

LAMPIRAN

LAMPIRAN – A. Provider IP address 183.91.65.119

```

Source: whois.apnic.net

IP Address: 183.91.65.119

% [whois.apnic.net]
% Whois data copyright terms
http://www.apnic.net/db/dbcopyright.html

% Information related to '183.91.64.0 - 183.91.95.255'

% Abuse contact for '183.91.64.0 - 183.91.95.255' is
'abuse@idnic.net'

inetnum:          183.91.64.0 - 183.91.95.255
netname:          LINTASARTA-NET
descr:           Indonesia Online Access
descr:           PT Aplikanusa Lintasarta
country:         ID
admin-c:         LA60-AP
tech-c:          LA60-AP
remarks:         spam and abuse report : abuse@idola.net.id
mnt-by:          MNT-APJII-ID
mnt-irt:         IRT-IDNIC-ID
mnt-lower:       MAINT-LINTASARTA
mnt-routes:     MAINT-LINTASARTA
status:          ALLOCATED PORTABLE
last-modified:  2015-12-01T22:26:00Z
source:          APNIC

irt:             IRT-IDNIC-ID
address:         INDONESIA NETWORK INFORMATION CENTER
address:         Cyber Building 11th Floor
address:         Jl. Kuningan Barat No.8
address:         Jakarta Selatan 12710
e-mail:         abuse@idnic.net
abuse-mailbox:  abuse@idnic.net
admin-c:        IA55-AP
tech-c:         IH123-AP
auth:           # Filtered
mnt-by:         MNT-APJII-ID
last-modified:  2018-05-31T22:29:03Z
source:         APNIC

role:           LINTASARTA ADMINISTRATOR
address:        PT Aplikanusa Lintasarta
address:        MH Thamrin Kav 3
address:        Menara Thamrin Bulding 12th Floor
address:        Jakarta 10250
country:       ID
phone:         +62-21-2302345
fax-no:        +62-21-2303883
e-mail:        hostmaster@lintasarta.net
remarks:       spam and abuse report : abuse@idola.net.id
remarks:       technical and routing : support@idola.net.id
remarks:       hostmasters : hostmaster@idola.net.id
remarks:       LINTASARTA administrators role object

```

```

admin-c:      GP509-AP
tech-c:      MT1062-AP
nic-hdl:     LA60-AP
notify:      hostmaster@lintasarta.net
mnt-by:      MAINT-LINTASARTA
last-modified: 2020-04-17T03:25:33Z
source:      APNIC

% Information related to '183.91.64.0/19AS4800'

route:       183.91.64.0/19
descr:       Route Object of PT Aplikanusa Lintasarta
descr:       ISP
descr:       MH Thamrin Kav 3
descr:       Menara Thamrin Bulding 12th Floor
descr:       Jakarta 10250
country:     ID
origin:      AS4800
remarks:     Email address for spam or abuse complaints
remarks:     abuse@idola.net.id
mnt-by:      MAINT-LINTASARTA
last-modified: 2010-04-21T03:52:01Z
source:      APNIC

% Information related to '183.91.65.112 - 183.91.65.119'

inetnum:     183.91.65.112 - 183.91.65.119
netname:     LA-AHK
descr:       ADHINIAGA KREASINUSA
descr:       LAMPUNG BARAT
country:     ID
admin-c:     LA60-AP
tech-c:     LA60-AP
status:      ASSIGNED NON-PORTABLE
mnt-by:     MAINT-LINTASARTA
mnt-irt:     IRT-LINTASARTA-ID
last-modified: 2019-09-27T08:03:40Z
source:     IDNIC

irt:         IRT-LINTASARTA-ID
address:     PT Aplikanusa Lintasarta
address:     MH Thamrin Kav 3
address:     Menara Thamrin Bulding 12th Floor
address:     Jakarta 10250
e-mail:     abuse@idola.net.id
abuse-mailbox: abuse@idola.net.id
admin-c:     LA60-AP
tech-c:     LA60-AP
auth:       # Filtered
mnt-by:     MAINT-LINTASARTA
last-modified: 2018-01-25T09:17:32Z
source:     IDNIC

role:        LINTASARTA ADMINISTRATOR
address:     PT Aplikanusa Lintasarta
address:     MH Thamrin Kav 3
address:     Menara Thamrin Bulding 12th Floor
address:     Jakarta 10250
country:     ID
phone:      +62-21-2302345
fax-no:     +62-21-2303883

```

```

e-mail:          hostmaster@lintasarta.net
remarks:        spam and abuse report : abuse@idola.net.id
remarks:        technical and routing : support@idola.net.id
remarks:        hostmasters : hostmaster@idola.net.id
remarks:        LINTASARTA administrators role object
admin-c:        GP509-AP
tech-c:         MT1062-AP
nic-hdl:        LA60-AP
notify:         hostmaster@lintasarta.net
mnt-by:         MAINT-LINTASARTA
last-modified:  2020-04-15T10:35:00Z
source:         IDNIC

```

```
% Information related to '183.91.64.0/19AS4800'
```

```

route:          183.91.64.0/19
descr:         Route Object of PT Aplikanusa Lintasarta
descr:         ISP
descr:         MH Thamrin Kav 3
descr:         Menara Thamrin Bulding 12th Floor
descr:         Jakarta 10250
country:       ID
origin:        AS4800
remarks:       Email address for spam or abuse complaints
remarks:       abuse@idola.net.id
mnt-by:        MAINT-LINTASARTA
last-modified: 2010-04-21T03:52:01Z
source:        IDNIC

```

```
% This query was served by the APNIC Whois Service version
1.88.15-SNAPSHOT (WHOIS-US4)
```

