strongSwan - Bug #2222

charon-systemd doesn't reopen the log file when SIGHUP is raised

15.01.2017 19:56 - Noel Kuntze

Status:	Closed	**Start date:**	15.01.2017
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon-systemd		
Target version:	5.5.2		
Affected version:	5.5.1	**Resolution:**	Fixed

Description

I have a logrotate setup with strongswan-swanctl. The daemon logs to /var/log/charon.log
logrotate rotates the logs to charon.log.[1-5], gzips and so on.

Now even if charon-systemd is raised SIGHUP, it continues logging to charon.log.1.
It never writes to charon.log, unless it is restarted. According to the [[|documentation]]
charon(-systemd) should reopen the log file when SIGHUP is raised.

I'm using 5.5.1

strongswan-swanctl.servicestrongswan-swanctl.service

```
[Unit]
Description=strongSwan IPsec IKEv1/IKEv2 daemon using swanctl
Requires=network.target
After=network.target

[Service]
Type=notify
ExecStartPre=/usr/bin/ip xfrm policy flush
ExecStartPre=/usr/bin/ip xfrm state flush
ExecStartPre=/usr/bin/ip route flush table 220
ExecStart=/usr/bin/charon-systemd
ExecStartPost=/usr/bin/swanctl --load-all --noprompt
ExecReload=/usr/bin/swanctl --reload
Restart=on-failure

[Install]
WantedBy=multi-user.target
```

ll /var/log/charon.log*ll /var/log/charon.log*

```
ll /var/log/charon.log*
-rw------- 1 root root    0 15. Jan 00:00 /var/log/charon.log
-rw------- 1 root root  76K 15. Jan 19:42 /var/log/charon.log.1
-rw------- 1 root root 880K 11. Nov 03:44 /var/log/charon.log.5.gz
```

strongswan-swanctl logrotate configstrongswan-swanctl logrotate config

/var/log/charon.log {

```
    missingok
    sharedscripts
    compress
    postrotate
        /usr/bin/killall -HUP /usr/bin/charon-systemd
        /usr/bin/killall -HUP /usr/lib/strongswan/charon
    endscript
```

```
}
```

strongswan.confstrongswan.conf

```
charon-systemd {
        load = random nonce af-alg openssl x509 revocation constraints curl pubkey pkcs1 pkcs7 pkc
s8 pem gmp attr kernel-netlink socket-default vici eap-identity eap-gtc eap-mschapv2 eap-radius xa
uth-generic xauth-eap unity eap-tls eap-ttls chapoly sha3 mgf1 bliss ntru newhope
        make_before_break=yes
        retransmit_tries = 6
        retransmit_timeout = 3.0
        retransmit_base = 1.7
        cisco_unity=yes
        dos_protection = yes
        threads = 32
        replay_window = 32
        retry_initiate_interval = 3
        interface_use = ens3
        send_vendor_id = yes
        crypt_test {
                on_add = yes
                required = yes
        }
        journal {
                time_format = %a, %Y-%m-%d %R
                default = 0
                append=yes
                ike_name=yes
                flush_line=yes
        }
        filelog {
                /var/log/charon.log {
                        time_format = %a, %Y-%m-%d %R
                        default = 2
                        mgr = 0
                        net = 1
                        enc = 1
                        asn = 1
                        job = 1
                        knl = 1
                        ike_name = yes
                        append = no
                }
        }
        plugins {
        }
        tls {
                ciphers = aes128, aes256
                key_exchange = ecdhe-ecdsa, ecdhe-rsa, dhe-rsa, rsa
                mac = sha256, sha384
        }
}

swanctl {
        load = test-vectors sqlite aes des rc2 sha1 sha2 md5 random nonce x509 revocation constrai
nts pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl mysql af-alg fips-prf gmp xcbc c
mac hmac ctr ccm gcm ntru curl
}
```

Associated revisions

Revision 68d97ac5 - 25.01.2017 15:03 - Tobias Brunner

Merge branch 'charon-systemd-reload-loggers'

Allows reloading strongswan.conf, the loggers, and the plugins in
charon-systemd by sending a SIGHUP (as already supported by charon).

Loggers are now also reloaded by VICI's `reload-settings` command (works
with both daemons).

Fixes #2222.

History

#1 - 16.01.2017 17:41 - Tobias Brunner

- Tracker changed from Issue to Bug

- Status changed from New to Feedback

- Target version set to 5.5.2

> Now even if charon-systemd is raised SIGHUP, it continues logging to charon.log.1.
> It never writes to charon.log, unless it is restarted. According to the [[|documentation]]
> charon(-systemd) should reopen the log file when SIGHUP is raised.

charon-systemd actually does not handle SIGHUP. I pushed a commit that changes this to the *2222-charon-systemd-sighup* branch. Let me know if that works for you.

Another option might be to reload the loggers after VICI's reload-settings command successfully reloaded the config (which it currently doesn't, probably because the plugin doesn't know the actual values of the two arguments if used with charon: source:src/libcharon/plugins/vici/vici_control.c#L624).

#2 - 16.01.2017 17:45 - Noel Kuntze

I think handling SIGHUP is the best solution, simply because people could edit settings when logrotate fires off and then the settings would be in an unknown state to the user (and he/she didn't know they were changed or why they daemon behaves differently).
I'll test and report.

EDIT: I think I misunderstood your comment. I thought SIGHUP only reopened the file and/or read the logger configuration. Well, if SIGUP also reads and updates strongswan.conf settings, I guess there's no advantage doing it either way. Having something to explicitely reopen the log files would be usefulm though.

#3 - 23.01.2017 02:00 - Noel Kuntze

That patch works fine.

#4 - 25.01.2017 15:05 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

Merged to master.