

# ***Zonemaster Updates***

*Sandoche Balakrichenan (Afnic)*



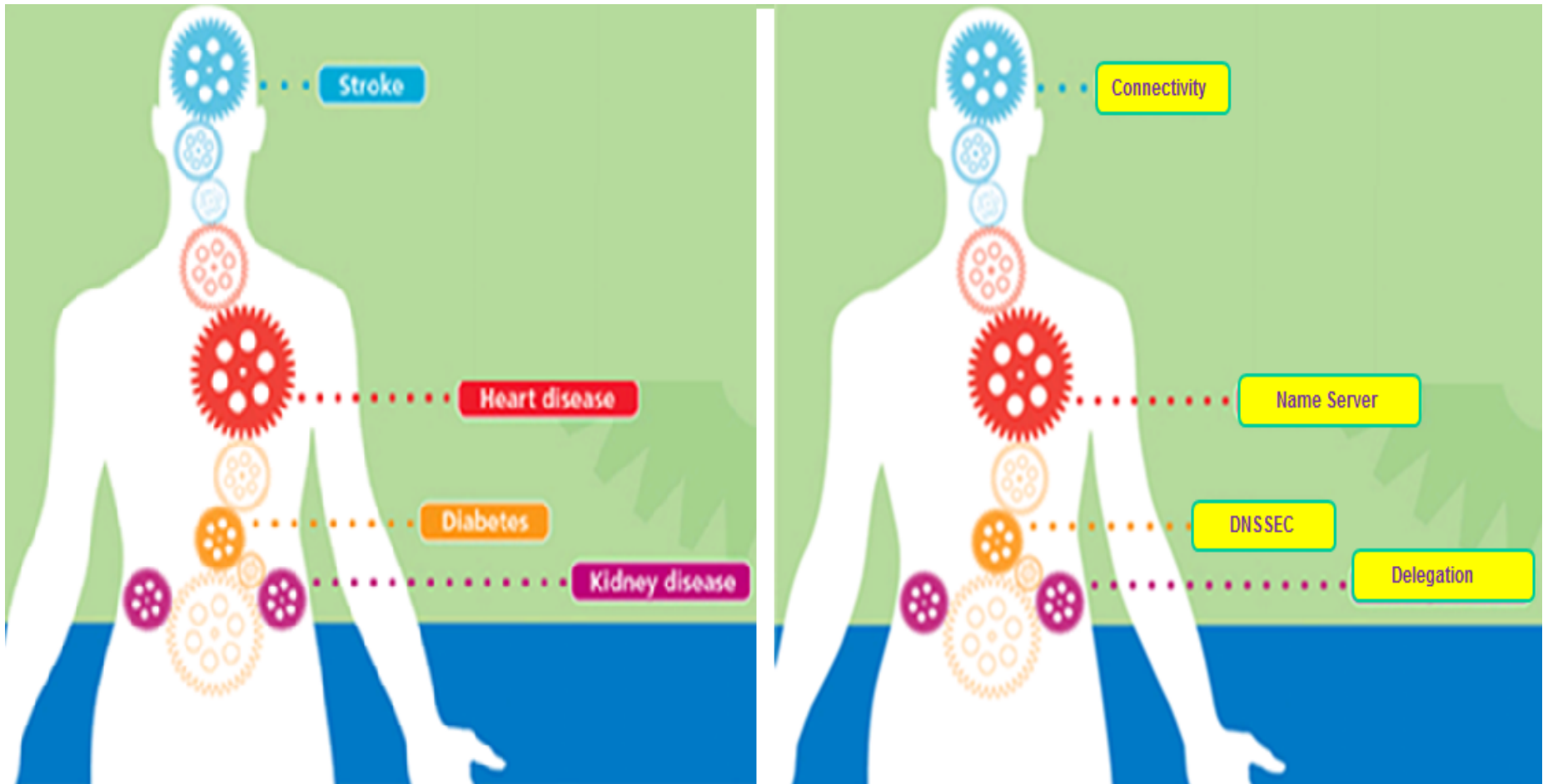


# Agenda

- ✓ Need for a DNS delegation validation tool
- ✓ Background
- ✓ Zonemaster
  - ✓ Documentation
  - ✓ Functional blocks
  - ✓ Different uses for different people
  - ✓ Features
  - ✓ Future directions