LAMPIRAN – B. DIG *dns.vasdev.co.id*

```

MacBook-Pro ~ dig dns.vasdev.co.id SOA

; <<>> DiG 9.10.6 <<>> dns.vasdev.co.id SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14312
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
;; QUESTION SECTION:
;dns.vasdev.co.id.      IN      SOA

```

```

;; AUTHORITY SECTION:
vasdev.co.id.      86400 IN      SOA     nsid1.rumahweb.com.
info.rumahweb.com. 2020073000 86400 7200 3600000 86400

;; Query time: 175 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 03 23:07:40 WIB 2020
;; MSG SIZE rcvd: 128

MacBook-Pro ~ dig . NS

; <<>> DiG 9.10.6 <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25241
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
;; QUESTION SECTION:
;                               IN      NS

;; ANSWER SECTION:
.           516080 IN      NS      a.root-servers.net.
.           516080 IN      NS      b.root-servers.net.
.           516080 IN      NS      c.root-servers.net.
.           516080 IN      NS      d.root-servers.net.
.           516080 IN      NS      e.root-servers.net.
.           516080 IN      NS      f.root-servers.net.
.           516080 IN      NS      g.root-servers.net.
.           516080 IN      NS      h.root-servers.net.

```

```

.           516080 IN      NS      i.root-servers.net.
.           516080 IN      NS      j.root-servers.net.
.           516080 IN      NS      k.root-servers.net.
.           516080 IN      NS      l.root-servers.net.
.           516080 IN      NS      m.root-servers.net.

;; Query time: 97 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 03 23:08:47 WIB 2020
;; MSG SIZE rcvd: 431

MacBook-Pro ~ dig dns.vasdev.co.id NS

; <<>> DiG 9.10.6 <<>> dns.vasdev.co.id NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39896
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags; udp: 1232
;; QUESTION SECTION:
;dns.vasdev.co.id.          IN      NS

;; AUTHORITY SECTION:
vasdev.co.id.              86400  IN      SOA     nsid1.rumahweb.com.
info.rumahweb.com. 2020073000 86400 7200 3600000 86400

;; Query time: 143 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 03 23:11:32 WIB 2020

```

```

;; MSG SIZE rcvd: 128

MacBook-Pro ~ dig twitter.com @a.root-servers.net.

; <<>> DiG 9.10.6 <<>> twitter.com @a.root-servers.net.

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47186

;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags; udp: 4096

;; QUESTION SECTION:
;twitter.com.          IN      A

;; AUTHORITY SECTION:
com.                  172800 IN      NS      e.gtld-servers.net.
com.                  172800 IN      NS      b.gtld-servers.net.
com.                  172800 IN      NS      j.gtld-servers.net.
com.                  172800 IN      NS      m.gtld-servers.net.
com.                  172800 IN      NS      i.gtld-servers.net.
com.                  172800 IN      NS      f.gtld-servers.net.
com.                  172800 IN      NS      a.gtld-servers.net.
com.                  172800 IN      NS      g.gtld-servers.net.
com.                  172800 IN      NS      h.gtld-servers.net.
com.                  172800 IN      NS      l.gtld-servers.net.
com.                  172800 IN      NS      k.gtld-servers.net.
com.                  172800 IN      NS      c.gtld-servers.net.
com.                  172800 IN      NS      d.gtld-servers.net.

```

```
;; ADDITIONAL SECTION:
```

```
e.gtld-servers.net. 172800 IN A 192.12.94.30
e.gtld-servers.net. 172800 IN AAAA 2001:502:1ca1::30
b.gtld-servers.net. 172800 IN A 192.33.14.30
b.gtld-servers.net. 172800 IN AAAA 2001:503:231d::2:30
j.gtld-servers.net. 172800 IN A 192.48.79.30
j.gtld-servers.net. 172800 IN AAAA 2001:502:7094::30
m.gtld-servers.net. 172800 IN A 192.55.83.30
m.gtld-servers.net. 172800 IN AAAA 2001:501:b1f9::30
i.gtld-servers.net. 172800 IN A 192.43.172.30
i.gtld-servers.net. 172800 IN AAAA 2001:503:39c1::30
f.gtld-servers.net. 172800 IN A 192.35.51.30
f.gtld-servers.net. 172800 IN AAAA 2001:503:d414::30
a.gtld-servers.net. 172800 IN A 192.5.6.30
a.gtld-servers.net. 172800 IN AAAA 2001:503:a83e::2:30
g.gtld-servers.net. 172800 IN A 192.42.93.30
g.gtld-servers.net. 172800 IN AAAA 2001:503:eea3::30
h.gtld-servers.net. 172800 IN A 192.54.112.30
h.gtld-servers.net. 172800 IN AAAA 2001:502:8cc::30
l.gtld-servers.net. 172800 IN A 192.41.162.30
l.gtld-servers.net. 172800 IN AAAA 2001:500:d937::30
k.gtld-servers.net. 172800 IN A 192.52.178.30
k.gtld-servers.net. 172800 IN AAAA 2001:503:d2d::30
c.gtld-servers.net. 172800 IN A 192.26.92.30
c.gtld-servers.net. 172800 IN AAAA 2001:503:83eb::30
d.gtld-servers.net. 172800 IN A 192.31.80.30
d.gtld-servers.net. 172800 IN AAAA 2001:500:856e::30
```

```
;; Query time: 263 msec
```

```

;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Mon Aug 03 23:12:47 WIB 2020
;; MSG SIZE rcvd: 836

MacBook-Pro ~ traceroute facebook.com
traceroute to facebook.com (157.240.7.35), 64 hops max, 52 byte packets
 1 192.168.100.1 (192.168.100.1) 1.499 ms 1.063 ms 0.901 ms
 2 162.subnet125-160-9.speedy.telkom.net.id (125.160.9.162) 4.250 ms 4.377 ms
 4.173 ms
 3 180.252.3.185 (180.252.3.185) 9.390 ms 21.245 ms 21.067 ms
 4 180.240.190.194 (180.240.190.194) 22.476 ms 21.494 ms 23.347 ms
 5 180.240.190.193 (180.240.190.193) 21.954 ms 22.557 ms 21.799 ms
 6 180.240.205.80 (180.240.205.80) 23.270 ms 23.309 ms 23.566 ms
 7 ae21.pr04.sin1.tfbnw.net (103.4.98.92) 23.745 ms 23.123 ms 23.916 ms
 8 po101.psw02.sin6.tfbnw.net (157.240.45.39) 25.311 ms
   po101.psw01.sin6.tfbnw.net (157.240.42.227) 29.999 ms 30.422 ms
 9 157.240.38.201 (157.240.38.201) 22.867 ms
   157.240.39.7 (157.240.39.7) 22.561 ms
   173.252.67.183 (173.252.67.183) 26.309 ms
10 edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35) 23.022 ms 22.994 ms
22.803 ms

MacBook-Pro ~ dig +trace twitter.com +nodnssec

;<<>> DiG 9.10.6 <<>> +trace twitter.com +nodnssec

;; global options: +cmd
.          514403 IN      NS       a.root-servers.net.
.          514403 IN      NS       b.root-servers.net.
.          514403 IN      NS       c.root-servers.net.
.          514403 IN      NS       d.root-servers.net.
.          514403 IN      NS       e.root-servers.net.

