Activer ou désactiver la fonctionnalité de récursivité du serveur DNS Bind9

Rapppel popur désactiver la récursivité du serveur DNS

Pour déactiver la récursivité, modifier **/etc/bind/named.conf.options** et ajoutez le paramètre **recursion** :

```
Options {
…
        recursion no;
…
};
```

Redémarrez ensuite le service DNS :

```
$ sudo systemctl restart bind9
```

Présentation

Pour chaque agence, il est nécessaire d'installer et configurer :

- le serveur DNS ayant autorité sur le domaine **<agence>.cub.fr (non récursif)** dans un conteneur Debian appelé **ns0** situé dans la **DMZ**;
- le serveur DNS ayant autorité sur la zone **lan.<agence>.cub.fr (non récursif)** dans un conteneur Debian appelé **ns0** situé dans le **VLAN Utilisateur**;
- le résolveur récursif dans un conteneur Debian appelé **dns0** situé dans le **VLAN Utilisateur**.

Vous devez :

- Mettre en place les serveurs DNS de votre agence.
- Procéder aux ajouts nécessaires sur le pare-feu pour le cas particulier du réseau Wan-CUB pour permettre notamment l'accessibilité des serveurs DNS et Web.
- Vérifier le fonctionnement des services DNS et Web.

Attention : lors des tests, il est nécessaire de vider le cache DNS et le cache de votre navigateur pour les tests sur le serveur Web (ou réaliser les tests en navigation privée).

Par exemple : À partir du résolveur (pour le domaine et le sous domaine) :

```
root@resolvDNSGaleway:~# unbound-control flush_zone galway.cub.fr
ok removed 4 rrsets, 4 messages and 0 key entries
root@resolvDNSGaleway:~# unbound-control flush_zone cub.fr
ok removed 0 rrsets, 1 messages and 0 key entries

ou
root@resolvDNSGaleway:~# unbound-control reload
```

À partir de n'importe quel Debian ou Ubuntu :

```
systemctl restart networking
```

La commande **dig** est plus verbeuse pour dépanner le service DNS que la commande **nslookup**.

Liste des tâches que vous devez effectuer

Tâche à faire sur le serveur DNS ns0

Les tâches d'administration sur le serveur qui héberge le service DNS vont être les suivantes :

- **Installer** puis **configurer** le service DNS (Bind9) dans un conteneur nommé **ns0** ;

- Vérifier **l'ordre** des méthodes de résolution dans le fichier **/etc/nsswitch.conf** ;
- Vérifier le fichier de **résolution** locale **/etc/hosts** ;
- Indiquer l'IP de votre serveur de noms dans **/etc/resolv.conf**, lorsque vous êtes client DNS ;
- Modifier le fichier de **configuration générale** du serveur DNS **/etc/named.conf.local** ;
- Créer le fichier de **zone maître utilisateurs.gsb.fr** (l'annuaire contenant les IP et les noms) ;
- Créer le fichier de **zone inverse** (un fichier qui permet de donner le nom à partir d'une IP. On appelle cela la résolution inverse) ;
- Tester.

Tâche à faire sur les postes client

Sur les postes clients, les tâches d'administration sont beaucoup plus simples. Il faut :

- Renseigner l'**adresse IP du serveur DNS** ;
- Renseigner le nom du domaine **<agence>.cub.fr** ;
- Tester (bien sûr).

Vérification de l'ordre des méthodes de résolution sur les postes clients

Avant que n'existent les serveurs DNS, la résolution de noms était locale à chaque machine. Le fichier **/etc/hosts** sous Linux contenait tous les noms DNS et toutes les adresses IP auxquelles on souhaitait accéder. La méthode du fichier local et celle du serveur DNS peuvent cohabiter notamment pour des raisons d'optimisation car il est plus rapide de regarder dans un fichier local que de contacter un serveur).

Historiquement, le fichier **/etc/host.conf** était utilisé par les outils de résolution de nom pour connaître l'ordre dans le choix de la méthode de résolution. Ce fichier est toujours présent pour des raisons de compatibilité ascendante, mais maintenant, c'est le fichier **/etc/nsswitch.conf**, plus complet, qui est utilisé.

Entre d'autres lignes, vous devriez voir dans ce fichier /etc/nsswitch.conf :

```
root@equipexdns:~# cat /etc/nsswitch.conf
hosts: files … dns …
```

La résolution la résolution locale (fichier **/etc/hosts**) est favorisée sur la résolution avec DNS comme vous pouvez le voir dans l'ordre indiqué : **files** puis ensuite **dns**. Mais vous allez changer cela dans la suite de l'atelier.

Vérifier le fichier de résolution locale

Dans un réseau avec serveur DNS, le fichier **/etc/hosts** devrait être réduit à sa plus simple expression, puisque c'est votre serveur qui servira à la résolution de noms.

Votre fichier /etc/hosts devrait avoir un contenu similaire à ce qui suit :

```
root@equipexdns:~# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain
adresseip equipexdns
…
```

Indiquer l'IP du serveur de noms

Le fichier **/etc/resolv.conf** doit contenir l'adresse IP du résolveur DNS. Ce fichier est vide par défaut.

Vous devez renseigner ce fichier pour tous les ordinateurs du réseau, PC et serveurs et même votre serveur DNS ns0 qui est aussi une machine cliente de son propre service DNS. Cette VM peut avoir besoin de trouver une IP à partir d'un nom.

