xmpp.chapril.org - Demande #3772

Fiabiliser la génération de certificats de XMPP

17/06/2019 10:13 - Quentin Gibeaux

Statut:	Fermé	**Début:**	17/06/2019
Priorité:	Élevée	**Echéance:**	13/09/2019
Assigné à:	pitchum .	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Sprint 2020 mars		
Difficulté:	3 Moyen		

Description

XMPP a besoin d'un certificat letsencrypt valide pour son service XMPP et sur du HTTP.
Du fait des complications de routage, ce n'est pas aisé de faire un challenge http et une conf valide.

Dans un premier temps un certificat a été généré manuellement, mais il expire dans 3 mois. Il a été copié manuellement.

Il faut probablement configurer un challenge DNS au niveau de l'infra.

Historique

#1 - 04/09/2019 21:33 - pitchum .

- Statut changé de Nouveau à Confirmé

Le certificat allait expirer dans 10 jours, je l'ai renouvelé manuellement (car on a déjà un utilisateur à ne pas décevoir) :

```
dehydrated -c
systemctl reload nginx
cat /var/lib/dehydrated/certs/xmpp.chapril.org/{fullchain,privkey}.pem > /etc/ejabberd/cert-and-key.xmpp.chapril.org.pem
sudo -u ejabberd ejabberdctl reload_config
```

#2 - 25/09/2019 19:57 - Quentin Gibeaux

- Assigné à mis à pitchum .

#3 - 06/10/2019 22:27 - pitchum .

Je viens de me souvenir ce qui pose problème avec la génération de certificats pour xmpp.chapril.org : c'est qu'on a besoin de ce certificat sur 2 machines différentes : celle qui héberge le site Web et celle qui héberge le service XMPP.
Actuellement le renouvellement se fait côté service XMPP et ça fonctionne. Mais maintenant je voudrais mettre ne ligne un site Web "vitrine" qui soit aussi accessible en HTTP et pour l'instant ce n'est pas possible à moins d'automatiser la copie des certificats de la machine xmpp vers la machine Web.

Une autre possibilité qui a déjà été envisagée serait de faire les modifs nécessaires côté serveurs DNS pour permettre de générer des certificats letsencrypt par challenge DNS. Ainsi les deux machines pourront créer chacune de son côté un certificat valide pour le même domaine.

#4 - 11/10/2019 01:38 - pitchum .

J'ai commencé la mise en place du sous-domaine _acme-challenge.chapril.org pour permettre les challenges DNS mais je suis bloqué à cause des vues interne/externe dans Bind.
Le fichier zone pour _acme-challenge.chapril.org ne peut être déclaré que dans une seule des deux vues.
Or les updates dynamiques fait pas dehydrated ou certbot arriveront par la vue interne mais les serveurs Letsencrypt arriveront par la vue externe.

Je n'ai pas encore exploré toute les options de Bind donc peut-être qu'il y a un moyen propre pour m'en sortir.

Sinon en dernier recours j'envisage de créer un la zone DNS _acme-challenge.chapril.org en double, pointant sur deux fichiers différents mais qui sont en fait le même (l'un sera un symlink ou un hardlink de l'autre).

#5 - 11/10/2019 11:01 - François Poulain

Pour l'April on a simplement la zone int à l'abandon:

```
zones-ext.conf: zone "acme-challenge.april.org" {
zones-ext.conf-         type master;
zones-ext.conf:         file "/etc/bind/zones/masters/acme-challenge.april.org";
zones-ext.conf-         allow-update { april_bastion; key "key-bastion"; };
```

```
zones-ext.conf- };
zones-ext.conf-
--
zones-int.conf: zone "acme-challenge.april.org" {
zones-int.conf-         type master;
zones-int.conf:         file "/etc/bind/zones/masters/acme-challenge.april.org-int";
zones-int.conf- };

# cat zones/masters/acme-challenge.april.org
$ORIGIN .
$TTL 3600    ; 1 hour
acme-challenge.april.org IN SOA    vip.april.org. hostmaster.april.org. (
                201803218  ; serial
                14400      ; refresh (4 hours)
                3600       ; retry (1 hour)
                604800     ; expire (1 week)
                3600       ; minimum (1 hour)
                )
            NS    vip.april.org.
            NS    galanga.april.org.
            A    195.154.56.24
$ORIGIN acme-challenge.april.org.
$TTL 60    ; 1 minute
_acme-challenge        TXT    "GSMiBc26ophFj9OwFUiJR8akeYK4Kk4mGiY5WE6ClTU"
_log-challenge        TXT    "Updated the lundi 23 septembre 2019, 18:24:35 (UTC+0200)"

# cat zones/masters/acme-challenge.april.org-int
$TTL 1h
@    IN    SOA    vip.april.org.    hostmaster.april.org. (
        201803190    ; Serial  - YYYYMMDDnn
        4h           ; Refresh
        1h           ; Retry
        1w           ; Expire
        1h           ; Minimum
)

        NS        dns.april.org.

        A        195.154.56.24        ; vip.april.org.

_acme-challenge TXT "bling"
```

