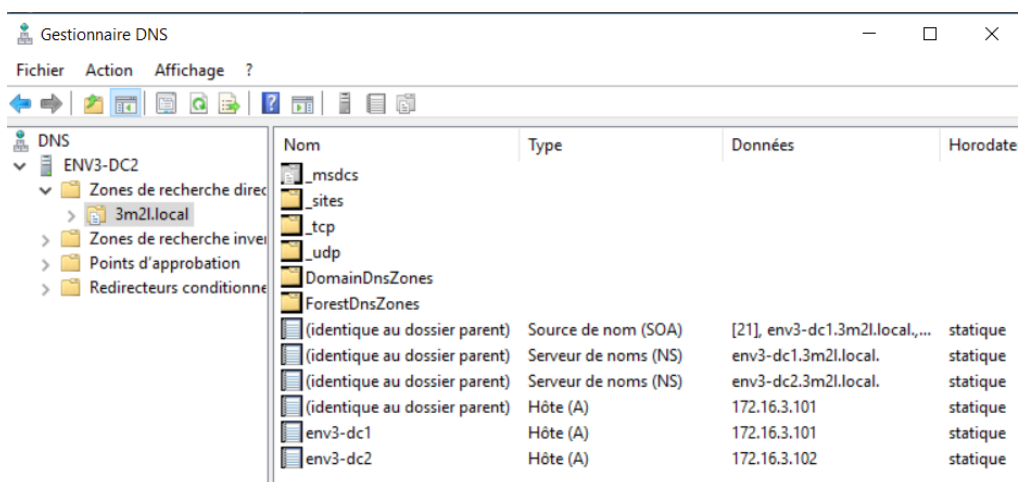
La logique reste la même que l'enregistrement A : on traduit le nom de domaine en @IP mais cette fois ci comme serveur de nom. L'enregistrement SN indique quel serveur de nom fait autorité sur le domaine.



Adresse IP	Validé
172.16.3.102	



Le résultat que nous devons obtenir doit être celui-ci. On revoit bien les enregistrements A et SN du DC1 et DC2.

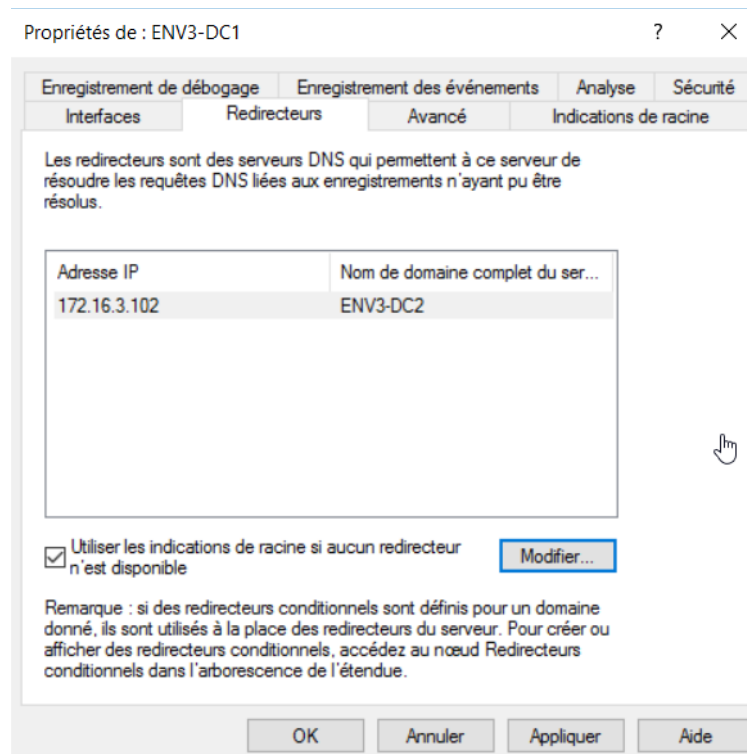


Redirection DNS :

Afin de sécuriser notre architecture nous mettons en place de la tolérance de panne. Celle-ci se met en place à l'aide de la configuration IP ainsi que des redirecteurs DNS. Le DNS préféré est le premier nécessité en tant que DNS, si celui-ci ne répond pas ou ne peut pas répondre à la demande, c'est le DNS du DC2 qui est à son tour interrogé par le biais du redirecteur. Si celui-ci n'est pas capable à son tour de répondre, le DNS secondaire dans la configuration IP prend le relais en dernier recours.

