

Включение валидации DNSSEC с доверием к корневому ключу в Unbound

Вам нужно зайти на машину с кэширующим сервером, т.е. для группы 1, вам нужно использовать `resolv.grp1.dns.nsrc`, так же, как вы делали в упражнении по конфигурированию unbound.

1. Получите корневой ключ

Замечание: это нужно только для целей данной лабораторки - в сети Интернет, вы просто использовали бы "unbound-anchor" для скачивания настоящего root.key, и указали бы "auto-trust-anchor-file:" в unbound.conf, и позволили бы unbound обновлять ключ при необходимости.

В этом упражнении, спросите преподавателя о том, используете ли вы "RZM" или нет.

С использованием RZM

Посетите <https://rzm.dnssek.org/>, и скопируйте строчку trust-anchor ЦЕЛИКОМ с этой страницы в файл `/usr/local/etc/unbound/root.key`

Без использования RZM

Скопируйте ключ с корневого сервера:

```
# scp sysadm@a.root-servers.net:root.key /usr/local/etc/unbound/root.key
```

Отредактируйте файл `/usr/local/etc/unbound/unbound.conf`:

Найдите строку "trust-anchor-file:", и измените ее с:

```
# trust-anchor-file: ""
```

на

```
trust-anchor-file: "/usr/local/etc/unbound/root.key"
```

2. Перезапустите DNS-сервер

```
# service unbound restart
```

3. dig @localhost +dnssec mytld. SOA

На что вы обратили внимание?