DNSCheck and DNS2db

Patrik Wallström, .SE
pawal@iis.se

Some background

As a registry we care about the quality of the delegations in our zone.

We also care about our name servers.

1999 - 2003

In the early days we tested all delegations before inserting the delegation into the .SE zone.

The registration procedure was a manual process.

2003

In 2003 we went from a manual process with limited registrations to a fully automatic system. But doing simpler pre-delegation checks.

We also had a web page where you could pre-test a delegation.

.se

First dnscheck

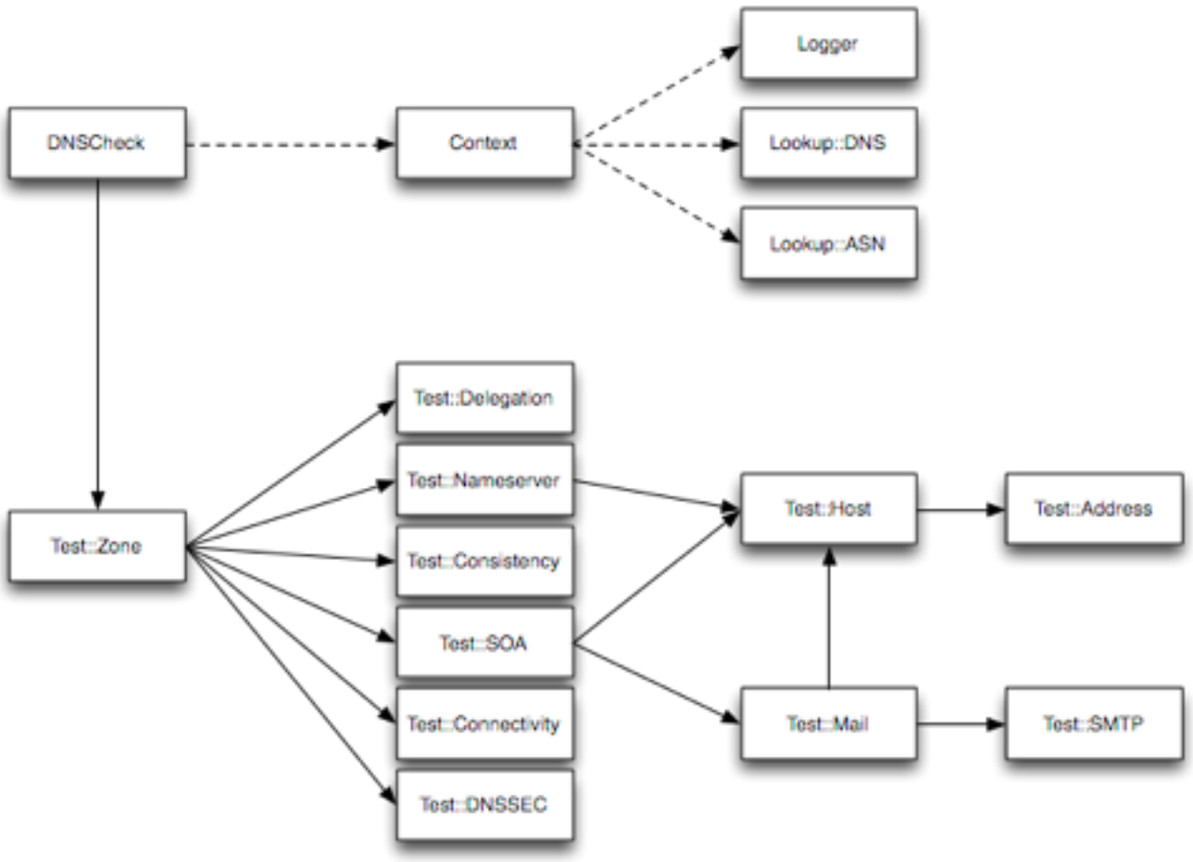
Also in 2003, we did post-checks using Patrik Fältström's dnscheck code.

It still lives on http://dnscheck.se/

We also published statistics from these checks on the web, categorized by name server operator.

