Troubleshooting DNSSEC

a few handles to get you started
Toolbag

- dig
- drill
- unbound-host
- Packet analysis
  - wireshark
  - tcpdump
  - dnscap (in combination with the above)
Try to understand the wire

- A DNS Packet has a header and 4 sections:
  - Question
  - Answer
  - Authoritative
  - Additional
<table>
<thead>
<tr>
<th>ID</th>
<th>QDCOUNT</th>
<th>ANCOUNT</th>
<th>NSCOUNT</th>
<th>ARCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Header

Opcode

Query (0)
Response (1)

Flag Description
--- ---------------------
AA Authoritative Answer
TC Truncated Response
RD Recursion Desired
RA Recursion Allowed
Reserved
AD Authentic Data
CD Checking Disabled

Opcode

0 Query [RFC1035]
1 IQuery (Inverse Query, Obsolete) [RFC3425]
2 Status [RFC1035]
3 Unassigned
4 Notify [RFC1996]
5 Update [RFC2136]
6-15 Unassigned

RCODE

Hexadecimal Name Description
---------- ---------- -----------------------------------
0 NoError No Error
1 FormErr Format Error
2 ServFail Server Failure
3 NXDomain Non-Existent Domain
4 NotImp Not Implemented
5 Refused Query Refused
6 YXDomain Name Exists when it should not
7 YXRRSet RR Set Exists when it should not
8 NXRRSet RR Set that should exist does not
9 NotAuth Server Not Authoritative for zone
10 NotZone Name not contained in zone
11-15 Unassigned
**Question to Authoritative Nameserver**

### Question Section

- **Query type:** NS
- **Domain:** `org`
- **TTL:** 86400
- **Resource Records:**
  - `b0.org.afilias-nst.org.
  - `d0.org.afilias-nst.org.
  - `a0.org.afilias-nst.info.
  - `a2.org.afilias-nst.info.
  - `b2.org.afilias-nst.org.
  - `c0.org.afilias-nst.info.
  - `b2.org.afilias-nst.org.
  - `d0.org.afilias-nst.org.
  - `a0.org.afilias-nst.info.
  - `a2.org.afilias-nst.info.

**Answer Section**

- **TTL:** 86400
- **Resource Records:**
  - `a0.org.afilias-nst.info.
  - `a0.org.afilias-nst.info.
  - `a2.org.afilias-nst.info.
  - `a2.org.afilias-nst.info.
  - `b0.org.afilias-nst.org.
  - `b0.org.afilias-nst.org.
  - `b2.org.afilias-nst.org.
  - `b2.org.afilias-nst.org.
  - `c0.org.afilias-nst.info.
  - `c0.org.afilias-nst.info.
  - `d0.org.afilias-nst.org.
  - `d0.org.afilias-nst.org.
  - `b0.org.afilias-nst.org.
  - `b2.org.afilias-nst.org.
  - `c0.org.afilias-nst.info.
  - `c0.org.afilias-nst.info.
  - `d0.org.afilias-nst.org.
  - `d0.org.afilias-nst.org.
  - `d0.org.afilias-nst.org.

**Authority Section**

- **Resource Records:**
  - `a0.org.afilias-nst.info.
  - `a0.org.afilias-nst.info.
  - `a2.org.afilias-nst.info.
  - `a2.org.afilias-nst.info.
  - `b0.org.afilias-nst.org.
  - `b0.org.afilias-nst.org.
  - `b2.org.afilias-nst.org.
  - `b2.org.afilias-nst.org.
  - `c0.org.afilias-nst.info.
  - `c0.org.afilias-nst.info.
  - `d0.org.afilias-nst.org.
  - `d0.org.afilias-nst.org.

