

Your submission was sent successfully! [Close](#)

You have successfully unsubscribed! [Close](#)

Recherche sur les documen

Soumettre

Service de noms de domaine (DNS)

Le service de noms de domaine (DNS) est un service Internet qui mappe les adresses IP et les noms de domaine entièrement qualifiés (FQDN) les uns aux autres. De cette façon, DNS atténue le besoin de mémoriser les adresses IP. Les ordinateurs qui exécutent DNS sont appelés *serveurs de noms*. Ubuntu est livré avec BIND (Berkley Internet Naming Daemon), le programme le plus utilisé pour maintenir un serveur de noms sous Linux.

Installation

À une invite de terminal, entrez la commande suivante pour installer dns:

```
sudo apt install bind9
```

Un package très utile pour tester et résoudre les problèmes DNS est le `dnsutils` paquet. Très souvent, ces outils seront déjà installés, mais pour vérifier et / ou installer `dnsutils` entrez ce qui suit:

```
sudo apt install dnsutils
```

Configuration

Il existe de nombreuses façons de configurer BIND9. Certaines des configurations les plus courantes sont un serveur de noms de mise en cache, un serveur principal et un serveur secondaire.

- Lorsqu'il est configuré en tant que serveur de noms de mise en cache, BIND9 trouvera la réponse aux requêtes de noms et se souviendra de la réponse lorsque le domaine est à nouveau interrogé.
- En tant que serveur principal, BIND9 lit les données d'une zone à partir d'un fichier sur son hôte et fait autorité pour cette zone.
- En tant que serveur secondaire, BIND9 obtient les données de zone d'un autre serveur de noms faisant autorité pour la zone.

Aperçu

Les fichiers de configuration DNS sont stockés dans le `/etc/bind` répertoire. Le fichier de configuration principal est `/etc/bind/named.conf`, qui dans la mise en page fournie par le package inclut simplement ces fichiers.

- `/etc/bind/named.conf.options`: options DNS globales
- `/etc/bind/named.conf.local`: pour vos zones
- `/etc/bind/named.conf.default-zones`: zones par défaut telles que localhost, son inverse et les indices racine

Les serveurs de noms racine étaient décrits dans le fichier `/etc/bind/db.root`. Ceci est maintenant fourni à la place par le `/usr/share/dns/root.hints` fichier livré avec le `dns-root-data` package, et est référencé dans le `named.conf.default-zones` fichier de configuration ci-dessus.

Il est possible de configurer le même serveur pour qu'il soit un serveur de noms de mise en cache, primaire et secondaire: tout dépend des zones qu'il dessert. Un serveur peut être le début de l'autorité (SOA) pour une zone, tout en fournissant un service secondaire pour une autre zone. Tout en fournissant des services de mise en cache pour les hôtes sur le LAN local.

Serveur de noms de mise en cache

La configuration par défaut agit comme un serveur de mise en cache. Décommentez et modifiez `/etc/bind/named.conf.options` pour définir les adresses IP des serveurs DNS de votre FAI:

```
forwarders {  
    1.2.3.4;  
    5.6.7.8;  
};
```

Remarque

Remplacer 1.2.3.4 et 5.6.7.8 avec les adresses IP des serveurs de noms réels.

Pour activer la nouvelle configuration, redémarrez le serveur DNS. À partir d'une invite de terminal:

```
sudo systemctl restart bind9.service
```

Voir [creuser](#) pour des informations sur les tests d'un serveur DNS de mise en cache.

Serveur principal

Dans cette section, BIND9 sera configuré comme serveur principal pour le domaine `example.com`. Remplacez simplement `example.com` avec votre FQDN (Nom de domaine dûment qualifié).

Fichier de zone avant

Pour ajouter une zone DNS à BIND9, en transformant BIND9 en serveur principal, modifiez d'abord `/etc/bind/named.conf.local`:

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};
```

Remarque

Si bind recevra des mises à jour automatiques du fichier comme avec DDNS, alors utilisez `/var/lib/bind/db.example.com` plutôt que `/etc/bind/db.example.com` ici et dans la commande de copie ci-dessous.

Utilisez maintenant un fichier de zone existant comme modèle pour créer le `/etc/bind/db.example.com` fichier:

```
sudo cp /etc/bind/db.local /etc/bind/db.example.com
```

Modifier le nouveau fichier de zone `/etc/bind/db.example.com` et changer `localhost.` au FQDN de votre serveur, laissant le supplément `.` à la fin. Changer `127.0.0.1` à l'adresse IP du serveur de noms et `root.localhost` à une adresse e-mail valide, mais avec un `.` au lieu de l'habituel `@` symbole, quittant à nouveau le `.` à la fin. Modifiez le commentaire pour indiquer le domaine auquel ce fichier est destiné.

Créer un *Un record* pour le domaine de base, `example.com`. Créer un *Un record* pour `ns.example.com`, le serveur de noms dans cet exemple:

```
;
; BIND data file for example.com
;
$TTL      604800
@         IN      SOA     example.com. root.example.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL

@         IN      NS      ns.example.com.
@         IN      A       192.168.1.10
@         IN      AAAA    ::1
ns        IN      A       192.168.1.10
```

Vous devez incrémenter le *Numéro de série* chaque fois que vous apportez des modifications au fichier de zone. Si vous effectuez plusieurs modifications avant de redémarrer BIND9, incrémentez simplement la série une fois.

Maintenant, vous pouvez ajouter des enregistrements DNS au bas du fichier de zone. Voir [Types d'enregistrements courants](#) pour plus de détails.

Remarque

De nombreux administrateurs aiment utiliser la dernière date modifiée comme série d'une zone, comme `2020012100` qui est `yyymmddss` (où `ss` est le numéro de série)

Une fois que vous avez apporté des modifications au fichier de zone, BIND9 doit être redémarré pour que les modifications prennent effet:

```
sudo systemctl restart bind9.service
```

Fichier de zone inversée

Maintenant que la zone est configurée et résout les noms en adresses IP, un *Zone inverse* doit être ajouté pour permettre à DNS de résoudre une adresse à un nom.

Modifier `/etc/bind/named.conf.local` et ajouter ce qui suit:

```
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

Remarque

Remplacer `1.168.192` avec les trois premiers octets du réseau que vous utilisez. Nommez également le fichier de zone `/etc/bind/db.192` convenablement. Il doit correspondre au premier octet de votre réseau.

Maintenant, créez le `/etc/bind/db.192` fichier:

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

Édition suivante `/etc/bind/db.192` changer les mêmes options que `/etc/bind/db.example.com`:

```
;
; BIND reverse data file for local 192.168.1.XXX net
;
$TTL      604800
@         IN      SOA      ns.example.com. root.example.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns.
10        IN      PTR      ns.example.com.
```

Le *Numéro de série* dans la zone inverse doit également être incrémenté à chaque changement. Pour chaque *Un record* vous configurez dans `/etc/bind/db.example.com`, c'est pour une adresse différente, vous devez créer un *Enregistrement PTR* dans `/etc/bind/db.192`.

Après avoir créé le fichier de zone inverse, redémarrez BIND9:

```
sudo systemctl restart bind9.service
```

Serveur secondaire

Une fois un *Serveur principal* a été configuré a *Serveur secondaire* est fortement recommandé afin de maintenir la disponibilité du domaine si la Primaire devenait indisponible.

Tout d'abord, sur le serveur principal, le transfert de zone doit être autorisé. Ajouter le `allow-transfer` option à l'exemple des définitions de zone avant et arrière dans `/etc/bind/named.conf.local`:

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
    allow-transfer { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
    allow-transfer { 192.168.1.11; };
};
```

Remarque

Remplacer `192.168.1.11` avec l'adresse IP de votre serveur de noms secondaire.

Redémarrez BIND9 sur le serveur principal:

```
sudo systemctl restart bind9.service
```

Ensuite, sur le serveur secondaire, installez le package `bind9` de la même manière que sur le primaire. Modifiez ensuite le `/etc/bind/named.conf.local` et ajouter les déclarations suivantes pour les zones avant et arrière:

```
zone "example.com" {
    type secondary;
    file "db.example.com";
    masters { 192.168.1.10; };
};

zone "1.168.192.in-addr.arpa" {
    type secondary;
    file "db.192";
    masters { 192.168.1.10; };
};
```

Remarque

Remplacer 192.168.1.10 avec l'adresse IP de votre serveur de noms principal.

Redémarrez BIND9 sur le serveur secondaire:

```
sudo systemctl restart bind9.service
```

Dans /var/log/syslog vous devriez voir quelque chose de similaire à (certaines lignes ont été divisées pour s'adapter au format de ce document):

