

DNS

DNS

Mise en place d'un résolveur DNS local

Le réseau contient un serveur DNS local.

screne

(schéma réseau avec DNS)

Installer bind9 avec apt-get install bind9.

Configurer le fichier /etc/bind/named.conf.options.

Activer la récursivité.

Ajouter allow-recursion et listen-on.

Ajouter un forwarder 8.8.8.8.

bien enlever les commentaire pour les forwarder

```
GNU nano 7.2                                named.conf.options
acl A { 192.168.100.0/28; 192.168.10.0/24; 192.168.90.0/28; 192.168.110.0/29; 192.168.130.0/24};

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;
    recursion yes;
    listen-on-v6 { any; };
    allow-query { A; };
};
```

<https://sioaubusson.fr/books/essentielle/page/dhcp-sur-serveur-dns-debian-12>

Le cache DNS accélère les requêtes suivantes.

Mise en place d'une zone DNS

Modifier le fichier `/etc/bind/named.conf.local`.

Ajouter une zone DNS.

```
GNU nano 7.2 nan
//
// 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 "gsb.sio.jja"{
    type master;
    file "/etc/bind/db.gsb.sio.jja";
};

zone "100.168.192.in-addr.arpa"{
    type master;
    file "/etc/bind/db.192.168.100";
};
```

Créer le fichier db.gchauquet.sio.jja à partir de db.local.

```
GNU nano 7.2
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      db.gsb.sio.jja. root.gsb.sio.jja. (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       db.gsb.sio.jja.
db        IN      A        192.168.100.2
lap       IN      A        192.168.90.2
lap2      IN      A        192.168.90.3
glpi      IN      CNAME    lap
next      IN      CNAME    lap2
```

Associer le domaine à l'IP du DNS.

Configurer le serveur NS.

Ajouter le serveur LAMP.

Créer un sous-domaine test.

Zones DNS inversées

Ajouter une zone inversée dans named.conf.local.

screne

(zone in-addr.arpa ajoutée)

Créer le fichier rev.gsb.sio.jja.

Ajouter un enregistrement PTR.

```
GNU nano 7.2
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      db.gsb.sio.jja. root.gsb.sio.jja. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       db.gsb.sio.jja.
;
2         IN      PTR      db.gsb.sio.jja
20        IN      PTR      glpi.gsb.sio.jja
```

Redémarrer bind9 pour appliquer.

Vérifier avec named-checkzone et named-checkconf.

Sécurisation du DNS

Configurer une ACL dans named.conf.options.

screne

(fichier avec ACL)

Autoriser les requêtes avec allow-query.

Autoriser la récursivité avec allow-recursion.

screne

(configuration finale sécurisée)

Revision #5

Created 2026-03-23 13:11:42 UTC by Admin

Updated 2026-04-21 09:17:08 UTC by Admin