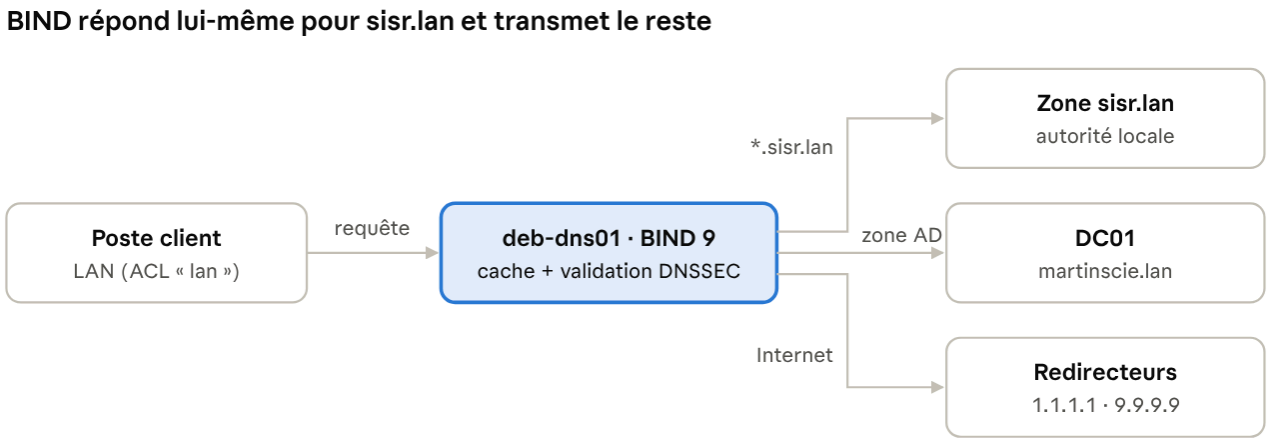
Serveur DNS sous Debian 13 avec BIND 9

Nov 27, 2026 · @Serge Martins

Objectif et architecture

Ce guide installe **BIND 9**, le serveur DNS libre de référence, sur Debian 13. Le serveur `deb-dns01` joue trois rôles : résolveur avec cache pour les postes, serveur **faisant autorité** pour une zone de lab `sisr.lan`, et relais vers DC01 pour le domaine Active Directory `martinscie.lan`.

Élément	Valeur (à adapter)
Serveur DNS	`deb-dns01` – `192.168.10.14/24`
Logiciel	BIND 9.20 (paquet `bind9` de Debian 13)
Zone faisant autorité	`sisr.lan` (fichier `/etc/bind/db.sisr.lan`)
Domaine AD	`martinscie.lan` et zones inverses → relayés vers DC01 `192.168.10.10`
Redirecteurs Internet	`1.1.1.1`, `9.9.9.9`
Clients autorisés	`192.168.10.0/24`, `192.168.20.0/24`



Les trois rôles de deb-dns01

1. Installation

```
hostnamectl set-hostname deb-dns01
# IP fixe 192.168.10.14/24 dans /etc/network/interfaces (passerelle
192.168.10.254)
apt update && apt full-upgrade -y
apt install -y bind9 bind9-utils bind9-dnsutils
systemctl status named
named -v                        # BIND 9.20.x
```

Les fichiers de configuration sont dans `/etc/bind/` : `named.conf.options` (réglages généraux) et `named.conf.local` (zones).

2. Résolveur sécurisé : `/etc/bind/named.conf.options`

```
acl "lan" {
    127.0.0.1;
    192.168.10.0/24;
    192.168.20.0/24;
};

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

    listen-on { 127.0.0.1; 192.168.10.14; };
    listen-on-v6 { none; };

    recursion yes;
    allow-query     { lan; };
    allow-recursion { lan; };
    allow-transfer  { none; };

    forwarders { 1.1.1.1; 9.9.9.9; };
    dnssec-validation auto;

    version "non communiquée";
};
```

- `allow-recursion { lan; }` : le serveur ne résout que pour le réseau interne (pas de **résolveur ouvert**, utilisé pour des attaques par amplification).
- `dnssec-validation auto` : les réponses signées sont vérifiées, ce qui protège contre l'empoisonnement du cache.

