Admins - Demande #3516

Mettre en place un certificat pour mail.april.org

13/12/2018 15:19 - Quentin Gibeaux

Statut:	Fermé	**Début:**	13/12/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	Quentin Gibeaux	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Décembre 2018	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Demande de gibus :

```
J'en ai déjà touché un mot à Polux sur IRC et à madix qui m'a conseillé
d'écrire ici. Depuis une récente mise à jour de thunderbird, ce dernier
refuse de se connecter en POP à mail.april.org:995 (SSL/TLS normal
password) sous prétexte que le certificat est auto-signé. Jusqu'à
maintenant ma configuration fonctionnait très bien en ayant ajouté une
exception permanente. Mais depuis la mise à jour, Thunderbird ne semble
plus tenir compte de cette exception et envoie un avertissement à chaque
fois, propose d'ajouter une exception (pourtant déjà permanente) et
abandonne la connexion quoique l'on fasse. (idem en IMAPS et idem le
SMTP en STARTTLS sur smpt.april.org:587)
```

Plusieurs pistes :
(PoluX)

```
Ce que je ferais :
- générer une clé ssh pour un usager letsencrypt sur la VM mail
- donner accès rw au certificat
- installer un hook letsencrypt qui pousse le cert par scp et
  reload les postfix/dovecot.
- monitorer le certificat sur imap/pop/smtp sicenédéjafé

(remarque)
    En configurerant l'accès ssh "letsencrypt" pour pouvoir faire un
     systemctl reload postfix/dovecot ?
Oui avec une conf sudo donc.

Autre possibilité :
- proxyfier les services mail sur le bastion avec nginx.
```

Historique

#1 - 13/12/2018 17:35 - Quentin Gibeaux

nginx-light et dehydrated installés sur mail, conf basique ajoutée :

```
server {
        listen 80;
        listen [::]:80;

        server_name mail.april.org imap.april.org smtp.april.org;

        location / {
                deny all;
        }
        location /.well-known/acme-challenge {
                alias /var/lib/dehydrated/acme-challenges;
        }
}
```

proxypass ajouté identique sur bastion.

Conf de postfix et dovecot modifée :

```
(April) root@mail:/etc/dovecot[master*+$]# git diff .
diff --git a/dovecot/dovecot.conf b/dovecot/dovecot.conf
index 83dfa86..161e7b9 100644
--- a/dovecot/dovecot.conf
+++ b/dovecot/dovecot.conf
@@ -24,9 +24,11 @@ plugin {
        sieve_global_path = /etc/dovecot/sieve/default.sieve
 }

-
-ssl_cert = </etc/ssl/certs/dovecot.pem
-ssl_key = </etc/ssl/private/dovecot.pem
+# old self signed cert
+#ssl_cert = </etc/ssl/certs/dovecot.pem
+#ssl_key = </etc/ssl/private/dovecot.pem
+ssl_cert = </var/lib/dehydrated/certs/mail.april.org/fullchain.pem
+ssl_key = </var/lib/dehydrated/certs/mail.april.org/privkey.pem

 protocols = imap pop3 sieve

(April) root@mail:/etc/postfix[master+$]# git diff --cached .
diff --git a/postfix/conf.d/20-ssl.conf b/postfix/conf.d/20-ssl.conf
index 81ea48e..7a390d6 100644
--- a/postfix/conf.d/20-ssl.conf
+++ b/postfix/conf.d/20-ssl.conf
@@ -1,6 +1,9 @@
 # TLS parameters
-smtpd_tls_cert_file=/etc/postfix/ssl/certs/mail.april.org.pem
-smtpd_tls_key_file=/etc/postfix/ssl/private/mail.april.org.key
+# old selfsigned cert
+#smtpd_tls_cert_file=/etc/postfix/ssl/certs/mail.april.org.pem
+#smtpd_tls_key_file=/etc/postfix/ssl/private/mail.april.org.key
+smtpd_tls_cert_file=/var/lib/dehydrated/certs/mail.april.org/fullchain.pem
+smtpd_tls_key_file=/var/lib/dehydrated/certs/mail.april.org/privkey.pem
 smtpd_use_tls=yes
 smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
 smtpd_tls_received_header = yes
diff --git a/postfix/main.cf b/postfix/main.cf
index db12baa..32e6f43 100644
--- a/postfix/main.cf
+++ b/postfix/main.cf
@@ -37,8 +37,11 @@ mynetworks = 127.0.0.0/8 172.16.0.0/24 192.168.0.0/16 192.168.25.117/32 88.191.2
 ### conf.d/20-ssl.conf

 # TLS parameters
-smtpd_tls_cert_file=/etc/postfix/ssl/certs/mail.april.org.pem
-smtpd_tls_key_file=/etc/postfix/ssl/private/mail.april.org.key
+#old selfsigned cert
+#smtpd_tls_cert_file=/etc/postfix/ssl/certs/mail.april.org.pem
+#smtpd_tls_key_file=/etc/postfix/ssl/private/mail.april.org.key
+smtpd_tls_cert_file=/var/lib/dehydrated/certs/mail.april.org/fullchain.pem
+smtpd_tls_key_file=/var/lib/dehydrated/certs/mail.april.org/privkey.pem
 smtpd_use_tls=yes
 smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
 smtpd_tls_received_header = yes
```

Cron rajouté pour charger les nouveaux cert.

Normalement tout est bon ! (vu avec etienne et gibus)

#2 - 13/12/2018 17:35 - Quentin Gibeaux

- Assigné à mis à Quentin Gibeaux

- Version cible changé de Backlog à Décembre 2018

#3 - 13/12/2018 17:42 - Quentin Gibeaux

manque le monitoring smtps imaps

#4 - 14/12/2018 09:26 - Quentin Gibeaux

```
gibus | QGuLL: depuis la maison avec thunderbird 60.2.1 (qui buggait avant avec le cert autosigné) je te confi
rme que ça va très bien (en pop ici)
```

C'est OK pour gibus, donc reste le monitoring des certs

#5 - 08/01/2019 14:15 - Quentin Gibeaux

- Statut changé de Nouveau à Résolu

Certificat monitoré sur le port 993 (c'est le même cert pour smtp) :

```
define service{
      use                     generic-service
      service_description     SSLCERT::MAIL
      check_command           check_ssl_cert!993
      host_name               mail
      check_interval          1440
}
```

Résultat :

```
Status Information:    SSL CERT OK - issuer=C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3 valid
until Mar 13 15:12:16 2019 GMT
```

#6 - 09/01/2019 22:15 - Quentin Gibeaux

- Statut changé de Résolu à Fermé