DNSSHIM [1]

DNSSHIM is an open-source software that implements the Domain Name Name System (DNS) protocol for the Internet. Its main feature is to work as a Hidden Master nameserver, that is, provide information only to authoritative slave servers. Furthermore he has the ability to manage, store and automatically resign zones using the security extension DNSSEC.

Features

- DNSSEC
- Zone Transfer via AXFR and IXFR
- TSIG Support
- Zone Notification with DNS NOTIFY
- Automatic Configuration of Slave Nameservers (BIND 9.7.2 only)

Compatibility

DNSSHIM follows the standards defined by RFCs for communication with the slave servers, which includes zone transfer via AXFR or IXFR, using TSIG keys. That makes DNSSHIM compatible to work with most major nameservers software on the market.

The feature of automatic configuration of slave nameservers is currently available only for servers running BIND.

1 Installation

This document contains information for the compilation and installation of DNSSHIM. All instructions are valid for all platforms and operating systems that have a Java Virtual Machine (JVM) installed and configured correctly.

1.1 Requirements

1.1.1 Basic Requirements

The following requirements are necessary to use:

- JRE 6 (or greater)

[1] Version: *Rev* : 1498

1.1.2 Automatic Configuration of Slaves (OPTIONAL)

In order for the automatic configuration of slave nameservers to work, the following tools are required:

Server Hidden Master

1. SSH client
2. Rsync
3. Bourne Shell

Server Slave

1. SSH server
2. Rsync
3. Bind (with DNSSEC bis support)

1.2 Download

All DNSSHIM files, including source, binaries and docs, can be downloaded at `http://registro.br/dnsshim/` .

1.3 Configuring

DNSSHIM configuration files, by default, are located under the user's home directory. To change it, you can set an enviroment variable named `DNSSHIM_HOME`. In order to provide a more scalable architecture all files related to zones are hashed and stored under a three level directory structure. This behaviour exists in both main directories under `DNSHIM_HOME`: `/xfrd` and `/signer`.

1.3.1 Signer

All signer configuration files and private keys are located under the `signer` directory. Each zone managed by DNSSHIM has a private key located under:

`signer/FIRST_LEVEL/SECOND_LEVEL/THIRD_LEVEL`

The key name format is:

YYYYMMDDHHmmSS`-ZSK-257-`*KEYTAG*`.private`

All key files are extremely important, keep them safe.
The file `signer.properties` has two entries described below:

allowed_hosts_regex: An regular expression that defines which IP address can access signer. The default value is *.+* (anyone)

server_port: The port signer server will listen on.

1.3.2 XFRD Server

All XFRD configuration files are located under the `xfrd` directory. This directory holds public keys, zone informations like resource records and individual properties, main server configurations and slave informations. The file xfrd.properties is the main configuration file for XFRD. All entries are described bellow:

allowed_hosts_regex An regular expression that defines which IP address is allowed to access XFRD server. The default value is *.+* (anyone).

dns_server_port The TCP and UDP port that listen DNS queries. Default value is 53.

scheduler_high_priority (in hours) All signatures that expire in less than *scheduler_high_priority* will be resigned immediately. Default is 120 hours (5 days).

scheduler_low_priority (in hours) All signatures that expire between *scheduler_high_priority* and *scheduler_low_priority* will be rescheduled for resigning in some time within that interval. Default is 240 hours (10 days).

signer_cert_file The file that contains a TLS certificate. By default the communication between xfrd and signer uses an embedded TLS certificate.

signer_cert_password Only necessary if the option above (*signer_cert_file*) is defined.

signer_host Host where signer server is running. Default value is *localhost*.

signer_port The TCP port that the signer server is listen. Default is 9797.

slave_user User used by SlaveSync.sh script to connect to slaves. Default is empty. Change it if you want enable automatic provisioning.

tsig_fudge The default fudge value for outgoing packets.

ui_cert_file The TLS certificate file used in communications between xfrd server and client. By default the communication use an embedded TLS certificate.

ui_cert_password Only necessary if the option above (*ui_cert_file*) is defined.

ui_port The TCP port where the server will receive client's requests.

slave_sync_enabled (true or false) If true the server will execute SlaveSync.sh script in order automatically configure slave nameservers.

slave_sync_period (in seconds) The period that the server rewrites zone configuration files used for configuration of the slaves. This option is only necessary if *slave_sync_enabled* option is true.

slave_sync_path The path where the script SlaveSync.sh is located. Default value is `./SlaveSync.sh` .

rndc_path Path where the `rndc` utility is located. Default value is `/usr/sbin/rndc`.

rndc_port Port `rndc` connects on the slave servers. Default value is 953.

shutdown_secret Shared secret with a client that allows it to stop the XFRD server gracefully.