```



```

.           514403 IN      NS      f.root-servers.net.
.           514403 IN      NS      g.root-servers.net.
.           514403 IN      NS      h.root-servers.net.
.           514403 IN      NS      i.root-servers.net.
.           514403 IN      NS      j.root-servers.net.
.           514403 IN      NS      k.root-servers.net.
.           514403 IN      NS      l.root-servers.net.
.           514403 IN      NS      m.root-servers.net.

```

```
;; Received 431 bytes from 127.0.0.1#53(127.0.0.1) in 26 ms
```

```

com.       172800 IN      NS      i.gtld-servers.net.
com.       172800 IN      NS      d.gtld-servers.net.
com.       172800 IN      NS      f.gtld-servers.net.
com.       172800 IN      NS      j.gtld-servers.net.
com.       172800 IN      NS      e.gtld-servers.net.
com.       172800 IN      NS      h.gtld-servers.net.
com.       172800 IN      NS      k.gtld-servers.net.
com.       172800 IN      NS      g.gtld-servers.net.
com.       172800 IN      NS      b.gtld-servers.net.
com.       172800 IN      NS      l.gtld-servers.net.
com.       172800 IN      NS      m.gtld-servers.net.
com.       172800 IN      NS      a.gtld-servers.net.
com.       172800 IN      NS      c.gtld-servers.net.

```

```
;; Received 836 bytes from 192.33.4.12#53(c.root-servers.net) in 193 ms
```

```

twitter.com. 172800 IN      NS      ns3.p34.dynect.net.
twitter.com. 172800 IN      NS      ns4.p34.dynect.net.
twitter.com. 172800 IN      NS      d01-01.ns.twtrdns.net.
twitter.com. 172800 IN      NS      d01-02.ns.twtrdns.net.
twitter.com. 172800 IN      NS      a.r06.twtrdns.net.

```

```

twitter.com.      172800 IN      NS      b.r06.twtrdns.net.
twitter.com.      172800 IN      NS      c.r06.twtrdns.net.
twitter.com.      172800 IN      NS      d.r06.twtrdns.net.
;; Received 211 bytes from 192.54.112.30#53(h.gtld-servers.net) in 221 ms

twitter.com.      1800  IN      A       104.244.42.65
twitter.com.      13999 IN      NS      a.r06.twtrdns.net.
twitter.com.      13999 IN      NS      b.r06.twtrdns.net.
twitter.com.      13999 IN      NS      c.r06.twtrdns.net.
twitter.com.      13999 IN      NS      d.r06.twtrdns.net.
twitter.com.      13999 IN      NS      d01-01.ns.twtrdns.net.
twitter.com.      13999 IN      NS      d01-02.ns.twtrdns.net.
twitter.com.      13999 IN      NS      ns1.p34.dynect.net.
twitter.com.      13999 IN      NS      ns2.p34.dynect.net.
twitter.com.      13999 IN      NS      ns3.p34.dynect.net.
twitter.com.      13999 IN      NS      ns4.p34.dynect.net.
;; Received 263 bytes from 205.251.192.179#53(a.r06.twtrdns.net) in 201 ms

MacBook-Pro ~ dig +trace kincir.com +nodnssec

; <<<>> DiG 9.10.6 <<<>> +trace kincir.com +nodnssec
;; global options: +cmd

.      517118 IN      NS      a.root-servers.net.
.      517118 IN      NS      b.root-servers.net.
.      517118 IN      NS      c.root-servers.net.
.      517118 IN      NS      d.root-servers.net.
.      517118 IN      NS      e.root-servers.net.
.      517118 IN      NS      f.root-servers.net.
.      517118 IN      NS      g.root-servers.net.
.      517118 IN      NS      h.root-servers.net.

