ZONEMASTER

A new DNS Delegation Testing Tool

Patrik Wallström, IIS
Vincent Levigneron, AFNIC

ccNSO Tech Day
ICANN-54 Dublin

iiS

afnic

Background

- DNSCheck (IIS)
  - Does not provide deterministic results
- Zonecheck (AFNIC)
  - Legacy code written in Ruby
- Both AFNIC and IIS wanted a new better tool to check delegations
- Collaborate to create a new reference tool
  - Joint requirements and specifications

Collaboration

- Project started in October 2013
- One year of work to...
  - Organise the project and tasks between IIS and AFNIC teams
  - Discuss and write common requirements and specifications
  - Develop a new tool from scratch in Perl
- First released in December 2014
- Stable and publicly announced release in February 2015

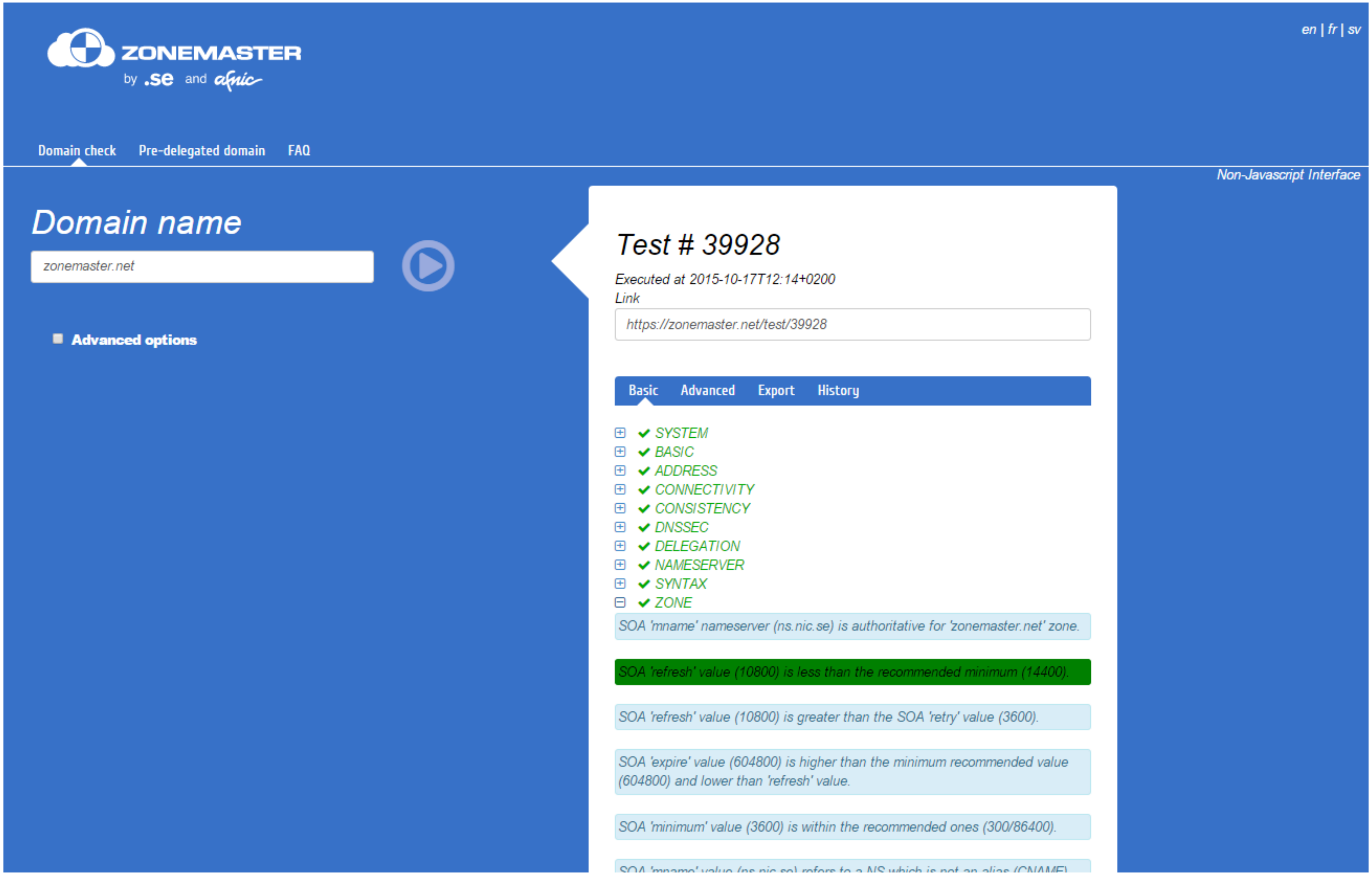
Zonemaster in ONE Slide

- **Open source** project written in **Perl** (+javascript)
- Aim to be a state-of-the-art checking tool for internet domain names
- Can check delegated and non-delegated zones
- Process hundreds of tests
- Provides CLI/Web/API interfaces
    - Can be used by non technicians on our website (WEB)
    - Can be used on local servers by technicians (CLI)
    - Can be used and integrated in your own systems (API)
- Provides high/medium/low levels of output
    - Web/Text output/JSON output
- Outputs in English, French and Swedish
- Can be tailored for your needs

Inside Zonemaster

- Engine (**Zonemaster::** *)
  - Implements all the test cases (**10** categories, **56** different test cases)
  - Uses its own resolver based on **Net::LDNS**
- CLI (Command Line user Interface)
  - Log as Text, raw text or JSON
- Backend (JSON-RPC interface to the **Engine**)
  - Store results in a database
- GUI (**http://zonemaster.net**)
  - The UI that runs the tests and present the results
  - Access to the history (stored in database)
- Quality considerations
  - Use of **Perl::Critic** and **Devel::Cover** (90%)
  - Hundreds of non regressions tests
  - Use of **Travis CI** in **GitHub**

Zonemaster Web Interface



Domain name

zonemaster.net

■ Advanced options

Test # 39928

Executed at 2015-10-17T12:14+0200

Link

https://zonemaster.net/test/39928

- ⊞ ✓ SYSTEM
- ⊞ ✓ BASIC
- ⊞ ✓ ADDRESS
- ⊞ ✓ CONNECTIVITY
- ⊞ ✓ CONSISTENCY
- ⊞ ✓ DNSSEC
- ⊞ ✓ DELEGATION
- ⊞ ✓ NAMESERVER
- ⊞ ✓ SYNTAX
- ⊟ ✓ ZONE

SOA 'mname' nameserver (ns.nic.se) is authoritative for 'zonemaster.net' zone.

SOA 'refresh' value (10800) is less than the recommended minimum (14400).

SOA 'refresh' value (10800) is greater than the SOA 'retry' value (3600).

SOA 'expire' value (604800) is higher than the minimum recommended value (604800) and lower than 'refresh' value.

SOA 'minimum' value (3600) is within the recommended ones (300/86400).

SOA 'mname' value (ns.nic.se) refers to a NS which is not an alias (CNAME).

