

Fangfrisch

Fangfrisch (German for "freshly caught") is a sibling to the [Clam Anti-Virus](#) freshclam utility. It allows downloading virus definition files that are not official ClamAV canon, e.g. from [Sanesecurity](#).

1. License

Copyright © 2020 Ralph Seichter

This file is part of "Fangfrisch".

Fangfrisch is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

Fangfrisch is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with Fangfrisch. If not, see <https://www.gnu.org/licenses/>.

2. Update strategy

Fangfrisch is expected to run periodically, for example using [cron](#). Download attempts are recorded in a database and new attempts are only made after the defined age threshold is reached. Additionally, Fangfrisch will check digests first (if available), and only download virus definitions when their recorded digest changes, minimising transfer volumes.

3. Installation

Fangfrisch requires Python 3.7 or newer. The recommended installation method is using the [pip command](#) in a virtual Python environment. Here is an example listing of commands for BASH:

```
# Create venv home directory
mkdir -p /var/lib/fangfrisch
cd /var/lib/fangfrisch

# Prepare and activate venv
python3 -m venv venv
source venv/bin/activate

# Install from PyPI.org
pip install fangfrisch
```

4. Configuration

A configuration file is mandatory and uses an INI File structure. It must contain at least a default section with the options shown below. A description of SQLAlchemy's DB URL syntax is available [here](#). Typically, a local [SQLite](#) database will suffice. Internal default values for Sanesecurity can be used by enabling the `[sanesecurity]` section.

```
# Mandatory section.
[DEFAULT]
db_url = sqlite:///var/lib/clamav/fangfrisch.sqlite
local_directory = /var/lib/clamav

# Optional section, enables internal defaults for Sanesecurity.
[sanesecurity]
enabled = yes
```

You can also add your own sections for additional virus definition providers. See [here](#) for a detailed description of the supported configuration file parser. The parser uses extended interpolation, i.e. `${section:option}` style references to options defined elsewhere in the file.

```
[fictional_provider]
enabled = yes
integrity_check = md5
# Download no more than once ever 12 hours
max_age = 720
prefix = http://fictional-provider.tld/clamav-unofficial/
url_eggs = ${prefix}eggs.ndb
url_spam = ${prefix}spam.hdb
```

Fangfrisch will scan enabled sections for lines prefixed with `url_` to determine download sources for virus definition files. The value of `integrity_check` determines both the expected filename suffix for digests and the hashing mechanism used for verification.

NOTE

Max age is specified in minutes. Integrity checks can be turned off by using the value **disabled**.

5. Usage

You can display command line arguments as follows:

```
$ python -m fangfrisch --help

usage: __main__.py [-h] [-c CONF] [-f] {dumpconf,initdb,refresh}

positional arguments:
  {dumpconf,initdb,refresh}
                        Action to perform

optional arguments:
  -h, --help            show this help message and exit
  -c CONF, --conf CONF  Configuration file
  -f, --force            Force action (default: False)
```

You can choose among following actions:

- **dumpconf**: Dump the effective configuration to stdout, combining both internal defaults and your own settings. The effective configuration for the example shown in the [Configuration](#) section is available [here](#).
- **initdb**: Create the database structure. This needs to be run only once, before the first refresh.
- **refresh**: Refresh the configured URLs. The **force** switch can be set to force downloads regardless of local file age.

Fangfrisch should never be run as **root**, but as your local ClamAV user (typically **clamav**). An example crontab looks like this:

```
# minute hour day-of-month month day-of-week user command
*/30 * * * * clamav python -m fangfrisch --conf /etc/fangfrisch.conf refresh
```