**Query time:** 409 msec

**SERVER:** 2001:500:e::1#53(2001:500:e::1)

**WHEN:** Thu Apr  8 08:44:33 2010

**MSG SIZE rcvd:** 597
Frame 203 (86 bytes on wire, 86 bytes captured)


User Datagram Protocol, Src Port: 50285 (50285), Dst Port: domain (53)

Domain Name System (query)

[Response In: 204]

Transaction ID: 0x9a3a

Flags: 0x0010 (Standard query)

0... ....... ....... = Response: Message is a query
000 0... ....... = Opcode: Standard query (0)
...... 0. ....... = Truncated: Message is not truncated
...... 0 ....... = Recursion desired: Don't do query recursively
...... 0... ....... = Z: reserved (0)
...... .....1 .... = Non-authenticated data OK: Non-authenticated data is acceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1

Queries

ns.majordomo.ru: type A, class IN

Additional records

<Root>: type OPT

Name: <Root>
Type: OPT (EDNS0 option)
UDP payload size: 4096
Higher bits in extended RCODE: 0x0
EDNS0 version: 0

Z: 0x8000

Bit 0 (DO bit): 1 (Accepts DNSSEC security RRs)
Bits 1:15: 0x0 (reserved)
Data length: 0

OPT RR: EDNS
EDNS

• Communicate ability to deal with 512+ IP packets (fragmentation buffers)
• Communicate willingness to receive DNSSEC resource records
• Space for much more resource
Deeper Understanding?

- http://www.iana.org/assignments/dns-parameters
- follow the links to the RFCs
What Can Go Wrong
Possible Failures

- Local Configuration
- Secure Delegation Failure
- True validation failure
- Transport problems
Local Configuration

• Time:
  DNSSEC is critically dependent on time. Check your NTP configuration

• use `date -u "+%Y%m%d%H%M%S"`

• Check signature validity times
DIG 9.7.0b2 @a0.org.afilias-nst.info. org NS +dnssec
(2 servers found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49574
; flags: qr aa rd; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 13
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; QUESTION SECTION:
; .org. IN NS

; ANSWER SECTION:
org. 86400 IN NS b0.org.afilias-nst.org.
org. 86400 IN NS d0.org.afilias-nst.org.
org. 86400 IN NS a0.org.afilias-nst.info.
org. 86400 IN NS a2.org.afilias-nst.info.
org. 86400 IN NS b0.org.afilias-nst.org.
org. 86400 IN NS b2.org.afilias-nst.info.
org. 86400 IN NS c0.org.afilias-nst.info.
org. 86400 IN RRSIG NS 7 1 86400 20100415154437 (20100401144437 79498 org.
BSO2Encp2iwDCteKXCy10PsVzFU8ailzInCveqPxBuW
gGIpy7HRamerEq7fQ+PWvxt3F0k/zTUDFifR1paOHbG
MRfOVG9XHskS xoUqwix2jRAIXXYmXz3A/NsjgoJVsIEj
3DWP43cTJMoOsS68qmK7CbbyLrSTRdg6/d/mK4= )

; ADDITIONAL SECTION:
a0.org.afilias-nst.info. 86400 IN A 199.19.56.1
a0.org.afilias-nst.info. 86400 IN AAAA 2001:500:e::1
a2.org.afilias-nst.info. 86400 IN A 199.249.112.1
a2.org.afilias-nst.info. 86400 IN AAAA 2001:500:40::1
b0.org.afilias-nst.org. 86400 IN A 199.19.54.1
b0.org.afilias-nst.org. 86400 IN AAAA 2001:500:c::1
b2.org.afilias-nst.org. 86400 IN A 199.249.120.1
b2.org.afilias-nst.org. 86400 IN AAAA 2001:500:48::1
c0.org.afilias-nst.info. 86400 IN A 199.19.53.1
c0.org.afilias-nst.info. 86400 IN AAAA 2001:500:b::1
d0.org.afilias-nst.org. 86400 IN A 199.19.57.1
d0.org.afilias-nst.org. 86400 IN AAAA 2001:500:f::1