```

```

.           517118 IN      NS      i.root-servers.net.
.           517118 IN      NS      j.root-servers.net.
.           517118 IN      NS      k.root-servers.net.
.           517118 IN      NS      l.root-servers.net.
.           517118 IN      NS      m.root-servers.net.
;; Received 431 bytes from 127.0.0.1#53(127.0.0.1) in 26 ms

com.        172800 IN      NS      a.gtld-servers.net.
com.        172800 IN      NS      b.gtld-servers.net.
com.        172800 IN      NS      c.gtld-servers.net.
com.        172800 IN      NS      d.gtld-servers.net.
com.        172800 IN      NS      e.gtld-servers.net.
com.        172800 IN      NS      f.gtld-servers.net.
com.        172800 IN      NS      g.gtld-servers.net.
com.        172800 IN      NS      h.gtld-servers.net.
com.        172800 IN      NS      i.gtld-servers.net.
com.        172800 IN      NS      j.gtld-servers.net.
com.        172800 IN      NS      k.gtld-servers.net.
com.        172800 IN      NS      l.gtld-servers.net.
com.        172800 IN      NS      m.gtld-servers.net.
;; Received 835 bytes from 192.58.128.30#53(j.root-servers.net) in 26 ms

kincir.com. 172800 IN      NS      ns-69.awsdns-08.com.
kincir.com. 172800 IN      NS      ns-703.awsdns-23.net.
kincir.com. 172800 IN      NS      ns-1861.awsdns-40.co.uk.
kincir.com. 172800 IN      NS      ns-1500.awsdns-59.org.
;; Received 191 bytes from 192.5.6.30#53(a.gtld-servers.net) in 206 ms

kincir.com. 300   IN      A       34.87.71.180
kincir.com. 3600  IN      NS      ns-1500.awsdns-59.org.

```

kincir.com.	3600	IN	NS	ns-1861.awsdns-40.co.uk.
kincir.com.	3600	IN	NS	ns-69.awsdns-08.com.
kincir.com.	3600	IN	NS	ns-703.awsdns-23.net.

;; Received 191 bytes from 205.251.192.69#53(ns-69.awsdns-08.com) in 198 ms

LAMPIRAN – C. *Script Stubby*

```
#####
##### STUBBY YAML CONFIG FILE #####
#####
# This is a yaml version of the stubby configuration file (it replaces the
# json based stubby.conf file used in earlier versions of getdns/stubby).
#
# For more information see
# https://dnsprivacy.org/wiki/display/DP/Configuring+Stubby
#
# This format does not fully support all yaml features - the restrictions are:
# - the outer-most data structure must be a yaml mapping
# - mapping keys must be yaml scalars
# - plain scalars will be converted to json unchanged
# - non-plain scalars (quoted, double-quoted, wrapped) will be interpreted
#   as json strings, i.e. double quoted.
# - yaml tags are not supported
# - IPv6 addresses ending in :: are not yet supported (use ::0)
#
# Also beware that yaml is sensitive to the indentation at the start of each
# line so if you encounter errors when parsing the config file then please check
# that. We will add better checking but a useful online tool to check yaml
# format is here (it also converts yaml to json)
# https://yaml-online-parser.appspot.com/
#
```

```

# Note that we plan to introduce a more compact format for defining upstreams
# in future: https://github.com/getdnsapi/stubby/issues/79

##### LOGGING #####
# Logging is currently configured at runtime using command line arguments. See
# > stubby -h
# for details.

##### BASIC & PRIVACY SETTINGS #####
# Specifies whether to run as a recursive or stub resolver
# For stubby this MUST be set to GETDNS_RESOLUTION_STUB
resolution_type: GETDNS_RESOLUTION_STUB

# Ordered list composed of one or more transport protocols:
# GETDNS_TRANSPORT_UDP, GETDNS_TRANSPORT_TCP or GETDNS_TRANSPORT_TLS
# If only one transport value is specified it will be the only transport used.
# Should it not be available basic resolution will fail.
# Fallback transport options are specified by including multiple values in the
# list. Strict mode (see below) should use only GETDNS_TRANSPORT_TLS.
dns_transport_list:
- GETDNS_TRANSPORT_TLS

# Selects Strict or Opportunistic Usage profile as described in
# https://datatracker.ietf.org/doc/draft-ietf-dprive-dtls-and-tls-profiles/
# Strict mode requires that authentication information for the upstreams is
# specified below. Opportunistic may fallback to clear text DNS if UDP or TCP
# is included in the transport list above.
# For Strict use    GETDNS_AUTHENTICATION_REQUIRED
# For Opportunistic use GETDNS_AUTHENTICATION_NONE
tls_authentication: GETDNS_AUTHENTICATION_REQUIRED

```

```
# EDNSO option to pad the size of the DNS query to the given blocksize
# 128 is currently recommended by
# https://tools.ietf.org/html/draft-ietf-dprive-padding-policy-03
tls_query_padding_blocksize: 128

# EDNSO option for ECS client privacy as described in Section 7.1.2 of
# https://tools.ietf.org/html/rfc7871
edns_client_subnet_private : 1

##### CONNECTION SETTINGS #####

# Set to 1 to instruct stubby to distribute queries across all available name
# servers - this will use multiple simultaneous connections which can give
# better performance in most (but not all) cases.
# Set to 0 to treat the upstreams below as an ordered list and use a single
# upstream until it becomes unavailable, then use the next one.
round_robin_upstreams: 1

# EDNSO option for keepalive idle timeout in milliseconds as specified in
# https://tools.ietf.org/html/rfc7828
# This keeps idle TLS connections open to avoid the overhead of opening a new
# connection for every query. Note that if a given server doesn't implement
# EDNSO keepalive and uses an idle timeout shorter than this stubby will backoff
# from using that server because the server is always closing the connection.
# This can degrade performance for certain configurations so reducing the
# idle_timeout to below that of that lowest server value is recommended.
idle_timeout: 10000

# Control the maximum number of connection failures that will be permitted
# before Stubby backs-off from using an individual upstream (default 2)
```



```

# Set the maximum acceptable TLS version. Works with OpenSSL >= 1.1.1 only.
# This option can also be given per upstream.
# tls_max_version: GETDNS_TLS1_3

##### LISTEN ADDRESS #####

# Set the listen addresses for the stubby DAEMON. This specifies localhost IPv4
# and IPv6. It will listen on port 53 by default. Use <IP_address>@<port> to
# specify a different port
listen_addresses:
- 127.0.0.1
- 0::1

##### DNSSEC SETTINGS #####

# Require DNSSEC validation. This will withhold answers with BOGUS DNSSEC
# status and answers that could not be validated (i.e. with DNSSEC status
# INDETERMINATE). Beware that if no DNSSEC trust-anchor is provided, or if
# stubby is not able to fetch and validate the DNSSEC trust-anchor itself,
# (using Zero configuration DNSSEC) stubby will not return answers at all.
# If DNSSEC validation is required, a trust-anchor is also required.
# dnssec: GETDNS_EXTENSION_TRUE

# Stubby tries to fetch and validate the DNSSEC root trust anchor on the fly
# when needed (Zero configuration DNSSEC), but only if it can store then
# somewhere. The default location to store these files is the ".getdns"
# subdirectory in the user's home directory on Unixes, and the %appdata%\getdns
# directory on Windows. If there is no home directory, or
# the required subdirectory could not be created (or is not present), Stubby
# will fall back to the current working directory to try to store the
# trust-anchor files.
#

