

# RPKI Validation

RPKI Validation is an important step for routing security. In this article we will look at installing the relying party software (or RPKI validator) required to validate Route Origin Authorization (ROAs).

The choice of which validator to use is yours, but please make sure you run at least two validators, not just for redundancy, but also because the validation states change to NOT FOUND for all routes when RPKI-enabled routers lose connection with the validators.

In this article we will show you how to install [Routinator](#) (by NLnetLabs) on a Ubuntu Linux System.

## How to install Routinator

### Preparations

To install a Routinator package, you need the 64-bit version of one of these Ubuntu versions:

- Ubuntu Jammy 22.04 (LTS)
- Ubuntu Focal 20.04 (LTS)
- Ubuntu Bionic 18.04 (LTS)
- Ubuntu Xenial 16.04 (LTS)

Packages are available for the `amd64/x86_64` architecture only.

First update the **apt** package index:

```
sudo apt update
```

Then install packages to allow **apt** to use a repository over HTTPS:

```
sudo apt install \  
  ca-certificates \  
  curl \  
  gnupg \  
  lsb-release
```

# Installing Routinator

Add the GPG key from NLnet Labs:

```
curl -fsSL https://packages.nlnetlabs.nl/aptkey.asc | sudo gpg --dearmor -o /usr/share/keyrings/nlnetlabs-archive-keyring.gpg
```

Now, use the following command to set up the *main* repository:

```
echo \  
"deb [arch=$(dpkg --print-architecture) signed-  
by=/usr/share/keyrings/nlnetlabs-archive-keyring.gpg]  
https://packages.nlnetlabs.nl/linux/ubuntu \  
$(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/nlnetlabs.list >  
/dev/null
```

Update the **apt** package index once more:

```
sudo apt update
```

You can now install Routinator with:

```
sudo apt install routinator
```

After installation Routinator will run immediately as the user *routinator* and be configured to start at boot. By default, it will run the RTR server on port 3323 and the HTTP server on port 8323. These, and other values can be changed in the [configuration file](#) located in `/etc/routinator/routinator.conf`.

```
repository-dir = "/var/lib/routinator/rpki-cache"  
  
rtr-listen = ["100.68.3.6:3323", "[2001:db8:3::4]:3323"]  
  
http-listen = ["100.68.3.6:8323"]
```

You can specify the location of the RPKI cache directory using the `--repository-dir` option. If you don't, one will be created in the default location `$HOME/.rpki-cache/repository`. The [HTTP service](#) and [RTR service](#) must be started explicitly using the command line options `--http` and `--rtr`, respectively, or via the configuration file.

You can view the default settings Routinator runs with using:

```
routinator config
```

It will return the list of defaults in the same notation that is used by the [configuration file](#), which will be largely similar to this and can serve as a starting point for making your own:

```
allow-dubious-hosts = false
```

```
dirty = false
disable-rrdp = false
disable-rsync = false
enable-bgpsec = false
exceptions = []
expire = 7200
history-size = 10
http-listen = []
http-tls-listen = []
log = "default"
log-level = "WARN"
max-ca-depth = 32
max-object-size = 20000000
refresh = 600
repository-dir = "/Users/routinator/.rpki-cache/repository"
retry = 600
rrdp-fallback-time = 3600
rrdp-max-delta-count = 100
rrdp-proxies = []
rrdp-root-certs = []
rrdp-timeout = 300
rsync-command = "rsync"
rsync-timeout = 300
rtr-client-metrics = false
rtr-listen = []
rtr-tcp-keepalive = 60
rtr-tls-listen = []
stale = "reject"
strict = false
syslog-facility = "daemon"
systemd-listen = false
unknown-objects = "warn"
unsafe-vrps = "accept"
validation-threads = 10
```

**Restart Routinator with:**

```
systemctl restart routinator
```

**You can check the status of Routinator with:**

```
sudo systemctl status routinator
```

**You can view the logs with:**

```
sudo journalctl --unit=routinator
```

**New in version 0.9.0: RPM packages**

**New in version 0.11.0: Debian packages for `armhf` and `arm64` architecture**

**New in version 0.11.2: Ubuntu packages for Jammy 22.04 (LTS)**

Deprecated since version 0.12.0: `routinator-init` and `--accept-arin-rpa`

Now the validator is ready to feed the validated cache to BGP speaking routers through the RTR protocol.

Confirm that Routinator is running using the following commands:

```
ps aux | grep routinator
netstat -tulnp | grep 3323
```

## Router Config

Cisco XE Example:

```
router bgp 65000
  bgp rpki server tcp 100.68.3.6 port 1029 refresh 600
```

Cisco XR Example:

```
router bgp 65000
  bgp router-id 10.1.1.1
  rpki server 100.68.3.6
    transport tcp port 3323
  refresh-time 900
```

Junos Example:

```
routing-options {
  router-id 1.1.1.1;
  autonomous-system 64496;
  validation {
    group rpki-validator {
      session 100.68.3.6{ # IP address of the RPKI cache server.
      port 3323; # Other validators may use different ports.
      refresh-time 900;
      local-address 100.68.3.5;
      }
    }
  }
}
```