Tuto – Le service DNS

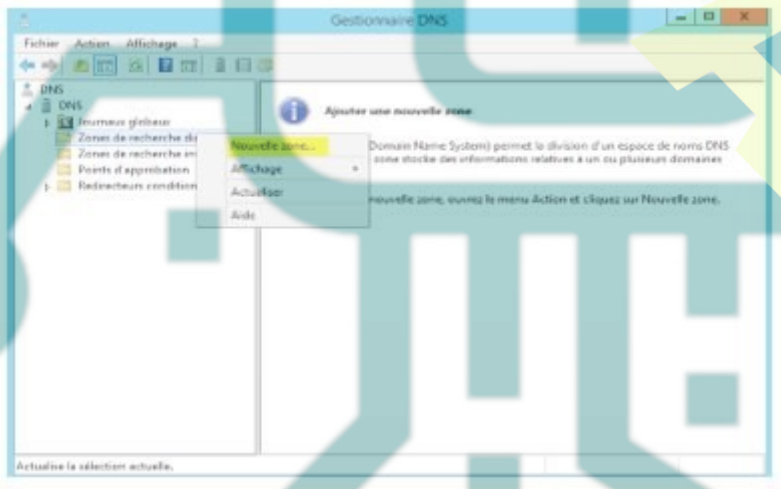
DNS – WINDOWS

Installation

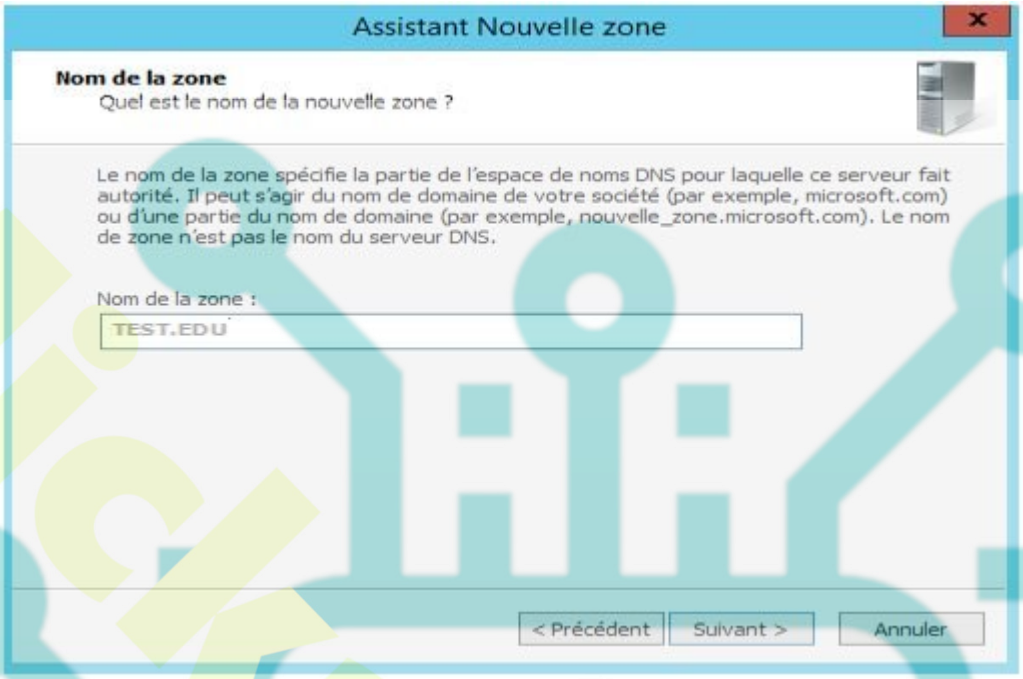
1. Aller dans le **Gestionnaire de serveur** et **Ajouter des rôles et des fonctionnalités.**
2. Sélectionner le serveur sur lequel installer le service.
3. Cocher **serveur DNS** dans la liste puis Suivant.
4. Cliquer sur **Suivant** plusieurs fois pour terminer l'installation.

Création d'une zone principale

1. Ouvrir le gestionnaire DNS dans les outils d'administration.
2. Cliquer avec le bouton droit sur **Zones de recherche directe**s et cliquer sur **nouvelle zone**.



