DNSSEC Validation using Unbound

Table of Contents

Enabling DNSSEC validation

Our goal is to enable Unbound as a DNSSEC validating resolver in Ubuntu. Unbound was designed by NLnet Labs as a recursive, caching DNS resolver for more on Unbound check out: https://nlnetlabs.nl/projects/unbound/about/

Getting Started

Open your browser and enter the URL: https://ng.te-labs.training

Access your server by clicking on the **grpX-resolv** URL. For example, if you are in group 11, click on the grp11-resolv URL: https://webssh.ng.te-labs.training/?hostname=10.11.1.2&username=sysadm

Login with the password: **ICANN+dns!**

Become the super user by issuing the command:

```
# sudo -s
[sudo] password for sysadm: ICANN+dns!
```

Note: Ensure you are logged into the **resolv** virtual machine and not the **soa** virtual machine.

Restarting Unbound

Unbound has already been installed but just in case you would like to play around with removing and installing unbound use the following commands:

```
# apt-get remove unbound
# apt-get install unbound
```

To restart unbound, by entering the command:

```
# service unbound restart
```

Set your Timezone

It is **very important** to synchronize the clock of your resolver. The following commands outline how to go about synchronization.

```
// Enter the timedatectl command
# timedatectl

// Disable time synchronization on your system
# timedatectl set-ntp off
```

```
// Toggle time synchronization on
# timedatectl set-ntp on

// To install ntp package (only if it isn't yet installed)
# apt install ntp

// Enable NTP at system startup
# systemctl enable ntp

// Start NTP
# systemctl start ntp

// List different time-zones
# timedatectl list-timezones | grep Africa

// Set the correct time-zone
# timedatectl set-timezone Africa/Lagos

// Check status of ntp and timezone
# timedatectl
```

Inspect the Unbound Configuration Files

Have a glance at the main unbound configuration files:

```
# more /etc/unbound/unbound.conf.d/class.conf
# more /etc/unbound/unbound.conf.d/root-auto-trust-anchor-file.conf
```

Edit the Trust Anchor Configuration file

On your terminal issue the command:

```
# nano /etc/unbound/unbound.conf.d/root-auto-trust-anchor-file.conf
```

Uncomment the line:

```
# trust-anchor-file: "/var/lib/unbound/root.key"
```

So that it reads:

```
trust-anchor-file: "/var/lib/unbound/root.key"
```

Download a copy of the latest trust anchor:

```
# unbound-anchor
```

Save the file and then restart unbound using the command:

```
# service unbound restart
```

Testing for DNSSEC Validation

Try to do some DNSSEC lookups:

```
# dig +dnssec @127.0.0.1 dnskey .
# dig +dnssec @10.X.1.2 dnskey .
# dig @10.X.1.2 www.icann.org A +dnssec
# dig icann.org A +dnssec
# for a in {1..5}; do dig A icann.org @10.X.1.2 +dnssec |grep -w 'Query time'; done
# for a in {1..5}; do dig A icann.org @8.8.8.8 |grep -w 'Query time'; done
# dig @10.X.1.2 servfail.nl A +dnssec
# dig @10.X.1.2 servfail.nl A +dnssec +cd
# dig @1.1.1.1 servfail.nl A +dnssec
# dig @1.1.1.1 servfail.nl A +dnssec +cd
# dig @8.8.8.8 servfail.nl A +dnssec
# dig @8.8.8.8 servfail.nl A +dnssec +cd
```

Note: Replace *X* with your group number

Observe the flags returned. Do you notice the **ad** flag?

Edit /etc/resolv.conf

To use your Unbound resolver as the default resolver, replace the line:

```
nameserver 10.0.0.254
```

With:

```
nameserver 10.X.1.2
```

Note: Replace *X* with your group number