.se

Third generation



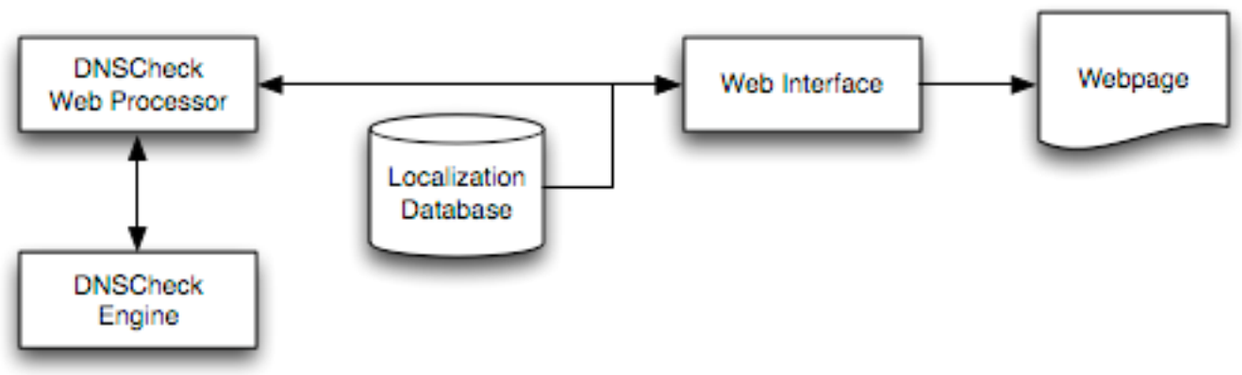
In 2005 .SE signed the zone with DNSSEC. We asked Jakob Schlyter to write a new modular code base for DNSCheck.

DNSCheck has support for DNSSEC and IPv6.

DNSCheck

The new DNSCheck has a web interface for "ordinary" users. With a basic and advanced view mode.

It also features the "Undelegated domain test".



.se

DNS Check

.se

- Home
- FAQ

Domain test | Undelegated domain test

Test your DNS-server and find errors

Domain name: iis.se

Enter your domain name in the field above to test the DNS-servers that are used. E.g. "iis.se"

Test now

Warnings found in test
iis.se, 2010-01-31 13:29:32
Test was performed with DNSCheck v1.0

Basic results | Advanced results

Delegation

- Too few IPv6 name servers (1).

Nameserver

- Nameserver ns.nic.se
- Nameserver ns2.nic.se
- Nameserver ns3.nic.se

Consistency

SOA

Connectivity

DNSSEC

Test history

- 2010-01-29 11:27:51
- 2010-01-29 10:16:46
- 2010-01-28 18:01:34
- 2010-01-28 13:42:32
- 2010-01-28 00:13:48
- 2010-01-27 21:22:29
- 2010-01-27 18:21:12
- 2010-01-26 21:27:16
- 2010-01-26 15:39:21
- 2010-01-25 12:20:42

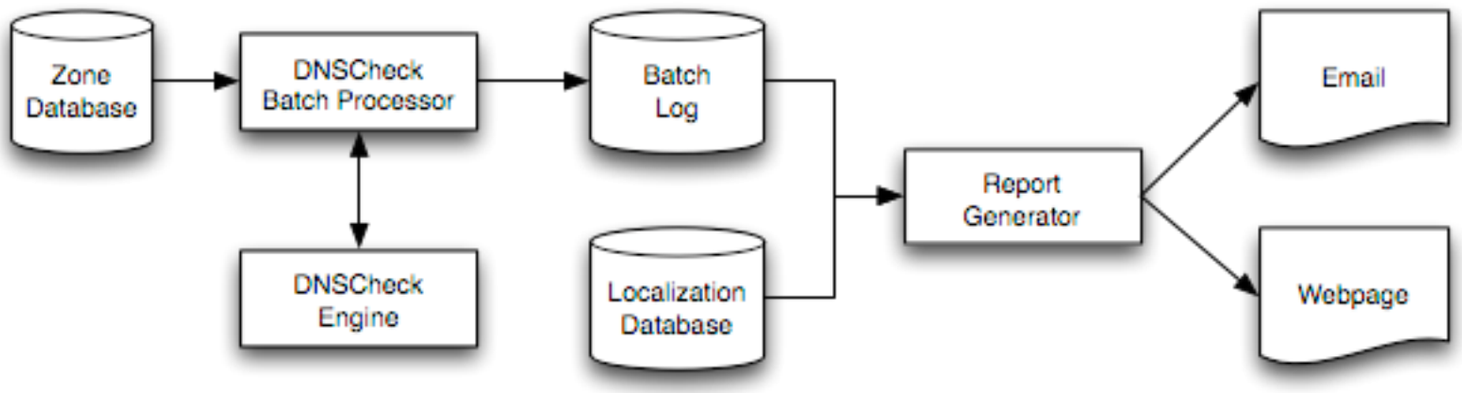
Page 1/65

Explanation

Test was ok

Batch mode

The new DNSCheck also features a back-end checker, which can be used for batch testing.