Dans le cas de notre architecture il y a 3 configurations de redondance possible que voici :

(les schémas représentent la redondance dans le cas où les 2 serveurs web sont indisponibles ou qu'ils n'ont pas la réponse)



- La configuration IP du DC1 :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 3 . 101

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 172 . 16 . 3 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

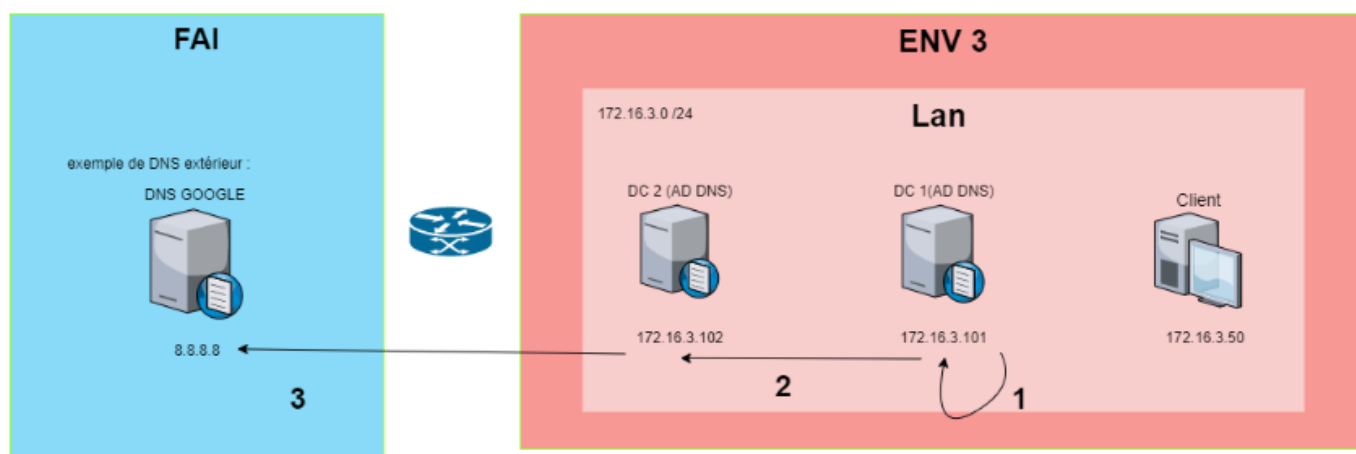
Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : 8 . 8 . 8 . 8

☐ Valider les paramètres en quittant

Avancé...

OK Annuler



- La configuration IP du DC2 et du client :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 172 . 16 . 3 . 102

