Enabling DNSSEC validation with the root trust anchor in BIND

You need to log in to your resolver (cache) machine, i.e. for group 1, you would use resolv.grp1.dns.nsrc.org, as you did when you enabled recursion on that server.

1. Grab the root key

    NOTE: This is only for the purpose of this lab - on the Internet, you would simply use "unbound-anchor" to download the real root.key, and set "auto-trust-anchor-file:" in unbound.conf, and let unbound update the key when necessary.

    In this lab, ask your instructor if we are using the "RZM" or not.

    With RZM

    Go to https://rzm.dnssek.org/, and copy the trust-anchor statement (the ENTIRE line) from this page and paste it into a file, /usr/local/etc/unbound/root.key

    Without RZM

    Grab the key from the root server:

    $ sudo scp sysadm@a.root-servers.net:root.key /tmp/root.key

    (Alternatively, your instructor may have made the file available on the Web - ask him!)

    View the contents of the key (/tmp/root.key or where you put it) and copy them.

    Edit the /etc/namedb/named.conf, and paste the contents at the bottom of the file, in the following format:

```
trusted-keys {
    // paste here the contents
};
```

    It should look something like this when done:

```
trusted-keys {
  . 257 3 5 "AwEAAaGF0WNdnZ9krIIBOZCgR7t6F5ikcKREeRkWQOxZGIRYKq1hgwu9
bd+yyg20+NPpfV1ThX5WD4/QJ/tgygLZKTjy3wYcSYBBwXPoTYY9/6lw
ysD6GjXDHsYHWmWE6usxaEwJNAk3Pfsy2q2ZN6LjcfcmZzKmB4saq1ph
h6nDiYfUJFLzXPRQtW1OisLxedCLYZ/IOUjx2MJd+xmKJ93wt9Du799RF4I+9ZsYMZ+aIRt3LWuq/
+g60Ipb4cqtUl5rnfYFpDmfq4QXf67tkvYk
aCaxv0bpd5vj2E86V5HfAQmeaKPX9sGG80LD+GNI53168OfZdHje58vZ sW765bV/iVk=";
};
```

2. Restart the nameserver

```
# service named restart
```

3. Run a few queries:

```
$ dig @localhost +dnssec . SOA
$ dig @localhost +dnssec mytld. SOA
```

What do you notice ?

4. If you haven't already done so, you can go back to the DNS logging exercise, and enable logging on your RESOLV host, and look at the dnssec log file...