; Query time: 409 msec
; SERVER: 2001:500:e::1#53(2001:500:e::1)
; WHEN: Thu Apr 8 08:44:33 2010
; MSG SIZE rcvd: 597

$ date -u "+%Y%m%d%H%M%S"
20100408095947
Secure delegations

• Secure delegations: Look for the DS
• Matching Key IDs?
• NSEC proof?
• Hard to do manually
Looking at the chain of trust

- CLI based
  - drill -T or drill -S (trace or chace)
  - dig +sigchace
- Web Based
  - dnsviz: http://dnsviz.net/
  - debugger: http://dnssec-debugger.verisignlabs.com/
drill -S

;; Chasing: example.net. SOA

DNSSEC Trust tree:
example.net. (SOA)
  |---example.net. (DNSKEY keytag: 17000)
  |---example.net. (DNSKEY keytag: 49656)
  |---example.net. (DS keytag: 49656)
  |---net. (DNSKEY keytag: 62972)
  |---net. (DNSKEY keytag: 13467)
  |---net. (DS keytag: 13467)
  |---. (DNSKEY keytag: 63380)
  |---. (DNSKEY keytag: 63276)

;; Chase successful
drill -T -k < root.ksk > example.net SOA

;; Domain: .
[T] . 100 IN DNSKEY 256 3 5 ;{id = 63380 (zsk), size = 1024b}
. 100 IN DNSKEY 257 3 5 ;{id = 63276 (ksk), size = 1280b}

Checking if signing key is trusted:
New key: . 100 IN DNSKEY 256 3 5 AQPQyahTO0aR/Pi6p ... Q== ;{id = 63380 (zsk), size = 1024b}
Trusted key: . 3600 IN DNSKEY 257 3 5 AQPv6tbkmM+ ... liY/ ;{id = 63276 (ksk), size = 1280b}
Trusted key: . 100 IN DNSKEY 256 3 5 AQPQyahTO0aR/ ... MiBmsMQ== ;{id = 63380 (zsk), size = 1024b}

Key is now trusted!
Trusted key: . 100 IN DNSKEY 257 3 5 AQOv6tbkmM+1 ... liY/ ;{id = 63276 (ksk), size = 1280b}

[T] net. 100 IN DS 13467 5 2 ec9b094786b82c46aa3054c7352b59904b697119d515b4ea536ec3dd9a10ed81
net. 100 IN DS 13467 5 1 de01426e08dab91e8502ccc1081390cd7da0e178

;; Domain: net.
[T] net. 100 IN DNSKEY 256 3 5 ;{id = 62972 (zsk), size = 1024b}
net. 100 IN DNSKEY 257 3 5 ;{id = 13467 (ksk), size = 1280b}

Checking if signing key is trusted:
New key: net. 100 IN DNSKEY 256 3 5 AQPVP6Je ... 8h3J3Gw== ;{id = 62972 (zsk), size = 1024b}
Trusted key: . 3600 IN DNSKEY 257 3 5 AQPv6tbkmM+ ... liY/ ;{id = 63276 (ksk), size = 1280b}
Trusted key: . 100 IN DNSKEY 256 3 5 AQPQyahT ... msMQ== ;{id = 63380 (zsk), size = 1024b}
Trusted key: net. 100 IN DNSKEY 257 3 5 AQOv6tbkmM ... oewiliY/ ;{id = 63276 (ksk), size = 1280b}
Trusted key: net. 100 IN DNSKEY 256 3 5 AQPVP6 ... 3J3Gw== ;{id = 62972 (zsk), size = 1024b}

Key is now trusted!
Trusted key: net. 100 IN DNSKEY 257 3 5 AQOsAH77.... QuH ;{id = 13467 (ksk), size = 1280b}

[T] example.net. 100 IN DS 49656 5 1 3850efb9133ec66275ca5321587d445702397e
example.net. 100 IN DS 49656 5 2 9e06b299ab8811d699e077ff990ff5a1b496c914deb22697ba22a1da31f0a6e