3. Choisir **Zone principale** et cliquer sur Suivant et donner un nom à votre zone



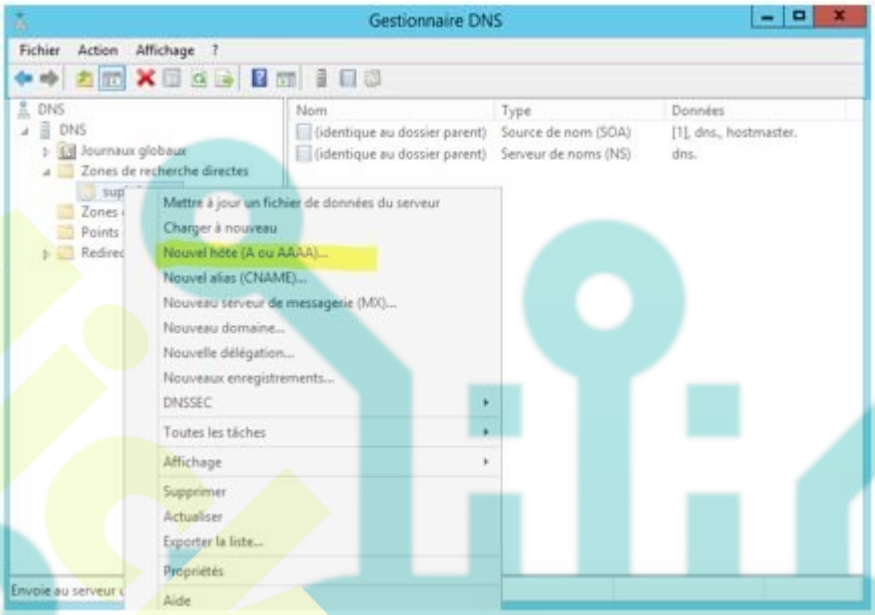
4. Puis créer le fichier de zone (pour des raisons de compatibilité)

NB. Sur la page suivante, vous pouvez choisir d'utiliser les MAJ dynamiques ou non. Si l'on choisit dynamique, cela permet aux clients DNS de s'inscrire automatiquement auprès du serveur (obligatoire dans un domaine AD mais choisir l'option sécurisées) **Pour le tuto on ne les active pas.**

Une boite de dialogue de résumé s'affiche et l'installation est terminée

Enregistrement DNS

1. Dans le gestionnaire DNS, choisir **nouvel hôte**

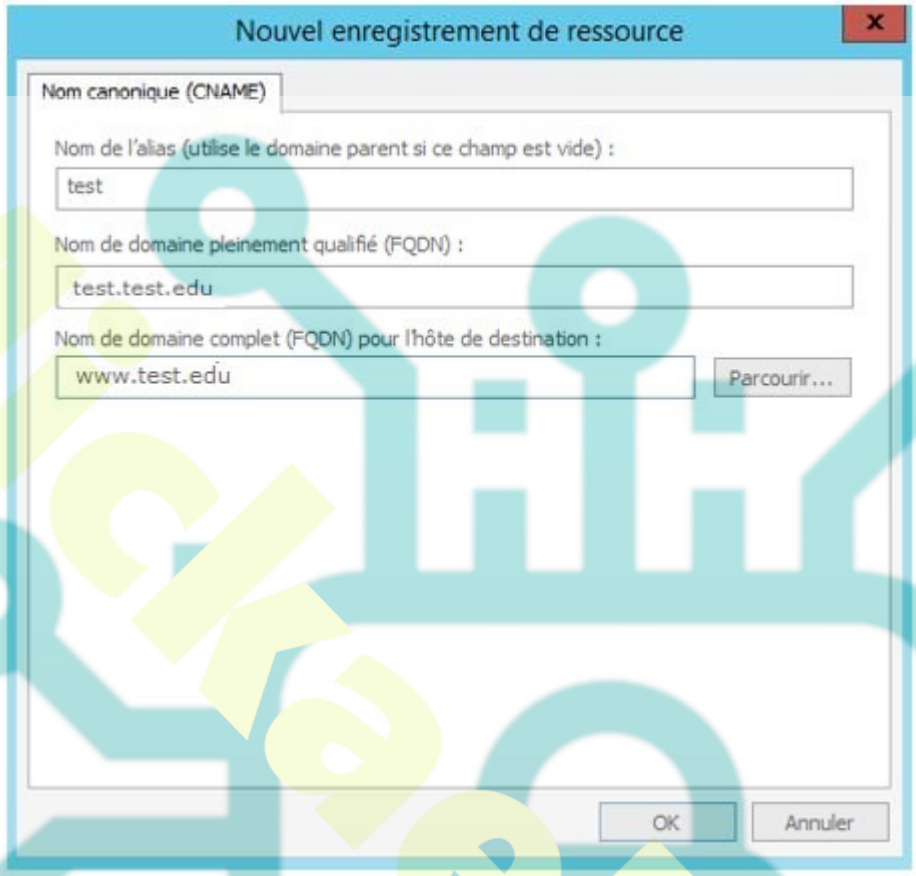


2. Renseigner le **nom de la machine et son adresse IP** et cliquer sur **Ajouter un hôte**

Faire autant d'enregistrements que nécessaire puis tester les nouveaux enregistrements par la commande PING.