#6 - 11/10/2019 11:04 - François Poulain

Le script de challenge :

```
# cat /usr/local/bin/update-dns-acme-challenge.sh
#!/bin/bash

date=$(date)

SERVER="dns.cluster.april.org"
DOMAIN="acme-challenge.april.org"
KEY="hmac-md5:key-bastion +bling=="
CREATE_RECORD="_acme-challenge.$DOMAIN"
LOGING_RECORD="_log-challenge.$DOMAIN"

nsupdate<<EOF
    key $KEY
    server $SERVER
    zone $DOMAIN in external
    update delete $CREATE_RECORD TXT
    update delete $LOGING_RECORD TXT
    update add $CREATE_RECORD 60 TXT $CERTBOT_VALIDATION
    update add $LOGING_RECORD 60 TXT "Updated the $date"
    show
    send
    quit
EOF
sleep 1
```

#7 - 11/10/2019 11:25 - François Poulain

Et tant que j'y suis à divulguer la conf april, j'avais siouxé un peu sur les clés et les vues :

```
named.conf.local:acl april_bastion {
named.conf.local-        172.16.0.1;
named.conf.local-};

named.conf.options:key "key-bastion" {
named.conf.options-     algorithm hmac-md5;
named.conf.options-     secret "+bling==";
named.conf.options-};

zones-ext.conf- zone "acme-challenge.april.org" {
zones-ext.conf-         type master;
zones-ext.conf-         file "/etc/bind/zones/masters/acme-challenge.april.org";
zones-ext.conf:         allow-update { april_bastion; key "key-bastion"; };
zones-ext.conf- };

zones-int.conf-view "internal" {
zones-int.conf-        match-clients {
zones-int.conf:                !key key-bastion;
zones-int.conf-                acl_internal;
zones-int.conf-        };
```

#8 - 13/10/2019 14:18 - pitchum .

- Priorité changé de Normale à Élevée

- % réalisé changé de 0 à 50

- Difficulté changé de 2 Facile à 3 Moyen

Yes merci François, tu m'enlèves une fière chandelle du pied.
Ta solution est plus propre que ce que je m'apprêtais à faire.

```
view "internal" {
        match-clients {
                !key rndc-acme;
                acl_internal;
        };
[...]
```

#9 - 20/10/2019 20:20 - pitchum .

- Statut changé de Confirmé à Résolu

Je passe le ticket en "Résolu" pendant 2 mois environ, le temps de vérifier que les renouvellements automatiques se font bien, à la fois sur bastion et sur xmpp.

#10 - 08/01/2020 21:31 - pitchum .

Le renouvellement automatique n'était pas activé... mea culpa.
Il y a maintenant une tâche cron : /etc/cron.weekly/acme-renew.

Je laisse le ticket encore en statut "résolu" pendant 2 mois au moins pour être sûr que tout marche bien comme prévu.

#11 - 04/03/2020 22:50 - pitchum .

- Statut changé de Résolu à Attente d'information

#12 - 10/03/2020 22:59 - pitchum .

À revérifier fin mars

```
</dev/null  2>/dev/null openssl s_client -connect xmpp.chapril.org:5269 -xmpphost chapril.org -starttls xmpp-s
erver | openssl x509 -noout -subject -dates
subject=CN = chapril.org
notBefore=Jan  8 18:45:16 2020 GMT
notAfter=Apr  7 18:45:16 2020 GMT
```

#13 - 15/03/2020 09:54 - pitchum .

- Statut changé de Attente d'information à Fermé

- % réalisé changé de 50 à 100

C'est bon, la tâche cron de renouvellement est bien passée ce matin.

```
$ </dev/null  2>/dev/null openssl s_client -connect xmpp.chapril.org:5222 -xmpphost chapril.org -starttls xmpp
 | openssl x509 -noout -subject -dates
subject=CN = chapril.org
notBefore=Mar 15 04:47:46 2020 GMT
notAfter=Jun 13 04:47:46 2020 GMT

$ </dev/null  2>/dev/null openssl s_client -connect xmpp.chapril.org:5269 -xmpphost chapril.org -starttls xmpp
-server | openssl x509 -noout -subject -dates
subject=CN = chapril.org
notBefore=Mar 15 04:47:46 2020 GMT
notAfter=Jun 13 04:47:46 2020 GMT
```

Ça a déclenché une alerte de supervision car le nouveau certificat est déployé dans /etc.
J'ai donc retiré ce fichier certificat du suivi git de etckeeper :

```
cd /etc
git rm --cached ejabberd/chapril.org-wildcard.ejabberd.pem
echo ejabberd/chapril.org-wildcard.ejabberd.pem >> .gitignore
git add .gitignore
etckeeper commit
```

#14 - 02/04/2020 00:32 - Christian P. Momon

- Version cible mis à Sprint 2020 mars