Passim

Passim means "*here, there and everywhere*" and is a local caching server for metadata on your local network

Richard Hughes
Senior Principal Software Engineer

Red Hat
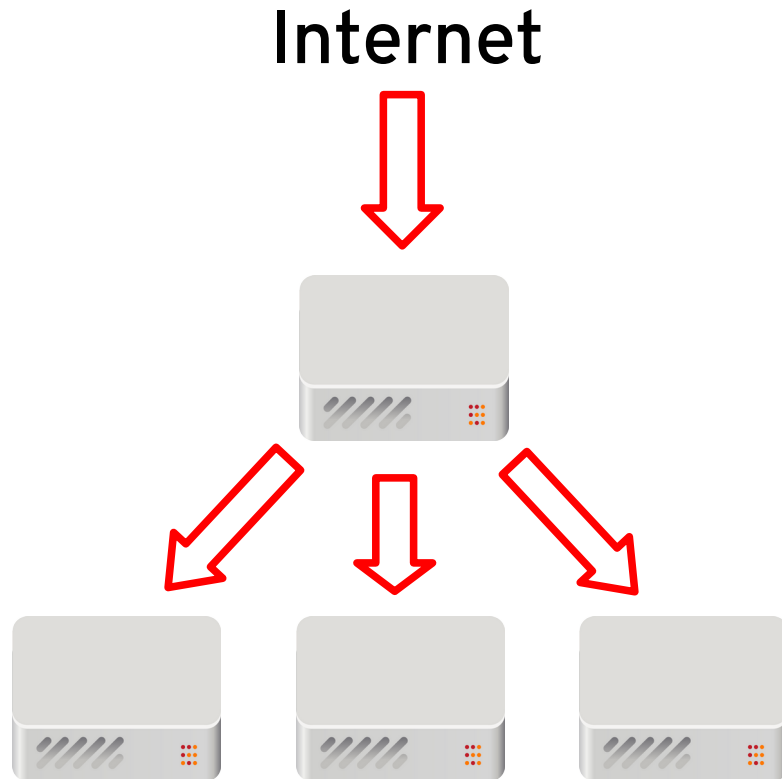
Who am I?

I've been building Open Source for **over 20 years,** 15 of which employed by Red Hat.

Red Hat

Every day over 12 million Linux users automatically download ~2Mb of metadata from the LVFS CDN.

Red Hat

Decentralized, Zero Configuration Architecture

Internet

Everybody downloads the same file from a CDN

 - CDN is not expensive, but it's certainly not free

 - We use less electricity (and therefore carbon) using Passim

Yesterdays metadata is useless today

 - We put a maximum age on each published file

Is my laptop now a server for the department?

 - We limit on the number of times each file can be shared

I don't like it!

- Set `P2pPolicy=nothing` in `/etc/fwupd/fwupd.conf`

- `systemctl mask passim.service`

- `rpm -e passim`

- block DNSSD on your firewall

Security Considerations

What extra components are running?

Passim is a daemon and uses Avahi and a self-signed certificate (using GnuTLS). 4Mb of RSS and ~300ms of CPU time.

Why not BitTorrent or IPFS?

ITAR puts restrictions on how we can share specific software, e.g. sending firmware implementing strong crypto.
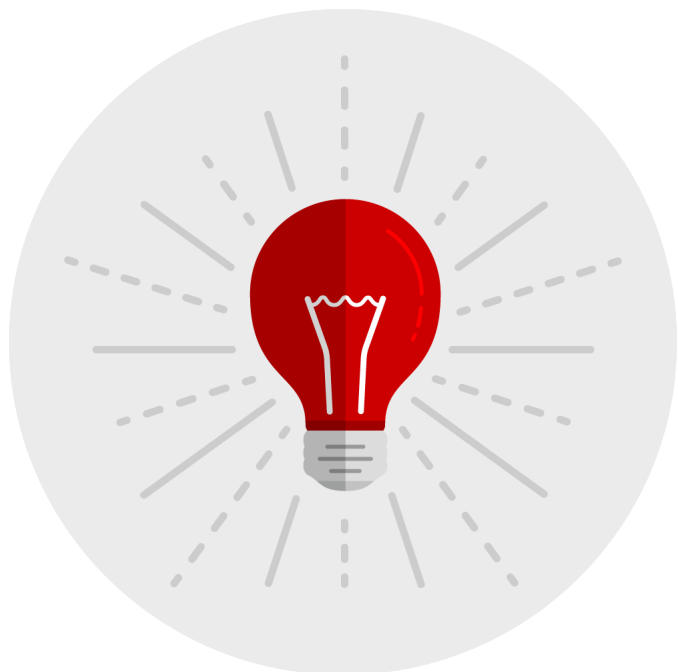
Who can download?

Anyone who has the SHA-256 of a published file can download a file a limited number of times.

Who can publish?

Only processes running as UID=0 can share files by **explicitly** publishing them. Files have xattrs for properties and are stored in `/var/lib/passim/data/`

But where does the hash come from?

Use the internet as the {existing} source of truth
We have to do one **tiny** request to get the SHA–256 of the latest metadata – e.g. `metalink.xml` or `jcat`.

Can a peer send `evil-payload.exe` for all hashes?
Sure! Any client using Passim **must** check the SHA–256 checksum of the result before parsing the file in any way.

If downloading using passim fails clients **must** also fall back to using the internet as they did before.

Red Hat

Debugging at `https://localhost:27500/`

Passim-A70B

A local caching server, version `0.1.7` with status `running`.

Shared Files:

Filename	Hash	Binary	Age	Shared	Size	Flags
metadata.xml.zst	0c5fdb1426fd6ad82e120d847db25d33d610af63d6eec74df07a83272da58c2c	fwupd	7/24h	0/50	181.7 kB	none
metadata.xml.zst	c92f1c42abc0bb23bb6c64e94ad39f9629a69419007b20c8fcaef21983d86c24	fwupd	7/24h	0/50	1.3 MB	none

Red Hat

Interface for `passim status`

```
$ passim status
Name:                   Passim-A70B
Status:                 Running
Network Saving:         27.2 MB
URI:                    https://localhost:27500/

c92f1c42abc0bb23bb6c64e94ad39f9629a69419007b20c8fcaef21983d86c24
├ Filename:             metadata.xml.zst
├ Command Line:         fwupd
├ Age:                  27093/86400
├ Share Limit:          0/50
└ Size:                 1.3 MB
```

Red Hat

Providing billions of files is not free

The internet isn't solar powered and it is our duty as developers to use it efficiently.

Red Hat

Call to action

What we should do:

 - Work out what other metadata can be shared. *Adblock*? *Repodata*?

 - Collect some statistics about how effective this actually is in the real world.

 - Keep talking about security and privacy, **but without Fear, Uncertainty and Doubt**.

Red Hat