Aller au contenu

Atelier n°3 - DNS

Installation et creation d'un serveur dns primaire et secondaire LECON
Un serveur primaire héberge le fichier de la zone de contrôle, qui contient toutes les informations faisant autorité pour un domaine. Ce sont des informations importantes, telles que l'adresse IP du domaine et qui est responsable de l'administration de ce domaine.
Les serveurs primaires reçoivent ces informations directement des fichiers locaux.
Les modifications apportées aux enregistrements DNS d'une zone ne peuvent être effectuées que sur le serveur primaire, qui peut ensuite mettre à jour les serveurs secondaires.

Les serveurs secondaires contiennent des copies en lecture seule du fichier de zone et ils reçoivent leurs informations d'un serveur primaires d'une communication appelée un transfert de zone. Chaque zone ne peut avoir qu'un serveur DNS primaire, mais plusieurs serveurs DNS secondaires. Les modifications apportées aux enregistrements DNS d'une zone ne peuvent pas être effectuées sur un serveur secondaire, mais dans certains cas, un serveur secondaire peut transmettre des requêtes de modification au serveur primaire.

Installation du service et création de la zone, procédure générale
1. Installer le paquetage bind9 bind9utils dnsutils
apt install bind9 bind9utils dnsutils
2. Déclarer la zone à gérer dans named.conf.local avec le type « master »
nano /etc/bind/named.conf.local

```
zone "m2l.org" IN {
type master; #serveur maître
file "/etc/bind/db.m2l.org"; #nom du fichier qui décrit la zone
};
```

3. Configurer le fichier de la zone en y ajoutant les enregistrements nécessaires (NS, A, …)
nano /etc/bind/db.m2l.org

```
@ IN SOA ns1.m2l.org. root.m2l.org. (
2021012201         ; numéro de série important pour les secondaires
43200              ; temps de rafraîchissement des secondaires
3600               ; temps d'attente entre deux tentatives de mise à jour pour lesseconda
3600000            ; Temps après lequel le serveur secondaire ne répond plus auxrequêtes
172800 )           ; ttl de mise en cache



@ IN A 10.31.112.1 ;
@ IN NS ns1.m2l.org.    ; déclaration serveurs de noms principaux et secondaires
@ IN MX 10 smtp         ; pointeur pour le serveur de messagerie avec numéro d'ordre
ns1 IN A 10.31.112.1    ; association pour le nom de machine ns1.m2l.org
www IN A 10.31.112.1    ; déclaration d'association pour le nom de machine www
smtp IN A 10.31.112.1   ; association pour le nom smtp
ftp IN A 10.31.112.1    ; association pour le serveur ftp

console IN CNAME www    ; alias pour le nom de machine www
```

Les 3 lignes de commandes a ajouter sont la declaration du serveur donc **@ IN A 10.31.112.1** et **IN NS ns1.m2l.org** la machine **ns1 IN A 10.31.112.1** qui est associe au serveur m2l.org

@ IN NS ns1.m2l.org. ; déclaration serveurs de noms principaux et secondaires
ftp IN A 10.31.112.1 ; association pour le serveur ftp
ns1 IN A 10.31.112.1 ; association pour le nom de machine ns1.m2l.org
Et puis dans le fichier **nano named.conf.options** on ecrit la récursion

```
options {
        directory "/var/cache/bind"; #repertoire de stockage des fichiers de zone
        dump-file "/var/data/cache_dump.db"; #repertoire de cache
        statistics-file "/var/bind/named_stats.txt"; #repertoire de statistiques
        recursion yes;
        forwarders { 8.8.8.8; 8.8.4.4; };
```

```
        forward only;

        // 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 {
        //      0.0.0.0;
        // };

        //========================================================================
        // 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
        //========================================================================
```

4. Vérifier la validité de la configuration du service : named-checkconf
named-checkconf
nano /etc/bind/named.conf
5. Vérifier la validité de la configuration de la zone : named-checkzone
named-checkzone m2l.org db.m2l.org

```
root@hadjgr7:/etc/bind# named-checkzone m2l.org  db.m2l.org
db.m2l.org:1: no TTL specified; using SOA MINTTL instead
zone m2l.org/IN: loaded serial 2021012201
OK
```

6. Recharger le fichier de configuration ou redémarrer le service
Systemctl restart bind9
Systemctl status bind9

7. Paramétrer un client pour qu'il utilise ce serveur, faire un ping sur un FQDN
On peut prendre le routeur comme client donc on va modifier le fichier **/etc/resolv.conf** dans le routeur et on met l'adresse ip du serveur

```
nameserver 10.31.112.1
```

Puis tester de ping m2l avec les commandes :
ping www.m2l.org [http://www.m2l.org]
ping ftp.m2l.org [ftp://ftp.m2l.org]
ping 8.8.8.8 (pour tester internet)