2 Client

In order to interact with DNSSHIM, it is necessary to have a client that supports its protocol. A python client library, named *pydnssshim*,that fully supports all commands, is distributed separately and is available at the DNSSHIM website. You are free to use it or implement your own client. Please visit DNSSHIM website for more information about clients.

3 Deployment

Starting Signer

```
$ java -jar -Dlog4j.configuration=log4j-signer.properties dnsshim-signer.jar [2]
```

Starting XFRD Server

```
$ java -jar -Dlog4j.configuration=log4j-xfrd.properties dnsshim-xfrd.jar
```

Important note: in order to start using DNSSHIM effectively, you must create a user and login to the server. These operations, as well as many others, should be performed by a client application. For more information see the section 2.

3.1 Troubleshooting

Could not determine local IP address. Using loopback In the */etc/hosts* file, check the IP address for the hostname of the machine.

[2]For convenience, DNSSHIM comes with two log4j pre-configured files. If you prefer you can use your own.

3.2 Automatic Configuration of Slave Nameservers

DNSSHIM has a feature which allows for automatic configuration of slave nameservers, so that once a new zone is created in DNSSHIM, the slave will be authoritative for that zone within a period of time with no further intervention. It works only on slaves running BIND 9.7.2 and above, using the rndc utility to automatically create new slave server.
In order to setup for automatic configuration of slave nameservers, there are several step that should be followed:

1. Make sure that BIND 9.7.2 or newer is properly installed on the DNSSHIM host and all the slave servers.

   On the DNSSHIM host

2. Open the xfrd.properties file.

3. Set the variable "slavesync_path" to the path where the SlaveSync.sh script is.

4. Make sure the SlaveSync.sh script is executable.

5. Set the variable "slave_sync_enable" to "true".

6. Optionally, set the variable "slave_sync_period" to the interval (in seconds) between two slave synchronizations.

7. Set the variable "rndc_path" to the path where rndc is.

8. Optionally, set the variable "rndc_port" to the port where rndc is going to listen on the slave servers. Default is 953.

9. Start the Signer and the DNSSHIM server (3).

10. Create a new slave group using the command `new-slavegroup` in the DNSSHIM client (2).

11. Add the desired slave(s) to the newly created slave group using the command `add-slave` in the DNSSHIM client (2).

12. Assign the slave group to the desired zone(s) using the command `assign-slavegroup` in the DNSSHIM client (2).

13. New zones should be created with the option `--slave-group=‘‘groupname’’` on the `new-zone` command

14. Create a TSIG key for the servers which will be synchronized using the command `new-tsig-key` in the DNSSHIM client (2).

15. Edit the file /etc/rndc.conf with the following directives:

```
key "tsig-key" { algorithm hmac-md5; secret "tsig-secret"; };
server slave_ip { key "tsig-key"; };
```

Where *tsig-key* is the name of the TSIG key assigned to the slave, *tsig-secret* is the secret of the key, *slave_ip* is the IP address of the slave server.

Make sure this is done for each slave server and TSIG key.

On each of the Slave hosts:

16. Edit the file named.conf with the following directives:

```
options { allow-new-zones yes; };
key "tsig-key" { algorithm hmac-md5; secret "tsig-secret"; };
server dnsshim_ip { keys "tsig-key"; };
controls {
                inet * allow { dnsshim_ip; } keys { "tsig-key"; };
};
```

Where *tsig-key* is the name of the TSIG key assigned to the slave, *tsig-secret* is the secret of the key, *dnsshim_ip* is the IP address of the host running DNSSHIM.

The first two lines tell BIND that DNSSHIM is using the specified TSIG key.

The `controls` ensures that the host running DNSSHIM is allowed to control the BIND server via rndc, mainly by adding and removing zones.

17. Copy the script CreateZoneDirs.sh, which comes with the DNSSHIM distribution, on the base directory of BIND and run it. This will create the directory structure for the zones that will be added by DNSSHIM via rndc.

18. Restart the BIND on the slave hosts.

4 Compilation

If you want build from source the following steps will guide you.

4.1 Requirements

The following requirements are necessary to compile:

- JDK 6 (or higher)
- Ant 1.7 (or higher)

- Apache Commons Codec 1.3 (or higher)
- Apache log4j 1.2.15 (or higher)

4.2 Build

Unzip source, in the directory DNSSHIM execute:

```
$ ant dist
```

After the execution of this target a directory named *dist* will be create containing two JARs (signer and XFRD).