# *Need for a DNS delegation validation tool*





# *Comprehensive verification of a DNS zone*

- ✓ Well known tools

- ✓ ZoneCheck
- ✓ DNScheck
- ✓ dnsviz

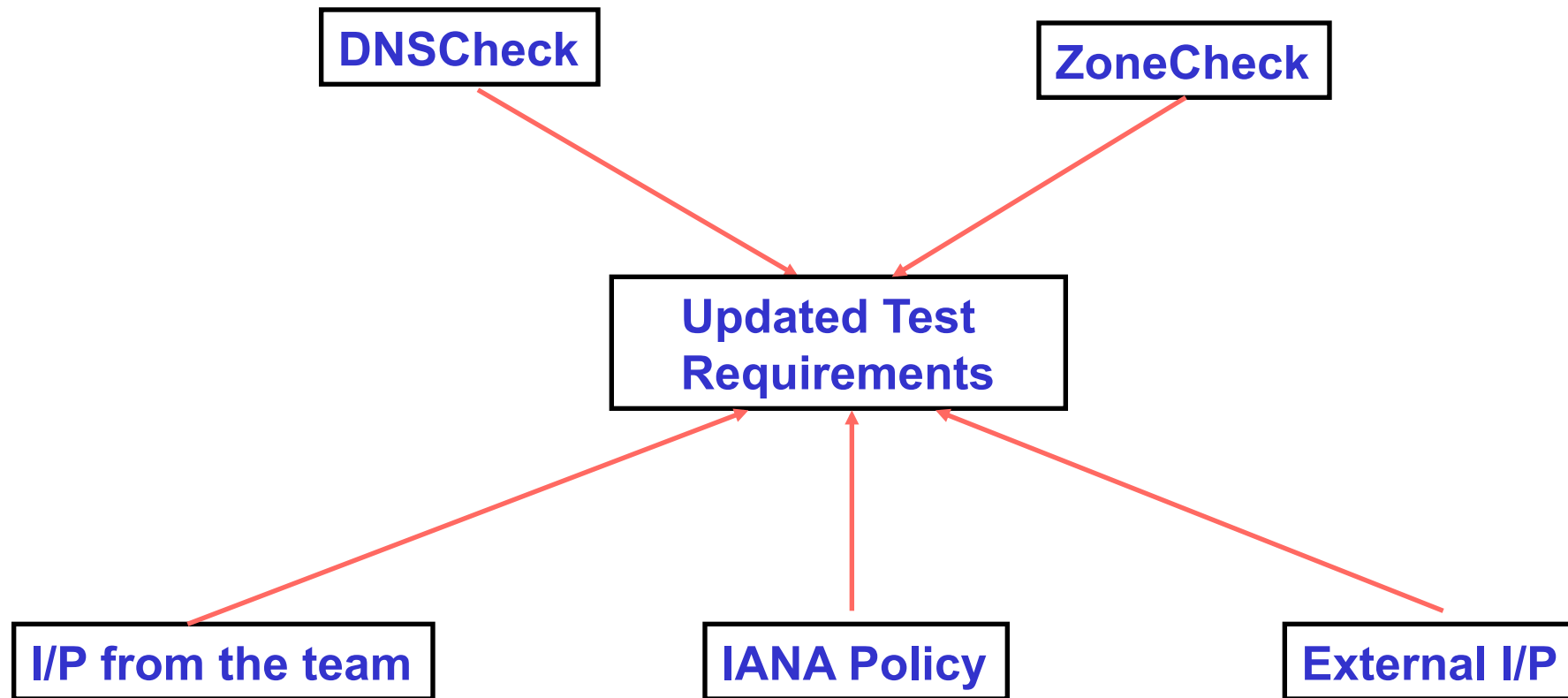


# *Why a new tool?*

- ✓ Scored the existing tool (DNScheck) on the following high level criterias
  - ✓ Modularity
  - ✓ Extensibility
  - ✓ Optimization of network resources
  - ✓ Optimization of system resources
  - ✓ I/O interfaces
  - ✓ Runtime behavior selection
- ✓ Final decision to develop a tool from scratch