La commande dig est utilisée pour tester un serveur de nom. Le commandes suivantes doivent fonctionner. Adaptez la zone et mettez l'adresse IP de votre serveur de nom.
Commande faites depuis le serveur **10.31.112.1**
dig ns m2l.org @10.31.112.1

```
root@hadjgr7:/etc/bind# dig ns m2l.org @10.31.112.1

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> ns m2l.org @10.31.112.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62105
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 890703fb3c36d9d9d61a5edc600a9760f1d7ae7dc5ac5a91 (good)
;; QUESTION SECTION:
;m2l.org.                       IN      NS

;; ANSWER SECTION:
m2l.org.                172800  IN      NS      ns1.m2l.org.

;; ADDITIONAL SECTION:
ns1.m2l.org.            172800  IN      A       10.31.112.1

;; Query time: 0 msec
;; SERVER: 10.31.112.1#53(10.31.112.1)
;; WHEN: ven. janv. 22 10:14:08 CET 2021
;; MSG SIZE  rcvd: 98
```

dig a m2l.org @10.31.112.1

```
root@hadjgr7:/etc/bind# dig a m2l.org @10.31.112.1

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> a m2l.org @10.31.112.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59992
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2f540525a18db38ad155daa4600a97699f70da7113f8b77a (good)
;; QUESTION SECTION:
;m2l.org.                       IN      A

;; ANSWER SECTION:
m2l.org.                172800  IN      A       10.31.112.1

;; AUTHORITY SECTION:
m2l.org.                172800  IN      NS      ns1.m2l.org.

;; ADDITIONAL SECTION:
ns1.m2l.org.            172800  IN      A       10.31.112.1

;; Query time: 0 msec
;; SERVER: 10.31.112.1#53(10.31.112.1)
;; WHEN: ven. janv. 22 10:14:17 CET 2021
;; MSG SIZE  rcvd: 114
```

dig mx m2l.org @10.31.112.1

```
root@hadjgr7:/etc/bind# dig mx m2l.org @10.31.112.1

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> mx m2l.org @10.31.112.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36675
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c4195381febb87eafe5573f5600a97721a88c20044429fc7 (good)
;; QUESTION SECTION:
;m2l.org.                       IN      MX

;; ANSWER SECTION:
m2l.org.                172800  IN      MX      10 smtp.m2l.org.

;; AUTHORITY SECTION:
m2l.org.                172800  IN      NS      ns1.m2l.org.

;; ADDITIONAL SECTION:
smtp.m2l.org.           172800  IN      A       10.31.112.1
ns1.m2l.org.            172800  IN      A       10.31.112.1

;; Query time: 0 msec
;; SERVER: 10.31.112.1#53(10.31.112.1)
;; WHEN: ven. janv. 22 10:14:26 CET 2021
;; MSG SIZE  rcvd: 135
```

Creation du serveur DNS secondaire

/etc/bind/m2l.org

```
@ IN SOA ns1.m2l.org. root.m2l.org. (
2021012201      ; numéro de série important pour les secondaires
43200           ; temps de rafraîchissement des secondaires
3600            ; temps d'attente entre deux tentatives de mise à jour pour lessecondaire
3600000         ; Temps après lequel le serveur secondaire ne répond plus auxrequêtes lor
172800 )        ; ttl de mise en cache



@ IN A 10.31.112.1          ;
@ IN NS ns1.m2l.org.        ; déclaration serveurs de noms principaux et secondaires
@ IN NS ns2                 ; serveur dns secondaire

ns1 IN A 10.31.112.1         ; association pour le nom de machine ns1.m2l.org
ns2 IN A 10.31.112.254       ; serveur secondaire
smtp IN A 10.31.112.1        ; association pour le nom smtp
ftp IN A 10.31.112.1         ; association pour le serveur ftp

console IN CNAME www         ; alias pour le nom de machine www
```

On rajoute les ligne :
@ IN NS ns2 ; serveur dns secondaire
ns2 IN A 10.31.112.254 ; serveur secondaire

Puis dans le fichier **/etc/bind/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 "m2l.org" IN {
type master; #serveur maître
file "/etc/bind/db.m2l.org"; #nom du fichier qui décrit la zone
allow-transfer { 10.31.112.254; localhost; };
};
```

On rajoute la ligne de transfert vers le routeur
allow-transfer { 10.31.112.254; localhost; };

Pui dans le routeur 10.31.112.254
Installer bind avec la commande :
apt install bind9 bind9utils dnsutils

Puis aller dans **nano /etc/bind/named.conf.local**

```
zone "m2l.org" {
        type slave;
        file "/var/lib/bind/db.m2l.org";
        masters { 10.31.112.1; };
};
```

Dans le fichier **/etc/bind/named.conf.options** on ajoute les forwaders et le directory

```
options {
        directory "/var/lib/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.
          allow-query { any; };
          forwarders { 8.8.8.8; 8.8.4.4; };
          forward only;
        //========================================================================
        // 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;

        // auth-nxdomain no;    # conform to RFC1035
        // listen-on-v6 { any; };
};
```

allow-query { any; }; permet a toutes les machines d'effectuer des requetes
Redemarrer le service DNS sur le routeur et serveur avec la commande :
systemctl restart bind9
————————————————————
Pour afficher le port udp qui est 53 du dns
netstat -nau **

sisr1-g7/mission_3.txt · Dernière modification: 2021/01/26 10:38 de h-benzahaf