Déploiement de BIND9 DNS avec Mises à Jour Dynamiques Sécurisées

1. Introduction

Ce document décrit la configuration d'un serveur DNS BIND 9 sécurisé pour le domaine techvault.fr, avec :

- Mises à jour dynamiques sécurisées via TSIG (HMAC-SHA256).
- Forwarders Google DNS (8.8.8.8/8.8.4.4) pour les requêtes externes.
- DNSSEC activé par défaut.
- Firewall nftables filtrant les accès DNS/SSH/.
- Zones directes et inverses gérées localement.

2. Prérequis

- Système : Linux (Debian/Ubuntu) avec accès root.
- Packages :
  - ➔ apt install bind9 nftables dnsutils

3. Génération de la Clé TSIG pour les Mises à Jour Dynamiques

Objectif : Authentifier les mises à jour DNS via nsupdate.

Étapes :

3.1. Générer une clé TSIG :

➔ *tsig-keygen -a hmac-sha256 maj-ddns > /etc/bind/cle-tsig.key*

```
root@DNS:~# tsig-keygen maj-ddns > cle-tsig.key
root@DNS:~# ls -la
total 28
drwx------  3 root root 4096  9 févr. 10:29 .
drwxr-xr-x 18 root root 4096  9 févr. 09:50 ..
-rw-r--r--  1 root root  607  7 nov.  18:40 .bashrc
-rw-rw-r--  1 root root  100  9 févr. 10:29 cle-tsig.key
-rw-------  1 root root   20  9 févr. 09:52 .lesshst
-rw-r--r--  1 root root  132  7 nov.  18:40 .profile
drwx------  2 root root 4096  9 févr. 09:49 .ssh
root@DNS:~# cat cle-tsig.key
key "maj-ddns" {
        algorithm hmac-sha256;
        secret "jSBiWfL3ZhrAsire0BTmHcmPyuR5Eg/DaE+Vkiebmdc=";
};
```

3.2. Synchroniser avec named.conf.local :

La clé doit être déclarée dans named.conf.local sous le nom ddns-key.laser-campus.local.

Vérification : Le secret doit être identique dans les deux fichiers.

3.3. Fichier named.conf.local

Chemin : /etc/bind/named.conf.local

Fonction : Déclaration des zones et clés TSIG.

```
 GNU nano 8.4                                          named.conf.local
//Zone Directe
zone "techvault.fr" {
    type master;
    file "/var/cache/bind/laser.dns";
    allow-update { key "ddns-key.laser-campus.local"; };
};

//Zone Inverse
zone "0.16.172.in-addr.arpa" {
    type master;
    file "/var/cache/bind/inverse.dns";
};

key "ddns-key.laser-campus.local" {
    algorithm hmac-sha256;
    secret "jSBiWfL3ZhrAsire0BTmHcmPyuR5Eg/DaE+Vkiebmdc=";
};

controls {
    inet 127.0.0.1 allow { 127.0.0.1; } keys { "ddns-key.laser-campus.local"; };
};
```

Critique :

- allow-update restreint les mises à jour à la clé TSIG spécifiée.
- controls sécurise l'accès à rndc.

4. Configuration des Zones DNS

4.1. Zone Directe (laser.dns)

Chemin : /var/cache/bind/laser.dns

Fonction : Résolution des noms vers IP pour techvault.fr.

```
 GNU nano 8.4                                                  laser.dns
$TTL    604800
@       IN      SOA     srv-dns.techvault.fr. admin-laser-campus.techvault.fr. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@                       NS      srv-dns
srv-dns                 A       172.16.0.116
```

Bonnes pratiques :

- Serial incrémenté manuellement après chaque modification.
- TTL de 1 semaine pour réduire le traffic DNS interne.

4.2. Zone Inverse (inverse.dns)

Chemin : /var/cache/bind/inverse.dns
Fonction : Résolution IP → nom pour le réseau 172.16.0.0/24.

```
 GNU nano 8.4                                                inverse.dns
$TTL    604800
@       IN      SOA     srv-dns.techvault.fr. admin-laser-campus.techvault.fr. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               NS      srv-dns.techvault.fr.
116             PTR     srv-dns.techvault.fr.
```

5. Configuration de BIND

5.1. Fichier named.conf.options
Chemin : /etc/bind/named.conf.options
Fonction : Paramètres globaux.

```
 GNU nano 8.4                                          named.conf.options
options {
    directory "/var/cache/bind";
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    forward only;
    dnssec-validation auto;
    listen-on-v6 { any; };
};
```

Sécurité :

- dnssec-validation auto : Vérification des signatures DNSSEC.
- forward only : Évite les requêtes récursives non sollicitées.

