Admins - Demande #2816

Déployer et monitorer le certificat SSL pour les sites du Libre en Fête

01/12/2017 14:27 - Frédéric Couchet

Statut:	Fermé	**Début:**	01/12/2017
Priorité:	Normale	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Backlog	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Déployer et monitorer le certificat SSL pour les sites du Libre en Fête :

- https://www.libre-en-fete.net

- https://2017.libre-en-fete.net (erreur, c'est https://libre-en-fete.net/2017)

- https://2016.libre-en-fete.net

etc

Historique

#1 - 01/12/2017 14:37 - François Poulain

Pour le www c'est déjà en place. Mais la création du site d'archive 2017.libre-en-fete.net nécessite :

- de ré-émettre un certificat TLS;
- d'émettre une conf de monitoring.

Pour le monitoring, c'est du copier/coller. Sur galanga:

```
--- /etc/icinga/objects/hosts/cluster-vms/bastion.cfg
+++ /etc/icinga/objects/hosts/cluster-vms/bastion.cfg
@@ -424,7 +424,7 @@ define service {
        host_name               bastion
        _fqdn                   libre-en-fete.net
        _string                 <title>Libre en Fête
-       _uri                    /2017/
+       _uri                    /2018/
 }

 define service {
@@ -433,7 +433,7 @@ define service {
        host_name               bastion
        _fqdn                   www.libre-en-fete.net
        _string                 <title>Libre en Fête
-       _uri                    /2017/
+       _uri                    /2018/
 }

 define service {
@@ -442,7 +442,7 @@ define service {
        host_name               bastion
        _fqdn                   libre-en-fete.org
        _string                 <title>Libre en Fête
-       _uri                    /2017/
+       _uri                    /2018/
 }

 define service {
@@ -451,7 +451,7 @@ define service {
        host_name               bastion
        _fqdn                   www.libre-en-fete.org
        _string                 <title>Libre en Fête
-       _uri                    /2017/
```

```
+       _uri                    /2018/
 }

 define service {
@@ -460,7 +460,24 @@ define service {
        host_name               bastion
        _fqdn                   spip.libre-en-fete.net
        _string                 <title>Libre en Fête
-       _uri                    /2017/
+       _uri                    /2018/
+}
+
+define service {
+       service_description     Check Secure Web Redirection 2017.libre-en-fete.org
+       use                     secure-web-redir-service
+       host_name               bastion
+       _fqdn                   2017.libre-en-fete.org
+       _redirect               libre-en-fete.org/2017/
+       _status                 302
+}
+
+define service {
+       service_description     Check Forced https 2017.libre-en-fete.net
+       use                     forced-https-service
+       host_name               bastion
+       _fqdn                   2017.libre-en-fete.net
+       _status                 302
 }

 define service {
```

Suivi de systemctl reload icinga.

#2 - 01/12/2017 14:56 - François Poulain

Pour le certificat ssl, ça se joue sur le bastion. Il faut que certbot réissue un certificat valie pour le nouveau domaine **et** pour les anciens domaines déjà utilisés. Il n'y a pas d'option out of the box pour faire ça, donc on va jouer un peu avec un dry-run :

```
certbot --dry-run certonly --renew-with-new-domains --webroot -w /var/www/acme-challenge -d $(awk '$3 ~ /acme-challenge/ {print $1 ","}' /etc/letsencrypt/renewal/libre-en-fete.net.conf | sed 's/\n/ -d /' | tr -d '\n')2017.libre-en-fete.net,2017.libre-en-fete.org
```

On doit voir quelque chose comme :

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-------------------------------------------------------------------------------
You have an existing certificate that contains a portion of the domains you
requested (ref: /etc/letsencrypt/renewal/libre-en-fete.net.conf)

It contains these names: libre-en-fete.net, 2007.libre-en-fete.net,
2007.libre-en-fete.org, 2008.libre-en-fete.net, 2008.libre-en-fete.org,
2009.libre-en-fete.net, 2009.libre-en-fete.org, 2010.libre-en-fete.net,
2010.libre-en-fete.org, 2011.libre-en-fete.net, 2011.libre-en-fete.org,
2012.libre-en-fete.net, 2012.libre-en-fete.org, 2013.libre-en-fete.net,
2013.libre-en-fete.org, 2014.libre-en-fete.net, 2014.libre-en-fete.org,
2015.libre-en-fete.net, 2015.libre-en-fete.org, 2016.libre-en-fete.net,
2016.libre-en-fete.org, libre-en-fete.org, spip.libre-en-fete.net,
spip.libre-en-fete.org, www.libre-en-fete.net, www.libre-en-fete.org

You requested these names for the new certificate: libre-en-fete.org,
2008.libre-en-fete.net, 2013.libre-en-fete.org, spip.libre-en-fete.net,
www.libre-en-fete.org, 2014.libre-en-fete.org, 2008.libre-en-fete.org,
2016.libre-en-fete.org, 2010.libre-en-fete.org, 2009.libre-en-fete.net,
2011.libre-en-fete.net, 2010.libre-en-fete.net, 2015.libre-en-fete.org,
2015.libre-en-fete.net, 2007.libre-en-fete.org, 2012.libre-en-fete.net,
2009.libre-en-fete.org, 2014.libre-en-fete.net, 2007.libre-en-fete.net,
2016.libre-en-fete.net, www.libre-en-fete.net, 2011.libre-en-fete.org,
2012.libre-en-fete.org, 2013.libre-en-fete.net, libre-en-fete.net,
spip.libre-en-fete.org, 2017.libre-en-fete.net, 2017.libre-en-fete.org.