;; Domain: example.net.
[T] example.net. 100 IN DNSKEY 256 3 5 ;{id = 17000 (zsk), size = 1024b}
example.net. 100 IN DNSKEY 257 3 5 ;{id = 49656 (ksk), size = 1280b}
[T] example.net. 100 IN SOA ns.example.net. olaf.nlnetlabs.nl. 2002050501 100 200 604800 100

[S] self sig OK; [B] bogus; [T] trusted
External views

- DNSVIZ: http://dnsviz.net/
- Verisign’s DNSSEC Debugger: http://dnssec-debugger.verisignlabs.com/
- Secspider: http://secspider.cs.ucla.edu/
DNSKEY represented as DLV

No connection between secret-wg.or and org
<table>
<thead>
<tr>
<th>Zone</th>
<th>DNSKEY Records</th>
<th>RRSIGs Over DNSKEY RRset</th>
<th>RRSIGs Over DS RRset</th>
<th>DNSSKEY Records for Domain</th>
<th>RRSIGs Over DNSSKEY RRset</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>org</td>
<td>2</td>
<td>RRSIG=51201</td>
<td>RRSIG=51201</td>
<td>4</td>
<td>RRSIG=21366</td>
</tr>
<tr>
<td>secret-wg.org</td>
<td>2</td>
<td>RRSIG=55440</td>
<td>RRSIG=55440</td>
<td>4</td>
<td>RRSIG=21366</td>
</tr>
</tbody>
</table>

Connection between secret-wg.org and org exist.
SecSpider the DNSSEC Monitoring Project

Check out our new sister-project Vantages with libdns, dnsfunnel, and vantaged!

We now have TA files for both modern resolvers and older instances of BIND that don't support all key types on our Trust Anchors Page

To add a zone for monitoring, please submit below:

Zone to add: secret-wg.org  Submit

Vouch for or against a zone's production status

For more information, questions, or comments please contact:
Eric Osterweil (eoster@cs.ucla.edu)
Dan Massey (massey@cs.colostate.edu)
Lixia Zhang (lixia@cs.ucla.edu)

DNSSEC Deployment status as of: Wed Dec 14 06:41:56 2011 UTC

Deployment Metrics:

Availability Metric: 0.743
Verifiability Metric: 0.423
Validity Metric: < 0.932, 0.937>
### DNSSEC Zone stats

**Zone**: secret-wg.org, status as of: Wed Dec 14 06:41:56 2011 UTC

**Parent Zone**: org.

**Reason for Monitoring this Zone:**
- DNSKEY Availability: Stale Refreshes: 1

**Data files for:**
- DNS records (signed)
- DNSKEY records (signed)

**Trust Anchor:**
- Consistency: 6/9
- Name: 6/9
- EDNS0: Yes
- DNSSEC deployed: Yes
- Production zone: Yes
- User Production: N/A

### Summary

<table>
<thead>
<tr>
<th>Property</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDNS0 capable</td>
<td>Yes</td>
</tr>
<tr>
<td>DNSSEC deployed</td>
<td>Yes</td>
</tr>
<tr>
<td>Production zone</td>
<td>Yes</td>
</tr>
<tr>
<td>User Production</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Name Servers