6. Configuration du Firewall (nftables)

Chemin : /etc/nftables.conf

Règles clés :

```
  GNU nano 8.4
#!/usr/sbin/nft -f
flush ruleset

table inet filter {
  chain input {
    type filter hook input priority 0; policy drop;

    ct state {established,related} accept
    iifname "lo" accept

    # DNS UDP/TCP - LAN interne seulement
    udp dport 53 ip saddr 172.16.0.0/24 accept
    tcp dport 53 ip saddr 172.16.0.0/24 accept

    # Admin SSH
    tcp dport 22 accept

    # ICMP diagnostic
    ip protocol icmp accept
  }
 chain output {
    type filter hook output priority 0; policy accept;
    ct state {established,related} accept

    # DNS forwarders Google
    udp dport 53 ip daddr 8.8.8.8 accept
    tcp dport 53 ip daddr 8.8.8.8 accept
  }
 chain forward {
    type filter hook forward priority 0; policy drop;
}

}
```

Sécurité :

- Seuls les clients du LAN (172.16.0.0/24) peuvent interroger le DNS.
- SSH limité aux administrateurs.
- Politique drop par défaut pour input.

7. Tests de fonctionnement

7.1. Test de Mise à Jour Dynamique

- Script d'exemple (nsupdate.sh) :

```
#!/bin/bash
nsupdate -k ./cle-tsig.key <<EOF
server 127.0.0.1
zone techvault.fr
update add test-vm01.techvault.fr 300 A 172.16.0.50
send
EOF
```

Vérification :

➔ *named-journalprint /var/cache/bind/laser.dns.jnl*

- Sortie attendue:

➔ add test-vm01.techvault.fr. 300 IN A 172.16.0.50

```
root@DNS:/var/cache/bind# named-journalprint /var/cache/bind/laser.dns.jnl
del techvault.fr.              604800  IN      SOA     srv-dns.techvault.fr. admin-laser-campus.techvault.fr. 2 604800 86400 2419200 604800
add techvault.fr.              604800  IN      SOA     srv-dns.techvault.fr. admin-laser-campus.techvault.fr. 3 604800 86400 2419200 604800
add test-vm01.techvault.fr.    300     IN      A       172.16.0.50
```

7.2. Vérification Finale

- Redémarrer BIND :

➔ *systemctl restart named*

- Tester la résolution :

➔ *Ping nfs*

```
root@DNS:~# ping nfs
PING nfs.techvault.fr (172.16.0.111) 56(84) bytes of data.
64 bytes from 172.16.0.111: icmp_seq=1 ttl=64 time=0.308 ms
64 bytes from 172.16.0.111: icmp_seq=2 ttl=64 time=0.127 ms
64 bytes from 172.16.0.111: icmp_seq=3 ttl=64 time=0.141 ms
64 bytes from 172.16.0.111: icmp_seq=4 ttl=64 time=0.159 ms
^C
--- nfs.techvault.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.127/0.183/0.308/0.072 ms
root@DNS:~#
```

➔ dig @127.0.0.1 test-vm01.techvault.fr

```
root@DNS:/var/cache/bind# dig 127.0.0.1 test-vm01.techvault.fr

; <<>> DiG 9.20.18-1~deb13u1-Debian <<>> 127.0.0.1 test-vm01.techvault.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 60587
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3a6c331434e02b3a0100000069943aaadd66ead6e97c302a (good)
;; QUESTION SECTION:
;127.0.0.1.                     IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2026021700 1800 900 604800 86400

;; Query time: 11 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Feb 17 10:53:46 CET 2026
;; MSG SIZE  rcvd: 141

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62369
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3a6c331434e02b3a0100000069943aaadd66ead6e97c302a (good)
;; QUESTION SECTION:
;test-vm01.techvault.fr.                IN      A

;; ANSWER SECTION:
test-vm01.techvault.fr. 300     IN      A       172.16.0.50

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Feb 17 10:53:46 CET 2026
;; MSG SIZE  rcvd: 95
```