LAB: Securing nameserver (DNSSEC)

Lab Environment

The workshop WiFi:

- SSID: `workshop`
- PASS: `iij/2497`

Hosts - Virtual machines (Ubuntu 18.04LTS/LXC)

- Hostname: `nsXX.workshop`
- IPv6: `fd00:2497:1::X`
- IPv4: `10.0.0.X`

Where `X` and `XX` is yoru group ID. For group 1, hostname is `ns01.workshop`, IPv6 address is `fd00:2497:1::1`, and IPv4 is `10.0.0.1`.

Domain names

- `groupXX.workshop`

Where `X` and `XX` is yoru group ID. For group 1, domain name is `group01.workshop`.

(Workshop Only) Change the trust anchor and root hint

Since this workshop provide a completely different DNS trust chain, we need to replace the trust anchor for the root domain. In the real operation, we don't need to do the process described in this section.

Create a new file at `/etc/bind/bind.keys`.

```
managed-keys {
    . initial-key 257 3 13 "I9jR4QIl/xSDyXgByM+Y51NNnHGLsVEUQy+z
                            DjaMLSLSJTT8icKPmTVXmyu7md85gPckbqMQ
                            CjvAZ5tXfpdILA==";
};
```

Create a new file at `/etc/bind/db.root`.

```
.                         1800      NS    a.fakeroot-servers.net.
a.fakeroot-servers.net.  1800      A     10.0.255.10
a.fakeroot-servers.net.  1800      AAAA  fd00:2497:1::255:10
```

Generate keys

ssh to your virtual server and create the `keys` directory under the `/etc/bind/` directory to store your two key pairs (Zone Singing Key (ZSK) and Key Signing Key (KSK)).

```
$ sudo mkdir /etc/bind/keys
$ cd /etc/bind/keys
$ sudo dnssec-keygen -3 -a ECDSAP256SHA256 -r /dev/urandom groupXX.workshop
$ sudo dnssec-keygen -f KSK -3 -a ECDSAP256SHA256 -r /dev/urandom groupXX.workshop
```

> Note: In the above example, we use the `/dev/urandom` device as a random source to generate keys quickly. If you care the quality of keys, you should use better random source.

Sign zone and update bind

Sign your zone with your keys.

```
$ cd /etc/bind
$ sudo dnssec-signzone -S -K keys -a -o groupXX.workshop groupXX.workshop
```

The signed zone file will be generates as `groupXX.workshop.signed`.

> Note: By default, the signed zone file is valid for 30 days. You need to re-sign your zone file in 30 days, even though there is no record change.

Edit your zone configuration file (`/etc/bind/named.conf.local`).

```
zone "groupXX.workshop" {
    type master;
    file "/etc/bind/groupXX.workshop.signed";
};
```

Restart bind9.

```
$ sudo systemctl restart bind9
```

Register your `DS` record to the parent zone

In the `/etc/bind/` directory, you also have `dsset-groupXX.workshop.` file. This file is generated when you sign your zone file, and includes the `DS` record information which need to be registered in your parent zone.

Copy the file to `/var/www/html/` directory so that the workshop instructor can check and register your `DS` records in the parent zone.

```
$ sudo cp /etc/bind/dsset-groupXX.workshop. /var/www/html/
```

Once instructors put your `DS` records in the parent zone, your zone should be able to use DNSSEC. Check the result of the following command and confirm that the response has the `ad` bit set.

```
$ dig any groupXX.workshop
```