# *Test requirements*





# Documentation (1/3)

Req	Requirement description	Level and Test Case
R01	UDP connectivity	CONNECTIVITY
R02	TCP connectivity	CONNECTIVITY
R03	Address in a private network	ADDRESS
R04	Address should not be part of a bogon prefix	ADDRESS
R05	Illegal symbols in domain name	SYNTAX
R06	Dash ('-') at start or beginning of domain name	SYNTAX
R07	Double dash in domain name	SYNTAX
R09	At least two nameservers for the domain	DELEGATION
R10	Identical addresses	DELEGATION
R11	Nameserver addresses on same subnet	CONNECTIVITY
R12	Nameserver addresses are all on the same subnet	CONNECTIVITY
R13	Delegation response fit in a 512 byte UDP packet	DELEGATION
R14	Delegation response with additional fit in a 512 byte UDP packet	DELEGATION



## Documentation (2/3)

Req	Requirement description	Level	Test Case ID	Test Description
R01	UDP connectivity	Connectivity-TP	CONNECTIVITY01	UDP connectivity
R02	TCP connectivity	Connectivity-TP	CONNECTIVITY02	TCP connectivity
R03	address in a private network	Address-TP	ADDRESS01	Name server address must be globally routable
R04	address should not be part of a bogon prefix	Address-TP	ADDRESS04	IPv6 address not part of bogon prefix
R05	illegal symbols in domain name	Syntax-TP	SYNTAX01	No illegal characters in the domain name
R06	dash ('-') at start or beginning of domain name	Syntax-TP	SYNTAX02	No hyphen ('-') at the start or end of the domain name



# Documentation (3/3)

## CONNECTIVITY01: UDP connectivity

### Test case identifier

CONNECTIVITY01: UDP connectivity

### Objective

DNS queries are sent using UDP on port 53, as described in section 4.2.1 of [RFC 1035](#).

The objective for this test is that all the authoritative name servers for the domain are accessible over UDP on port 53

### Inputs

The domain to be tested.

### Ordered description of steps to be taken to execute the test case

1. Obtains the IP address of the name servers from [Method4](#) and [Method5](#)
2. A SOA query is sent over UDP to distinct IP addresses of each name server found in step 1.
3. If all queries in step 2 receive a DNS answer (bogus responses are not checked here) then the test case succeed.

### Outcome(s)

If there is any name server that fails to answer queries over port 53 using UDP, this test case fails

### Special procedural requirements

If either IPv4 or IPv6 transport is disabled, ignore the evaluation of the result of any test using this transport protocol. Log a message reporting on the ignored result.

### Intercase dependencies

None



# TRTF

✓ Zonemaster requirements → TRTF :

<https://github.com/CENTRccTLDs/TRTF>

✓ Purpose:

- ✓ Requirements to set up a fully functional DNS delegation for a domain name.
- ✓ Create a set of test specifications for how to test a DNS delegation
- ✓ Informative document






# @ the IETF

- ✓ DNSOP WG
- ✓ Goal is to reach consensus on:
  - ✓ Organization of the document
  - ✓ Categories of requirements (remove/add ?)
  - ✓ RFC level of compliance (rephrase requirements as many as necessary)
- ✓ There are already some feedbacks on ML
- ✓ <https://tools.ietf.org/id/draft-wallstrom-dnsop-dns-delegation-requirements-02.txt>