Examples of tests

Tests for valid (and resonable) IP addresses.

The following tests are made:

- Addresses must be syntactically correct.
- Private IPv4 Addresses (RFC 1918) must not be used.
- Special-Use IPv4 Addresses (RFC 5735) must not be used.
- Special-Use IPv6 Addresses must not be used.
- There should exist a PTR record for the address.
- The hostname(s) pointed to by the PTR record(s) should exist.

This test is implemented by DNSCheck::Test::Address.

.se

Examples of tests

Test a single name server for a specific zone.

The following tests are made:

- The nameserver must be a valid hostname.
- The nameserver should not be recursive.
- The nameserver must be authoritative for the zone.
- The SOA record for the zone must be fetchable over both UDP and TCP.
- The nameserver may provide AXFR for the zone.

This test is implemented by DNSCheck::Test::Nameserver.

.se

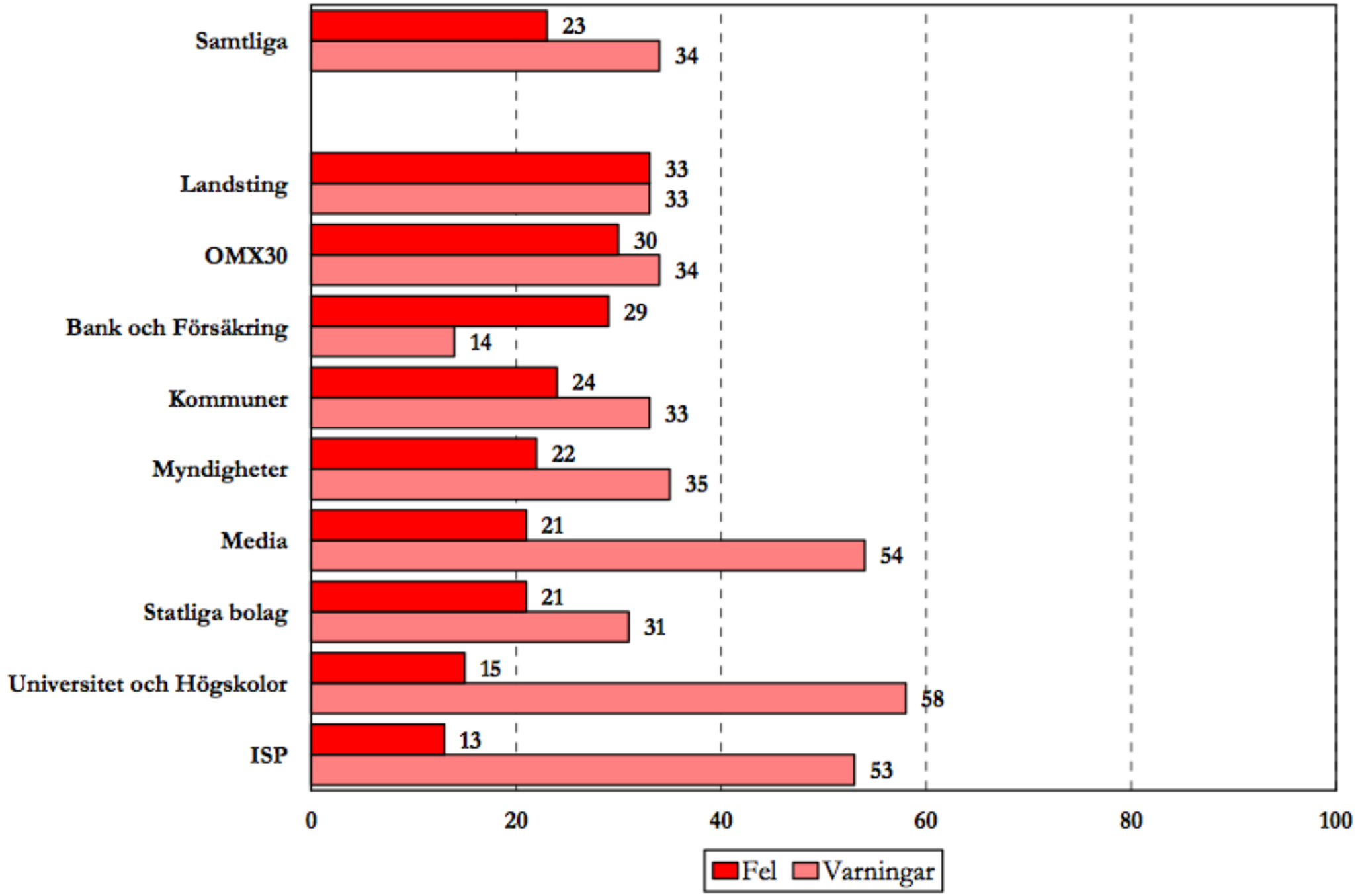
The Healthcheck Report

A yearly report on the health of the Swedish Internet. Primarily focused on DNS.

Published since 2007.

