Doc DNS maitre-esclave / délégation DNS

Question :

Le DNS (domaine name système) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP.

Les principaux fichiers a modifier pour configurer un DNS maître/esclave et une délégation sont les fichiers « db » et « rev », mais aussi les fichiers « named.conf.options » et « named.conf.local », sans oublier le serial.

DNS maitre-esclave :

Pour le DNS maitre :

Se rendre dans **/etc/bind** et modifier le fichier **named.conf.options**

Modifier le fichier pour que le DNS réponde qu'il ne peut pas répondre, capture ci-dessous :

```
acl trusted { };

options {
        directory "/var/cache/bind";

        // 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.

        forwarders {
                [redacted]8.8.8.8;
        };

        //========================================================================
        // 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
        //========================================================================
        allow-query { };
        allow-recursion { };
        dnssec-validation auto;

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

Toujours dans **/etc/bind** modifier cette fois le fichier **db.[nom de domaine]** de manière à renseigner le DNS-esclave dans fichier.

```
;
; BIND data file for nico.sisr zone
;
$TTL    604800
@       IN      SOA     nico.sisr. root.nico.sisr. (
                      2022092201               ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.nico.sisr.
@       IN      NS      ns-esclave.nico.sisr.
@       IN      A       192.168.11.2

ns              IN      A       192.168.11.2
ns-esclave      IN      A       192.168.11.4

lamp    IN      A       192.168.11.3
serv2   IN      A       192.168.11.5
creuse  IN      CNAME   lamp
```

Ensuite modifier le **rev.[nom de domaine]** pour renseigner le DNS-esclave dans le reverse.

```
;
; BIND reverse data file for nico.sisr zone
;
$TTL    604800
@       IN      SOA     nico.sisr. root.nico.sisr. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.nico.sisr.
@       IN      NS      ns-esclave.nico.sisr.
@       IN      A       192.168.11.2

ns              IN      A       192.168.11.2
ns-esclave      IN      A       192.168.11.4

3       IN      PTR     lamp
5       IN      PTR     serv3
```

Il faut ensuite modifier le fichier **named.conf.local** dans **/etc/bind** pour permettre le partage du DNS-maitre au DNS-esclave en rajoutant un ligne « allow-tranfert » pour chaque zone.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "nico.sisr" IN {
        type master;
        file "/etc/bind/db.nico.sisr";
        allow-transfer { 192.168.11.4; };
};

zone "11.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/rev.nico.sisr";
        allow-transfer { 192.168.11.4; };
};
```

Pour le DNS-esclave :

Pour commencer nous allons dans **/etc/bind** pour modifier le fichier **named.conf.options** pour renseigner les ACL et les forwarders. On rajoute aussi les lignes « allow-query » et « allow-recursion ».

```
acl trusted { 192.168.10.0/24; 192.168.11.0/24; };

options {
        directory "/var/cache/bind";

        // 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.

        forwarders {
                8.8.8.8;
         };

        //========================================================================
        // 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;
        allow-query { trusted; };
        allow-recursion { trusted; };

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

Il faut ensuite aller modifier le fichier **named.conf.local** toujours dans le dossier **/etc/bind** pour renseigner les zones et le DNS-maitre.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";


zone "nico.sisr" IN {
        type slave;
        file "/var/cache/bind/db.nico.sisr";
        masters { 192.168.11.2; };
};

zone "11.168.192.in-addr.arpa" IN {
        type slave;
        file "/var/cache/bind/rev.nico.sisr";
        masters { 192.168.11.2; };
};
```

Ensuite il ne faut pas oublier de changer le DNS dans pare-feu pour que notre service DHCP fournisse l'adresse ip de notre DNS-esclave. Il faut également vérifier et modifier si nécessaire les règles de pare-feu.