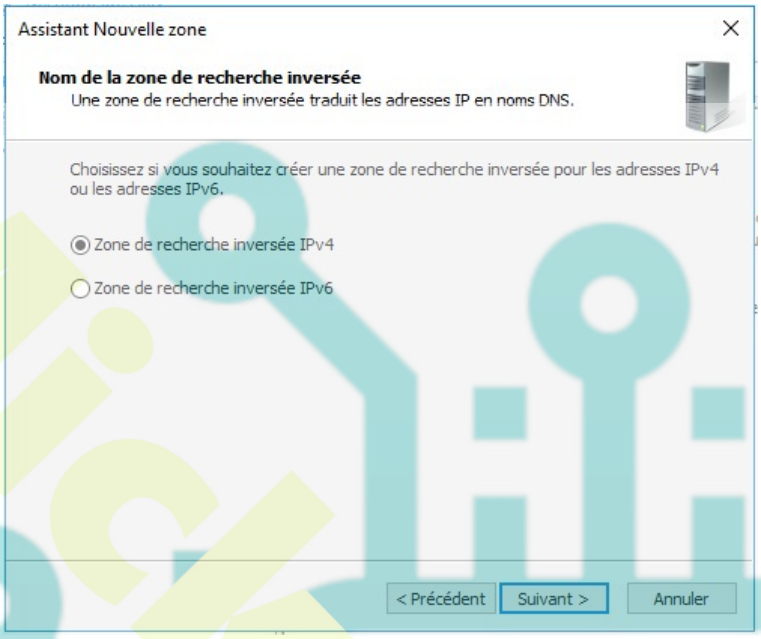
Créer un alias (CNAME)

Notre alias sera test et nom de domaine complet sera www.test.edu cela permettra de contacter www.test.edu avec le nom test.test.edu.

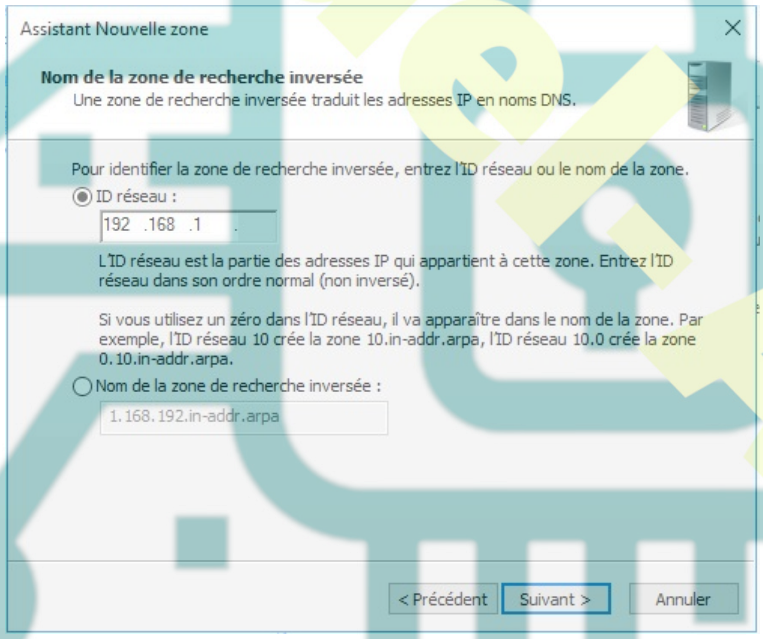


Créer une zone de recherche inversée

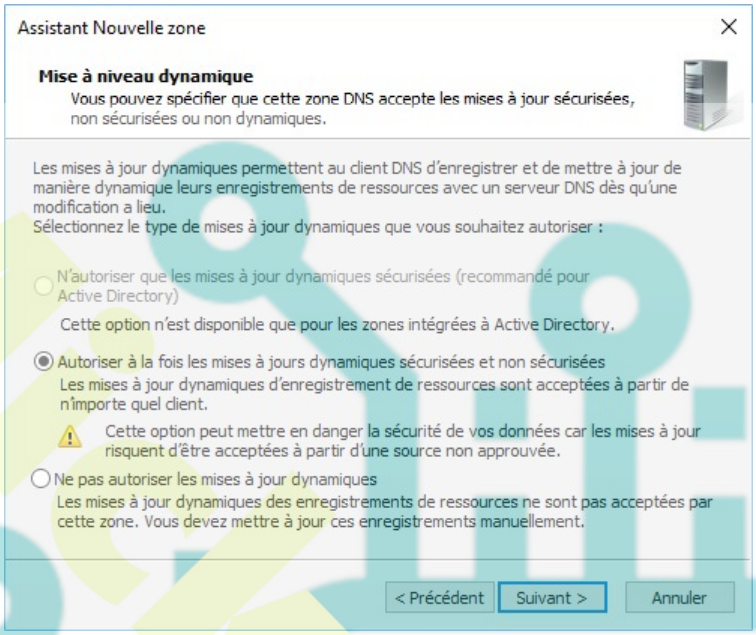
1. Ouvrir le gestionnaire DNS dans les outils d'administration.
2. Cliquer avec le bouton droit sur **Zones de recherche directes** et cliquer sur Nouvelle zone Sélectionnez **Zone principale**. Cliquez sur suivant.
3. Choisir **Zone de recherche inversée**.