<table>
<thead>
<tr>
<th>Consistency</th>
<th>Online</th>
<th>NS Name</th>
<th>NS IP</th>
<th>Server Version</th>
<th>First Queried</th>
<th>Last Queried</th>
<th>NS Serial Number</th>
<th>EDNS0 Capable</th>
<th>DNSSEC Deployed</th>
<th>Pointed to by Which Zone (Parent/Authoritative/Both)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/9</td>
<td>Yes</td>
<td>mcvax.ninetlabs.nl</td>
<td>192.16.197.229</td>
<td>NSD 3.2.8</td>
<td>Sun May 29 14:49:08 2011 UTC</td>
<td>Thu Nov 17 02:07:21 2011 UTC</td>
<td>501</td>
<td>Yes</td>
<td>Yes</td>
<td>Parent</td>
</tr>
<tr>
<td>7/9</td>
<td>Yes</td>
<td>sec2.authdns.ripe.net</td>
<td>193.0.9.4</td>
<td>9.7.3-P3</td>
<td>Sun Jul 11 04:47:00 2010 UTC</td>
<td>Thu Nov 17 02:07:22 2011 UTC</td>
<td>501</td>
<td>Yes</td>
<td>Yes</td>
<td>Both</td>
</tr>
<tr>
<td>8/9</td>
<td>Yes</td>
<td>ns.secret-wg.org</td>
<td>213.154.224.48</td>
<td>NSD 3.2.8</td>
<td>Tue Aug 24 19:15:39 2009 UTC</td>
<td>Thu Nov 17 02:07:23 2011 UTC</td>
<td>501</td>
<td>Yes</td>
<td>Yes</td>
<td>Both</td>
</tr>
<tr>
<td>7/9</td>
<td>Yes</td>
<td>open.ninetlabs.nl</td>
<td>213.154.224.1</td>
<td>NSD 3.2.8</td>
<td>Wed Apr 22 22:11:23 2009 UTC</td>
<td>Thu Nov 17 02:07:23 2011 UTC</td>
<td>501</td>
<td>Yes</td>
<td>Yes</td>
<td>Both</td>
</tr>
</tbody>
</table>

### DS Records from parent zone: Consistency: 7/9

**Key Tag** | **Digest** | **Verified (Yes/No)**
--- | --- | ---
SECRET-WG.ORG | 18786 | Yes
SECRET-WG.ORG | 18786 | Yes

### DNSKEYs: Consistency: 7/9

**Key Verified [Yes/No/Unknown]** | **Key Tag** | **Key Type** | **Algorithm** | **Key**
--- | --- | --- | --- | ---
Yes | secret-wg.org | 18786 | KSK | SDSA159 Nissan 159
Yes | secret-wg.org | 35973 | ZSK | SDSA159 Nissan 159
Yes | secret-wg.org | 61956 | ZSK | SDSA159 Nissan 159
Case Study

• NASA DS Rollover failure impacting Comcast:
  http://www.dnssec.comcast.net/DNSSEC_Va
didation_Failure_NASAGOV_20120118_FINAL.pdf
looking at a validating server

- So you got a SERVAIL
- `dig +cd` will disable checking
  - you get an answer?
  - likely validation failure
Transport problems

• If responses grow beyond 512 octets:
  • UDP may see fragmentation and dropped fragments (firewalls etc)
  • Fragmentation problems on path?
  • Fallback to TCP
  • Port 53 TCP sometimes blocked
Does the network support DNSSEC?

• One tool you could use for a quick assessment:

  • http://netalyzr.icsi.berkeley.edu/

  • you contribute to good science too!
The ICSI Netalyzr

Debug your Internet.

1. What's up with my network?
   Some services seem broken? Things are very slow? Is there something wrong?

2. Run the Netalyzr.
   We test your internet connection for signs of trouble.

3. Understand your connectivity.
   A detailed report shows performance & security issues.

Learn more, see an example report, check out the NetaMap, look at the FAQ, or try the new commandline client. Netalyzr requires Java to operate.

Start analysis »

Please note: Netalyzr is not only a debugging tool — it is also the foundation of a comprehensive measurement study compiling a survey of the health of the Internet's edge. By running Netalyzr and helping us spread the word you are contributing crucially to the quality of our study. Thanks for your help!
An applet from “n2.netalyzr.icsi.berkeley.edu" is requesting access to your computer.

The digital signature from “International Computer Science Institute” has been verified.