```



```

# When stubby runs as a special system-level user without a home directory
# however (such as in setups using systemd), it is recommended that an explicit
# location for storing the trust-anchor files is provided that is writable (and
# readable) by that special system user.
# appdata_dir: "/var/cache/stubby"

# When Zero configuration DNSSEC failed, because of network unavailability or
# failure to write to the appdata directory, stubby will backoff trying to
# refetch the DNSSEC trust-anchor for a specified amount of time expressed
# in milliseconds (which defaults to two and a half seconds).
# trust_anchors_backoff_time: 2500

# Specify the location of the installed trust anchor file to override the
# default location (see above)
# dnssec_trust_anchors: "/etc/unbound/getdns-root.key"

##### UPSTREAMS #####

# Specify the list of upstream recursive name servers to send queries to
# In Strict mode upstreams need either a tls_auth_name or a tls_pubkey_pinset
# so the upstream can be authenticated.
# The list below includes all the available test servers but only has the subset
# operated the stubby/getdns developers enabled. You can enable any of the
# others you want to use by uncommenting the relevant section. See:
# https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers
# If you don't have IPv6 then comment then out those upstreams.
# In Opportunistic mode they only require an IP address in address_data.
# The information for an upstream can include the following:
# - address_data: IPv4 or IPv6 address of the upstream
# port: Port for UDP/TCP (default is 53)

```

```

# tls_auth_name: Authentication domain name checked against the server
#       certificate
# tls_pubkey_pinset: An SPKI pinset verified against the keys in the server
#       certificate
#   - digest: Only "sha256" is currently supported
#   value: Base64 encoded value of the sha256 fingerprint of the public
#       key
# tls_port: Port for TLS (default is 853)

# To always use the DHCP resolvers provided by the local network in Opportunistic
# mode then
# 1) In the dns_transport_list after TLS add UDP then TCP
# 2) Change to tls_authentication: GETDNS_AUTHENTICATION_NONE
# 3) Remove all the upstream_recursive_servers listed below

upstream_recursive_servers:
##### DEFAULT UPSTREAMS #####
##### IPv4 addresses #####

### Test servers ###
# The Surfnet/Sinodun servers
# - address_data: 145.100.185.15
#   tls_auth_name: "dnsovertls.sinodun.com"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#     value: 62lKu9HsDVbyiPenApnc4sfmSYTHOVfFgL3pyB+cBL4=
# - address_data: 145.100.185.16
#   tls_auth_name: "dnsovertls1.sinodun.com"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#     value: cE2ecALeE5B+urJhDrJIVFmf38cJLAvqekONvjyppqUA=

```

```

# The getdnsapi.net server
# - address_data: 185.49.141.37
#  tls_auth_name: "getdnsapi.net"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: foxZRnlh9gZpWnl+zEiKa0EJ2rdCGroMWm02gaxSc9Q=
##### IPv6 addresses #####

### Test servers ###

# The Surfnet/Sinodun servers
# - address_data: 2001:610:1:40ba:145:100:185:15
#  tls_auth_name: "dnsovertls.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 62IKu9HsDVbyiPenApnc4sfmSYTHOVfFgL3pyB+cBL4=
# - address_data: 2001:610:1:40ba:145:100:185:16
#  tls_auth_name: "dnsovertls1.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: cE2ecALeE5B+urJhDrJIVFmf38cJLAvqekONvjyppqUA=

# The getdnsapi.net server
# - address_data: 2a04:b900:0:100::38
#  tls_auth_name: "getdnsapi.net"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: foxZRnlh9gZpWnl+zEiKa0EJ2rdCGroMWm02gaxSc9Q=

##### OPTIONAL UPSTREAMS #####

##### IPv4 addresses #####

### Anycast services ###

