

Voorgestelde waarden voor Advanced tab in Unbound

Screenshots staan onderaan deze post.

Basisinstellingen voor privacy en veiligheid:

1. **Hide Identity:**

- **Aan:** Verbergt de identiteit van de Unbound-server (zoals het feit dat je Unbound gebruikt) in DNS-responses. Dit is handig voor privacy.

2. **Hide Version:**

- **Aan:** Verbergt de versie van Unbound die wordt gebruikt in de DNS-responses. Dit voorkomt dat een aanvaller de versie van je server kan achterhalen.

3. **Prefetch DNS Key Support:**

- **Aan:** Verbeterd de prestaties van DNSSEC-queries door vooraf de sleutels van de domeinen in te laden, wat de latentie kan verminderen.

4. **Harden DNSSEC Data:**

- **Aan:** Zorgt ervoor dat DNSSEC-resolutie strikt wordt gehandhaafd. Dit betekent dat alle DNSSEC-handtekeningen strikt worden gecontroleerd, wat de veiligheid verhoogt.

5. **Aggressive NSEC:**

- **Aan:** Verhoogt de veiligheid door gebruik te maken van de agressieve NSEC-beveiliging, wat voorkomt dat er onterechte 'NXDOMAIN' antwoorden worden gegeven voor niet-bestaande domeinen.

6. **Strict QNAME Minimisation:**

- **Aan:** Minimaliseert de hoeveelheid informatie die Unbound naar upstream DNS-servers stuurt, wat kan helpen om je privacy te beschermen en gegevenslekken te verminderen.

7. **Rebind protection networks:**

- **Aan:** Activeer dit om rebind-aanvallen te voorkomen, waarbij een aanvaller je DNS-resolver probeert te misleiden door interne IP-adressen te maskeren.

Prestatiesettings:

8. **Outgoing TCP Buffers:**

- Standaardinstellingen zijn vaak prima, maar je kunt het verhogen als je een snelle verbinding hebt met veel gelijktijdige queries. Dit kan helpen bij het omgaan met grotere verzoeken via TCP.

9. **Incoming TCP Buffers:**

- Eveneens kun je de standaardinstellingen gebruiken, maar bij hoge verkeersvolumes kan het verhogen van de bufferwaarde helpen om betere prestaties te bereiken.

10. **Number of queries per thread:**

- **2 tot 4** is een goede instelling voor de meeste omgevingen, afhankelijk van de belasting. Verhoog dit als je veel queries verwerkt.

11. **Outgoing Range:**

- Standaard is 10-20 prima. Verhoog dit om grotere hoeveelheden gelijktijdige uitgaande verzoeken te verwerken.

12. **Jostle Timeout** en **Discard Timeout:**

- Deze zijn goed ingesteld op **default**, maar als je last hebt van time-outs bij het resolveren van verzoeken, kun je experimenteren met langere time-outs.

Cachinginstellingen:

13. **Message Cache Size:**

- Dit kan verhoogd worden voor grotere netwerken (bijv. 50-100 MB), afhankelijk van de hoeveelheid DNS-verkeer die je genereert.

14. **RRset Cache Size:**

- Vergroot deze als je veel verzoeken hebt naar dezelfde domeinen. Standaardwaarden zijn vaak voldoende, maar grotere netwerken kunnen baat hebben bij een grotere cache.

15. **Maximum TTL for RRsets and messages:**

- **Maximaal 86400 (1 dag)** is een gangbare instelling voor de TTL. Dit bepaalt hoe lang records worden bewaard. Dit kan de prestaties verbeteren, maar verhoogt het risico van verouderde informatie.

16. **Minimum TTL for RRsets and messages:**

- **Standaardinstelling** van 0 is prima, tenzij je wilt forceren dat bepaalde records voor een minimumtijd worden bewaard.

17. **TTL for Host Cache entries:**

- Dit moet niet te hoog ingesteld worden. **900 seconden (15 minuten)** is een gangbare waarde, wat een goede balans biedt tussen prestaties en actualiteit van gegevens.

18. **Keep probing down hosts:**

- **Uit** is vaak goed, tenzij je wilt dat Unbound blijft proberen om onbereikbare hosts te bereiken, wat de prestaties kan beïnvloeden.

19. **Number of Hosts to cache:**

- Een hogere waarde, zoals **1000**, kan nuttig zijn voor grotere netwerken. Dit bepaalt hoeveel hostnamen in het cachegeheugen worden bewaard.

Logginginstellingen:

20. **Log Queries:**

- **Uit** voor minder logverkeer en meer privacy, tenzij je specifieke diagnostiek nodig hebt.

21. **Log Replies:**

- **Uit** is meestal voldoende om de belasting op je logs laag te houden.

22. **Tag Queries and Replies:**

- **Uit** voor betere prestaties, tenzij je een gedetailleerde audit nodig hebt.

23. **Log local actions:**

- **Aan** kan handig zijn voor probleemoplossing, maar dit kan leiden tot veel logverkeer.

24. **Log SERVFAIL:**

- **Aan** kan nuttig zijn voor diagnostiek van problemen, maar zet het uit voor meer geoptimaliseerde prestaties.

Diverse instellingen:

25. **Serve Expired Settings:**

- **Aan:** Verbetert de beschikbaarheid van gegevens door verlopen gegevens toch te serveren als tijdelijke oplossing (bijvoorbeeld als de upstream DNS niet reageert).

