pfSense Packages - Bug #10642

ACME certificate renewal with DNS-Gandi method fails when using multiple Gandi keys

06/08/2020 03:17 PM - Oriane Tury

Status:	New	**Start date:**	06/08/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	ACME	**Estimated time:**	0.00 hour
Target version:			
Affected Version:		**Affected Architecture:**	All

Description

With the ACME service, when trying to issue/renew a certificate on 2 domain names (or more) using the DNS-Gandi Live DNS validation method, with each domain name using a distinct Gandi LiveDNS API Key, pfSense will only use the API key registered for the last domain in the Domain SAN list of the certificate. Thus the validation for the first domain fails unexpectedly.

(The whole setup is intended for a HTTPS reverse proxy in front of multiple webservers whose domain names pertain to different people.)

Here is the report printed after trying to issue/renew a certificate with oriane.ink and minuscheri.com (in this order) in the Domain SAN list. Validation method for both is DNS-Gandi LiveDNS, but API keys are distinct.

```
certificat_bug_reproductible
Renewing certificate
account: TEST
server: letsencrypt-staging-2

/usr/local/pkg/acme/acme.sh  --issue  -d 'oriane.ink' --dns 'dns_gandi_livedns'  -d 'minuscheri.co
m' --dns 'dns_gandi_livedns'  --home '/tmp/acme/certificat_bug_reproductible/' --accountconf '/tmp
/acme/certificat_bug_reproductible/accountconf.conf' --force --reloadCmd '/tmp/acme/certificat_bug
_reproductible/reloadcmd.sh' --log-level 3 --log '/tmp/acme/certificat_bug_reproductible/acme_issu
ecert.log'
Array
(
    [path] => /etc:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin/
    [PATH] => /etc:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin/
    [GANDI_LIVEDNS_KEY] => <KEY_MINUSCHERI_COM>
)
[Mon Jun  8 21:46:41 CEST 2020] Multi domain='DNS:oriane.ink,DNS:minuscheri.com'
[Mon Jun  8 21:46:41 CEST 2020] Getting domain auth token for each domain
[Mon Jun  8 21:46:45 CEST 2020] Getting webroot for domain='oriane.ink'
[Mon Jun  8 21:46:45 CEST 2020] Getting webroot for domain='minuscheri.com'
[Mon Jun  8 21:46:45 CEST 2020] Adding txt value: 6fwWiw6znabab0nuzw4MUHPOo1l8_qftNOZvWXXXXXX for
domain:  _acme-challenge.oriane.ink
[Mon Jun  8 21:46:46 CEST 2020] Error add txt for domain:_acme-challenge.oriane.ink
[Mon Jun  8 21:46:46 CEST 2020] Please check log file for more details: /tmp/acme/certificat_bug_r
eproductible/acme_issuecert.log
```

History

#1 - 06/09/2020 07:55 AM - Jim Pingle

- Project changed from pfSense to pfSense Packages

- Category set to ACME

- Affected Version deleted (2.4.5)

Have you tried doing this with acme.sh on its own (not through pfSense)? It may be a problem in the Gandi script, it may not support multiple domains like that.

You should probably be using separate cert files for each domain anyhow. That wouldn't be a problem for haproxy, it should let you use a different

certificate for each hostname it covers.

#2 - 06/10/2020 05:28 PM - Oriane Tury

I don't have SSH access to the router, so unfortunately I cannot run acme.sh outside pfSense. I suppose the answer lies in the accountconf.conf generated through pfSense, which might rely on the Gandi script.

Anyway I went with your suggestion to use separate certs for each domain. I'd forgotten that you could do that these days, thanks to the SNI extension for TLS. It's properly implemented in the HAProxy module and worked as expected. Thanks for the advice!