Délégation DNS :

Pour le DNS-master :

Pour commencer on modifie le fichier **named.conf.local** du DNS-master dans le dossier **/etc/bind** des deux DNS pour que nos DNS ne consulte pas leurs forwarders si un requête concerne notre domaine.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "nico.sisr" IN {
        type master;
        file "/etc/bind/db.nico.sisr";
        allow-transfer { 192.168.11.4; };
        forwarders { };
};

zone "11.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/rev.nico.sisr";
        allow-transfer { 192.168.11.4; };
        forwarders { };
};
```

Nous devons ensuite modifier dans le dossier **/etc/bind** le fichier **db.nico.sisr** de manière a renseigner le DNS-delegation dans notre fichier, faire de même pour le reverse.

```
root@DNS-deb:/etc/bind# cat db.nico.sisr
;
; BIND data file for nico.sisr zone
;
$TTL    604800
@       IN      SOA     nico.sisr. root.nico.sisr. (
                      2022092201                ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.nico.sisr.
@       IN      NS      ns-esclave.nico.sisr.
tp      IN      NS      ns-deleg.tp.nico.sisr.
@       IN      A       192.168.11.2

ns              IN      A       192.168.11.2
ns-esclave      IN      A       192.168.11.4
ns-deleg.tp     IN      A       192.168.11.5

lamp    IN      A       192.168.11.3
serv2   IN      A       192.168.11.6
creuse  IN      CNAME   lamp
glpi    IN      CNAME   lamp
```

Pour le DNS-delegation :

Nous installons ensuite un DNS sur une nouvelle machine et configurons ses paramètre ip.

Une fois cela fait nous configurons dans le dossier **/etc/bind** le fichier **named.conf.options**, nous lui renseignez-nous les acl nécessaire à son bon fonctionnement et nous mettons l'adresse de notre DNS master dans les forwarders.

```
acl trsuted { 192.168.10.0/24; 192.168.11.0/24; };

options {
        directory "/var/cache/bind";

        // 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.

        // forwarders {
        //      192.168.11.2;
        // };

        //========================================================================
        // 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;
        allow-query { trusted; };
        allow-recursion { trusted; };

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

Nous devons ensuite créer le fichier **db.tp.nico.sisr** et sont reverse (**rev.tp.nico.sisr**) puis les compléter. Nous nous trouvons toujours dans le dossier **/etc/bind**.

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     tp.nico.sisr. root.tp.nico.sisr. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      ns-deleg.tp.nico.sisr.
ns-deleg        IN      A       192.168.11.5
```

Pour finir nous allons déclarer nos zone dns dans le fichier **named.conf.local.**

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "tp.nico.sisr" IN {
        type master;
        file "/etc/bind/db.tp.nico.sisr";
        allow-transfer { none; };
};

zone "11.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/rev.tp.nico.sisr";
        allow-transfer { none; };
};
```

On utilise cette commande dans notre DNS-maitre : **rndc reload**, elle permet de forcer le DNS-esclave à récupérer la configuration du DNS-maître.

Pour finir nous testons si la délégation fonctionne avec la commande dig.

```
; <<>> DiG 9.11.36-RedHat-9.11.36-1.fc33 <<>> @192.168.11.4 test.tp.nico.sisr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11916
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3adf07b78fa2201e21e0c50d637e2918e9a160c3da83b335 (good)
;; QUESTION SECTION:
;test.tp.nico.sisr.             IN      A

;; ANSWER SECTION:
test.tp.nico.sisr.      604752  IN      A       192.168.11.56

;; AUTHORITY SECTION:
tp.nico.sisr.           604800  IN      NS      ns-deleg.tp.nico.sisr.

;; ADDITIONAL SECTION:
ns-deleg.tp.nico.sisr.  604707  IN      A       192.168.11.5

;; Query time: 1 msec
;; SERVER: 192.168.11.4#53(192.168.11.4)
;; WHEN: mer. nov. 23 15:07:21 CET 2022
;; MSG SIZE  rcvd: 129
```