Zonemaster CLI Interface

```
bash-4.3$ zonemaster-cli dnssec05-algorithm-deprecated.zut-root.rd.nic.fr
Seconds Level     Message
======= ========= =======
  22.35 WARNING   All nameservers have IPv4 addresses in the same AS (16276).
  22.35 WARNING   All nameservers are in the same AS (16276).
  22.45 ERROR     No DS record had a DNSKEY with a matching keytag.
  22.55 WARNING   The DNSKEY with tag 7533 uses deprecated algorithm number 1/(RSA/MD5).
  22.55 WARNING   The DNSKEY with tag 24113 uses deprecated algorithm number 1/(RSA/MD5).
  22.59 ERROR     Server at 178.33.232.188 sent 2 DNSKEY records, and 0 RRSIG records.
  22.59 ERROR     Server at 46.105.116.200 sent 2 DNSKEY records, and 0 RRSIG records.
  22.64 ERROR     Trying to verify NSEC RRset with RRSIG 21288 gave error 'No keys with the
                  keytag and algorithm from the RRSIG found'.
  22.64 ERROR     No signature correctly signed the NSEC RRset.
  22.70 NOTICE    Delegation from parent to child is not properly signed (no_dnskey).
  24.17 NOTICE    SOA 'refresh' value (3600) is less than the recommended minimum (14400).
  24.17 NOTICE    SOA 'retry' value (1800) is less than the recommended minimum (3600).
  24.60 NOTICE    No target (MX, A or AAAA record) to deliver e-mail for the domain name.
```

Tailoring

- Add your own langage
  - Only one file to create, no need to understand Perl
  - If you do that, **please** create a pull request
- Adapt Zonemaster policy to yours
  - JSON file to modify
  - Choose tests to execute
  - Modify severity levels
- And if you are a Perl developer…
  - use Zonemaster;

How to Contribute

- Use the tool (Web and/or CLI interfaces)
- Report bugs on GitHub

  https://github.com/dotse/zonemaster
- Ask for enhancements
- Git clone Zonemaster components
- Develop your own tools based on the API and share with the community
- Need Help? Ask Patrik and Vincent during meeting…

ZONEMASTER

Applications

IIS Use

- IIS used/uses DNSCheck for
  - The Healthcheck report
  - Report to registrars
  - Status of the .se zone - Zone Cleaning
  - http://dnscheck.iis.se/
- Now we’re switching to Zonemaster

use Zonemaster;

First step - how to use Zonemaster?

```
sh -c "zonemaster-cli --level DEBUG --json $domain >> result/$domain”
```

or

```
use Zonemaster;
@log = Zonemaster->test_zone( $domain );
```

Mass Measurements

- A tool I wrote - zonemaster-collector
- Runs Zonemaster multi-threaded
- Stores results in a directory or a MongoDB database - directly as JSON documents

How to collect

```
./collect.pl --mongo --db results --collection tlds --threads 150 --level DEBUG -f tlds.txt
```

But how to analyze?

Using MongoDB… Search directly in JSON documents:

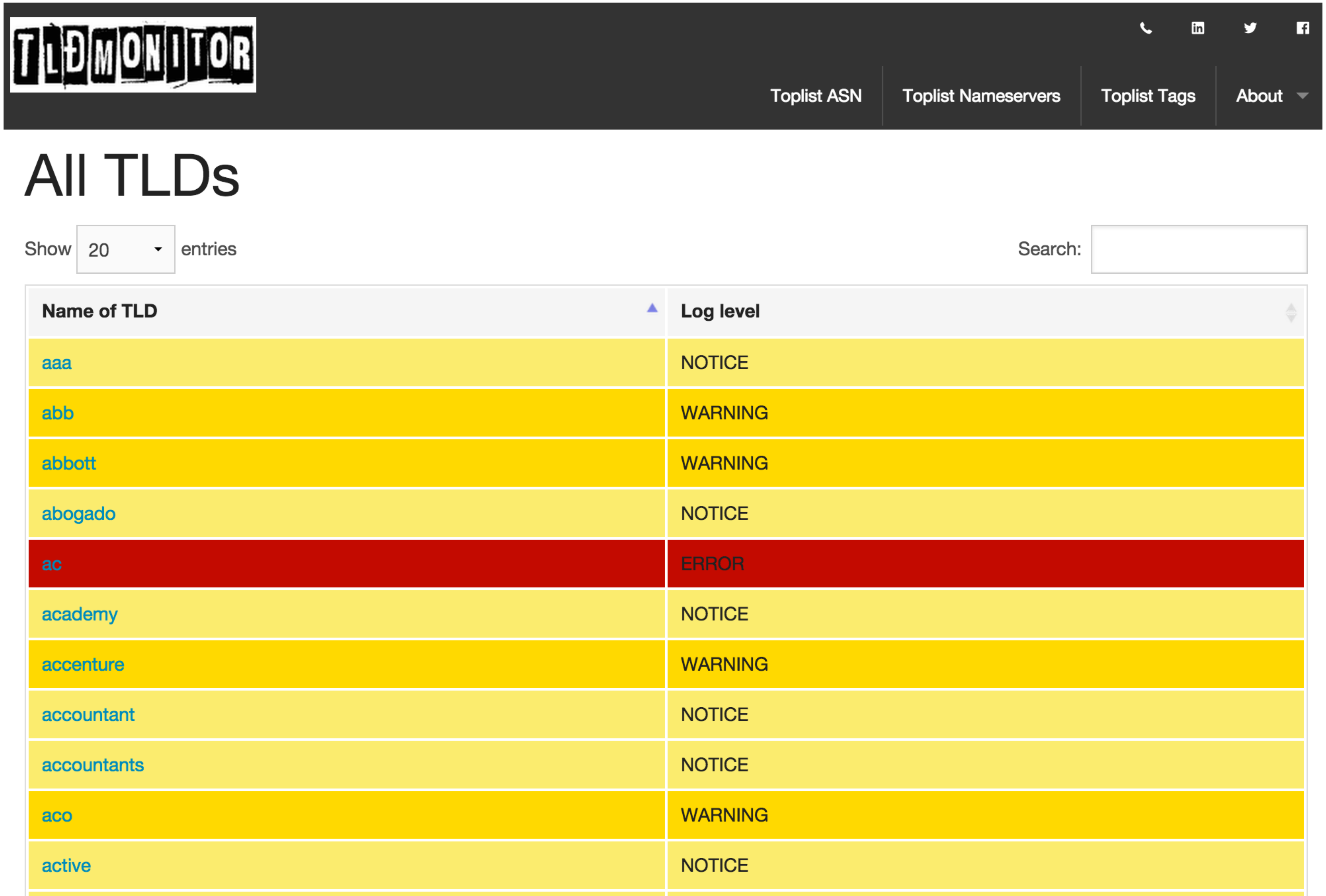
```
db.tlds.find({ "result.level": "ERROR" },
    { "name": 1, "_id": 0 } );

 db.tlds.find({ "result.args.ns": "ns.example.com"},
    { "name": 1, "result.$.args": 1, "_id": 0 } );
```