4. Indiquer l'adresse IP de votre réseau 192.168.1

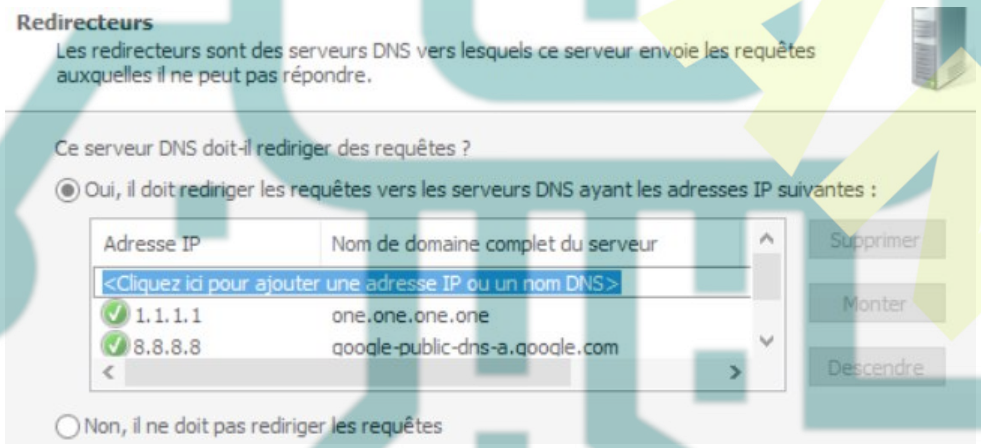


Sélectionner "Créer un nouveau fichier nommé:". Le champ devrait être prérempli si ce n'est pas le cas saisir **1.168.192.in-addr.arpa.dns**



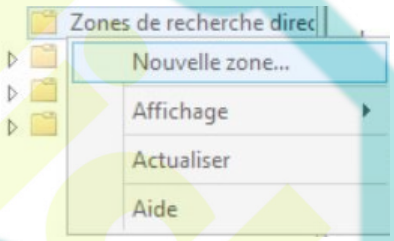
Mettre en œuvre un redirecteur

1. Ouvrir la console DNS et faire un clic droit sur le nom du serveur puis cliquer sur **Propriétés**.
2. Aller sur l'onglet Redirecteurs puis cliquer sur le bouton **Modifier**.
3. Entrer l'adresse IP du serveur DNS google 8.8.8.8 et celui de one.one.one.one 1.1.1.1 puis valider.
5. Cliquer sur **Appliquer** et OK pour fermer les propriétés du serveur.