3. Zones : `/etc/bind/named.conf.local`

```
// Zone de lab dont deb-dns01 est l'autorité
zone "sisr.lan" {
    type primary;
    file "/etc/bind/db.sisr.lan";
    allow-update { none; };
};

// Domaine Active Directory : demandé à DC01
zone "martinscie.lan" {
    type forward;
    forward only;
    forwarders { 192.168.10.10; };
};

// Résolution inverse des VLAN : gérée par DC01
zone "10.168.192.in-addr.arpa" { type forward; forward only; forwarders {
192.168.10.10; }; };
zone "20.168.192.in-addr.arpa" { type forward; forward only; forwarders {
192.168.10.10; }; };
```

Pour les zones relayées vers DC01 (domaine `.lan` non signé), désactiver la validation DNSSEC de ces noms en ajoutant dans `options` : `validate-except { "martinscie.lan"; "10.168.192.in-addr.arpa"; "20.168.192.in-addr.arpa"; };`

4. Fichier de zone : `/etc/bind/db.sisr.lan`

```
$TTL 86400
@   IN  SOA deb-dns01.sisr.lan. admin.sisr.lan. (
        2026112701 ; serial (AAAAMMJJnn) : à incrémenter à chaque
modification
        3600       ; refresh
        900        ; retry
        604800     ; expire
        86400 )    ; TTL négatif

@           IN  NS     deb-dns01.sisr.lan.
@           IN  MX 10  mail.sisr.lan.
deb-dns01   IN  A      192.168.10.14
www         IN  A      192.168.10.40
intranet    IN  CNAME  www
mail        IN  A      192.168.10.41
```

5. Vérification et démarrage

```
named-checkconf                                    # syntaxe de la
configuration
named-checkzone sisr.lan /etc/bind/db.sisr.lan     # syntaxe de la zone
systemctl restart named
rndc reload sisr.lan                               # après chaque modification
de zone
```

6. Tests

```
dig @192.168.10.14 www.sisr.lan                # zone locale : flag aa
(autorité)
dig @192.168.10.14 intranet.sisr.lan           # CNAME
dig @192.168.10.14 sisr.lan MX
dig @192.168.10.14 dc01.martinscie.lan         # relayé vers DC01
dig @192.168.10.14 www.debian.org              # Internet ; 2e essai : temps ≈
0 ms (cache)
dig @192.168.10.14 isc.org +dnssec             # flag ad = réponse validée
DNSSEC
journalctl -u named -f
```

Pour que les postes utilisent deb-dns01, mettre `192.168.10.14` dans l'option DNS du DHCP. Attention : les postes Windows membres du domaine doivent garder **DC01 en DNS principal** (enregistrements dynamiques sécurisés de l'AD).

Symptôme	Cause probable	Correction
`named` ne démarre pas	Erreur de syntaxe	`named-checkconf`, `journalctl -u named`
`REFUSED` depuis un poste	Poste hors de l'ACL `lan`	Ajouter son réseau à l'ACL
Modification de zone non prise en compte	Serial non incrémenté	Augmenter le serial, `rndc reload`
`SERVFAIL` sur martinscie.lan	Validation DNSSEC d'une zone non signée	Ajouter la zone à `validate-except`
Pas de résolution Internet	Redirecteurs bloqués	Autoriser UDP/TCP 53 sortant sur pfSense

7. Sécurisation

- [ ] Appliquer les mises à jour de sécurité Debian : BIND en a reçu plusieurs en 2025-2026.
- [ ] Garder la récursion limitée au LAN et les transferts de zone interdits (ou limités à un secondaire, avec clé TSIG).
- [ ] Pare-feu nftables : port 53 depuis le LAN seulement, `rndc` (953) en local uniquement.
- [ ] Ajouter un serveur secondaire (`type secondary;`) pour la zone `sisr.lan` .
- [ ] Sauvegarder `/etc/bind/` .