.se

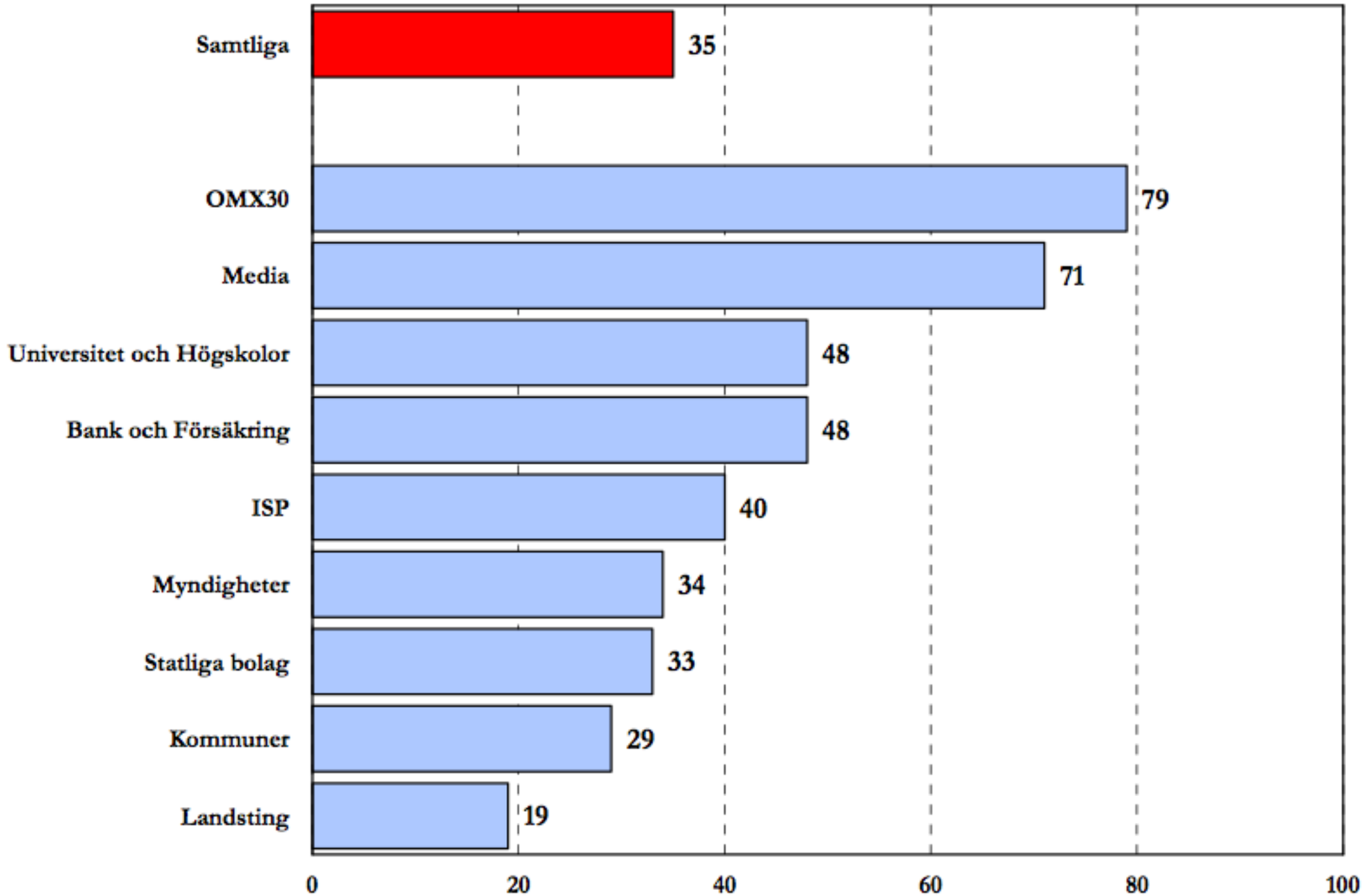
The Healthcheck Report



The numbers or errors and warning from DNSCheck

.se

The Healthcheck Report



Domains with name servers on more than one AS

.se

The Healthcheck Report

The report 2009 was based on a fully automatic analysis made by our new Healthcheck Platform.

Based on DNSCheck.

It is a web based report system.

.se

The Healthcheck Platform

Integrates a lot of current and future components:

DNSCheck

MailCheck

Page Analyzer (from LoadImpact.com)

.se

	Hälsoläget (Myndigheter) 091008 11:14	Hälsoläget (ISP) 091008 11:13	Information
Domains using IPv6	18.18% (42)	26.67% (4)	A domain is counted as using IPv6 if it has at least one server for DNS, SMTP or HTTP that has an IPv6 address announced.
Domains announced in more than one AS (IPv4)	33.77% (78)	40.00% (6)	A domain is counted here if its DNSCheck report includes the message `CONNECTIVITY:ASN_COUNT_OK`. Unless DNSCheck's default settings have been changed, this means that the domain has DNS servers reachable in more than one AS.
Domains announced in more than one AS (IPv6)	0.00% (0)	0.00% (0)	A domain is counted here if its DNSCheck report includes the message `CONNECTIVITY:V6_ASN_COUNT_OK`.
Domains using DNSSEC	1.73% (4)	0.00% (0)	A domain is counted here if its DNSCheck report includes the message `DNSSEC:DS_FOUND`. This only means that the domain has DNSSEC keys in its parent zone, not necessarily that it has DNSSEC correctly set up.
Domains with open recursive nameserver(s)	15.15% (35)	6.67% (1)	A domain is counted here if DNSCheck found that at least one of the nameservers for the domain allows recursive queries.