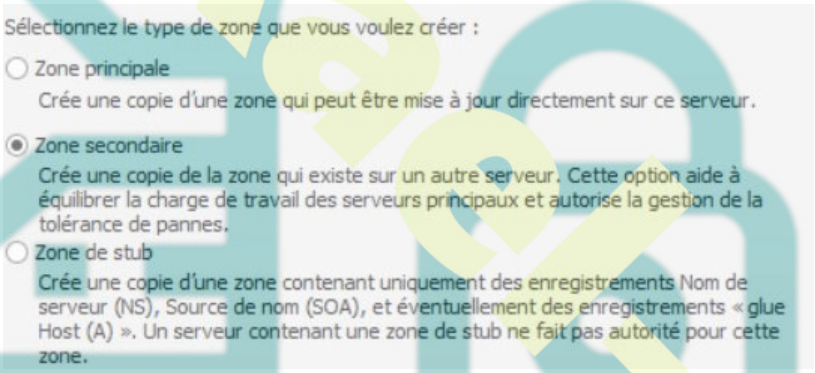


Installer un DNS secondaire

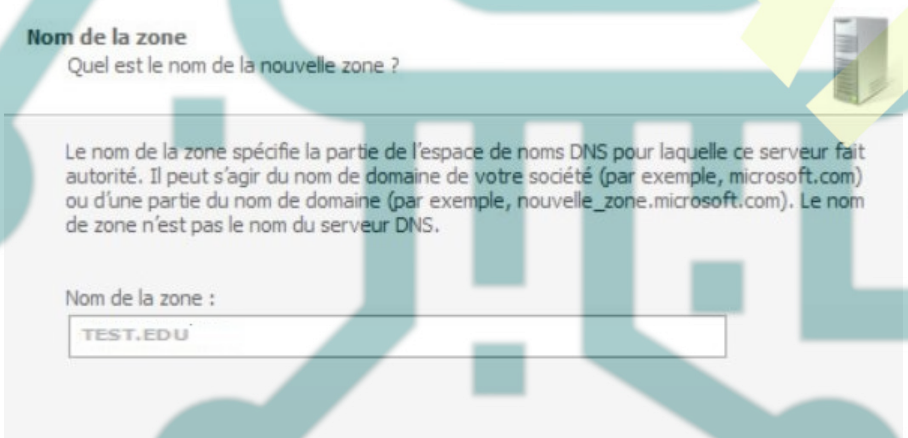
1. Dans le gestionnaire DNS, choisir nouvelle zone



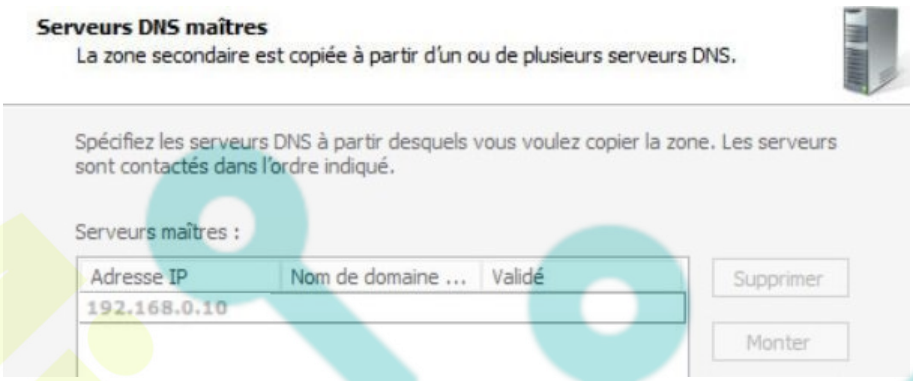
2. Puis dans l'assistant nouvelle zone, choisir zone secondaire



3. Indiquer le nom du domaine à répliquer



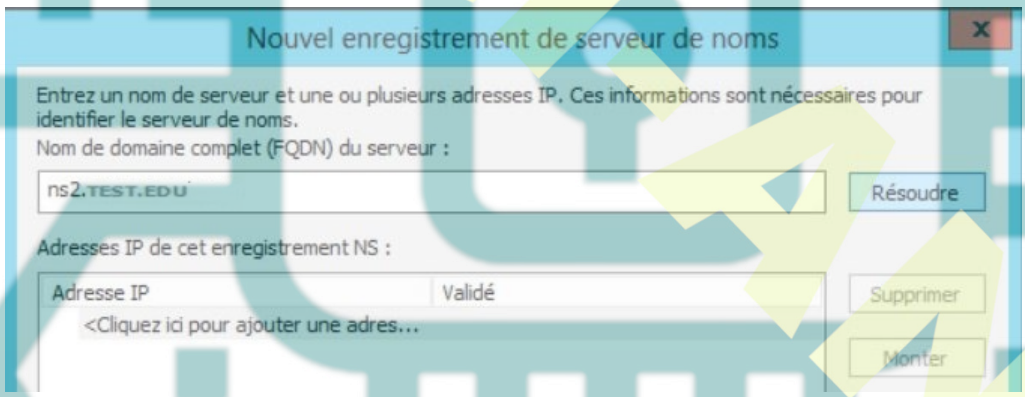
4. Indiquez l'adresse IP de votre serveur DNS maitre (principal) où vous gérez actuellement cette zone.