Get a specific error

```
db.tlds.aggregate(
  { $match: { "result.tag": "IS_A_RECURSOR" } },
  { $unwind: "$result" },
  { $match: { "result.tag": "IS_A_RECURSOR" } },
  { $project: { "name":1, "result": 1, "_id": 0 } },
  { $group: { _id: "$result.args.ns", nscount: { $sum: 1 } } },
  { $sort: { nscount: -1 } },
  { $limit: 25 }
);
```

Not very user friendly…

Complicated - so I created a web interface



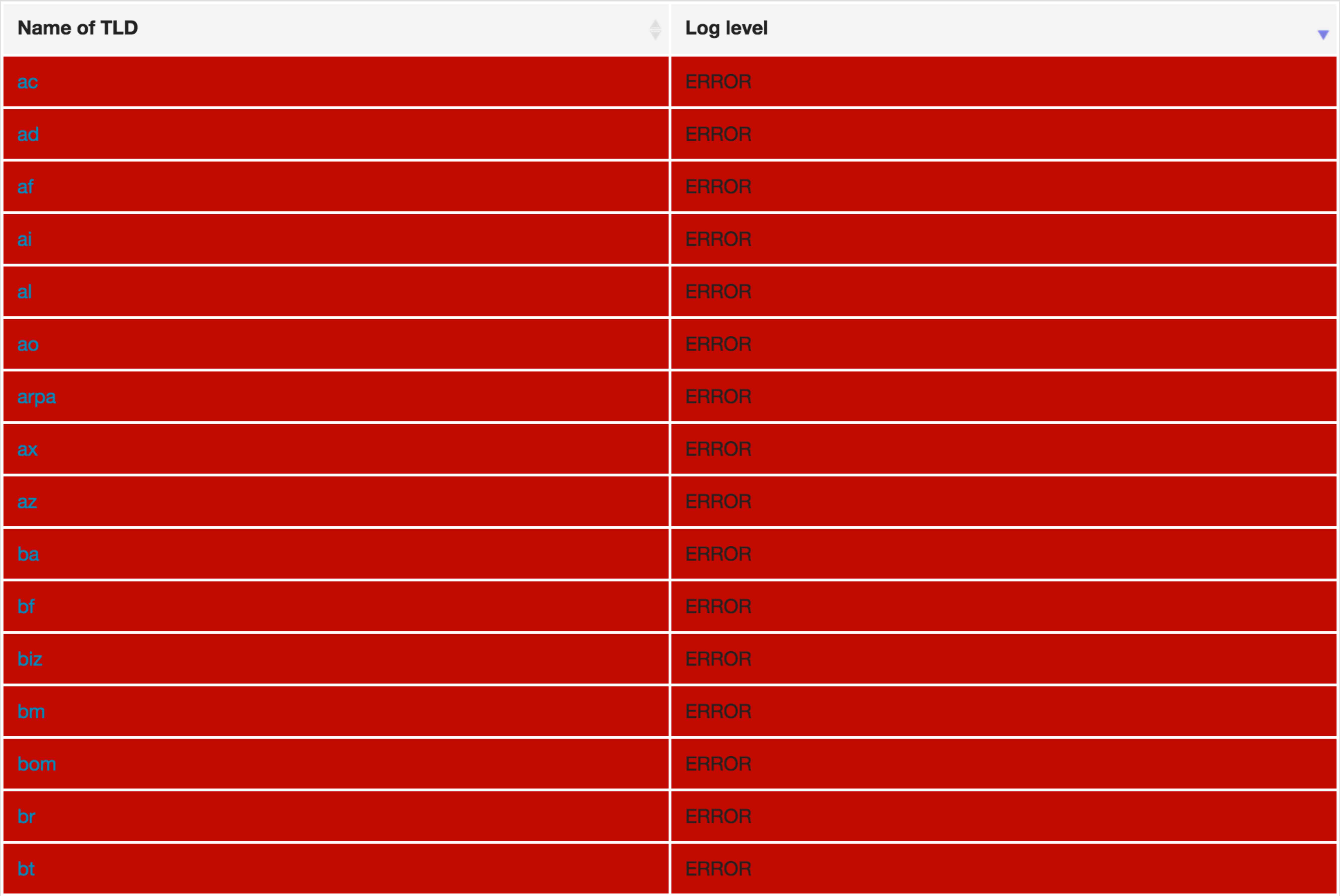
All TLDs

Show 20 entries

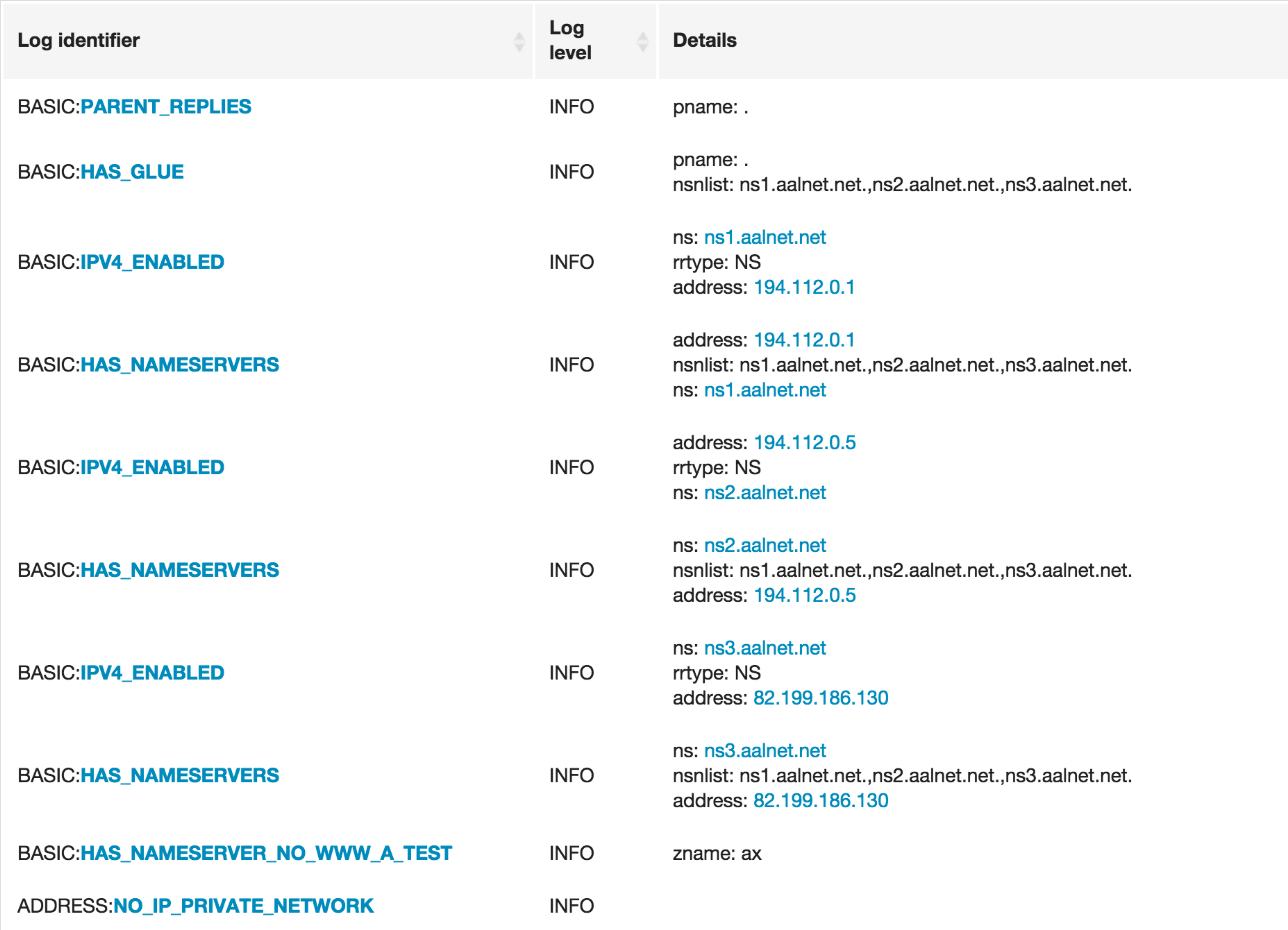
Search:

Name of TLD	Log level
aaa	NOTICE
abb	WARNING
abbott	WARNING
abogado	NOTICE
ac	ERROR
academy	NOTICE
accenture	WARNING
accountant	NOTICE
accountants	NOTICE
aco	WARNING
active	NOTICE

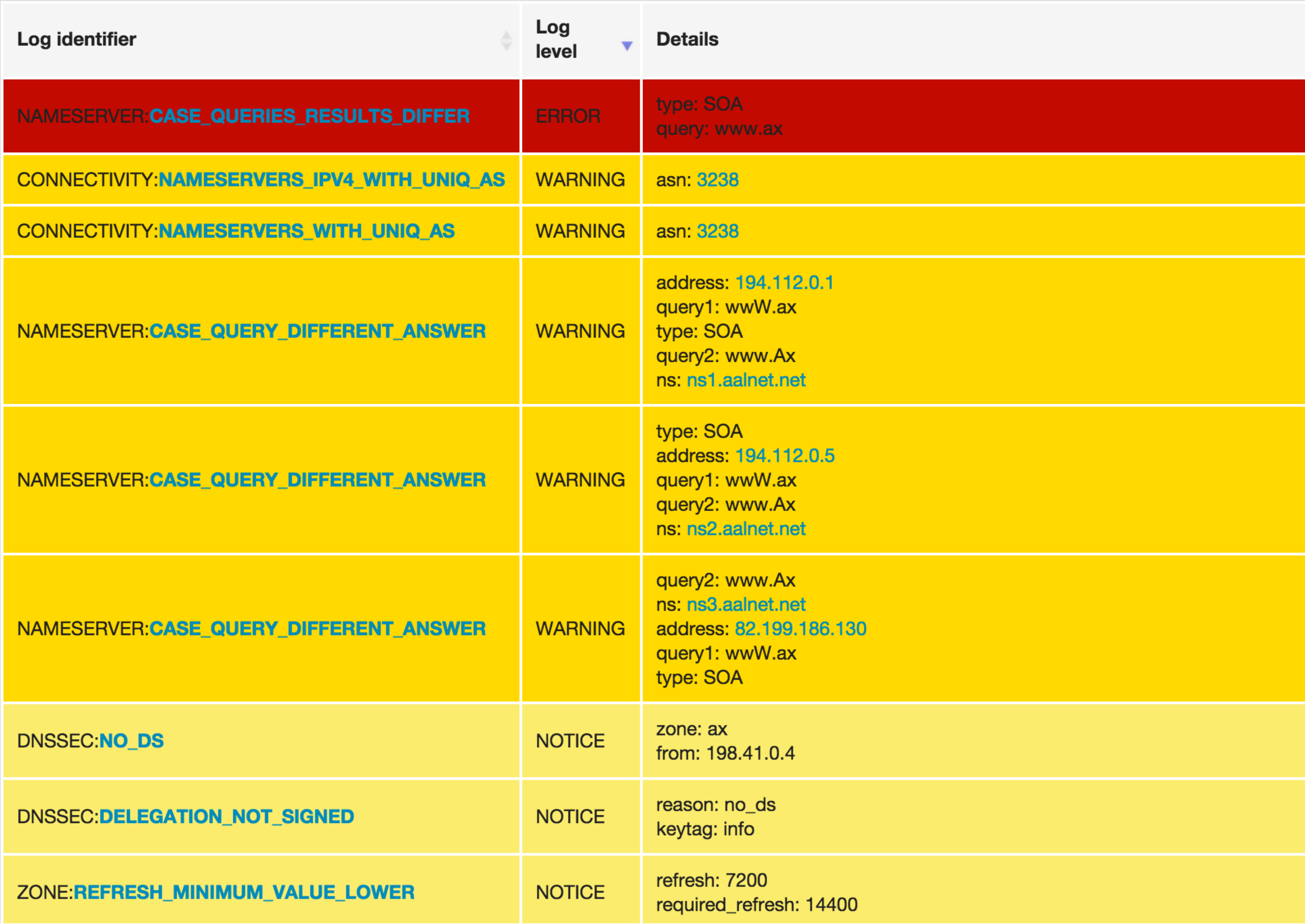
<DEMO>



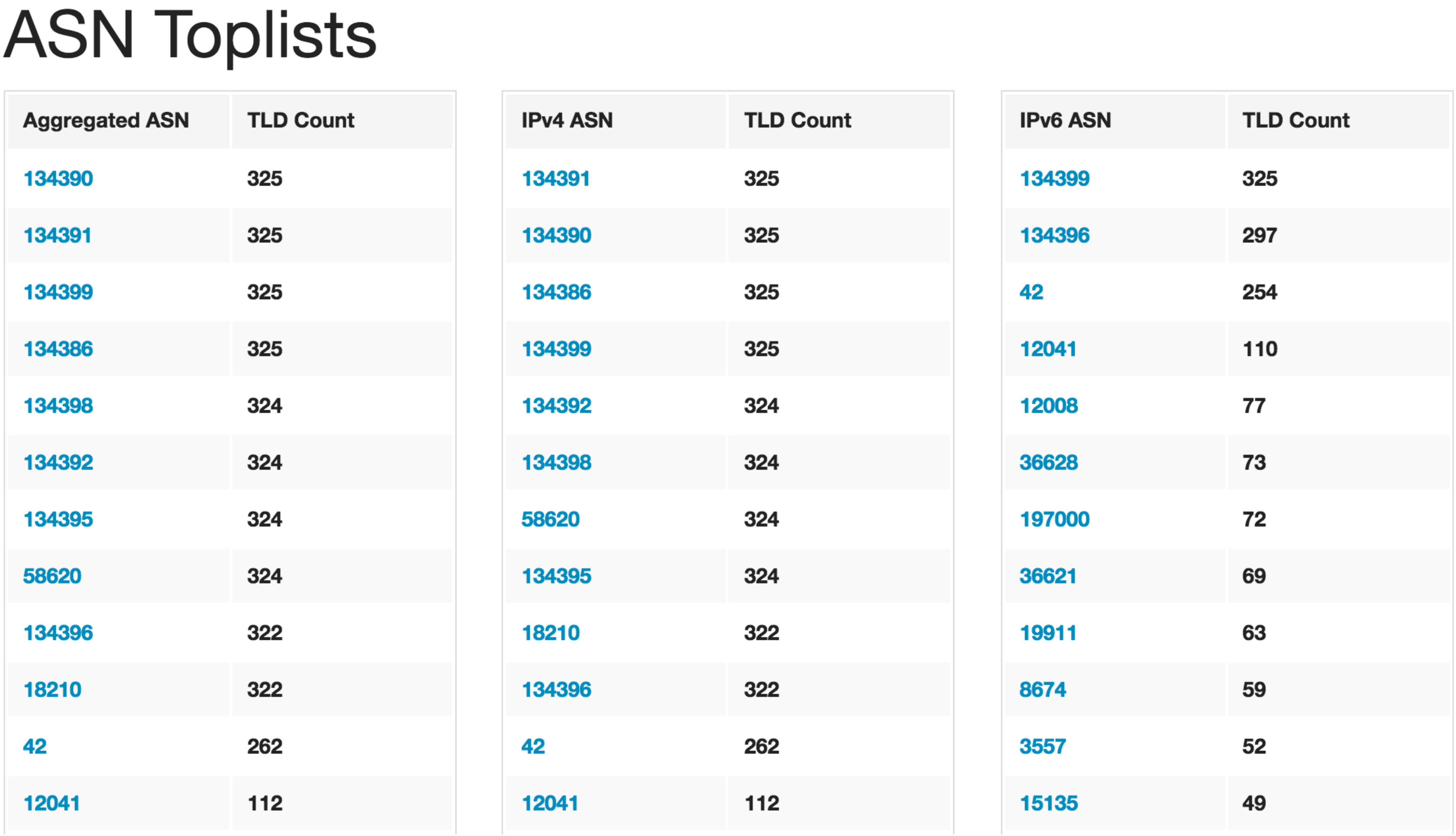
Name of TLD	Log level
ac	ERROR
ad	ERROR
af	ERROR
ai	ERROR
al	ERROR
ao	ERROR
arpa	ERROR
ax	ERROR
az	ERROR
ba	ERROR
bf	ERROR
biz	ERROR
bm	ERROR
bom	ERROR
br	ERROR
bt	ERROR



Log identifier	Log level	Details
BASIC:**PARENT_REPLIES**	INFO	pname: .
BASIC:**HAS_GLUE**	INFO	pname: . nsnlist: ns1.aalnet.net.,ns2.aalnet.net.,ns3.aalnet.net.
BASIC:**IPV4_ENABLED**	INFO	ns: ns1.aalnet.net rrtype: NS address: 194.112.0.1
BASIC:**HAS_NAMESERVERS**	INFO	address: 194.112.0.1 nsnlist: ns1.aalnet.net.,ns2.aalnet.net.,ns3.aalnet.net. ns: ns1.aalnet.net
BASIC:**IPV4_ENABLED**	INFO	address: 194.112.0.5 rrtype: NS ns: ns2.aalnet.net
BASIC:**HAS_NAMESERVERS**	INFO	ns: ns2.aalnet.net nsnlist: ns1.aalnet.net.,ns2.aalnet.net.,ns3.aalnet.net. address: 194.112.0.5
