# BIND9 : zone secondaire, délégation et transferts

**Formation :** BTS SIO — Option SISR

## 1. Rôle et architecture

BIND9 peut publier des zones DNS faisant autorité. Dans l'exemple, ns0 (192.36.3.10) est primaire et ns1 (192.36.3.11) est secondaire pour `californie.cub.sioplc.fr`. Les résolveurs dns0 et dns1 remplissent un autre rôle.

Les changements de zone se font sur le primaire. Le secondaire conserve la copie transférée ; il ne faut pas éditer cette copie comme un fichier de zone de référence.

## 2. Identification locale

La correspondance entre le nom court et le FQDN dans `/etc/hosts` facilite la résolution locale. Elle ne définit ni l'adresse de l'interface ni un enregistrement public.

```
etudiant@ns1:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       ns1.californie.cub.sioplc.fr    ns1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
etudiant@ns1:~$
```

*Identification locale du secondaire ns1.*

## 3. Déclarer la zone secondaire

Extrait de `/etc/bind/named.conf.local`, reprenant la syntaxe observée :

```
zone "californie.cub.sioplc.fr" {
    type slave;
    masters { 192.36.3.10; };
    file "/var/cache/bind/db.californie.cub.sioplc.fr";
};
```

`secondary` et `primaries` sont les termes actuels correspondant à `slave` et `masters`. Vérifier la version installée avant de modifier une configuration existante.




*Zone secondaire et adresse du primaire.*

Le primaire doit autoriser le transfert vers le secondaire et le réseau doit laisser passer les échanges nécessaires, notamment TCP 53 pour AXFR. La déclaration locale ne prouve pas à elle seule que le transfert fonctionne.

## 4. Journaliser les événements

Dans `/etc/bind/named.conf.log` :

```
logging {
    channel bind_log {
        file "/var/log/bind.log" versions 3 size 100m;
        severity info;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    category default { bind_log; };
};
```

Inclure ce fichier depuis la configuration générale :

```
include "/etc/bind/named.conf.log";
```

```
etudiant@ns1:~$ cat /etc/bind/named.conf.log
logging {

    channel bind_log {
                    file "/var/log/bind.log" versions 3 size 100m;
                   severity info;
                    print-category  yes;
                    print-severity  yes;
                    print-time      yes;
    };

    category default { bind_log; };
};
etudiant@ns1:~$
```

*Canal de journalisation avec rotation.*

```
etudiant@ns1:~$ cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.root-hints";

// Ajout du fichier de parametrage de la journalisation du service BIND
include "/etc/bind/named.conf.log";
etudiant@ns1:~$
```

*Inclusion du fichier de journalisation.*

Vérifier les droits d'écriture et le confinement AppArmor. La catégorie `default` ne signifie pas que toutes les requêtes des clients seront journalisées.

# 5. Déléguer la zone depuis son parent

Dans la zone parente `cub.sioplc.fr`, les enregistrements concernés sont :

```
californie       IN NS ns0.californie.cub.sioplc.fr.
californie       IN NS ns1.californie.cub.sioplc.fr.
ns0.californie   IN A  192.36.3.10
ns1.californie   IN A  192.36.3.11
```

Les enregistrements A fournissent les données de raccordement pour ces serveurs situés dans la zone déléguée. Augmenter le numéro de série de la zone parente lors de sa modification, contrôler sa

syntaxe puis la recharger.

```
; Création de la délégation de zone pour Californie
californie.cub.sioplc.fr. IN NS ns0.californie.cub.sioplc.fr.
californie.cub.sioplc.fr. IN NS ns1.californie.cub.sioplc.fr.
; Création des enregistrements A pour la délégation Anvers
ns0.californie IN A 192.36.3.10
ns1.californie IN A 192.36.3.11
```

*Délégation et glue records dans la zone parente.*

Le commentaire « délégation Anvers » visible dans la capture provient d'un modèle ; les enregistrements montrés concernent Californie.

```
sudo named-checkconf -z
# Après contrôle réussi, sur le serveur de la zone parente :
sudo rndc reload cub.sioplc.fr
```

```
etudiant@ns0:~$ sudo named-checkconf -z
zone cub.sioplc.fr/IN: loaded serial 2026100802
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
etudiant@ns0:~$ sudo systemctl reload bind9
```

*Chargement de la zone parente, série 2026100802.*

## 6. Vérifier le transfert

```
tail -n 80 /var/log/bind.log
dig @192.36.3.10 californie.cub.sioplc.fr SOA +norecurse
dig @192.36.3.11 californie.cub.sioplc.fr SOA +norecurse
```