Allow all applets from “n2.netalyzr.icsi.berkeley.edu" with this signature

Show Details... Deny Allow
The ICSI Netalyzr

Checking the network's MTU...

Please be patient, the tests may take several minutes to complete.

ID 43ca208a-31459-b0d9c6ce-d2c8-450f-8272
Result Summary +/- (help)

- nl/83

Recorded at 04:14 EST (09:14 UTC), Feb 14 2012. Permalink Client/server transcript.

Summary of Noteworthy Events –

- Minor Aberrations
  - Network packet buffering may be excessive
  - We received unexpected and possibly dangerous results when looking up important names
  - The path between our system and your network does not appear to handle fragmented IPv6 traffic properly

Address-based Tests +

- NAT detection (2): No NAT Detected
- Local Network Interfaces (2): OK
- DNS-based host information (2): OK

Reachability Tests +

- TCP connectivity (2): OK
- UDP connectivity (2): OK
- Traceroute (2): OK
- Path MTU (2): OK
### DNS Tests

- **Restricted domain DNS lookup (?): OK**
  - We can successfully look up a name which resolves to the same IP address as our webserver. This means we are able to conduct many of the tests on your DNS server.

- **Unrestricted domain DNS lookup (?): OK**
  - We can successfully look up arbitrary names from within the Java applet. This means we are able to conduct all tests on your DNS server.

- **Direct DNS support (?): OK**
  - All tested DNS types were received OK.

- **Direct EDNS support (?): OK**
  - EDNS-enabled requests for small responses are answered successfully.
  - EDNS-enabled requests for medium-sized responses are answered successfully.
  - EDNS-enabled requests for large responses are answered successfully.

- **DNS resolver address (?): OK**
  - The IP address of your ISP's DNS Resolver is 213.154.224.59, which resolves to alpha.nlnetlabs.nl.

- **DNS resolver properties (?): Lookup latency 240ms**
  - Your ISP's DNS resolver requires 240 msec to conduct an external lookup. It takes 200 msec for your ISP's DNS resolver to lookup a name on our server.
  - Your resolver correctly uses TCP requests when necessary.
  - Your resolver is using QTYPE=A for default queries.
  - Your host or resolver also performs IPv6 queries in addition to IPv4 queries.
  - Your DNS resolver requests DNSSEC records.
  - Your DNS resolver advertises the ability to accept DNS packets of up to 4096 bytes.
  - Your DNS resolver can successfully receive a smaller (~1400 byte) DNS response.
  - Your DNS resolver can successfully receive a large (>1500 byte) DNS response.
  - Your DNS resolver can successfully accept large responses.
  - Your resolver does not use 0x20 randomization, but will pass names in a case-sensitive
On your server

- val-log-level:
  - val-log-level: 0 - prints nothing
  - val-log-level: 1 - print queries that fail
  - val-log-level: 2 - print reason why it failed

- remember `unbound-control set_option`?
Apr 08 12:31:06 unbound[853:0] info: validation failure
<dnssec1.qsa.dnsops.gov. A IN>: signature expired from 159.142.174.98
for key gsa.dnsops.gov. while building chain of trust

Apr 08 10:28:01 unbound[853:0] info: validation failure
<barney.llnl.dnsops.gov. SOA IN>: No DNSKEY record from 128.115.249.61
for key barney.llnl.dnsops.gov. while building chain of trust
Unbound-host

- Unbound-host tool is useful for taking a first stab
- Runs the unbound validator from the command line
  - unbound-host -v -f trustanchor example.com
  - prints the val-log-level 2 error message if it fails.
  - with -C it can read unbound.conf for settings.
  - with -d (or -ddddd) you get a high verbosity trace
Remedies

• Clean your cache in case of problems locally
• Bind:
  • `rndc flush`
  • `rndc flushname`
• Unbound
  • `unbound-control flush`
  • `unbound-control flush_zone`
  • `unbound-control flush_infra`