```

```
## Quad 9 'secure' service - Filters, does DNSSEC, doesn't send ECS
# - address_data: 9.9.9.9
#  tls_auth_name: "dns.quad9.net"
## Quad 9 'insecure' service - No filtering, no DNSSEC, doesn't send ECS
# - address_data: 9.9.9.10
#  tls_auth_name: "dns.quad9.net"
# DNS-over-TLS 183.91.65.119
## - address_data: 183.91.65.119
##  tls_auth_name: "dns.vasdev.co.id"
## Cloudflare 1.1.1.1 and 1.0.0.1
## (NOTE: recommend reducing idle_timeout to 9000 if using Cloudflare)
- address_data: 1.1.1.1
  tls_auth_name: "cloudflare-dns.com"
- address_data: 1.0.0.1
  tls_auth_name: "cloudflare-dns.com"
## The Uncensored DNS servers
# - address_data: 89.233.43.71
#  tls_auth_name: "unicast.censurfridns.dk"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: wikE3jYAA6jQmXYTr/rbHeEPmC78dQwZbQp6WdrseEs=
## Fondation RESTENA (NREN for Luxembourg)
# - address_data: 158.64.1.29
#  tls_auth_name: "kaitain.restena.lu"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 7ftvIkA+UeN/ktVkovd/7rPZ6mbkhVI7/8HnFJiLa4=
## Google
# - address_data: 8.8.8.8
#  tls_auth_name: "dns.google"
```

```
# - address_data: 8.8.4.4
#  tls_auth_name: "dns.google"
## Adguard Default servers
# - address_data: 176.103.130.130
#  tls_auth_name: "dns.adguard.com"
# - address_data: 176.103.130.131
#  tls_auth_name: "dns.adguard.com"
## Adguard Family Protection servers
# - address_data: 176.103.130.132
#  tls_auth_name: "dns-family.adguard.com"
# - address_data: 176.103.130.134
#  tls_auth_name: "dns-family.adguard.com"
### Test servers ###
## A Surfnet/Sinodun server supporting TLS 1.2 and 1.3
# - address_data: 145.100.185.18
#  tls_auth_name: "dnsovertls3.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 5SpFz7JEPzF71hditH1v2dBhSErPUMcLPJx1uk2svT8=
## A Surfnet/Sinodun server using Knot resolver. Warning - has issue when used
## for DNSSEC
# - address_data: 145.100.185.17
#  tls_auth_name: "dnsovertls2.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: NAXBESvpjZMnPWQcrra2KFikHV/pDEIjRkA3hLWogSg=
## dns.cmrg.net server using Knot resolver. Warning - has issue when used for
## DNSSEC.
# - address_data: 199.58.81.218
#  tls_auth_name: "dns.cmrg.net"
```

```

# tls_pubkey_pinset:
# - digest: "sha256"
# value: 3IOHSS48KOC/zlkKGtI46a9TY9PPKDVGH3W2ZS4JZo=
# - digest: "sha256"
# value: 5zFN3smRPuHlIM/8L+hANT99LW26T97RFHqHv90awjo=
## dns.larsdebruin.net (formerly dns1.darkmoon.is)
# - address_data: 51.15.70.167
# tls_auth_name: "dns.larsdebruin.net "
# tls_pubkey_pinset:
# - digest: "sha256"
# value: AAT+rHoKx5wQkWhxlfriybFocBu3RBrPD2/ySwlwvmvA=
## dot.securedns.eu
# - address_data: 146.185.167.43
# tls_auth_name: "dot.securedns.eu"
# tls_pubkey_pinset:
# - digest: "sha256"
# value: h3mufC43MEqRD6uE4lz6gAgULZ5/riqH/E+U+jE3H8g=
## dns-tls.bitwiseshift.net
# - address_data: 81.187.221.24
# tls_auth_name: "dns-tls.bitwiseshift.net"
# tls_pubkey_pinset:
# - digest: "sha256"
# value: YmcYWZU5dd2EoblZHNf1jTUPVS+uK3280YYCdz4l4wo=
## ns1.dnsprivacy.at
# - address_data: 94.130.110.185
# tls_auth_name: "ns1.dnsprivacy.at"
# tls_pubkey_pinset:
# - digest: "sha256"
# value: vqVQ9TcoR9RDY3TpO0MTXw1YQLjF44zdN3/4PkLwtEY=
## ns2.dnsprivacy.at

```

```
# - address_data: 94.130.110.178
#  tls_auth_name: "ns2.dnsprivacy.at"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: s5Em89o0kigwfbF1gcXWd8zIATSWVXsJ6ecZfmBDTKg=
## dns.bitgeek.in
# - address_data: 139.59.51.46
#  tls_auth_name: "dns.bitgeek.in"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: FndaG4ezEBQs4k0Ya3xt3z4BjFEyQHd7B75nRyP1nTs=
## Lorraine Data Network (self-signed cert).
# - address_data: 80.67.188.188
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: WaG0kHUS5N/ny0labz85HZg+v+f0b/UQ73IZjFep0nM=
## dns.neutopia.org
# - address_data: 89.234.186.112
#  tls_auth_name: "dns.neutopia.org"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: wTeXHM8aczhRSi0cv2qOXkXInoDU+2C+M8MpRyT3OI=
## NIC Chile (self-signed cert)
# - address_data: 200.1.123.46
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: sG6kj+XJToXwt1M6+9BeCz1SOj/1/mdZn56OZvCyZZc=
## Foundation for Applied Privacy
# - address_data: 93.177.65.183
#  tls_auth_name: "dot1.applied-privacy.net"
```

```

## # OARC. Note: this server currently doesn't support strict mode!
## - address_data: 184.105.193.78
##  tls_auth_name: "tls-dns-u.odvr.dns-oarc.net"
##  tls_pubkey_pinset:
##    - digest: "sha256"
##      value: pOXrpUt9kgPgbWxBFFcBTbRH2heo2wHwXp1fd4AEVXI=

##### IPv6 addresses #####
### Anycast services ###
## Quad 9 'secure' service - Filters, does DNSSEC, doesn't send ECS
# - address_data: 2620:fe::fe
#  tls_auth_name: "dns.quad9.net"
## Quad 9 'insecure' service - No filtering, does DNSSEC, may send ECS (it is
## unclear if it honours the edns_client_subnet_private request from stubby)
# - address_data: 2620:fe::10
#  tls_auth_name: "dns.quad9.net"
## Cloudflare servers
## (NOTE: recommend reducing idle_timeout to 9000 if using Cloudflare)
# - address_data: 2606:4700:4700::1111
#  tls_auth_name: "cloudflare-dns.com"
# - address_data: 2606:4700:4700::1001
#  tls_auth_name: "cloudflare-dns.com"
## Google
# - address_data: 2001:4860:4860::8888
#  tls_auth_name: "dns.google"
# - address_data: 2001:4860:4860::8844
#  tls_auth_name: "dns.google"
## Adguard Default servers
# - address_data: 2a00:5a60::ad1:0ff
#  tls_auth_name: "dns.adguard.com"

