Zonecheck, testing a DNS zone

Stéphane Bortzmeyer
AFNIC ("`.fr`" registry)
`bortzmeyer@nic.fr`

16 november 2006

Why testing a DNS zone?

Why testing a DNS zone?

- To be sure it works,

Why testing a DNS zone?

- To be sure it works,
- To be sure it works fast (no timeouts or retransmissions).

Why testing a DNS zone?

- To be sure it works,
- To be sure it works fast (no timeouts or retransmissions).

It is not because "it works" that everything is perfect.

See Ilya Sukhar's slides about the consequences of bad delegation.

The requirments

When we started designing the new Zonecheck in 2002 (version 2, a program by the same name, but completely different, existed before):

The requirments for the new version:

The requirments

When we started designing the new Zonecheck in 2002 (version 2, a program by the same name, but completely different, existed before):

The requirments for the new version:

- Command-line (so it can be run everywhere) and Web tool,

The requirments

When we started designing the new Zonecheck in 2002 (version 2, a program by the same name, but completely different, existed before):

The requirments for the new version:

- Command-line (so it can be run everywhere) and Web tool,
- Free software,

The requirments

When we started designing the new Zonecheck in 2002 (version 2, a program by the same name, but completely different, existed before):

The requirments for the new version:

- Command-line (so it can be run everywhere) and Web tool,
- Free software,
- Quite general tool, not a small ad hoc hack,

The requirments

When we started designing the new Zonecheck in 2002 (version 2, a program by the same name, but completely different, existed before):

The requirments for the new version:

- Command-line (so it can be run everywhere) and Web tool,
- Free software,
- Quite general tool, not a small ad hoc hack,
- Separated policy and engine (more on that later).

The result

The result

- Made by Stéphane d'Alu,

The result

- Made by Stéphane d'Alu,
- Written in Ruby,

The result

- Made by Stéphane d'Alu,
- Written in Ruby,
- Available under the GPL free licence, a very important point, since it allows people to run it at their site and to do the same tests as AFNIC does (administrators of zones under ".fr" are encouraged to run ZC before submitting their request for creation/modification),

The result

- Made by Stéphane d'Alu,
- Written in Ruby,
- Available under the GPL free licence, a very important point, since it allows people to run it at their site and to do the same tests as AFNIC does (administrators of zones under ".fr" are encouraged to run ZC before submitting their request for creation/modification),
- Hosted at the hosting service Savannah,

The result

- Made by Stéphane d'Alu,
- Written in Ruby,
- Available under the GPL free licence, a very important point, since it allows people to run it at their site and to do the same tests as AFNIC does (administrators of zones under ".fr" are encouraged to run ZC before submitting their request for creation/modification),
- Hosted at the hosting service Savannah,
- Completely IPv4 and IPv6,

The result

- Made by Stéphane d'Alu,
- Written in Ruby,
- Available under the GPL free licence, a very important point, since it allows people to run it at their site and to do the same tests as AFNIC does (administrators of zones under ".fr" are encouraged to run ZC before submitting their request for creation/modification),
- Hosted at the hosting service Savannah,
- Completely IPv4 and IPv6,
- Used in daily production at AFNIC since.

Engine, not policy

Zonecheck is an engine, not a policy

This is probably the main feature of Zonecheck: unlike all the other similar tools, the policy is not hardwired in the code.

Engine, not policy

Zonecheck is an engine, not a policy

This is probably the main feature of Zonecheck: unlike all the other similar tools, the policy is not hardwired in the code.

The code defines all the tests you **can** run, the configuration file defines the subset of the tests that you **do** run and their result (fatal error or just a warning).

Example of configuration

```
<check name="icmp" severity="w" category="connectivity:l3"/>
<check name="udp"  severity="f" category="connectivity:l4"/>
<check name="tcp"  severity="f" category="connectivity:l4"/>
```

Example of configuration

```
<check name="icmp" severity="w" category="connectivity:l3"/>
<check name="udp"  severity="f" category="connectivity:l4"/>
<check name="tcp"  severity="f" category="connectivity:l4"/>
```

A program can translate this configuration file to HTML, for information of the users.

Using it to check delegations from a registry

AFNIC uses Zonecheck **prior** to every delegation. One fatal error and the domain is not created. (Every name server change triggers a Zonecheck, too.)

Using it to check delegations from a registry

AFNIC uses Zonecheck **prior** to every delegation. One fatal error and the domain is not created. (Every name server change triggers a Zonecheck, too.)

The policy is quite strict. A few examples:

- TCP connectivity is mandatory,
- If the server is recursive, a lot of tests occur (such as whether the loopback address is delegated in in-addr.arpa).

Using it to check delegations from a registry

AFNIC uses Zonecheck **prior** to every delegation. One fatal error and the domain is not created. (Every name server change triggers a Zonecheck, too.)

The policy is quite strict. A few examples:

- TCP connectivity is mandatory,
- If the server is recursive, a lot of tests occur (such as whether the loopback address is delegated in in-addr.arpa).

As a side effect, this creates a large number of support tickets (that may be used to measure the current skills level of some registrars :-) and (without smiley) the current level of professionalism of many DNS administrators

Using it to check delegations from a registry

AFNIC uses Zonecheck **prior** to every delegation. One fatal error and the domain is not created. (Every name server change triggers a Zonecheck, too.)

As a side effect, this creates a large number of support tickets (that may be used to measure the current skills level of some registrars :-) and (without smiley) the current level of professionalism of many DNS administrators

But it makes a much better zone and strongly diminishes the post-registration complaints “My site does not work”.

Lessons for IANA checks

Context: IANA asks for comments about delegation checks (`http://www.icann.org/announcements/announcement-18aug06.htm`).

[Generally speaking, the quality of DNS delegation is a very common issue today.]

Lessons for IANA checks

Context: IANA asks for comments about delegation checks (`http://www.icann.org/announcements/announcement-18aug06.htm`).

[Generally speaking, the quality of DNS delegation is a very common issue today.]

Many registries (CENTR, ccNSO) asked that such tests must be clearly described, and executed in a predictable way. An automatic tool, such as Zonecheck, allows to fulfill these requirments.

Lessons for IANA checks

Context: IANA asks for comments about delegation checks (`http://www.icann.org/announcements/announcement-18aug06.htm`).

[Generally speaking, the quality of DNS delegation is a very common issue today.]

Many registries (CENTR, ccNSO) asked that such tests must be clearly described, and executed in a predictable way. An automatic tool, such as Zonecheck, allows to fulfill these requirments.

Remember that using Zonecheck does not mean using AFNIC policy.

Future tests?

- DNSsec tests (see Eric Osterweil's slides)
- "OR" tests: "at least M among N nameservers", "TCP or EDNS0", ...

Other users

- .de
- .ch
- .no

Other users

- .de
- .ch
- .no

Tomorrow, you?

http://www.zonecheck.fr/