Dans les journaux conservés, une première tentative échoue avec SERVFAIL. Une tentative ultérieure réussit : le secondaire affiche `Transfer status: success` et `Transfer completed` pour la série **2026100801**. Le primaire enregistre le même numéro de série et un AXFR de six enregistrements.

```
etudiant@ns1:~$ tail -f /var/log/bind.log
08-Oct-2026 10:47:14.333 xfer-in: info: zone californie.cub.sioplc.fr/IN: refresh: unexpected
 rcode (SERVFAIL) from primary 192.36.3.10#53 (source 0.0.0.0#0)
08-Oct-2026 11:00:08.699 notify: info: client @0x7fad3bf20000 192.36.3.10#38518: received not
ify for zone 'californie.cub.sioplc.fr'
08-Oct-2026 11:00:08.699 xfer-in: info: zone californie.cub.sioplc.fr/IN: notify from 192.36.
3.10#38518: no serial
08-Oct-2026 11:00:08.699 xfer-in: info: zone californie.cub.sioplc.fr/IN: Transfer started.
08-Oct-2026 11:00:08.699 xfer-in: info: 0x7fad39442000: transfer of 'californie.cub.sioplc.fr
/IN' from 192.36.3.10#53: connected using 192.36.3.10#53
08-Oct-2026 11:00:08.699 xfer-in: info: zone californie.cub.sioplc.fr/IN: transferred serial
2026100801
08-Oct-2026 11:00:08.699 xfer-in: info: 0x7fad39442000: transfer of 'californie.cub.sioplc.fr
/IN' from 192.36.3.10#53: Transfer status: success
08-Oct-2026 11:00:08.699 xfer-in: info: 0x7fad39442000: transfer of 'californie.cub.sioplc.fr
/IN' from 192.36.3.10#53: Transfer completed: 1 messages, 6 records, 222 bytes, 0.001 secs (2
22000 bytes/sec) (serial 2026100801)
08-Oct-2026 11:00:08.699 notify: info: zone californie.cub.sioplc.fr/IN: sending notifies (se
rial 2026100801)
08-Oct-2026 11:00:08.703 notify: info: zone californie.cub.sioplc.fr/IN: sending notify to 19
2.36.3.10#53
```

*Transfert réussi sur ns1 après une première erreur.*

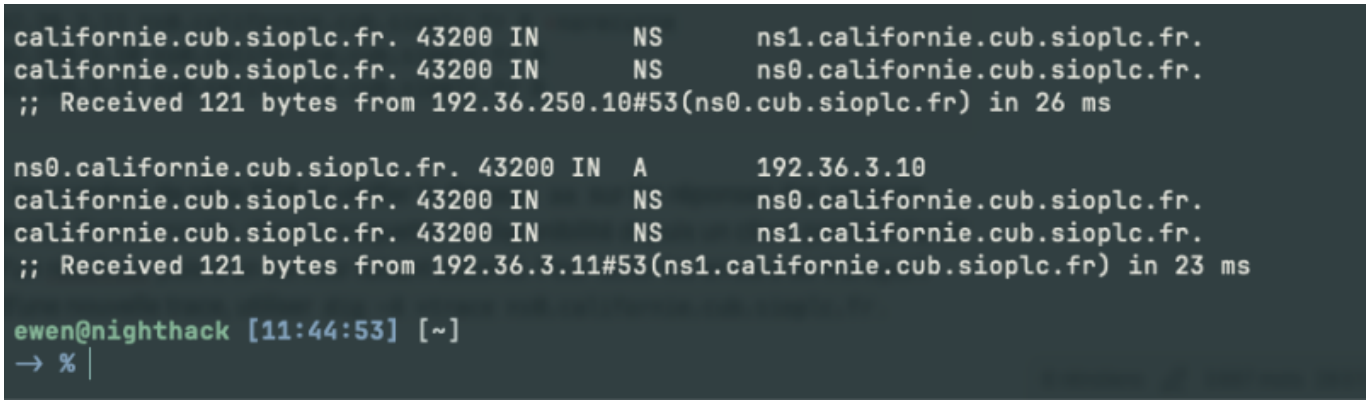
```
etudiant@ns0:~$ tail -f /var/log/bind.log
08-Oct-2026 11:00:08.680 lame-servers: info: network unreachable resolving './DNSKEY/IN': 200
1:503:c27::2:30#53
08-Oct-2026 11:00:08.680 lame-servers: info: network unreachable resolving './NS/IN': 2001:50
0:9f::42#53
08-Oct-2026 11:00:08.684 xfer-out: info: client @0x7fb019e30c00 192.36.3.11#56022 (californie
.cub.sioplc.fr): transfer of 'californie.cub.sioplc.fr/IN': AXFR started (serial 2026100801)
08-Oct-2026 11:00:08.684 xfer-out: info: client @0x7fb019e30c00 192.36.3.11#56022 (californie
.cub.sioplc.fr): transfer of 'californie.cub.sioplc.fr/IN': AXFR ended: 1 messages, 6 records
, 222 bytes, 0.001 secs (222000 bytes/sec) (serial 2026100801)
08-Oct-2026 11:00:08.684 notify: info: client @0x7fb01c96e000 192.36.3.11#55113: received not
ify for zone 'californie.cub.sioplc.fr'
08-Oct-2026 11:00:08.708 lame-servers: info: network unreachable resolving './DNSKEY/IN': 200
1:500:2f::f#53
08-Oct-2026 11:00:08.708 lame-servers: info: network unreachable resolving './DNSKEY/IN': 200
1:500:a8::e#53
08-Oct-2026 11:00:08.708 lame-servers: info: network unreachable resolving './DNSKEY/IN': 200
1:500:2::c#53
08-Oct-2026 11:00:09.516 dnssec: info: managed-keys-zone: Key 20326 for zone . is now trusted
 (acceptance timer complete)
08-Oct-2026 11:00:09.516 dnssec: info: managed-keys-zone: Key 38696 for zone . is now trusted
 (acceptance timer complete)
```

*AXFR vers ns1 enregistré sur le primaire.*

Ces événements valident le transfert à l'instant capturé. Les messages IPv6 `network unreachable` restent un diagnostic distinct du transfert IPv4 réussi.

# 7. Contrôler le parcours de résolution

```
dig +trace ns0.californie.cub.sioplc.fr
```




*Fin de la trace : réponse provenant du secondaire 192.36.3.11.*

La trace aboutit à `ns0.californie.cub.sioplc.fr A 192.36.3.10`. Elle démontre ce parcours et cette réponse, pas le basculement automatique d'un client entre dns0 et dns1.

# 8. Références

- ISC — configuration BIND9
- Comprendre la résolution et lire dig

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
**https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:services:bind9**

Last update: **2026/10/18 01:23**