26. **Serve Expired Responses:**

- **Aan** zorgt ervoor dat verouderde gegevens toch kunnen worden bediend, maar dit kan veiligheidsrisico's inhouden als je vertrouwt op de validiteit van de gegevens.

27. **Extended Statistics:**

- **Aan** voor gedetailleerdere statistieken, maar dit verhoogt de belasting op de server.

28. **Log Level Verbosity:**

- **2 of 3** voor gedetailleerde logs. Je kunt dit verhogen naar **4** als je gedetailleerde foutopsporingsinformatie nodig hebt.





















29. **Log validation level:**

- **Minimaal** of **Fouten** voor minder logverkeer, tenzij je actief DNSSEC-validatieproblemen onderzoekt.

Aanbevolen instellingen (samenvatting):














- **Privacy:** Hide Identity, Hide Version, Harden DNSSEC Data, Strict QNAME Minimisation.
- **Veiligheid:** Rebind protection networks, Aggressive NSEC.
- **Prestaties:** Prefetch DNS Key Support, Outgoing Range, Number of queries per thread.
- **Cache:** Message Cache Size, RRset Cache Size, Maximum TTL for RRsets.
- **Logging:** Zet logging zoveel mogelijk uit voor betere prestaties, maar log SERVFAIL als je problemen wilt onderzoeken.


Door deze instellingen zorgvuldig af te stemmen, kun je de prestaties, privacy en veiligheid van je DNS-resolutie optimaliseren.

-  Lobby
-  Reporting
-  System
-  Interfaces
-  Firewall
-  VPN
-  Services
 - ACME Client 
 - Adguardhome 
 - Captive Portal 
 - CrowdSec 
 - DHCRelay 
 - Dnsmasq DNS & DHCP 
 - Intrusion Detection 
 - ISC DHCPv4 
 - ISC DHCPv6 
 - Kea DHCP 
 - Monit 
 - Network Time 
 - Nginx 
 - OpenDNS 
 - Unbound DNS 
 - General
 - Overrides
 - Advanced
 - Access Lists
 - Blocklist
 - Query Forwarding
 - DNS over TLS
 - Statistics
 - Log File
 - Wazuh Agent 
-  Power
-  Help

















Services: Unbound DNS: Advanced

General Settings

-  Hide Identity ☒
-  Hide Version ☒
-  Prefetch DNS Key Support ☒
-  Harden DNSSEC Data ☒
-  Aggressive NSEC ☒
-  Strict QNAME Minimisation ☒
-  Outgoing TCP Buffers
-  Incoming TCP Buffers
-  Number of queries per thread
-  Outgoing Range
-  Jostle Timeout
-  Discard Timeout
-  Private Domains





 Clear All  Copy  Paste  Text

Rebind protection networks


0.0.0.0/8  10.0.0.0/8  100.64.0.0/10 
169.254.0.0/16  172.16.0.0/12 
192.0.2.0/24  192.168.0.0/16 
198.18.0.0/15  198.51.100.0/24 
203.0.113.0/24  233.252.0.0/24  ::1/128 
2001:db8::/32  fc00::/8  fd00::/8 
fe80::/10 

 Clear All  Copy  Paste  Text

Insecure Domains

 Clear All  Copy  Paste  Text

Serve Expired Settings

-  Serve Expired Responses ☐

Logging Settings

-  Extended Statistics ☐
-  Log Queries ☐
-  Log Replies ☐
-  Tag Queries and Replies ☐

Lobby

Reporting

System

Interfaces

Firewall

VPN

Services

ACME Client

Adguardhome

Captive Portal

CrowdSec

DHCRelay

DNSCrypt-Proxy

Dnsmasq DNS & DHCP

Intrusion Detection

ISC DHCPv4

ISC DHCPv6

Kea DHCP

Monit

Network Time

Nginx

OpenDNS

Unbound DNS

General

Overrides

Advanced

Access Lists

Blocklist

Query Forwarding

DNS over TLS

Statistics

Log File

Wazuh Agent

Power

Help

2001:db8::/32 × fc00::/8 × fd00::/8 ×
fe80::/10 ×

✖ Clear All 📄 Copy 📄 Paste 📄 Text

ⓘ Insecure Domains

✖ Clear All 📄 Copy 📄 Paste 📄 Text

▼ Serve Expired Settings

ⓘ Serve Expired Responses

☐

▼ Logging Settings

ⓘ Extended Statistics

☐

ⓘ Log Queries

☐

ⓘ Log Replies

☐

ⓘ Tag Queries and Replies

☐

ⓘ Log local actions

☐

ⓘ Log SERVFAIL

☐

ⓘ Log Level Verbosity

Level 2 ▲

ⓘ Log validation level

Level 0 (Default) ▲

▼ Cache Settings

ⓘ Prefetch Support

☒

ⓘ Unwanted Reply Threshold

ⓘ Message Cache Size

256M

ⓘ RRset Cache Size

ⓘ Maximum TTL for RRsets and messages

86400

ⓘ Maximum Negative TTL for RRsets and messages

ⓘ Minimum TTL for RRsets and messages

300

ⓘ TTL for Host Cache entries

900

ⓘ Keep probing down hosts

☐

ⓘ Number of Hosts to cache

1000

Apply

Revisie #1

Gemaakt: 3 juni 2025 14:37:22 door Gert

Bijgewerkt: 3 juni 2025 14:40:14 door Gert