```



```

# - address_data: 2a00:5a60::ad2:0ff
#  tls_auth_name: "dns.adguard.com"
## Adguard Family Protection servers
# - address_data: 2a00:5a60::bad1:0ff
#  tls_auth_name: "dns-family.adguard.com"
# - address_data: 2a00:5a60::bad2:0ff
#  tls_auth_name: "dns-family.adguard.com"

### Test servers ###

## The Uncensored DNS server
# - address_data: 2a01:3a0:53:53::0
#  tls_auth_name: "unicast.censurfridns.dk"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: wike3jYAA6jQmXYTr/rbHeEPmC78dQwZbQp6WdrseEs=
## Fondation RESTENA (NREN for Luxembourg)
# - address_data: 2001:a18:1::29
#  tls_auth_name: "kaitain.restena.lu"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 7ftvIkA+UeN/ktVkovd/7rPZ6mbkhVI7/8HnFJiLa4=
## A Surfnet/Sinodun server supporting TLS 1.2 and 1.3
# - address_data: 2001:610:1:40ba:145:100:185:18
#  tls_auth_name: "dnsovertls3.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 5SpFz7JEPzF71hditH1v2dBhSErPUMcLPJx1uk2svT8=
## A Surfnet/Sinodun server using Knot resolver. Warning - has issue when used
## for DNSSEC
# - address_data: 2001:610:1:40ba:145:100:185:17
#  tls_auth_name: "dnsovertls2.sinodun.com"

```

```

# tls_pubkey_pinset:
#   - digest: "sha256"
#   value: NAXBESvpjZMnPWQcrxa2KFikHV/pDEIjRkA3hLWogSg=
## dns.cmrg.net server using Knot resolver. Warning - has issue when used for
## DNSSEC.
# - address_data: 2001:470:1c:76d::53
#   tls_auth_name: "dns.cmrg.net"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#     value: 3IOHSS48KOC/zlkKGtI46a9TY9PPKDVGH3WZS4JZo=
#     - digest: "sha256"
#     value: 5zFN3smRPuHIIIM/8L+hANT99LW26T97RFHqHv90awjo=
## dot.securedns.eu
# - address_data: 2a03:b0c0:0:1010::e9a:3001
#   tls_auth_name: "dot.securedns.eu"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#     value: h3mufC43MEqRD6uE4Iz6gAgULZ5/riqH/E+U+jE3H8g=
## dns-tls.bitwiseshift.net
# - address_data: 2001:8b0:24:24::24
#   tls_auth_name: "dns-tls.bitwiseshift.net"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#     value: YmcYWZU5dd2EoblZHNf1jTUPVS+uK3280YYCdz4I4wo=
## ns1.dnsprivacy.at
# - address_data: 2a01:4f8:c0c:3c03::2
#   tls_auth_name: "ns1.dnsprivacy.at"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#     value: vqVQ9TcoR9RDY3TpO0MTXw1YQLjF44zdN3/4PkLwtEY=

```

```
## ns2.dnsprivacy.at
# - address_data: 2a01:4f8:c0c:3bfc::2
#  tls_auth_name: "ns2.dnsprivacy.at"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: s5Em89o0kigwfbF1gcXWd8zIATSWVXsJ6ecZfmBDTKg=
## Go6Lab
# - address_data: 2001:67c:27e4::35
#  tls_auth_name: "privacydns.go6lab.si"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: g5lqtwHia/plKqWU/Fe2Woh4+7MO3d0JYqYJpj/iYAw=
## Lorraine Data Network (self-signed cert).
# - address_data: 2001:913::8
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: WaG0kHUS5N/ny0labz85HZg+v+f0b/UQ73IZjFep0nM=
## dns.neutopia.org
# - address_data: 2a00:5884:8209::2
#  tls_auth_name: "dns.neutopia.org"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: wTeXHM8aczhvRSi0cv2qOXkXInoDU+2C+M8MpRyT3OI=
## NIC Chile (self-signed cert)
# - address_data: 2001:1398:1:0:200:1:123:46
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: sG6kj+XJToXwt1M6+9BeCz1SOj/1/mdZn56OZvCyZZc=
## Foundation for Applied Privacy
# - address_data: 2a03:4000:38:53c::2
```

```

#  tls_auth_name: "dot1.applied-privacy.net"
### # OARC. Note: this server currently doesn't support strict mode!
##  - address_data: 2620:ff:c000:0:1::64:25
##  tls_auth_name: "tls-dns-u.odvr.dns-oarc.net"
##  tls_pubkey_pinset:
##    - digest: "sha256"
##      value: pOXrpUt9kgPgbWxBFFcBTbRH2heo2wHwXp1fd4AEVXI=

##### Servers that listen on port 443 (IPv4 and IPv6) #####
### Test servers ###
## Surfnets/Sinodun servers
# - address_data: 145.100.185.15
#  tls_port: 443
#  tls_auth_name: "dnsovertls.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 62lKu9HsDVbyiPenApnc4sfmSYTHOVfFgL3pyB+cBL4=
# - address_data: 145.100.185.16
#  tls_port: 443
#  tls_auth_name: "dnsovertls1.sinodun.com"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: cE2ecALeE5B+urJhDrJIVFmf38cJLAVqekONvjypqUA=
## dns.cmrg.net server using Knot resolver
# - address_data: 199.58.81.218
#  tls_port: 443
#  tls_auth_name: "dns.cmrg.net"
#  tls_pubkey_pinset:
#    - digest: "sha256"
#      value: 3IOHSS48KOC/zlkKGtI46a9TY9PPKDVGH3W2ZS4JZo=

