Serveur DNS récursif avec Unbound

Objectif

Mettre en place un serveur DNS récursif avec **Unbound** permettant :

- la résolution récursive des domaines Internet sans utiliser de DNS public comme résolveur intermédiaire ;
- la mise en cache des réponses DNS ;
- la résolution de noms DNS internes ;
- l'utilisation depuis plusieurs réseaux IPv4 ;
- le support d'IPv6 ;
- le contrôle des réseaux autorisés à utiliser le resolver.

---

1. Fichier de configuration principal

La configuration Unbound est organisée dans :

```
/etc/unbound/unbound.conf
```

Les configurations supplémentaires peuvent être placées dans :

```
/etc/unbound/unbound.conf.d/
```

Par exemple :

```
/etc/unbound/unbound.conf.d/local.conf
```

Le fichier `unbound.conf` charge généralement les fichiers présents dans `unbound.conf.d`.

---

2. Configuration réseau

Dans :

```
/etc/unbound/unbound.conf.d/local.conf
```

Ajouter ou adapter la section `server:` :

```
server:
    verbosity: 0

    # Écoute IPv4
    interface: 0.0.0.0

    # Écoute IPv6
    interface: ::0

    # Réseaux IPv4 autorisés
    access-control: 127.0.0.0/8 allow
    access-control: 192.168.10.0/24 allow
    access-control: 10.20.0.0/24 allow

    # Réseaux IPv6 autorisés
    access-control: ::1 allow
    access-control: fd00::/8 allow

    # Protocoles
    do-ip4: yes
    do-ip6: yes

    # Ne privilégie pas IPv6 pour les communications sortantes
    prefer-ip6: no
```

Écoute IPv4

```
interface: 0.0.0.0
```

Unbound écoute sur toutes les interfaces IPv4 disponibles.

Écoute IPv6

```
interface: ::0
```

Unbound écoute sur les interfaces IPv6 disponibles.

Contrôle d'accès

Les directives `access-control` déterminent quels réseaux peuvent interroger le serveur DNS.

Exemple :

```
access-control: 192.168.10.0/24 allow
```

autorise les clients du réseau `192.168.10.0/24`.

Pour IPv6, le préfixe doit être adapté au réseau réellement utilisé.

Exemple avec un réseau ULA :

```
access-control: fd00::/8 allow
```

Il est préférable d'utiliser le préfixe IPv6 réel du réseau plutôt qu'une plage plus large que nécessaire.

---

3. Support IPv4 et IPv6

Les deux protocoles sont activés avec :

```
do-ip4: yes
do-ip6: yes
```

Cela concerne les communications d'Unbound avec les autres serveurs DNS.

L'écoute des clients est configurée séparément avec :

```
interface: 0.0.0.0
interface: ::0
```

Il faut donc distinguer :

- `do-ip6` → permet à Unbound d'utiliser IPv6 ;
- `interface: ::0` → permet aux clients IPv6 de contacter Unbound.

4. Résolution DNS locale

Unbound peut également gérer une zone locale pour résoudre des noms internes.

Dans :

```
/etc/unbound/unbound.conf.d/local.conf
```

Déclarer la zone :

```
server:
    local-zone: "lan." static
```

Puis ajouter les enregistrements avec `local-data`.

Exemple générique :

```
server:
    local-zone: "lan." static

    local-data: "serveur.lan. IN A 192.168.10.10"
    local-data: "nas.lan. IN A 192.168.10.20"
    local-data: "proxy.lan. IN A 192.168.10.30"
```

Un enregistrement IPv6 peut être ajouté avec `AAAA` :

```
local-data: "serveur.lan. IN AAAA fd00::10"
```

Un même nom peut donc avoir simultanément un enregistrement `A` et un `AAAA`.

---

5. Validation de la configuration

Après toute modification, vérifier la configuration avec :

```
sudo unbound-checkconf
```

Si aucune erreur n'est retournée, la configuration est syntaxiquement valide.

---

6. Redémarrage ou rechargement

Après modification de la configuration :

```
sudo systemctl restart unbound
```

Pour vérifier l'état du service :

```
sudo systemctl status unbound
```

Les logs peuvent être consultés avec :

```
sudo journalctl -u unbound
```

ou en temps réel :

```
sudo journalctl -u unbound -f
```

---

7. Tests DNS

Test d'un domaine Internet

```
dig example.com @127.0.0.1
```

Test d'un enregistrement IPv4

```
dig A example.com @127.0.0.1
```

Test d'un enregistrement IPv6

```
dig AAAA example.com @::1
```

Cette commande teste également que le serveur Unbound est joignable via IPv6 sur l'interface loopback.

Test d'un nom local

```
dig serveur.lan @127.0.0.1
```

---

8. Statistiques

Unbound fournit l'outil `unbound-control`.

État du serveur :

```
sudo unbound-control status
```

Statistiques :

```
sudo unbound-control stats
```

Statistiques sans réinitialisation :

```
sudo unbound-control stats_noreset
```

Quelques métriques utiles :

```
total.num.queries
total.num.cachehits
total.num.cachemiss
```

Elles permettent notamment de suivre :

- le nombre total de requêtes ;
- le nombre de réponses provenant du cache ;
- le nombre de requêtes nécessitant une résolution.

---

9. Pare-feu

Le DNS utilise principalement :

```
UDP/53
TCP/53
```

Le pare-feu doit autoriser ces ports depuis les réseaux qui doivent utiliser le resolver.

Pour IPv6, les règles du pare-feu IPv6 doivent également autoriser les connexions vers UDP/TCP 53.

L'accès doit rester limité aux réseaux nécessaires.

Structure des fichiers

La configuration finale peut être organisée ainsi :

```
/etc/unbound/
├── unbound.conf
└── unbound.conf.d/
    └── local.conf
```

Le fichier `local.conf` contient notamment :

```
server:
    verbosity: 0

    interface: 0.0.0.0
    interface: ::0

    access-control: 127.0.0.0/8 allow
    access-control: 192.168.10.0/24 allow
    access-control: 10.20.0.0/24 allow

    access-control: ::1 allow
    access-control: fd00::/8 allow

    do-ip4: yes
    do-ip6: yes
    prefer-ip6: no
```

```
    local-zone: "lan." static

    # Enregistrements DNS locaux à ajouter ici
    # local-data: "serveur.lan. IN A 192.168.10.10"
```

Cette organisation permet de conserver la configuration spécifique au serveur dans `unbound.conf.d/local.conf`, sans modifier inutilement le fichier principal `/etc/unbound/unbound.conf`.

Revision #1
Created 2026-09-02 14:00:23 UTC by Axolito
Updated 2026-09-02 14:00:38 UTC by Axolito