BASIC:**IPV4_ENABLED**	INFO	ns: ns3.aalnet.net rrtype: NS address: 82.199.186.130
BASIC:**HAS_NAMESERVERS**	INFO	ns: ns3.aalnet.net nsnlist: ns1.aalnet.net.,ns2.aalnet.net.,ns3.aalnet.net. address: 82.199.186.130
BASIC:**HAS_NAMESERVER_NO_WWW_A_TEST**	INFO	zname: ax
ADDRESS:**NO_IP_PRIVATE_NETWORK**	INFO	



Log identifier	Log level	Details
NAMESERVER:CASE_QUERIES_RESULTS_DIFFER	ERROR	type: SOA query: www.ax
CONNECTIVITY:NAMESERVERS_IPV4_WITH_UNIQ_AS	WARNING	asn: 3238
CONNECTIVITY:NAMESERVERS_WITH_UNIQ_AS	WARNING	asn: 3238
NAMESERVER:CASE_QUERY_DIFFERENT_ANSWER	WARNING	address: 194.112.0.1 query1: wwW.ax type: SOA query2: www.Ax ns: ns1.aalnet.net
NAMESERVER:CASE_QUERY_DIFFERENT_ANSWER	WARNING	type: SOA address: 194.112.0.5 query1: wwW.ax query2: www.Ax ns: ns2.aalnet.net
NAMESERVER:CASE_QUERY_DIFFERENT_ANSWER	WARNING	query2: www.Ax ns: ns3.aalnet.net address: 82.199.186.130 query1: wwW.ax type: SOA
DNSSEC:NO_DS	NOTICE	zone: ax from: 198.41.0.4
DNSSEC:DELEGATION_NOT_SIGNED	NOTICE	reason: no_ds keytag: info
ZONE:REFRESH_MINIMUM_VALUE_LOWER	NOTICE	refresh: 7200 required_refresh: 14400