Domains using ADSP	0.00% (0)	0.00% (0)	A domain is counted here if it has an `_adsp._domainkeys.` record.
Domains using SPF	26.41% (61)	20.00% (3)	A domain is counted here if it has either an `SPF` record or a TXT record for the domain name.
Domains using STARTTLS	39.83% (92)	33.33% (5)	A domain is counted here if at least one of the servers pointed out by its `MX` records announces the `STARTTLS` capability in response to the `SMTP EHLO` command.
Percentage of mail servers located in Sweden (IPv4)	76.42%	76.00%	The fraction of IPv4 SMTP servers found that are located in Sweden (according to GeoIP).
Percentage of mail servers located in Sweden (IPv6)	0.00%	0.00%	The fraction of IPv6 SMTP servers found that are located in Sweden. At the moment, this number i almost certainly wildly wrong, since the GeoIP IPv6 data is much less reliable than their IPv4 data.
Number of tested domains	231	15	
Number of distinct nameservers (IPv4)	335	37	By "distinct nameserver" here and on the following row is meant different IP addresses. This may be strictly incorrect both by one server answering on more than one address (giving an artificially high count) and by one address being served by a cluster of servers (giving an artificially low count). Hopefully these two error sources mostly cancel each other out.
Number of distinct nameservers (IPv6)	21	3	

.se

ASNs hosting most domains (ipv4)

This table (and the next) presents the number of domains that have at least one nameserver announced in the given AS. Given big ISPs with servers providing information for many domains, the actual number of nameservers in a particular AS is likely to be lower than the number of domains with nameservers there.

