1. Configurer le service DNS pour les ordinateurs du réseau utilisateurs

1.1. 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 :

1. Mettre en place les serveurs DNS de votre agence.
2. 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.
3. Vérifier le fonctionnement des services DNS et Web.

1.1.1. Liste des tâches que vous devez effectuer

1.1.1.1. 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.

1.1.1.2. 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).

1.1.2. 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.

1.1.3. 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
…
```

1.1.4. 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)
```

1.2. Installer le service DNS (Bind)

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

1.3. Configurer le service DNS (Bind)

1.3.1. 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;
};
```

1.3.2. 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;

1.3.2.1. 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).	Nom du serveur de nom maître sur la zone agence.cub.fr.**Attention au point à la fin !!!**	Email (sans @) de l'administrateur de la zone**Attention au point à la fin !!!**	Une série de valeurs numériques utilisées pour la synchronisation entre le serveur maître et ses esclaves.\\La première parenthèse doit être sur la même ligne que le SOA.

La quatrième ligne est un enregistrement NS (Name Server) qui donne le nom du serveur maître sur la zone (vous). La cinquième ligne est un enregistrement A (Address) qui donne l'IP de la machine dont le nom est indiqué à droite.

1.3.2.2. Création du fichier de zone inverse

Le fichier de zone inverse (/etc/bind/db.agence.cub.fr.inv) doit contenir :

```
$TTL 3D
@ IN SOA ns0.agence.cub.fr. root.agence.cub.fr. (
        2006031201      ; serial
        28800           ; refresh
        14400           ; retry
        3600000         ; expire
        86400 )         ; minimum

    NS  ns0.agence.cub.fr.
444 PTR ns0.agence.cub.fr.
445 PTR dhcp.agence.cub.fr.
```

Les informations sont sensiblement identiques. La différence réside sur les enregistrements décrivant les machines. On indique la fin de l'adresse IP. PTR indique qu'il s'agit d'un enregistrement inverse.

Ensuite, on indique le nom FQDN des machines suivi d'un point.

1.3.2.3. Configurer la résolution DNS récursive.

Quand le serveur DNS va recevoir une requête pour laquelle il n'a pas de réponse, ce qui est le cas pour accéder à des serveurs sur Internet, il va transmettre la requête aux serveurs listés dans le paramètre **forwarders**. En principe on indique le serveur **DNS** de son **FAI**. Vous pouvez aussi pour cet atelier mettre les serveurs DNS publics **8.8.8.8** ou **8.8.4.4** ou **1.1.1.1**ou **9.9.9.9**.

1.3.2.4. Test de la configuration

Utilisez la commande suivante pour tester voter configuration

```
# named-checkconf -z
```

1.3.3. Sécuriser le serveur DNS

Par défaut le **serveur DNS** ne va répondre qu'aux requêtes des clients **situés sur le même sous-réseau** qui est ici **192.168.xxx.xxx/xx**. Cela permet de limiter les attaques basées sur le service DNS. Pour autoriser des clients d'autres sous-réseaux, utilisez l'option **allow-query** :

```
Options {
```

```
…
        allow-query {
          192.168.xxx.yyy/24;
        } ;
…
};
```

allow-query { 192.168.1/24; } ;

1.3.4. Lancer et tester le service DNS (Bind)

De nombreuses modifications ont été réalisées. Des erreurs ont pu être introduites dans les fichiers. Cette partie a pour but de vous présenter les erreurs généralement rencontrées. Plusieurs outils permettent de valider la configuration (au niveau de la syntaxe tout au moins) :

Commande	**Effet**
named-checkzone	Valide le fichier /etc/named.conf et /etc/named.conf.local
named-checkzone <nom_de_zone> <nom_du_fichier>	Valide le fichier de zone
named –g	
host <nom_de_machine>	Interroge le serveur DNS au sujet de la machine indiquée.
hostname –f	Donne le nom FQDN de la machine local

Ensuite, lancez le serveur en mode débogage, vous aurez déjà pas mal d'informations sur les éventuels problèmes :

```
root@equipexdns:~# named -g
```

Analyser les messages d'erreur obtenus puis faites éventuellement un CTRL-C pour stopper le serveur afin d'éditer le fichier concerné.

Si vous avez une erreur du type

```
none:0: open: /etc/bind/rndc.key: permission denied
```

Ignorez là.

S'il n'y a plus d'erreurs de syntaxe, arrêtez puis relancez le serveur de la façon habituelle :

```
root@equipexdns:~# service bind9 restart
Stopping domain name service...: bind9.
Starting domain name service...: bind9.
```

Ensuite, faites quelques tests :

```
root@ns0:~# hostname
ns0
root@ns0:~# host ns0
ns0.agence.cub.fr has address 111.222.333.444
```

La commande ci-dessous est particulièrement intéressante. Elle permet de lister les informations sur la zone mais « vues » par le serveur :

```
root@ns0:~# host -lv agence.cub.fr
```

Maintenant, vos hôtes peuvent accéder à Internet avec une résolution de noms comme vous pouvez le vérifier à partir d'une autre VM de votre réseau utilisateur correctement configurée.