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 172 . 16 . 3 . 254

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 172 . 16 . 3 . 101

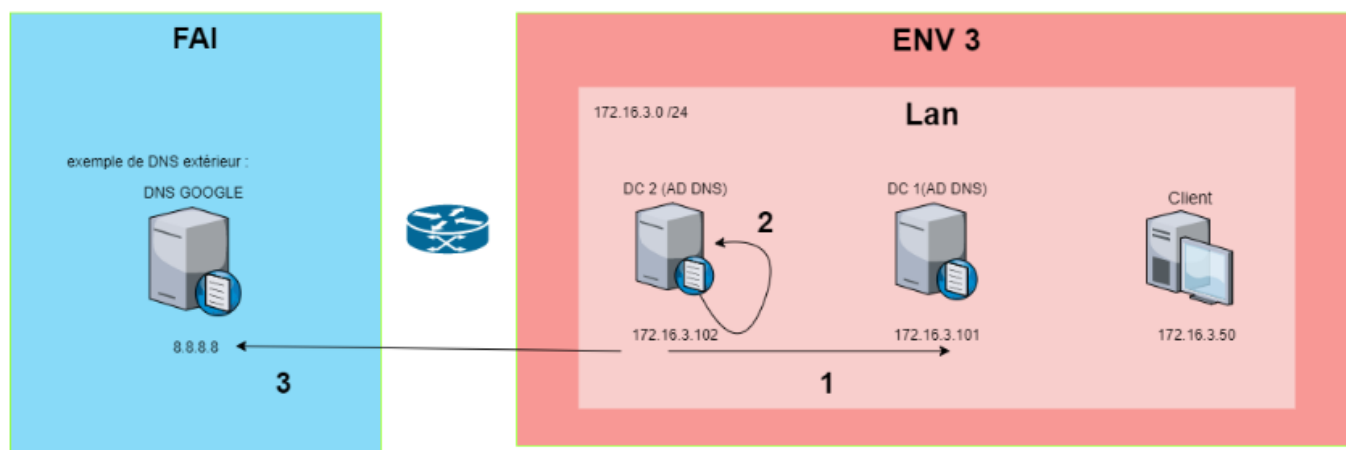
Serveur DNS auxiliaire : 8 . 8 . 8 . 8

☐ Valider les paramètres en quittant

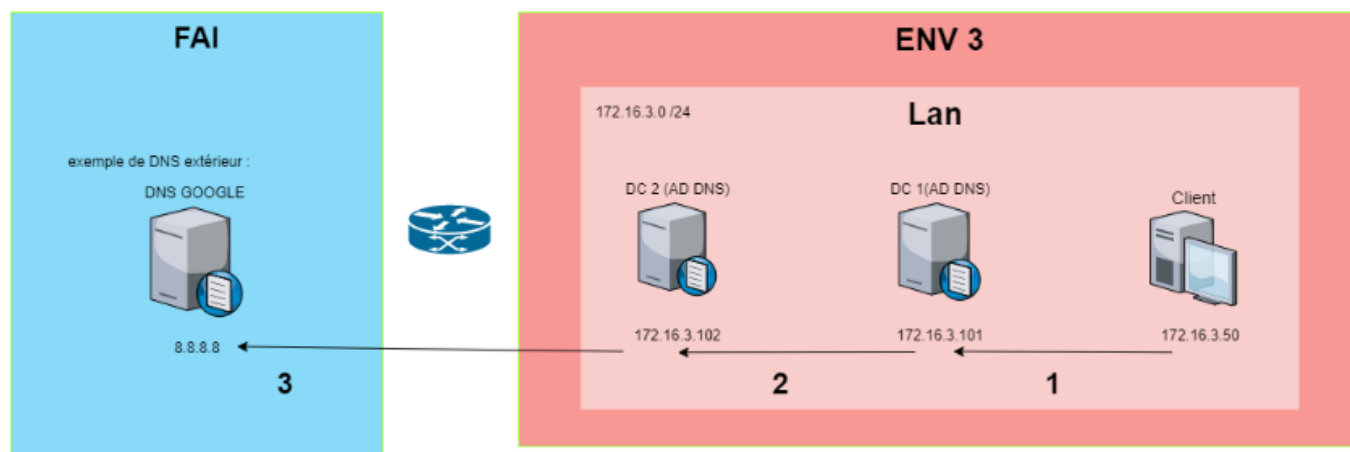
Avancé...

OK Annuler

- Le DC2 :



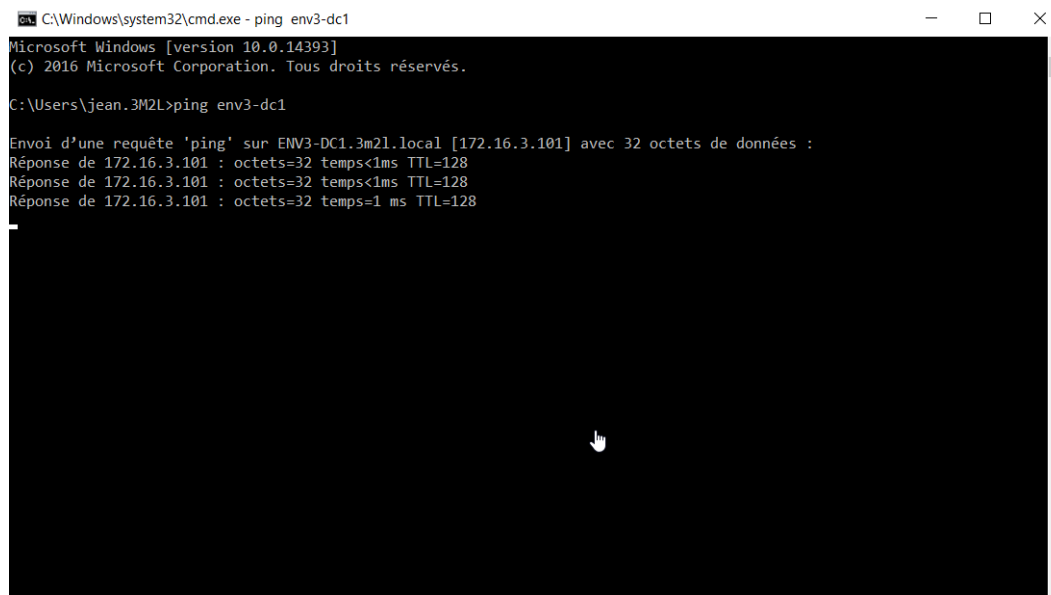
- Les machines clientes :