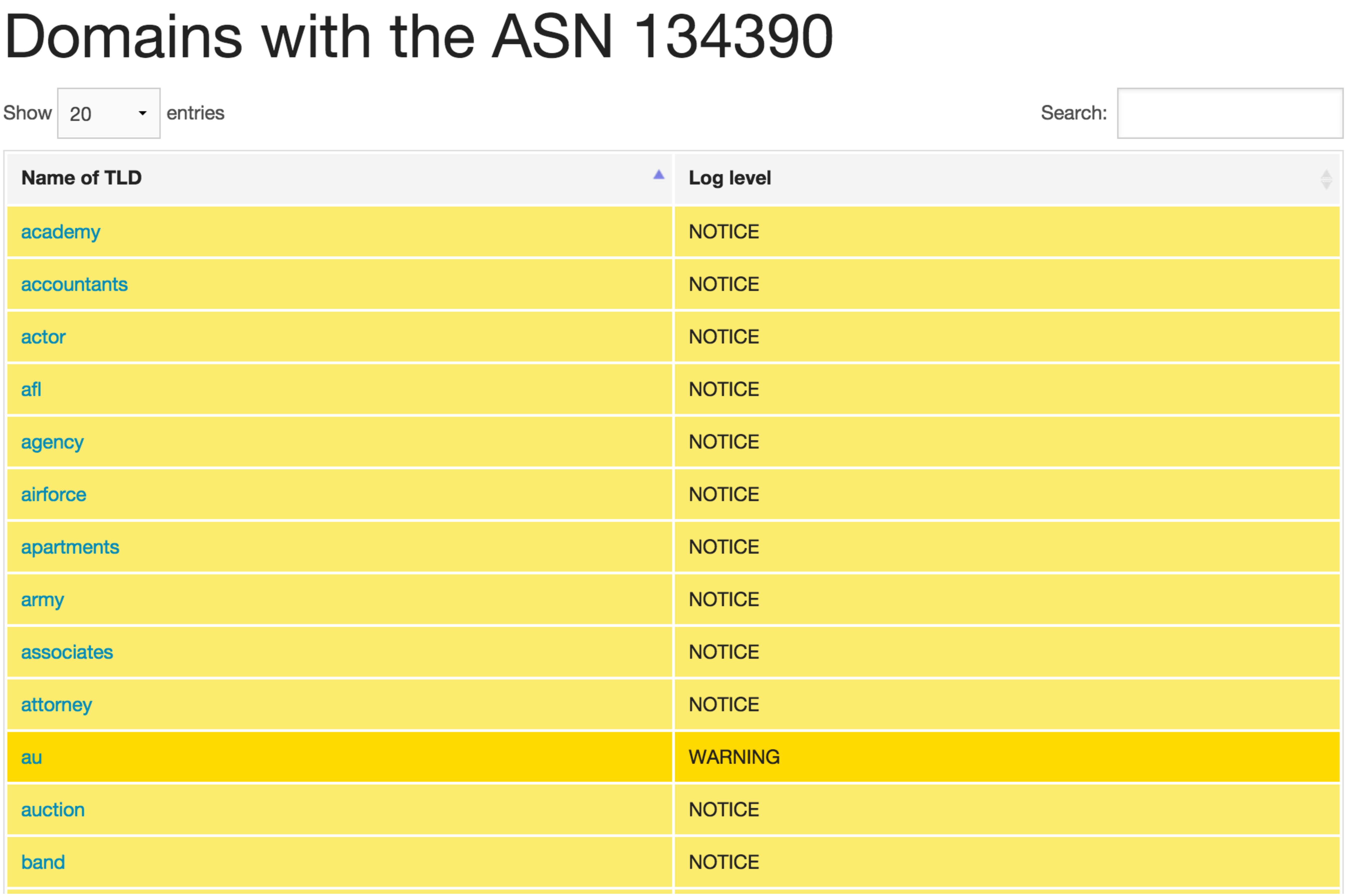


ASN Toplists

Aggregated ASN	TLD Count
134390	325
134391	325
134399	325
134386	325
134398	324
134392	324
134395	324
58620	324
134396	322
18210	322
42	262
12041	112

IPv4 ASN	TLD Count
134391	325
134390	325
134386	325
134399	325
134392	324
134398	324
58620	324
134395	324
18210	322
134396	322
42	262
12041	112

IPv6 ASN	TLD Count
134399	325
134396	297
42	254
12041	110
12008	77
36628	73
197000	72
36621	69
19911	63
8674	59
3557	52
15135	49



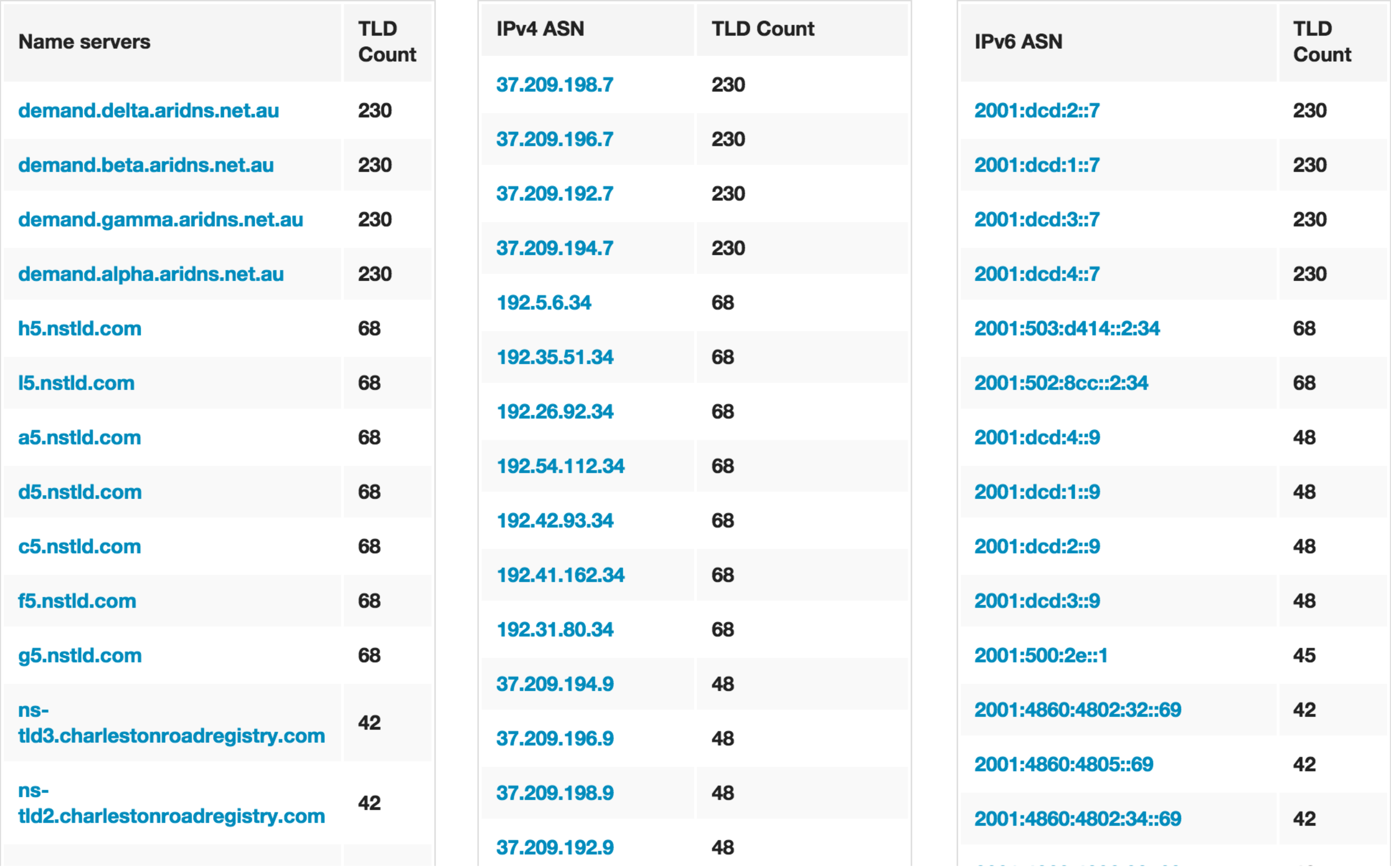
Domains with the ASN 134390

Show 20 entries

Search:

Name of TLD	Log level
academy	NOTICE
accountants	NOTICE
actor	NOTICE
afl	NOTICE
agency	NOTICE
airforce	NOTICE
apartments	NOTICE
army	NOTICE
associates	NOTICE
attorney	NOTICE
au	WARNING
auction	NOTICE
band	NOTICE