# Basic use (Zonemaster.net)

 **ZONEMASTER**  
by  and 

Domain check   Pre-delegated domain   FAQ

Domain name

afnic.fr

▶

■ Advanced options

### Test # 211977

Executed at 2016-10-21T14:52+0200

Link

https://zonemaster.net/test/8502d7dc00c504a1

Basic   Advanced   Export   History

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



# Slightly advanced use (Zonemaster.net)

## Domain name

afnic.fr



☒ Advanced options

☒ IPv4

☒ IPv6

☒ Default  
IANA profile  
Test profile 2

## Test # 216985

Executed at 2016-10-26T22:20+0200

Link

<https://zonemaster.net/test/d6d49c3b8a8220e4>

[Basic](#) [Advanced](#) [Export](#) [History](#)

### SYSTEM

Using version v1.0.14 of the Zonemaster engine.

Configuration was read from DEFAULT CONFIGURATION

Policy was read from DEFAULT POLICY




### BASIC

Nameserver for zone fr replies when trying to fetch glue.

Nameserver for zone fr listed these nameservers as glue: ns1.nic.fr., ns2.nic.fr., ns3.nic.fr..



# Pre-delegated domains (Zonemaster.net)

**ZONEMASTER**  
by  and 

Domain checkPre-delegated domainFAQ

Notice! This is an undelegated test  
What is an undelegated domain test?

Domain name

Nameservers

NSIP

Digests

Key Tag	Algorithm	Digest type	Digest
Key tag			Digest

Fetch data from parent zone

☐ Advanced options

Zonemaster Test Engine Version:v1.0.14, IP address: 83.34.174.190



# *Zonemaster Engine*

- ✓ A Perl library
  - ✓ Test cases
  - ✓ Framework
    - ✓ Configuration
    - ✓ Logging
    - ✓ Translation
    - ✓ Own resolver



# Zonemaster CLI

```
usage: zonemaster-cli [-?h] [long options...]
-h -? --usage --help    Prints this usage information.
--version                Print version information and exit.
--level                  The minimum severity level to display. Must be
                        one of CRITICAL, ERROR, WARNING, NOTICE, INFO or
                        DEBUG.
--locale                  The locale to use for messages translation.
--json                   Flag indicating if output should be in JSON or
                        not.
--raw                    Flag indicating if output should be translated
                        to human language or dumped raw.
--time                   Print timestamp on entries.
--show_level             Print level on entries.
--show_module            Print the name of the module on entries.
--ns                     A name/ip string giving a nameserver for
                        undelegated tests. Can be given multiple times.
--save                   Name of a file to save DNS data to after running
                        tests.
--restore                Name of a file to restore DNS data from before
                        running test.
--ipv4                   Flag to permit or deny queries being sent via
                        IPv4. --ipv4 permits IPv4 traffic, --no-ipv4
                        forbids it.
--ipv6                   Flag to permit or deny queries being sent via
                        IPv6. --ipv6 permits IPv6 traffic, --no-ipv6
                        forbids it.
--list_tests             Instead of running a test, list all available
                        tests.
--test                   Specify test to run. Should be either the name
                        of a module, or the name of a module and the
                        name of a method in that module separated by a
                        "/" character (Example: "Basic/basic1"). The
                        method specified must be one that takes a zone
                        object as its single argument. This switch can
                        be repeated.
--stop_level             As soon as a message at this level or higher is
                        logged, execution will stop. Must be one of
                        CRITICAL, ERROR, WARNING, NOTICE, INFO or DEBUG.
--config                 Name of configuration file to load.
--policy                 Name of policy file to load.
--ds                     Strings with DS data on the form
                        "keytag,algorithm,type,digest"
--count                  Print a count of the number of messages at each
                        level
--progress               Boolean flag for activity indicator. Defaults to
                        on if STDOUT is a tty, off if it is not.
--encoding               Name of the character encoding used for command
                        line arguments
--nstimes                At the end of a run, print a summary of the
                        times the zone's name servers took to answer.
--dump_config            Print the effective configuration used in JSON
                        format, then exit.
--dump_policy            Print the effective policy used in JSON format,
                        then exit.
```