```
client 192.168.1.10#39448: received notify for zone '1.168.192.in-addr.arpa'
zone 1.168.192.in-addr.arpa/IN: Transfer started.
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
  connected using 192.168.1.11#37531
zone 1.168.192.in-addr.arpa/IN: transferred serial 5
transfer of '100.18.172.in-addr.arpa/IN' from 192.168.1.10#53:
  Transfer completed: 1 messages,
6 records, 212 bytes, 0.002 secs (106000 bytes/sec)
zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 5)

client 192.168.1.10#20329: received notify for zone 'example.com'
zone example.com/IN: Transfer started.
transfer of 'example.com/IN' from 192.168.1.10#53: connected using 192.168.1.11#38577
zone example.com/IN: transferred serial 5
transfer of 'example.com/IN' from 192.168.1.10#53: Transfer completed: 1 messages,
8 records, 225 bytes, 0.002 secs (112500 bytes/sec)
```

Remarque

Remarque: Une zone n'est transférée que si le *Numéro de série* sur la primaire est plus grand que celui du secondaire. Si vous souhaitez que votre DNS principal notifie d'autres serveurs DNS secondaires de changements de zone, vous pouvez ajouter `also-notify { ipaddress; };` à /etc/bind/named.conf.local comme indiqué dans l'exemple ci-dessous:

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
    allow-transfer { 192.168.1.11; };
    also-notify { 192.168.1.11; };
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
    allow-transfer { 192.168.1.11; };
    also-notify { 192.168.1.11; };
};
```

Remarque

Le répertoire par défaut pour les fichiers de zone non faisant autorité est /var/cache/bind/. Ce répertoire est également configuré dans AppArmor pour permettre au démon nommé de lui écrire. Pour plus d'informations sur AppArmor voir [Sécurité - AppArmor](#).

Dépannage

Cette section couvre les problèmes de diagnostic avec les configurations DNS et BIND9.

Test

resolv.conf

La première étape du test de BIND9 consiste à ajouter l'adresse IP du serveur de noms à un résolveur d'hôtes. Le serveur de noms principal doit être configuré ainsi qu'un autre hôte pour vérifier les choses. Se référer à [Configuration du client DNS](#) pour plus de détails sur l'ajout d'adresses de serveur de noms à vos clients réseau. À la fin votre nameserver ligne en /etc/resolv.conf devrait pointer du doigt 127.0.0.53 et vous devriez avoir un search paramètre pour votre domaine. Quelque chose comme ça:

```
nameserver 127.0.0.53
search example.com
```

Pour vérifier quel serveur DNS votre résolveur local utilise, exécutez:

```
systemd-resolve --status
```

Remarque

Vous devez également ajouter l'adresse IP du serveur de noms secondaire à la configuration de votre client au cas où le primaire deviendrait indisponible.

creuser

Si vous avez installé le package dnsutils, vous pouvez tester votre configuration à l'aide de la recherche d'utilitaire DNS:

- Après avoir installé BIND9, utilisez dig contre l'interface de bouclage pour vous assurer qu'il écoute sur le port 53. À partir d'une invite de terminal:

```
dig -x 127.0.0.1
```

Vous devriez voir des lignes similaires à celles suivantes dans la sortie de commande:

```
;; Query time: 1 msec
;; SERVER: 192.168.1.10#53(192.168.1.10)
```

- Si vous avez configuré BIND9 en tant que *Entraînement* serveur de noms " dig " un domaine extérieur pour vérifier l'heure de la requête:

```
dig ubuntu.com
```

Notez le temps de requête vers la fin de la sortie de commande:

```
;; Query time: 49 msec
```

Après une deuxième fouille, il devrait y avoir une amélioration:

```
;; Query time: 1 msec
```

ping

Maintenant, pour démontrer comment les applications utilisent DNS pour résoudre un nom d'hôte, utilisez l'utilitaire ping pour envoyer une demande d'écho ICMP:

```
ping example.com
```

Ce test si le serveur de noms peut résoudre le nom ns.example.com à une adresse IP. La sortie de commande doit ressembler:

```
PING ns.example.com (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.800 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.813 ms
```

zone de contrôle nommée

Un excellent moyen de tester vos fichiers de zone est d'utiliser le named-checkzone utilitaire installé avec le bind9 paquet. Cet utilitaire vous permet de vous assurer que la configuration est correcte avant de redémarrer BIND9 et de mettre les modifications en ligne.

- Pour tester notre exemple de fichier de zone Transférer, entrez ce qui suit à partir d'une invite de commande:

```
named-checkzone example.com /etc/bind/db.example.com
```

Si tout est configuré correctement, vous devriez voir une sortie similaire à:

```
zone example.com/IN: loaded serial 6
OK
```

- De même, pour tester le fichier de zone inverse, entrez ce qui suit:

```
named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192
```

La sortie doit être similaire à:

```
zone 1.168.192.in-addr.arpa/IN: loaded serial 3
OK
```

Remarque

Le *Numéro de série* de votre fichier de zone sera probablement différent.