```

```

# - digest: "sha256"
#   value: 5zFN3smRPuHlIM/8L+hANt99LW26T97RFHqHv90awjo=
## Lorraine Data Network (self-signed cert)
# - address_data: 80.67.188.188
#   tls_port: 443
#   tls_pubkey_pinset:
#     - digest: "sha256"
#       value: WaG0kHUS5N/ny0labz85HZg+v+f0b/UQ73IZjFep0nM=
## dns.neutopia.org
# - address_data: 89.234.186.112
#   tls_port: 443
#   tls_auth_name: "dns.neutopia.org"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#       value: wTeXHM8acvzhRSi0cv2qOXkXInoDU+2C+M8MpRyT3OI=
## The Surfnet/Sinodun servers
# - address_data: 2001:610:1:40ba:145:100:185:15
#   tls_port: 443
#   tls_auth_name: "dnsovertls.sinodun.com"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#       value: 62IKu9HsDVbyiPenApnc4sfmSYTHOVfFgGL3pyB+cBL4=
# - address_data: 2001:610:1:40ba:145:100:185:16
#   tls_port: 443
#   tls_auth_name: "dnsovertls1.sinodun.com"
#   tls_pubkey_pinset:
#     - digest: "sha256"
#       value: cE2ecALeE5B+urJhDrJIVFmf38cJLAvqekONvjvpqUA=
## dns.cmrg.net server using Knot resolver
# - address_data: 2001:470:1c:76d::53

```

```

# tls_port: 443
# tls_auth_name: "dns.cmrg.net"
# tls_pubkey_pinset:
#   - digest: "sha256"
#     value: 3IOHSS48KOC/zlKKGtI46a9TY9PPKDVGH3W2ZS4JZo=
#   - digest: "sha256"
#     value: 5zFN3smRPuHIIIM/8L+hANT99LW26T97RFHqHv90awjo=
## Lorraine Data Network (self-signed cert)
# - address_data: 2001:913::8
# tls_port: 443
# tls_pubkey_pinset:
#   - digest: "sha256"
#     value: WaG0kHUS5N/ny0labz85HZg+v+f0b/UQ73IZjFep0nM=
## dns.neutopia.org
# - address_data: 2a00:5884:8209::2
# tls_port: 443
# tls_auth_name: "dns.neutopia.org"
# tls_pubkey_pinset:
#   - digest: "sha256"
#     value: wTeXHM8aczhRSi0cv2qOXkXIInoDU+2C+M8MpRyT3OI=
## Foundation for Applied Privacy
# - address_data: 93.177.65.183
# tls_port: 443
# tls_auth_name: "dot1.applied-privacy.net"
# - address_data: 2a03:4000:38:53c::2
# tls_port: 443
# tls_auth_name: "dot1.applied-privacy.net"

```

LAMPIRAN – D. Unbound

a. unbound.conf

```

verbosity: 0

```

```

#interface: 192.168.171.40
#interface: 127.0.0.1
interface: 0.0.0.0
access-control: 192.168.0.0/16 allow
port: 7777
do-ip4: yes
do-udp: yes
do-tcp: yes
do-ip6: no
prefer-ip6: no
root-hints: "/etc/unbound/root.hints"
harden-glue: yes
harden-dnssec-stripped: yes
use-caps-for-id: no
edns-buffer-size: 1472
prefetch: yes
num-threads: 1
so-rcvbuf: 1m
private-address: 192.168.0.0/16
private-address: 169.254.0.0/16
private-address: 172.16.0.0/12
private-address: 10.0.0.0/8
private-address: fd00::/8
private-address: fe80::/10

```

b. root.hints

```

; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
; file /domain/named.cache
; on server FTP.INTERNIC.NET
; -OR- RS.INTERNIC.NET
;
; last update: June 08, 2020
; related version of root zone: 2020060801
;
; FORMERLY NS.INTERNIC.NET
;
; 360000 NS A.ROOT-SERVERS.NET.

```

```

A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4
A.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.          3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 199.9.14.201
B.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.          3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
C.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.          3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A 199.7.91.13
D.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.          3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10
E.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:a8::e
;
; FORMERLY NS.ISC.ORG
;
.          3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000 A 192.5.5.241
F.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.          3600000 NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET. 3600000 A 192.112.36.4
G.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:12::d0d
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.          3600000 NS H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET. 3600000 A 198.97.190.53

```



```

H.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:1::53
;
; FORMERLY NIC.NORDU.NET
;
.           3600000 NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET. 3600000 A 192.36.148.17
I.ROOT-SERVERS.NET. 3600000 AAAA 2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
.           3600000 NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET. 3600000 A 192.58.128.30
J.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
.           3600000 NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET. 3600000 A 193.0.14.129
K.ROOT-SERVERS.NET. 3600000 AAAA 2001:7fd::1
;
; OPERATED BY ICANN
;
.           3600000 NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET. 3600000 A 199.7.83.42
L.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:9f::42
;
; OPERATED BY WIDE
;
.           3600000 NS M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET. 3600000 A 202.12.27.33
M.ROOT-SERVERS.NET. 3600000 AAAA 2001:dc3::35

```

c. root-auto-trust-anchor-file.conf

```

server:
# The following line will configure unbound to perform cryptographic
# DNSSEC validation using the root trust anchor.
auto-trust-anchor-file: "/var/lib/unbound/root.key"

```

d. qname-minimisation.conf

```

server:

```

```
# Send minimum amount of information to upstream servers to
enhance
# privacy. Only sends minimum required labels of the QNAME and
sets
# QTYPE to NS when possible.

# See RFC 7816 "DNS Query Name Minimisation to Improve Privacy"
for
# details.
qname-minimisation: yes
```