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. 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.

2. 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 configuration.
- **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
```

3. Configuration

A configuration file is mandatory and must contain a `db_url` entry. For example:

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

[sanesecurity]
enabled = yes
```

See here for a detailed description of the supported configuration file syntax with extended interpolation. 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]` config section as shown above. The resulting effective configuration can be displayed using the `dumpconf` action.

You can add your own sections for additional virus definition providers:

```
[exampleprovider]
enabled = yes
integrity_check = md5
# Set max age to 12 hours
max_age = 720
prefix = http://example.tld/clamav-unofficial/
url_eggs = ${prefix}eggs.ndb
url_spam = ${prefix}spam.hdb
```

Fangfrisch will scan enabled sections for lines with the prefix `url_` to determine download sources for virus definition files. Supported schemas include FTP, HTTP and HTTPS. 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 using the value `disabled`.