III] Tests

Pour vérifier si notre service est bien configuré, on peut tester de ping l'autre Domain Controller non pas par l'@IP mais par le nom de domaine pour vérifier si la résolution de nom s'effectue bien :

- Du DC2 vers le DC1 DNS primaire : 127.0.0.1

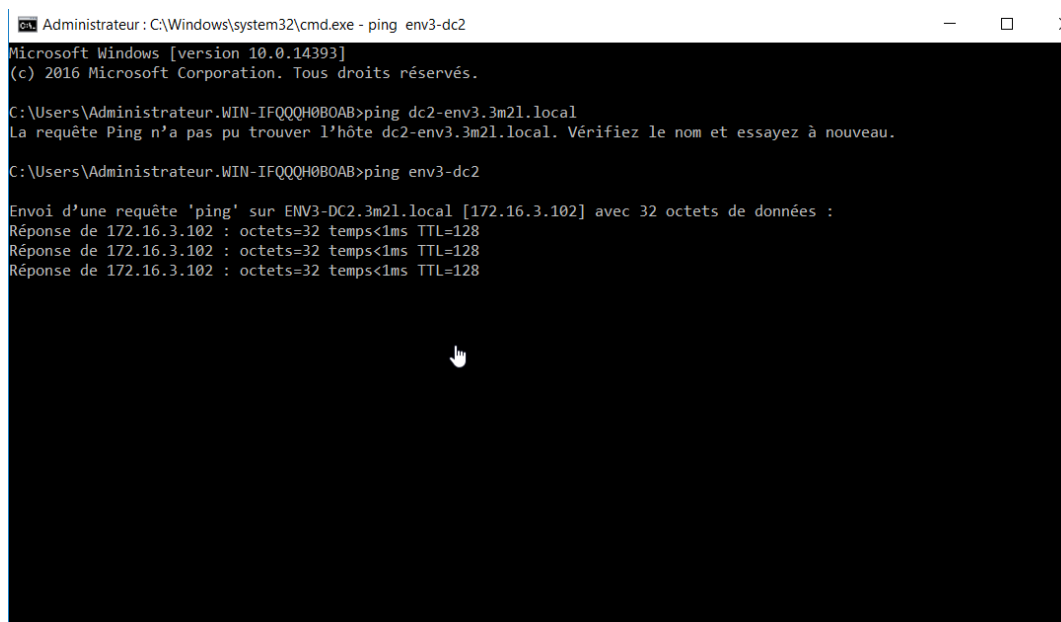


```
C:\Windows\system32\cmd.exe - ping env3-dc1
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\jean.3M2L>ping env3-dc1

Envoi d'une requête 'ping' sur ENV3-DC1.3m2l.local [172.16.3.101] avec 32 octets de données :
Réponse de 172.16.3.101 : octets=32 temps<1ms TTL=128
Réponse de 172.16.3.101 : octets=32 temps<1ms TTL=128
Réponse de 172.16.3.101 : octets=32 temps=1 ms TTL=128
```

- Du DC1 vers le DC2 DNS primaire : 127.0.0.1



```
Administrateur : C:\Windows\system32\cmd.exe - ping env3-dc2
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.WIN-IFQQQH0B0AB>ping dc2-env3.3m2l.local
La requête Ping n'a pas pu trouver l'hôte dc2-env3.3m2l.local. Vérifiez le nom et essayez à nouveau.

C:\Users\Administrateur.WIN-IFQQQH0B0AB>ping env3-dc2

Envoi d'une requête 'ping' sur ENV3-DC2.3m2l.local [172.16.3.102] avec 32 octets de données :
Réponse de 172.16.3.102 : octets=32 temps<1ms TTL=128
Réponse de 172.16.3.102 : octets=32 temps<1ms TTL=128
Réponse de 172.16.3.102 : octets=32 temps<1ms TTL=128
```

On peut vérifier que la résolution de nom s'effectue bien, en testant de ping le domaine sur les 2 DC. On peut conclure que nos DC accèdent bien à la zone et que celle-ci est bien configurée.