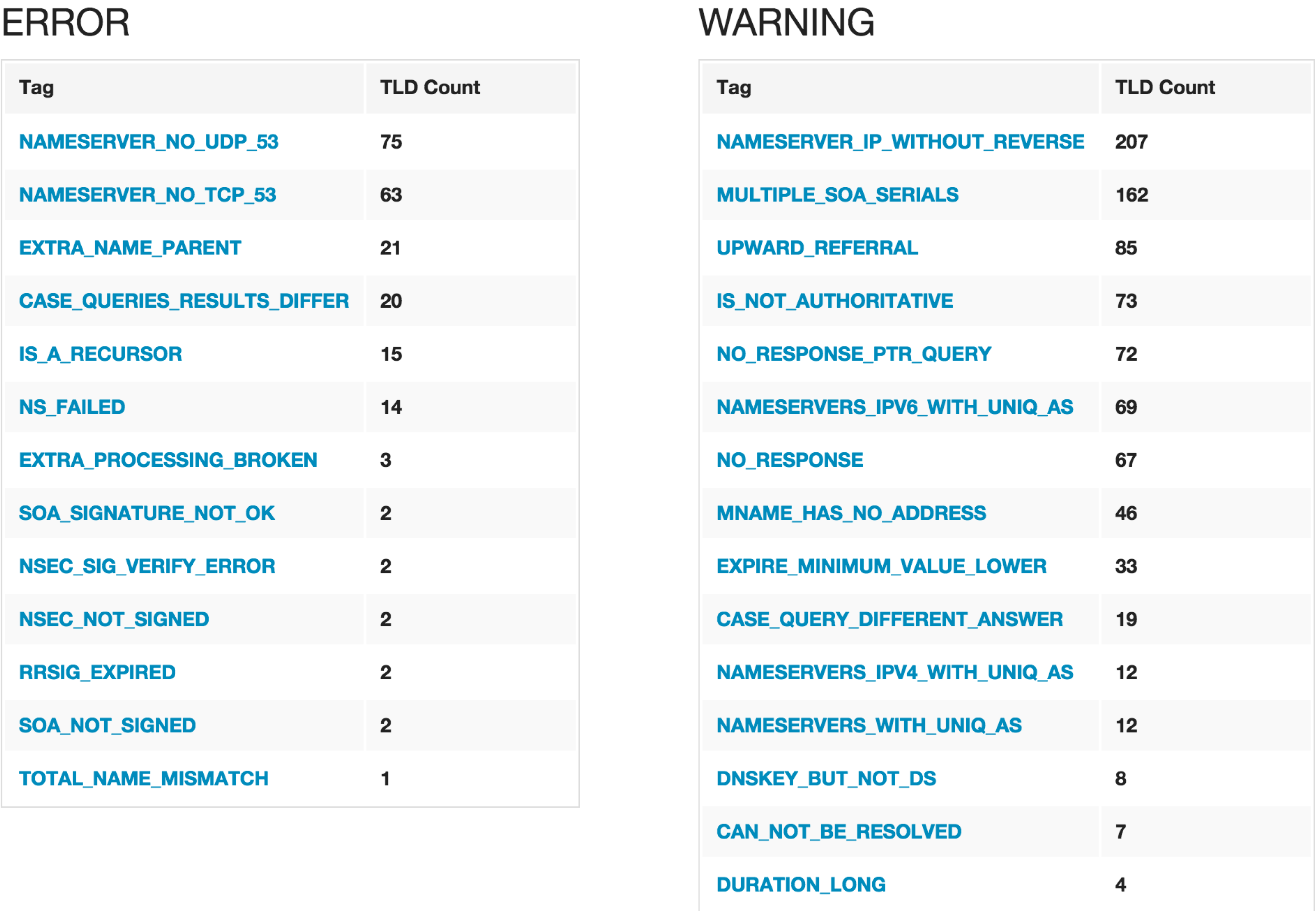
Name Server Toplist



Name servers	TLD Count
demand.delta.aridns.net.au	230
demand.beta.aridns.net.au	230
demand.gamma.aridns.net.au	230
demand.alpha.aridns.net.au	230
h5.nstld.com	68
l5.nstld.com	68
a5.nstld.com	68
d5.nstld.com	68
c5.nstld.com	68
f5.nstld.com	68
g5.nstld.com	68
ns-tld3.charlestonroadregistry.com	42
ns-tld2.charlestonroadregistry.com	42

IPv4 ASN	TLD Count
37.209.198.7	230
37.209.196.7	230
37.209.192.7	230
37.209.194.7	230
192.5.6.34	68
192.35.51.34	68
192.26.92.34	68
192.54.112.34	68
192.42.93.34	68
192.41.162.34	68
192.31.80.34	68
37.209.194.9	48
37.209.196.9	48
37.209.198.9	48
37.209.192.9	48

IPv6 ASN	TLD Count
2001:dcd:2::7	230
2001:dcd:1::7	230
2001:dcd:3::7	230
2001:dcd:4::7	230
2001:503:d414::2:34	68
2001:502:8cc::2:34	68
2001:dcd:4::9	48
2001:dcd:1::9	48
2001:dcd:2::9	48
2001:dcd:3::9	48
2001:500:2e::1	45
2001:4860:4802:32::69	42
2001:4860:4805::69	42
2001:4860:4802:34::69	42