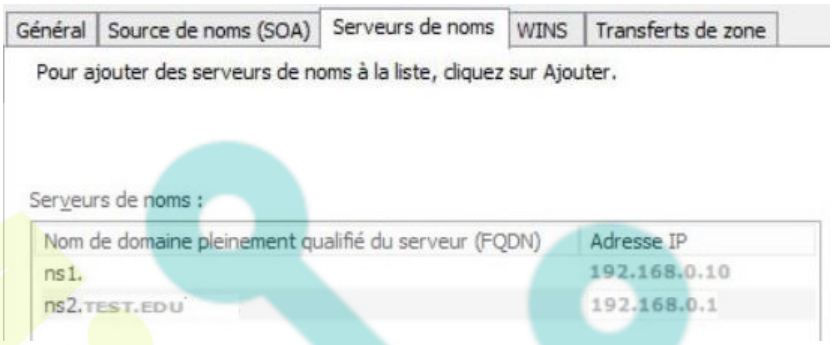
Une fois la zone secondaire créée, il est possible que le message "Zone non chargée par le serveur DNS" s'affiche.
En effet, pour que le serveur DNS puisse obtenir une copie de la zone depuis votre serveur DNS principal, vous devez d'abord autoriser le transfert de la zone vers votre serveur DNS secondaire.

Autoriser le transfert

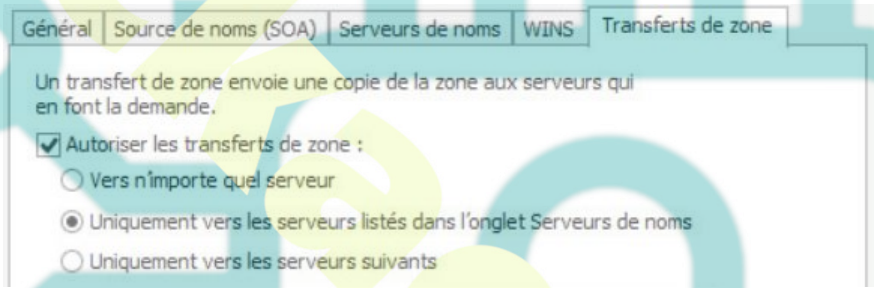
1. Pour autoriser le transfert de la zone DNS du serveur maitre (principal) vers le serveur secondaire, allez sur votre serveur DNS **principal** et créez un nouvel enregistrement de type A avec le nom et l'adresse IP du serveur DNS secondaire.



2. Ensuite, allez dans les propriétés de votre zone DNS principale et **ajoutez un serveur de noms**.
3. Ajoutez le nom ou l'adresse IP de votre serveur DNS secondaire et cliquez sur : **Résoudre**.
Maintenant, vos 2 serveurs DNS sont référencés comme serveurs de noms pour cette zone.



4. Pour finir, autorisez le transfert de la zone vers les serveurs listés dans l'onglet Serveurs de noms.



5. Sélectionnez l'option "**Uniquement vers les serveurs suivants**" en indiquant l'adresse IP du serveur DNS secondaire ou"**Uniquement vers les serveurs listés dans l'onglet Serveur de noms**".

6. Créez un nouvel enregistrement sur le serveur principal et vérifiez que cet enregistrement est bien répliqué.

DNS – DEBIAN

Préparation

Vérifier que votre machine virtuelle a accès à internet

Installer / désinstaller le service DNS

```
sudo apt install bind9
sudo apt remove bind9 (pour désinstaller si besoin)
```

Installer les outils supplémentaires

```
sudo apt install dnsutils
```

Mettre à jour la liste des serveurs racine

Création du fichier contenant la liste des serveurs racines

```
touch /etc/bind/db.root
```