ASN	HÄLSOLÄGET (MYNDIGHETER) 091008 11:14	HÄLSOLÄGET (ISP) 091008 11:13
AS1653 (SUNET)	147	4
AS3301 (TELIANET-SWEDEN)	88	3
AS3292 (TDC)	79	2
AS1257 (SWIPNET)	49	2
AS8434 (TELENOR-SE)	33	3
AS12552 (IPO-EU)	14	3
AS2119 (TELENOR-NEXTEL)	12	5
AS20773 (HOSTEUROPE-AS)	12	
AS29217 (WM-DATA)	10	
AS43018 (VINNOVA-ASN)	8	
AS21195 (DGCSYSTEMS)	7	2
AS2874 (ORANGE-BUSINESS-SERVICES-NORDICS)	7	
AS2846 (UNSPECIFIED)	7	
AS21503 (ARETE-AS)	6	2
AS2841 (CHALMERS)	6	
AS41175 (INTERNETBORDER)	6	
AS34385 (TRIPNET)	5	
AS2833 (SUNET-UMU)	5	
AS8220 (COLT)	5	
AS21844 (No name)	4	
CSV FILE		

.se

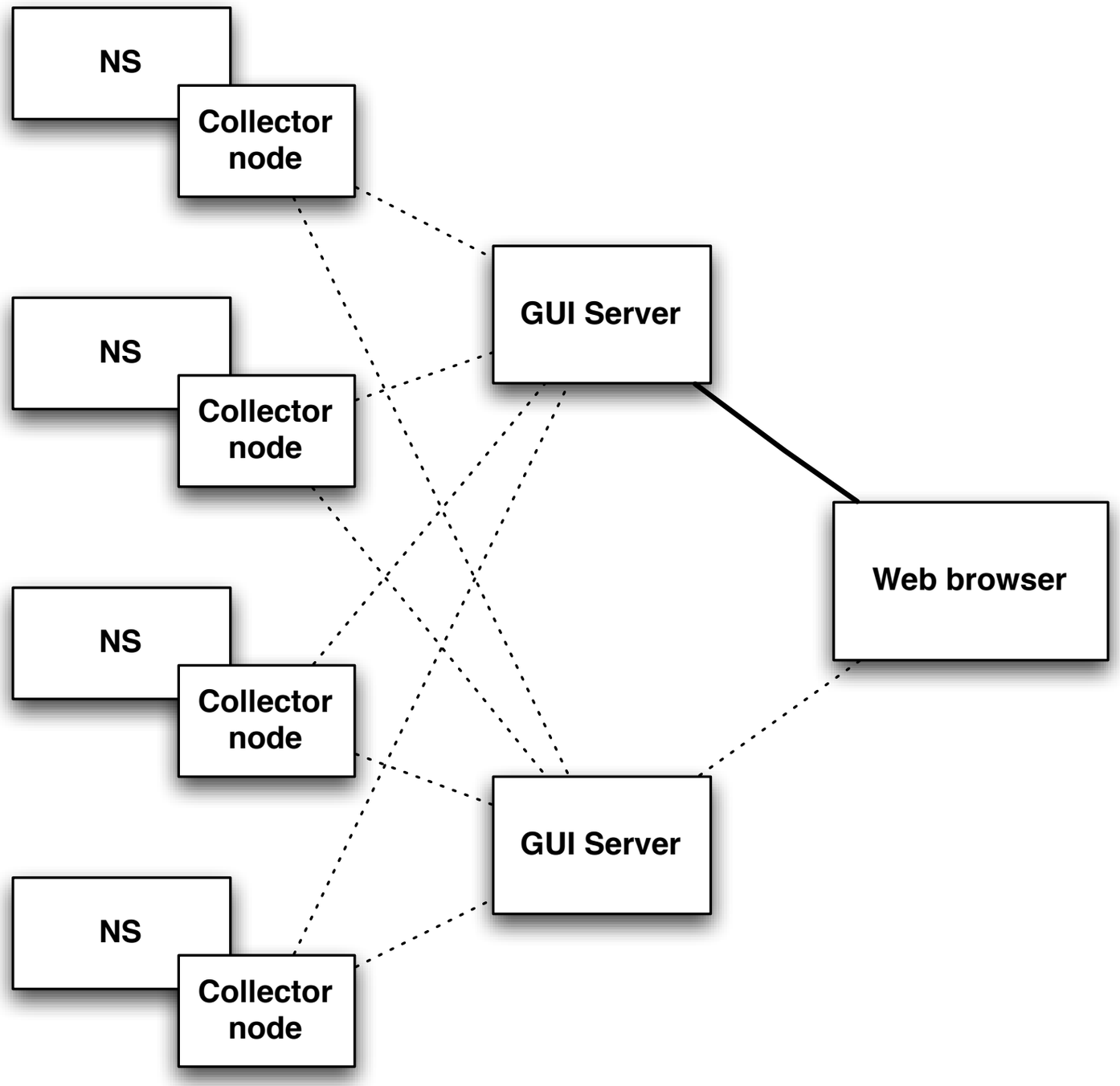
DNS2db

DNS2db is a tool for analyzing DNS data. It converts raw pcap-files with DNS-traffic to SQLite-databases, which then can be used to dig into and analyze the traffic.

The distribution also includes a simple interactive GUI for analyzing the collected data.

.se

DNS2db architecture



DNS2db

+ Stores more data much faster than DSC.

+ All data is kept at the node.

+ A minimal amount of data is exchanged between the collector node and the GUI server.

- Not DSC compatible.

.se

Trafficanalysis

Filters

☑ tcp ☑ udp ☑ v4 ☑ v6 qtype ALL

Nodes

☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]

Top domains for 2010-01-21 12:50

2010-01-21 | 12 | 50 | | 20

Pos	Load (q/	Domain
1	3878	ns.se
2	1270	se
3	1211	domainnetwork.se
4	1071	sunet.se
5	922	ballou.se
6	856	netnod.se
7	768	uu.se
8	612	prq.se
9	589	loopia.se
10	495	kth.se
11	492	telenor.se
12	489	alltele.se

Top servers for 2010-01-21 12:50

2010-01-21 | 12 | 50 | | 20

Pos	Load (q/m)	Server
1	1030	[redacted].se
2	539	[redacted].se
3	482	[redacted]
4	268	[redacted]
5	260	::209.[redacted]
6	236	::74.12[redacted]
7	230	pc041[redacted]
8	221	::74.12[redacted]
9	220	::216.2[redacted]