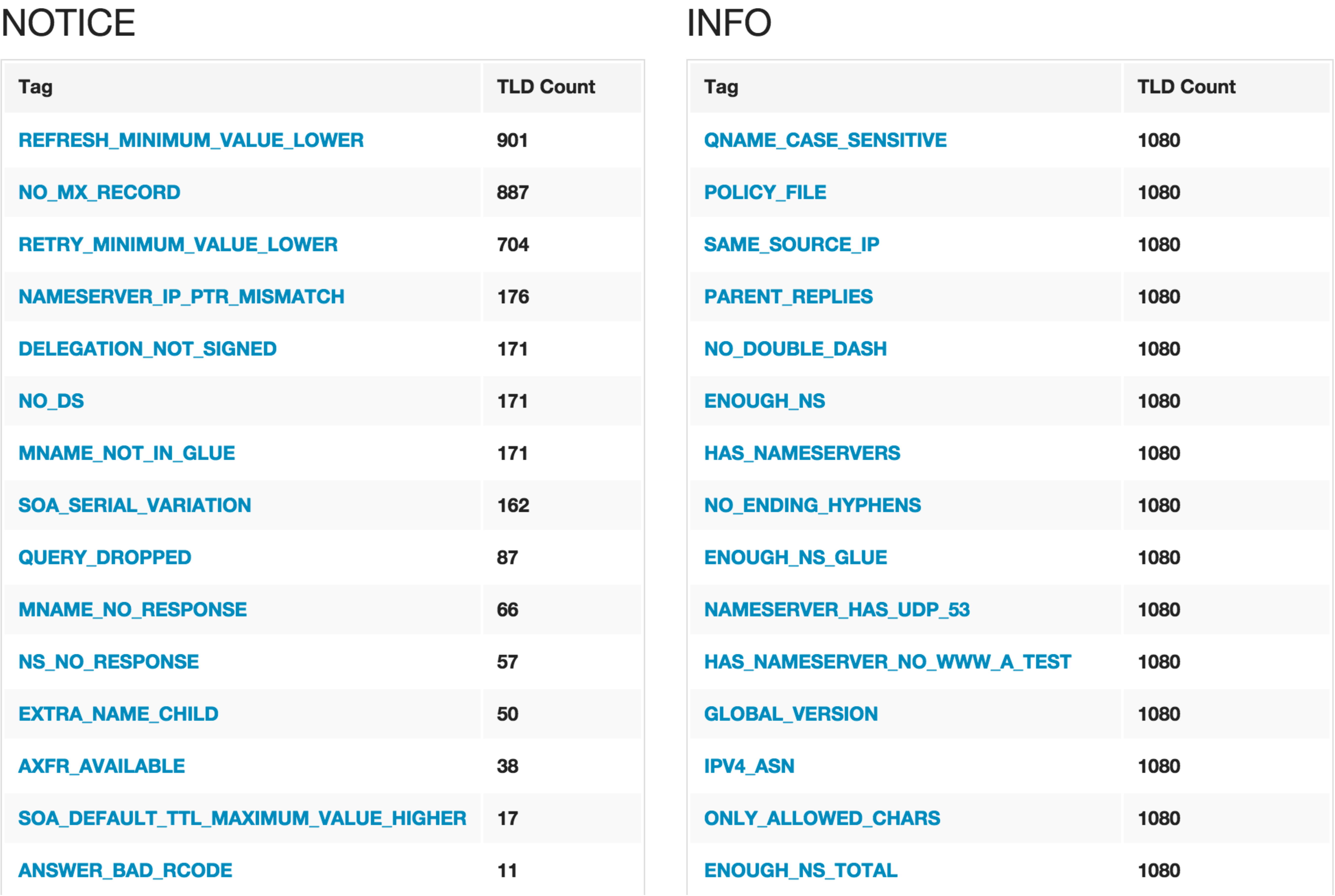


ERROR

Tag	TLD Count
NAMESERVER_NO_UDP_53	75
NAMESERVER_NO_TCP_53	63
EXTRA_NAME_PARENT	21
CASE_QUERIES_RESULTS_DIFFER	20
IS_A_RECURSOR	15
NS_FAILED	14
EXTRA_PROCESSING_BROKEN	3
SOA_SIGNATURE_NOT_OK	2
NSEC_SIG_VERIFY_ERROR	2
NSEC_NOT_SIGNED	2
RRSIG_EXPIRED	2
SOA_NOT_SIGNED	2
TOTAL_NAME_MISMATCH	1

WARNING

Tag	TLD Count
NAMESERVER_IP_WITHOUT_REVERSE	207
MULTIPLE_SOA_SERIALS	162
UPWARD_REFERRAL	85
IS_NOT_AUTHORITATIVE	73
NO_RESPONSE_PTR_QUERY	72
NAMESERVERS_IPV6_WITH_UNIQ_AS	69
NO_RESPONSE	67
MNAME_HAS_NO_ADDRESS	46
EXPIRE_MINIMUM_VALUE_LOWER	33
CASE_QUERY_DIFFERENT_ANSWER	19
NAMESERVERS_IPV4_WITH_UNIQ_AS	12
NAMESERVERS_WITH_UNIQ_AS	12
DNSKEY_BUT_NOT_DS	8
CAN_NOT_BE_RESOLVED	7
DURATION_LONG	4



NOTICE

Tag	TLD Count
REFRESH_MINIMUM_VALUE_LOWER	901
NO_MX_RECORD	887
RETRY_MINIMUM_VALUE_LOWER	704
NAMESERVER_IP_PTR_MISMATCH	176
DELEGATION_NOT_SIGNED	171
NO_DS	171
MNAME_NOT_IN_GLUE	171
SOA_SERIAL_VARIATION	162
QUERY_DROPPED	87
MNAME_NO_RESPONSE	66
NS_NO_RESPONSE	57
EXTRA_NAME_CHILD	50
AXFR_AVAILABLE	38
SOA_DEFAULT_TTL_MAXIMUM_VALUE_HIGHER	17
ANSWER_BAD_RCODE	11

INFO

Tag	TLD Count
QNAME_CASE_SENSITIVE	1080
POLICY_FILE	1080
SAME_SOURCE_IP	1080
PARENT_REPLIES	1080
NO_DOUBLE_DASH	1080
ENOUGH_NS	1080
HAS_NAMESERVERS	1080
NO_ENDING_HYPHENS	1080
ENOUGH_NS_GLUE	1080
NAMESERVER_HAS_UDP_53	1080
HAS_NAMESERVER_NO_WWW_A_TEST	1080
GLOBAL_VERSION	1080
IPV4_ASN	1080
ONLY_ALLOWED_CHARS	1080
ENOUGH_NS_TOTAL	1080

Test Specifications

- All tests in Zonemaster has a Test Specification coming from a Requirement
- Log Message maps to Test Specification: https://goo.gl/SviNiy

Mapping test messages to test module

Log message identifier	Implemented test case
BASIC:HAS_NAMESERVERS	Basic::basic02
BASIC:IPV4_DISABLED	Basic::basic02
BASIC:IPV4_ENABLED	Basic::basic02
BASIC:IPV6_DISABLED	Basic::basic02
BASIC:IPV6_ENABLED	Basic::basic02
BASIC:NO_GLUE_PREVENTS_NAMESERVER_TESTS	Basic::basic02
BASIC:NS_FAILED	Basic::basic02
BASIC:NS_NO_RESPONSE	Basic::basic02
BASIC:A_QUERY_NO_RESPONSES	Basic::basic03
BASIC:HAS_A_RECORDS	Basic::basic03
BASIC:IPV4_DISABLED	Basic::basic03
BASIC:IPV4_ENABLED	Basic::basic03
BASIC:IPV6_DISABLED	Basic::basic03
BASIC:IPV6_ENABLED	Basic::basic03

Test Profiles

- Zonemaster supports other test profiles
  - However, there are only one, the default
- Ongoing work on an IANA test profile (for TLDs)

Technical requirements for authoritative name servers

This article describes the baseline technical conformance criteria for authoritative name servers. These are evaluated by ICANN as the IANA functions operator for changes to delegations in IANA-managed zones such as the DNS root zone and .INT zone.

Definitions

For purposes of this document, an authoritative name server is a DNS server that has been designated to answer authoritatively for the designated zone, and is being requested to be listed in the delegation. It is recorded by its fully-qualified domain name, potentially along with its IP addresses.

Name server tests are completed against each unique tuple of a hostname, an IP address, and a protocol. If a hostname has multiple IP addresses, for example, the tests will be conducted against each IP address.

Detailed requirements

Minimum number of name servers

There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.

Valid hostnames

The hostnames used for the name servers must comply with the requirements for valid hostnames described in RFC 1123, section 2.1.

Name server reachability

The name servers must answer DNS queries over both the UDP and TCP protocols on port 53. Tests will be conducted from multiple network locations to verify the name server is responding.

TRTF

- A CENTR “Test Requirements Task Force” to write requirements on a DNS delegation based on the Zonemaster Test Specifications
- Current status: writing an I-D aimed at DNSOP wg

Thank you!

https://github.com/dotse/zonemaster

http://tldmonitor.blipp.com/

https://github.com/pawal/zonemaster-collector

ccNSO Tech Day
ICANN-54 Dublin