Récupérer la liste des serveurs racine auprès du serveur a.root

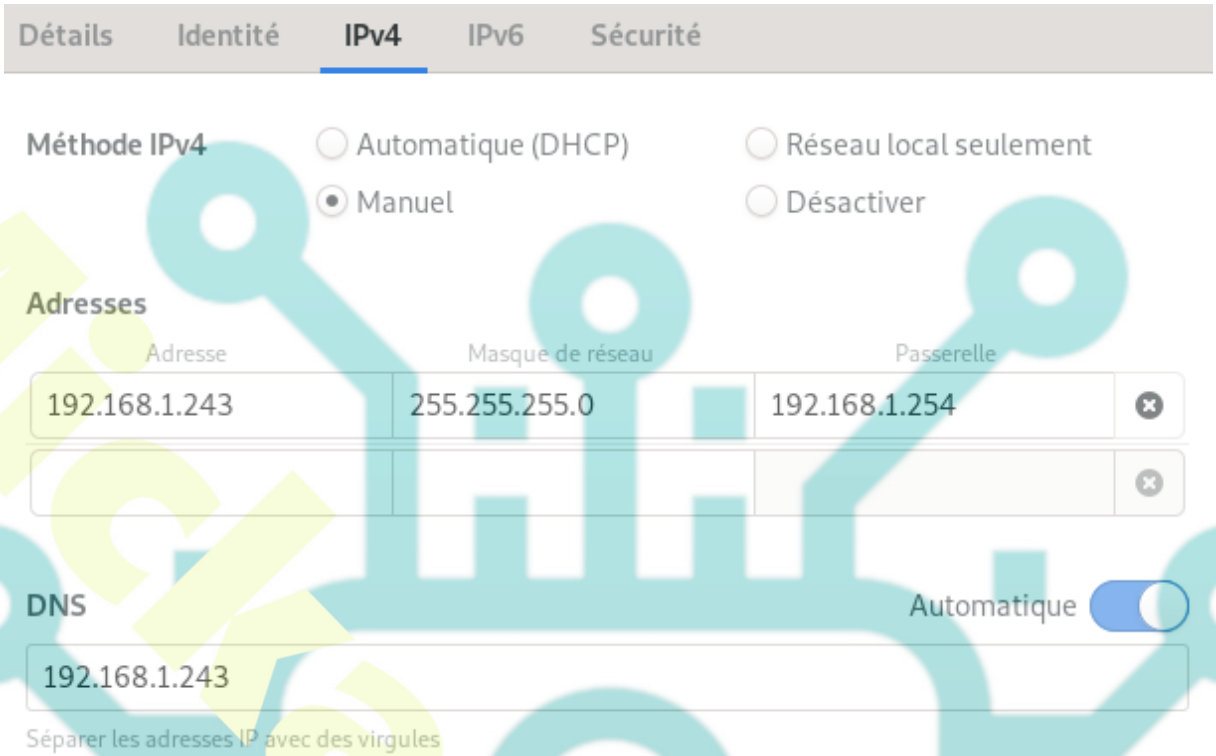
```
dig NS . @a.root-servers.net >/etc/bind/db.root
```

Vérifier le contenu du fichier

```
nano /etc/bind/dbroot
```

Configuration carte réseau

Dans les paramètres filaire, indiquer votre adresse IP et comme DNS l'adresse IP de votre serveur (c'est à dire vous même)



Puis redémarrer **sudo systemctl reboot**

Modification des fichiers de configuration avant installation

Fichier etc/hostname

```
debian.societe.com
```

Vérifier en saisissant la commande hostname

Fichier /etc/hosts

```
127.0.0.1       localhost
192.168.1.243   debian.societe.com
```

Vérifier en saisissant la commande ping debian.societe.com. Puis supprimer la ligne du fichier hosts

Configurer le DNS

Les fichiers importants sont :

/etc/bind/named.conf qui permet de charger les zones et les options
/etc/bind/named.conf.local qui permet de déclarer les zones et domaines
/etc/bind/named.conf.options qui permet de configurer les options de redirecteur, des adresses IP à écouter, la récursivité …
/etc/bind/named.conf.default-zones qui permet de charger les adresses de loopback.
/etc/bind/db.root qui contient la liste des serveurs racine

Modifier le fFichier /etc/bind/named.conf.options

Permettre l'écoute sur ipv4

```
options {
directory "/var/cache/bind";
listen-on-v6 { any; };
listen-on { any; };
```

Interdire l'écoute sur ipv6

```
options {
directory "/var/cache/bind";
listen-on-v6 { none; };
listen-on { any; };
```

Création des zones

Modification du fichier /etc/bind/named.conf.local

```
//include « /etc/bind/zones.rfc1918 » ;
zone "societe.com" {
        type master ;
```

```
        file "/etc/bind/db.societe.com" ;
} ;

zone "1.168.192.in-addr.arpa"  {
        type master ;
        file "/etc/bind/db.1.168.192.in-addr.arpa" ;
} ;
```

Configuration des zones

Création du fichier /etc/bind/db.societe.com

```
$TTL 9600
$ORIGIN societe.com.
@       IN SOA debian.societe.com. root.societe.com. (
        20181028; #Serial
        3h; #Refresh
        1h; #Retry
        1w; #Expire
        1h); #Negative cache TTL
@               IN          NS          debian.societe.com.
debian          IN          A           192.168.1.243
routeur         IN          A           192.168.1.254
www IN A 192.168.1.243
```

Serial — le numéro de série de la zone, incrémenté lorsque le fichier de zone est modifié, afin que les serveurs de noms secondaires sachent quand la zone a été modifiée et doit être rechargée.

Actualiser — Il s'agit du nombre de secondes entre les demandes de mise à jour des serveurs de noms secondaires.

Réessayer — Il s'agit du nombre de secondes que le secondaire attendra avant de réessayer lorsque la dernière tentative a échoué.

Expire — Il s'agit du nombre de secondes qu'un maître ou un esclave attendra avant de considérer les données périmées si elles ne peuvent pas atteindre le serveur de noms

principal.

Le minimum— Auparavant utilisé pour déterminer le TTL minimum, il est utilisé pour la mise en cache négative. Il s'agit du TTL par défaut si le domaine ne spécifie pas de TTL.