10	218	::209.8[redacted]
11	214	::74.12[redacted]
12	213	port06[redacted]

Top rr types for 2010-01-21 12:50

2010-01-21 | 12 | 50

Pos	Q Count	%	RR Type
1	268657	53.7	A
2	135607	27.1	MX
3	57972	11.6	AAAA
4	17349	3.5	DS
5	6035	1.2	DNSKEY
6	4266	0.9	NS
7	3737	0.7	A6
8	2775	0.6	TXT
9	1551	0.3	*
10	883	0.2	SOA
11	355	0.1	PTR
12	343	0.1	SRV

Top repeating resolvers for 2010-01-21 12:50

2010-01-21 | 12 | 50 | 20

Pos	Count	Resolver (query & type)
1	2599	[redacted].se (. DNSKEY)
2	2241	::[redacted] (. DNSKEY)
3	1152	[redacted]t (sas.sas.se. A)
4	647	[redacted]e (s-kvinnor.a.se.
5	483	[redacted] (. DNSKEY)
6	297	[redacted]n (panel.r
7	260	[redacted]e (. DNSKEY)
8	144	[redacted]n (mailgate01.bdnc.se. A)
9	120	[redacted]n (mailgate01.bdnc.se. A)
10	89	[redacted]n (ns1.
11	88	[redacted] (ns2.
12	86	[redacted] (. DNSKEY)

DNS2DB Traffic analysis GUI prototype. (c) Rickard Dahlstrand, IIS 2009.

Instructions:
- The first windows displays the top 20 domains and servers. The serverlist takes a bit longer to load because it resolves each
- Double-click on a domain to open a window with all servers that are asking for that domain. Double-click on a server to open
- If you click on a query you will get the servers asking for that domain. A single-click on a row copies the content to the clipbo
- When a row is selected in a window you can use the left and right arrows to change the time five minutes. Holding down SHIFT
- You can search for a domain/server by typing in a text in the textbox. You can also change the number of lines that are displa
- You can close a windows by clicking on the cross in the top right corner. Double-click on the title bar to hide it temporarily or

.se

Open source

All code is BSD licensed.

Available at http://opensource.iis.se/

Thank you!

.se