Unbound : résolveur récursif, cache et DNSSEC

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

Unbound fournit une résolution récursive avec cache et validation DNSSEC. Les root hints indiquent les serveurs racine ; l'ancre de confiance sert à la validation DNSSEC. Ce sont deux éléments distincts.

Dans cet exemple, `dns0` utilise `192.168.3.10/25`. Les réseaux autorisés à interroger le résolveur doivent être définis explicitement afin d'éviter un service récursif ouvert à tous.

2. Configuration minimale de maquette

Installer le paquet Debian puis ajouter un fichier dans le répertoire de configuration inclus par le paquet, après vérification des fichiers déjà présents :

```
sudo apt update
sudo apt install unbound dnsutils
```

```
server:
    interface: 127.0.0.1
    interface: 192.168.3.10
    access-control: 127.0.0.0/8 allow
    access-control: 192.168.3.0/25 allow
    access-control: 192.168.3.128/26 allow
    access-control: 192.168.3.192/28 allow
    access-control: 192.168.3.208/29 allow
```

Cet extrait ne remplace pas toute la configuration du paquet. Examiner notamment les réglages DNSSEC déjà fournis pour éviter des définitions contradictoires. Unbound possède des informations racine intégrées ; un fichier root hints externe n'est pas systématiquement nécessaire.

3. Vérification

```
sudo unbound-checkconf
sudo systemctl restart unbound
systemctl status unbound
dig @192.168.3.10 example.org
dig @192.168.3.10 example.org +tcp
sudo journalctl -u unbound -b --no-pager
```

Comparer plusieurs requêtes pour observer le cache. Tester un nom inexistant et un client situé hors des réseaux autorisés.

4. Zones internes et dépannage

Une `stub-zone` dirige la résolution d'une zone vers ses serveurs faisant autorité ; une `forward-zone` s'appuie sur un autre résolveur. Choisir le mécanisme selon le rôle réel de la cible.

Pour les erreurs de journalisation, vérifier les permissions puis AppArmor. Pour SERVFAIL, contrôler aussi l'heure, la connectivité sortante et DNSSEC avant de modifier la politique de sécurité.

5. Configuration observée dans le laboratoire d'Unbound (''/etc/unbound/unbound.conf'')

Fichier de configuration de ce résolveur :

```
# Unbound configuration file for Debian.
#
# See the unbound.conf(5) man page.
#
# See /usr/share/doc/unbound/examples/unbound.conf for a commented
# reference config file.

# Inclusion des fichiers de configuration supplémentaires
include-toplevel: "/etc/unbound/unbound.conf.d/*.conf"


server:

    # Interface d'écoute IPv4 sur le réseau
    interface: 192.168.3.10
    interface: 127.0.0.1


    # Quels réseaux ont le droit de se servir du serveur DNS récursif
    # Ne jamais laisser son serveur récursif ouvert à tous
    #
```

```
    # allow_snoop autorise aussi les requêtes non récursives

    access-control: 192.168.3.0/24 allow_snoop
    access-control: 192.168.33.248/29 allow_snoop
    access-control: 127.0.0.0/8 allow_snoop


    # Fichier indiquant les serveurs DNS racines
    root-hints: "/var/lib/unbound/root.hints"


    # On cache la version de Unbound
    # et on augmente la sécurité

    hide-version: yes
    hide-identity: yes
    qname-minimisation: yes


    # On autorise l'IPv4
    do-ip4: yes


    # Domaine interne
    domain-insecure: "sio.lan."
    private-domain: "sio.lan."


    # Journalisation
    logfile: "/var/log/unbound.log"
    verbosity: 1
    log-queries: yes


# Serveurs DNS faisant autorité pour sio.lan.
# Cette section doit être en dehors de "server:"

stub-zone:
    name: "sio.lan."
    stub-addr: 172.16.20.10
    stub-addr: 172.16.20.11
```

Lecture de la configuration :

- **`interface`** : le résolveur écoute sur l'adresse du VLAN Production et en localhost.
- **`access-control`** : la règle `192.168.3.0/24` couvre tous les sous-réseaux de ce bloc, pas uniquement le VLAN Production. Le réseau `192.168.33.248/29` et la boucle locale sont aussi autorisés. `allow_snoop` autorise la récursion et des requêtes non récursives ; `allow` suffit aux clients récursifs ordinaires. Ces règles sont celles relevées, à restreindre selon les flux réellement nécessaires.
- **`root-hints`** : pointe vers le fichier des serveurs racines téléchargé précédemment.

- **`hide-version`** / **`hide-identity`** : durcissement (ne pas divulguer la version du serveur).
- **`qname-minimisation`** : préserve la confidentialité en minimisant le nom envoyé aux serveurs parents (minimisation QNAME).
- **`domain-insecure`** : désactive la validation DNSSEC pour `sio.lan.`. **`private-domain`** exempte ce domaine du filtrage des adresses privées lorsqu'un tel filtrage est configuré ; cette directive ne crée pas de zone DNS.
- **`logfile`** / **`log-queries`** : journalisation des requêtes dans `/var/log/unbound.log`.
- **`stub-zone`** : le résolveur est configuré localement pour interroger `172.16.20.10` et `172.16.20.11` pour `sio.lan.`. Ce réglage ne crée pas une délégation dans la zone parente. Les paramètres DNSSEC peuvent aussi provenir des fichiers inclus : leur contenu n'est pas reproduit ici.

6. Diagnostic des root hints et du journal

Un contrôle a échoué car le fichier explicitement déclaré était absent :

```
/var/lib/unbound/root.hints: No such file or directory
```

Dans cette configuration, la liste a été récupérée puis rendue lisible par le service :

```
sudo curl --fail --show-error --output /var/lib/unbound/root.hints
https://www.internic.net/domain/named.cache
sudo chown unbound:unbound /var/lib/unbound/root.hints
sudo unbound-checkconf
```

Un second problème concernait `/var/log/unbound.log` : le message `Permission denied` imposait de vérifier les permissions classiques et les refus AppArmor. Un chemin autorisé dans un profil ne remplace pas les permissions du fichier, et inversement.

```
ls -ld /var/log
ls -l /var/log/unbound.log
sudo journalctl -k -b | grep -i apparmor
```

Le dépannage du confinement est détaillé dans AppArmor.

7. Résultats conservés

Contrôle	Observation du laboratoire
google.fr A via dns0	NOERROR et adresse IPv4 retournée
Nom littéral 8.8.8.8. demandé en A	NXDOMAIN ; il ne s'agissait pas d'une recherche inverse
Journal Unbound	Requêtes google.fr et 8.8.8.8. enregistrées
Arrêt d'un résolveur	Continuité déclarée fonctionnelle dans le compte rendu ; la capture retrouvée montre une réponse du secondaire faisant autorité, pas le basculement entre résolveurs

Ces observations ne constituent pas une recette actuelle. Le test de continuité reste à documenter avec le système client et les délais mesurés.

8. Références

- NLnet Labs — manuel unbound.conf

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

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

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