```
root@dhcp:~# lynx http://www.ac-limoges.fr
```

1.4. Les outils de diagnostic nslookup et dig

Les commandes dig et nslookup qui permettent de tester la configuration du serveur DNS et de pouvoir détecter des erreurs de configuration sur les serveurs DNS pour les corriger.

1.4.1. nslookup

La commande nslookup est plus ancienne que la commande dig, il est possible de lui passer soit le nom d'une station ou l'adresse d'un serveur pour obtenir les informations fournies par le serveur DNS. Voici ci-dessous deux exemples :

```
$ nslookup dhcp
Server: 192.168.50.90
Address: 192.168.50.90#53
Name: dhcp.mondomaine.org
Address: 192.168.1.2
$ nslookup 192.168.1.2
2.1.168.192.in-addr.arpa name = dhcp.mondomaine.org.
```

Tapez la commande nslookup sur une des stations du réseau pour obtenir et vérifier les informations fournies par le serveur DNS.

1.4.2. dig

La commande **dig** fournit plus d'information en interrogeant directement un serveur DNS spécifié (l'adresse du serveur doit être indiquée en premier paramètre) en plus des informations de résolution de noms. Voici ci-dessous quelques exemples d'utilisation :

- Test d'une zone :

```
$ dig ns1.mondomaine.org
; <<>> DiG 9.16.22-Debian <<>> ns1.mondomaine.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34654
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8a3cc0da0dea6eaf3506eba35e6121ea484f5e9d41ee1144 (good)
;; QUESTION SECTION:
;ns1.mondomaine.org. IN A
RSX103 – Cnam Paris
;; ANSWER SECTION:
ns1.mondomaine.org. 604800 IN A 192.168.50.90
;; ADDITIONAL SECTION:
ns2.mondomaine.org. 604800 IN A 192.168.50.91
;; Query time: 0 msec
;; SERVER: 192.168.50.90#53( 192.168.50.90)
;; WHEN: Mon Feb 03 15:59:38 UTC 2022
;; MSG SIZE rcvd: 139
```

- Récupération enregistrement SOA d'une zone :

```
$ dig soa mondomaine.org
; <<>> DiG 9.16.22-Debian <<>> soa mondomaine.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38518
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 8333ab9fd5d0555621ef9a4e5e6123e1312c74e39b52d58e (good)
;; QUESTION SECTION:
;mondomaine.org. IN SOA
;; ANSWER SECTION:
mondomaine.org. 604800 IN SOA ns1.mondomaine.org.
root.mondomaine.org. 1 604800 86400 2419200 604800
;; ADDITIONAL SECTION:
ns1.mondomaine.org. 604800 IN A 192.168.50.90
ns2.mondomaine.org. 604800 IN A 192.168.50.91
;; Query time: 0 msec
;; SERVER: 192.168.50.90#53(192.168.50.90)
;; WHEN: Mon Feb 03 16:08:01 UTC 2022
;; MSG SIZE rcvd: 192
```

- Résolution de nom pour www.mondomaine.org :

```
$ dig www.mondomaine.org
; <<>> DiG 9.16.22-Debian <<>> www.mondomaine.org
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20402
RSX103 — Cnam Paris
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 95f0892417ed967cf361e6965e6125932ec00d08cde00be4 (good)
;; QUESTION SECTION:
;www.mondomaine.org. IN A
;; ANSWER SECTION:
www.mondomaine.org. 604800 IN CNAME srv.mondomaine.org.
srv.mondomaine.org. 604800 IN A 192.168.50.100
;; ADDITIONAL SECTION:
ns1.mondomaine.org. 604800 IN A 192.168.50.90
ns2.mondomaine.org. 604800 IN A 192.168.50.91
;; Query time: 0 msec
;; SERVER: 192.168.50.90#53(192.168.50.90)
;; WHEN: Mon Feb 03 16:15:15 UTC 2022
;; MSG SIZE rcvd: 177
```

- Résolution inverse :

```
$ dig ptr 100.50.168.192.in-addr.arpa
; <<>> DiG 9.16.22-Debian <<>> ptr 100.50.168.192.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21895
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d55d2ee64d3f84bf9565d5b75e61267cf152fde2ee26b21e (good)
;; QUESTION SECTION:
;100.50.168.192.in-addr.arpa. IN PTR
;; ANSWER SECTION:
100.50.168.192.in-addr.arpa. 604800 IN PTR srv.mondomaine.org.
;; Query time: 0 msec
;; SERVER: 192.168.50.90#53(192.168.50.90)
;; WHEN: Mon Feb 03 16:19:08 UTC 2022
;; MSG SIZE rcvd: 149
```

1.4.3. Retour Configurer le service DNS

- Configurer le service DNS

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/dns/dnslaninverse?rev=1696491404

Last update: **2023/10/05 07:36**