DNS/DNSSEC Workshop in conjunction with Lanka Network Operators Group (LKNOG) Conference 12-16 August 2024

Lab Exercises

Champika Wijayatunga
Technical Engagement Sr. Manager - Asia Pacific
<champika.wijayatunga@icann.org>

Introduction

Tsig KEY Base security

Goals

Instead of using IP addresses, we'll now be using cryptographic keys to authenticate zone transfer – this uses TSIG, a mechanism by which the communication between the master and slave server will be authenticated using this key.

Note:

> Commands preceded with $ imply that you should execute the command as a general user - not as root.
> Commands preceded with "#" imply that you should be working as root.
> Commands with more specific command lines (e.g. “rtrX>"or “mysql>") imply that you are executing commands on remote equipment.

On your primary server (SOA server)

Generate the tsig key

```
$ sudo tsig-keygen -a hmac-sha256 grpX-key > /tmp/grpX-key.txt
```

Check the content of the file. Should look similar to this:

```
key "grpX-key" {
    algorithm hmac-sha256;
    secret "THIS_IS_MY_KEY";
};
```

Add the tsig key at the bottom of **named.conf.options** config file.

```
key "grpX-key" {
algorithm hmac-sha256;
        secret "THIS_IS_MY_KEY";
};
server 100.100.X.130 {
     keys {grpX-key ; };
};
server 100.100.X.131 {
     keys {grpX-key ; };
};
```

Don't forget to replace X in "**grpX-key**" ....!

Then in your zone, change allow-transfer line

```
zone "grpX.<lab_domain>.te-labs.training" {
        type master;
        file "/etc/bind/db.grpX";
        allow-transfer { key grpX-key; };
        also-notify { 100.100.X.130; 100.100.X.131; };
};
```

As you can see above, we've changed “allow-transfer” statement allowing transfer of the zone for holders of the "tsig-key".

Restart *named* service

```
$ sudo named-checkconf
$ sudo rndc reconfig
```

On NS1 server

Test that zone transfer has stopped working.
```
$ dig @100.100.X.66 axfr grpX..te-labs.training

...
; Transfer failed.
```

A look into the SOA server logs should show something like:

```
$ tail /var/log/bind/general

24-May-2022 10:03:29.433 client @0x7f185c006920 100.100.1.130#38993 (grp
```

We need the key!

You can also test manually as follows:

```
$ dig @100.100.X.66 -y hmac-sha256:grpX-key:THIS_IS_MY_KEY axfr grpX.<la
```

Add the TSIG key to your NS1 configuration

In **/etc/bind/named.conf.options**, add the tsig key, and a statement to tell which key to use when talking to “100.100.X.66;” (the soa server):

```
key "grpX-key" {
        algorithm hmac-sha256;
        secret "THIS_IS_MY_KEY";
};

server 100.100.X.66 {       // here you put the IP of YOUR primary serve
        keys { grpX-key; };
};
```

Save, exit and restart bind9.

Testing the configuration

On SOA server increase the serial and reload the zone. Then,
`$ sudo rndc reload grpX.<lab_domain>.te-labs.training`

In ns1, go to logs and validate that the transfer was successful.

```
$ tail /var/log/syslog

zone grp2.<lab_domain>.te-labs.training/IN: Transfer started.
transfer of 'grp2.<lab_domain>.te-labs.training/IN' from 100.100.2.66#53
zone grp2.<lab_domain>.te-labs.training/IN: transferred serial 202205240
transfer of 'grp2.<lab_domain>.te-labs.training/IN' from 100.100.2.66#53
transfer of 'grp2.<lab_domain>.te-labs.training/IN' from 100.100.2.66#53
zone grp2.<lab_domain>.te-labs.training/IN: sending notifies (serial 202
managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer
resolver priming query complete
```

On NS2 server

Edit **/etc/nsd/nsd.conf** file, create key section and add the tsig key grpX-key

```
key:
        name: "grpX-key"
        algorithm: hmac-sha256
        secret: "THIS_IS_MY_KEY"
```

and Fix pattern:

change these lines

```
allow-notify: 100.100.X.66 NOKEY
request-xfr: AXFR 100.100.X.66 NOKEY
```

with this:

```
allow-notify: 100.100.X.66 grpX-key
request-xfr: AXFR 100.100.X.66 grpX-key
```

Save, exit, verify and restart NSD service.

```
$ nsd-checkconf /etc/nsd/nsd.conf
$ sudo nsd-control reconfig
$ sudo nsd-control reload grpX.<lab_domain>.te-labs.training
```

Check the logs on NS2 and on SOA.