# *Additional features in CLI with respect to the GUI*

## ✓ Advantages

- ✓ Pre-delegation tests
- ✓ Have your own profile
- ✓ Have your own filter
- ✓ Have the output in raw/text/JSON



# *To use the CLI*

- ✓ Need installation of engine and CLI to use CLI
- ✓ Currently support Debian, Ubuntu, CentOS and FreeBSD
- ✓ Installation procedure for all different OS documented. Just need to copy/paste the commands

## **Instructions for Ubuntu 12.04, Ubuntu 14.04 and Debian 7**

1) Make sure the package database is up to date.

```
sudo apt-get update
```

2) Install all necessary packages.

```
sudo apt-get install build-essential libfile-slurp-perl libjson-perl liblist-moreutils-perl libio-socket-inet6-perl  
libmodule-find-perl libmoose-perl libfile-sharedir-perl libhash-merge-perl libreadonly-perl libmail-rfc822-address-  
perl libintl-xs-perl libssl-dev libdevel-checklib-perl libtest-fatal-perl libtie-simple-perl libio-capture-perl  
libgeography-countries-perl libidn11-dev
```


3) Install non-packaged software.

```
sudo cpan -i Zonemaster
```



# Need for the backend

## Domain name



☐ Advanced options

### Test # 183533

Executed at 2016-09-20T08:59+0200

Link

Basic

Advanced

Export

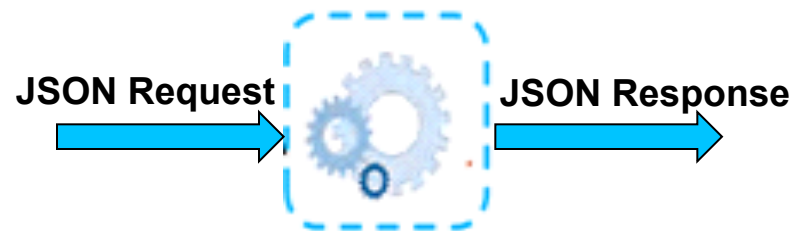
History

- 2016-10-25T14:50+0200
- 2016-10-25T11:04+0200
- 2016-10-21T14:52+0200
- 2016-10-12T11:02+0200
- 2016-10-12T10:34+0200
- 2016-10-08T17:23+0200
- 2016-10-05T11:56+0200
- 2016-09-24T15:18+0200
- 2016-09-20T11:21+0200
- 2016-09-20T08:59+0200
- 2016-09-15T08:42+0200
- 2016-09-06T17:01+0200
- 2016-09-04T21:52+0200
- 2016-08-29T11:55+0200
- 2016-08-03T13:06+0200
- 2016-07-24T13:17+0200
- 2016-07-24T05:32+0200
- 2016-07-24T05:15+0200
- 2016-07-21T11:48+0200