Vous allez indiquer également le domaine dans lequel vous êtes situés (domain) et comment compléter un nom DNS si on n'indique pas le domaine (search) :

```
root@ns0:~# nano /etc/resolv.conf
domain agence.cub.fr
search agence.cub.fr
nameserver adresseIPdeVotreServeurDNS
```

Vérifiez que la résolution de noms ne fonctionne pas pour l'instant :

```
root@ns0:~# host ns0
Host ns0 not found: 5(REFUSED)
```

Installer le service DNS (Bind)

```
root@ns0:~# apt update && apt upgrade
root@ns0:~# apt -y install bind9 dnsutils
```

Configurer le service DNS (Bind)

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

Editez le fichier **/etc/bind/named.conf.options** pour :

- désactiver la récusivité,
- indiquer l'interface d'écoute du serveur (127.0.0.1 et 172.166.10.10) :

```
options {
    directory "/var/cache/bind";
    listen-on port 53 { 127.0.0.1; 172.16.10.10; };
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    //========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //========================================================================
    dnssec-validation auto;
    recursion no;
    version none;
};
```

Modifiez le fichier de configuration /etc/bind/named.conf.local

> Attention : Respectez rigoureusement la syntaxe. Bind est très sensible à la moindre erreur !!! Le fichier de configuration de Bind contient de très nombreuses options de configuration qui ne seront pas toutes abordées. Vous allez vous contenter d'un fichier minimaliste

Editez le fichier **/etc/bind/named.conf.local** et ajoutez les informations de zones suivantes :

```
zone "agence.cub.fr" {
    type master;
    file "/etc/bind/db.agence.cub.fr";
};

// zone de résolution inverse
zone "168.192.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.agence.cub.fr.inv";
};
```

Voyons la signification de chaque champ :

Option	Commentaires
zone “agence.cub.fr” {	Le nom de la zone entre guillemets et suivi d'une accolade.
type master;	**Master** indique que vous avez l'autorité sur la zone. D'autres serveurs (esclaves) pourront se synchroniser avec votre serveur.
file “/etc/bind/db.agence.cub.fr”;	Emplacement et nom du fichier de zone. Il sera placé dans /etc/bind/ et s'appellera db.agence.cub.fr
};	L'accolade ferme la définition de la zone.

La zone suivante porte la mention « **in-addr.arpa** » qui indique la zone inverse. Cette zone inverse permet au serveur de fournir un nom d'hôte à partir d'une adresse IP.

Cette fonctionnalité est rendue nécessaire par certains services réseau. Le nom de la zone répond à une structure très précise. Le début du nom de la zone est constitué par le préfixe réseau de l'adresse IP. Les conventions sont les suivantes :

- Pour les réseaux IP de classe A (a.0.0.0), il faut un fichier de zone inverse a.in-addr.arpa;
- Pour les réseaux IP de classe B (a.b.0.0), il faut un fichier de zone inverse b.a.in-addr.arpa;
- Pour les réseaux IP de classe C (a.b.c.0), il faut un fichier de zone inverse c.b.a.in-addr.arpa

Notez bien au passage l'inversion des octets !

Pour le contexte CUB, et compte tenu du sous-réseau il faut un fichier de zone inverse c.b.a.in-addr.arpa;

Création du fichier de zone maître

Vous devez maintenant créer les deux fichiers indiqués pour nos zones dans **/etc/bind/named.conf.local**.

Dans votre zone, vous avez plusieurs serveurs avec des adresses IP précises. Choisissez de créer des enregistrements pour vos serveurs DHCP et DNS.

Voici un contenu minimaliste pour ce fichier /etc/bind/db.agence.cub.fr que vous devez créer :

```
$TTL 1D
agence.cub.fr.       IN      SOA     ns0.agence.cub.fr. root.agence.cub.fr. (
        2006031201      ; serial
        1D.             ; refresh
        1H.             ; retry
        1W.             ; expire
        3H)             ; Negative Cache TTL

agence.cub.fr. IN      NS      ns0.agence.cub.fr.

ns0            IN      A       111.222.333.444
www            IN.     A.      111.222.333.444
dhcp           IN      A       111.222.333.445
```

Chaque ligne (qui ne commence pas par un $) s'appelle un enregistrement DNS.

La première ligne ($TTL 1D) indique la durée de vie des informations transmises par votre serveur DNS. En effet, les machines qui feront appel à votre serveur vont conserver dans un cache les informations découvertes afin de ne pas refaire en permanence les mêmes demandes. Ici, au bout de trois jours (1D = 1 day), les informations doivent être retirées du cache. Comment déterminer ce TTL ? Cela dépend de votre zone. Si elle change souvent, il faut un TTL court.

La deuxième ligne définit le nom du domaine (Notez bien le point à la fin du nom de domaine) et est importante. C'est un enregistrement SOA (Start Of Authority) qui indique que les informations en-dessous sont de votre responsabilité. En effet, vous êtes le serveur maître de la zone agence.cub.fr.

Voici sa structure :

agence.cub.fr. IN SOA	ns0.agence.cub.fr.	root.agence.cub.fr.	(2006031201; serial\\1D; refresh\\1H; retry\\1W; expire\\3H); Negative Cache TTL
Enregistrement DNS de type Internet (IN) déclarant notre autorité (SOA).			