Enregistrement rapide de la requête temporaire

Avec le `rndc` outil, vous pouvez activer et désactiver rapidement la journalisation des requêtes, sans redémarrer le service ni modifier le fichier de configuration.

Pour transformer la journalisation de la requête *sur*, courir:

```
sudo rndc querylog on
```

De même, pour l'éteindre, exécutez:

```
sudo rndc querylog off
```

Les journaux seront envoyés au syslog et apparaîtront dans `/var/log/syslog` par défaut:

```
Jan 20 19:40:50 new-n1 named[816]: received control channel command 'querylog on'
Jan 20 19:40:50 new-n1 named[816]: query logging is now on
Jan 20 19:40:57 new-n1 named[816]: client @0x7f48ec101480 192.168.1.10#36139 (ubuntu.com): query: ubuntu.com IN A +E(0)K (:
```

Remarque

La quantité de journaux générés en activant `querylog` pourrait être énorme!

Journalisation

BIND9 propose une grande variété d'options de configuration de journalisation, mais les deux principales sont *canal* et *catégorie*, qui configurent où vont les journaux et quelles informations sont enregistrées, respectivement.

Si aucune option de journalisation n'est configurée, la configuration par défaut est:

```
logging {
    category default { default_syslog; default_debug; };
    category unmatched { null; };
};
```

Configurons plutôt BIND9 à envoyer *débogage* messages liés aux requêtes DNS dans un fichier séparé.

Nous devons configurer un *canal* de spécifier le fichier auquel envoyer les messages et un *catégorie*. Dans cet exemple, le *catégorie* enregistrera toutes les requêtes. Modifier `/etc/bind/named.conf.local` et ajouter ce qui suit:

```
logging {
    channel query.log {
        file "/var/log/named/query.log";
        severity debug 3;
    };
    category queries { query.log; };
};
```

Remarque

Le *débogage* l'option peut être définie de 1 à 3. Si un niveau n'est pas spécifié, le niveau 1 est la valeur par défaut.

- Depuis le *nom de démon* fonctionne comme le *lier* utilisateur le `/var/log/named` le répertoire doit être créé et la propriété modifiée:

```
sudo mkdir /var/log/named
sudo chown bind:bind /var/log/named
```

- Redémarrez maintenant BIND9 pour que les modifications prennent effet:

```
sudo systemctl restart bind9.service
```

Vous devriez voir le fichier `/var/log/named/query.log` remplissez d'informations sur la requête. Ceci est un exemple simple des options de journalisation BIND9. Pour la couverture des options avancées, voir [Plus d'informations](#).

Références

Types d'enregistrements courants

Cette section couvre certains des types d'enregistrements DNS les plus courants.

- Aenregistrement: cet enregistrement mappe une adresse IP à un nom d'hôte.

```
www      IN      A      192.168.1.12
```

- CNAME enregistrement: utilisé pour créer un alias sur un enregistrement A existant. Vous ne pouvez pas créer un CNAME enregistrement pointant vers un autre CNAME record.

```
web      IN      CNAME  www
```

- MX enregistrement: utilisé pour définir où envoyer le courrier électronique. Doit pointer vers un A record, pas un CNAME.

```
@        IN      MX      1      mail.example.com.
mail     IN      A      192.168.1.13
```

- NS enregistrement: utilisé pour définir quels serveurs servent des copies d'une zone. Il doit pointer vers un A record, pas un CNAME. C'est là que les serveurs principaux et secondaires sont définis.

```
@        IN      NS      ns.example.com.
@        IN      NS      ns2.example.com.
ns       IN      A      192.168.1.10
ns2      IN      A      192.168.1.11
```

Plus d'informations

- [Documentation BIND9 en amont <https://bind9.readthedocs.io/en/latest/>](https://bind9.readthedocs.io/en/latest/)
- [DNS et BIND <http://shop.oreilly.com/product/9780596100575.do>](http://shop.oreilly.com/product/9780596100575.do) est un livre populaire maintenant dans sa cinquième édition. Il y a maintenant aussi un [DNS et BIND sur IPv6 <http://shop.oreilly.com/product/0636920020158.do>](http://shop.oreilly.com/product/0636920020158.do) livre.
- A great place to ask for BIND9 assistance, and get involved with the Ubuntu Server community, is the `#ubuntu-server` IRC channel on [freenode <http://freenode.net>](http://freenode.net).

[Previous Debuginfod FAQ Next FTP](#)

Last updated 6 months ago. [Help improve this document in the forum <https://discourse.ubuntu.com/t/service-domain-name-service-dns/11318>](https://discourse.ubuntu.com/t/service-domain-name-service-dns/11318).