# *Need for local installation of the backend*

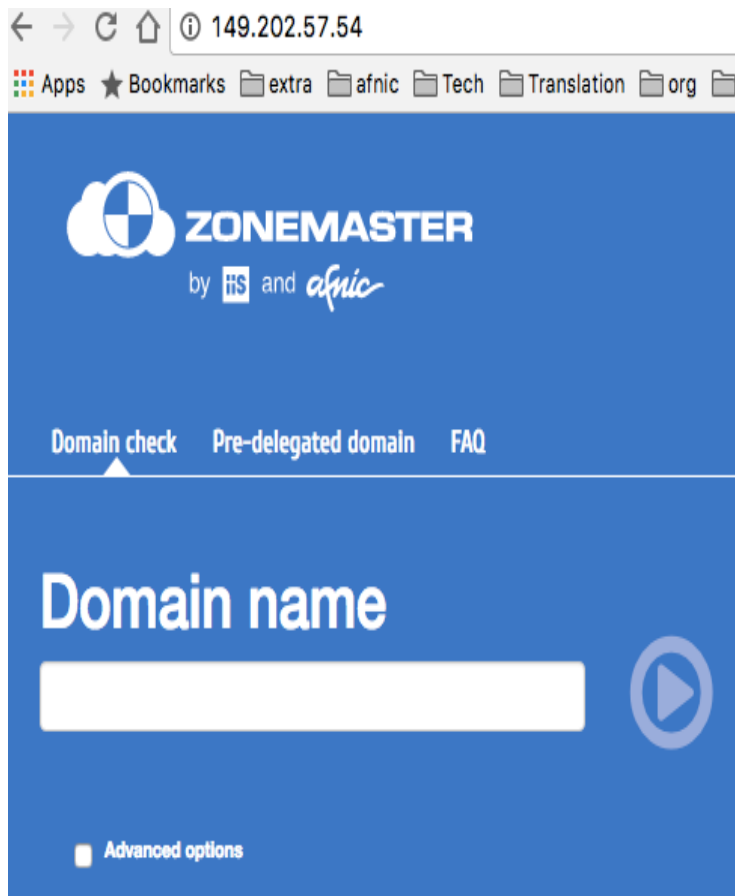
- ✓ JSON-RPC interface to the engine
- ✓ Currently supports MySQL and PostgreSQL
- ✓ Batch tests



```
{
  "method" : "add_batch_job",
  "params" : {
    "domains" : [
      "domain0.fr",
      "domain1.fr",
      "domain2.fr",
    ],
    "username" : "dnssdolve",
    "test_params" : {

    },
    "api_key" : "API_KEY_dnesdolve"
  },
  "jsonrpc" : "2.0",
  "id" : 147559211348450
}
```





cira

## D-Zone DNS Configuration Test

The .CA D-Zone Anycast DNS Secondary Service helps organizations doing business in Canada to optimize and secure their websites. The D-Zone DNS Configuration Test is a free tool that lets you analyze the health of your DNS by traversing from the root to the domain.

This comprehensive test takes about 60 seconds. To begin, enter your domain name below (Exclude prefixes, like www):

**Domain name:**

Start

[FAQ](#)

[Intpreting the Results](#)

Based on work done by [IIS](#) and [AFNIC](#) on [ZONEMASTER](#)



# Current Status

- ✓ Last full release release



The screenshot shows a GitHub release page for version 1.0.15. On the left, a green box labeled "Latest release" contains a tag icon next to "v1.0.15" and a commit hash "8397d58". On the right, the title "Release v1.0.15" is displayed in large blue font. Below it, a user profile picture and the name "matsduf" are followed by the text "released this 12 days ago". Further down, the commit message "Update KNOWN\_ISSUES" and the description "Preparing for 1.0.15." are visible.

- ✓ Components can have individual release
- ✓ IIS and Afnic **plan** to support officially Zonemaster for another two years



# *Contributing to the Zonemaster project*

- ✓ Use the tool
- ✓ Report bugs/enhancements using the github issue tracker
- ✓ Contribute code/documentation using git pull request
- ✓ For adding a new test
  - ✓ Add an issue in gituhb
  - ✓ If accepted, requirements/specifications are added
  - ✓ Adding a test case in the code (“zonemaster::Test::Example”)
- ✓ Create your own applications based on Zonemaster
- ✓ Add translation files
- ✓ Beta testers
- ✓ Mentors



# Useful links

## ✓ github

- ✓ <https://github.com/dotse/zonemaster>
- ✓ <https://github.com/dotse/zonemaster-engine>
- ✓ <https://github.com/dotse/zonemaster-cli>
- ✓ <https://github.com/dotse/zonemaster-backend>
- ✓ <https://github.com/dotse/zonemaster-gui>

✓ [zonemaster-devel@lists.iis.se](mailto:zonemaster-devel@lists.iis.se)

✓ [zonemaster-users@lists.iis.se](mailto:zonemaster-users@lists.iis.se)

✓ [contact@zonemaster.net](mailto:contact@zonemaster.net)

✓