TTL (durée de vie) – Le nombre de secondes pendant lesquelles un nom de domaine est mis en cache localement avant expiration et renvoyé aux serveurs de noms faisant autorité pour des informations mises à jour.

Création du fichier /etc/bind/db.1.168.192.in-addr.arpa

```
$TTL 9600
@       IN SOA debian.societe.com. root.societe.com. (
20181028;
3h;
1h;/
1w;
1h);
@               IN      NS      debian.societe.com.
243             IN      PTR     debian.societe.com.
254             IN      PTR     routeur.societe.com.
```

Tester la configuration

```
named-checkconf  -z
```

Redémarrer le service DNS

```
service bind9 restart
```

Recharger une zone

```
rndc reload
```

Tester le domaine

```
dig debian.societe .com
```

Test de ping vers les noms d'hôtes crées dans la zone DNS

Mettre en place un redirecteur

Préparation

Remettre la machine virtuelle avec un accès internet

Fichier /etc/bind/named.conf.options

```
options {
        directory "/var/cache/bind";
        forwarders {
                8.8.8.8;
        };

        listen-on-v6 { any; };
        listen-on { any; };
```

Faire un test vers un nom de domaine internet

Créer un sous domaine

Préparation

Remettre la machine virtuelle avec un accès internet

Fichier /etc/bind/named.conf.local

```
//include « /etc/bind/zones.rfc1918 » ;
zone “societe.com” {
        type master ;
        file “/etc/bind/db.societe.com” ;
} ;
zone “1.168.192.in-addr.arpa” {
        type master ;
        file “/etc/bind/db.1.168.192.in-addr.arpa” ;
} ;

zone “test.societe.com” {
        type master ;
        file “/etc/bind/db.test.societe.com” ;
} ;
```

Fichier /etc/bind/db.test.societe.com

```
$TTL 9600
$ORIGIN test.societe.com.
@       IN SOA debian.societe.com. root.societe.com. (
        20181028;
        3h;
        1h;
        1w;
        1h);
@               IN      NS      debian.societe.com.

debian1         IN      A       192.168.1.243
router1         IN      A       192.168.1.254
```

Création d'un cname

Création du cname dans le domaine societe.com faisant référence à l'enregistrement web du sous domaine test.societe.com et création d'un cname pour le domaine.

Fichier /etc/bind/db.societe.com

```
$TTL 9600
$ORIGIN societe.com.
@       IN SOA debian.societe.com. root.societe.com. (
          20181028;
          3h;
          1h;
          1w;
          1h);
@ IN      NS              debian.societe.com.
debian    IN      A               192.168.1.243
routeur   IN      A               192.168.1.254
www       IN      CNAME   web1.test.societe.com.
societe.com. IN   A               192.168.1.243
dom       IN      CNAME           societe.com.
```

DNS secondaire

Configuration du DNS principal

Fichier /etc/bind/named.conf.local

```
//include « /etc/bind/zones.rfc1918 » ;
zone « societe.com » {
type master ;
```

```
also-notify {192.168.1.89 ;} ;
allow-update {none ;} ;
allow-query {any ;};
notify no ;
file "/etc/bind/db.societe.com" ;
} ;
```

Configuration du DNS secondaire

Installation d'une deuxième machine virtuelle et paramétrer l'adresse IP en 192.168.1.89

Installation de bind

```
sudo apt install bind9
```

Fichier etc/hostname

```
debianbis.societe.com
```

Fichier /etc/hosts

```
127.0.0.1       localhost
```

Fichier /etc/bind/named.conf.local

```
//include « /etc/bind/zones.rfc1918 » ;
zone "societe.com" {
type slave ;
masters {192.168.1.243 ;}
file "/etc/bind/db.societe.com";
} ;
```

Fichier /etc/bind/named.conf.options

```
Permettre l'écoute sur ipv4
options {
directory "/var/cache/bind";
listen-on-v6 { any; };
listen-on { any; };
```

Délégation de zones

Si le domaine societe.com veut déléguer la gestion des sous-domaines division1.societe.com au serveur de noms debian.division1.societe.com (192.168.1.89), il faut que dans le **fichier de zone de societe.com** figurent les lignes suivantes :

```
; Delegation des sous domaines division1.societe.com
division1.societe.com. IN   NS debian1.division1.societe.com.
debian1.division1.societe.com.   IN   A   192.168.1.89
```

Pour la résolution inverse, il faut compléter le fichier de résolution inverse **db.inverse** comme suit :

```
1.168.192.in-addr.arpa.   IN   NS   debian1.division1.societe.com.
```