Do you want to expand and replace this existing certificate with the new
certificate?
```

```
-------------------------------------------------------------------------------
(E)xpand/(C)ancel: E
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for libre-en-fete.org
http-01 challenge for 2008.libre-en-fete.net
http-01 challenge for 2013.libre-en-fete.org
http-01 challenge for spip.libre-en-fete.net
http-01 challenge for www.libre-en-fete.org
http-01 challenge for 2014.libre-en-fete.org
http-01 challenge for 2008.libre-en-fete.org
http-01 challenge for 2016.libre-en-fete.org
http-01 challenge for 2010.libre-en-fete.org
http-01 challenge for 2009.libre-en-fete.net
http-01 challenge for 2011.libre-en-fete.net
http-01 challenge for 2010.libre-en-fete.net
http-01 challenge for 2015.libre-en-fete.org
http-01 challenge for 2015.libre-en-fete.net
http-01 challenge for 2007.libre-en-fete.org
http-01 challenge for 2012.libre-en-fete.net
http-01 challenge for 2009.libre-en-fete.org
http-01 challenge for 2014.libre-en-fete.net
http-01 challenge for 2007.libre-en-fete.net
http-01 challenge for 2016.libre-en-fete.net
http-01 challenge for www.libre-en-fete.net
http-01 challenge for 2011.libre-en-fete.org
http-01 challenge for 2012.libre-en-fete.org
http-01 challenge for 2013.libre-en-fete.net
http-01 challenge for libre-en-fete.net
http-01 challenge for spip.libre-en-fete.org
http-01 challenge for 2017.libre-en-fete.net
http-01 challenge for 2017.libre-en-fete.org
Using the webroot path /var/www/acme-challenge for all unmatched domains.
Waiting for verification...
Cleaning up challenges
Unable to clean up challenge directory /var/www/acme-challenge/.well-known/acme-challenge
Generating key (2048 bits): /etc/letsencrypt/keys/0110_key-certbot.pem
Creating CSR: /etc/letsencrypt/csr/0110_csr-certbot.pem

IMPORTANT NOTES:
 - The dry run was successful.
```

Si le résultat est le bon, on peut relancer la commande pour de vrai :

```
certbot certonly --renew-with-new-domains --webroot -w /var/www/acme-challenge -d $(awk '$3 ~ /acme-challenge/
 {print $1 ","}' /etc/letsencrypt/renewal/libre-en-fete.net.conf | sed 's/\n/ -d /' | tr -d '\n')2017.libre-en
-fete.net,2017.libre-en-fete.org
```

Alors on reload nginx et tout devrait aller :

```
systemctl reload nginx
```

#3 - 01/12/2017 14:59 - François Poulain

Et on pense à commiter dans /etc. :)

#4 - 01/12/2017 15:02 - Frédéric Couchet

- Description mis à jour

#5 - 01/12/2017 15:18 - François Poulain

Sur lamp il faut aussi activer le site 2017.libre-en-fete.net. Vu que c'est un spip, on n'a plus un documentroot différent, on fait une simple redirection :

```
--- a/apache2/sites-available/libre-en-fete.net.conf
+++ b/apache2/sites-available/libre-en-fete.net.conf
@@ -1,4 +1,14 @@
 <VirtualHost *:80>
+        ServerName 2017.libre-en-fete.net
+       ServerAlias 2017.libre-en-fete.org
+
+        ErrorLog /var/log/apache2/libre-en-fete.net/libre-en-fete.net-error.log
```

```
+         CustomLog /var/log/apache2/libre-en-fete.net/libre-en-fete.net-access.log combined-proxy
+
+       RedirectMatch 302 ^.* https://libre-en-fete.net/2017/
+</VirtualHost>
+
+<VirtualHost *:80>
          ServerName 2016.libre-en-fete.net
         ServerAlias 2016.libre-en-fete.org
```

Puis

```
systemctl reload apache2
```

#6 - 01/12/2017 15:25 - François Poulain

Nota: on aurait pu tout faire sur le reverse proxy, j'ai séparé entre le proxy et le apache pour maintenir l'homogénéité avec l'historique.

#7 - 01/02/2018 11:22 - François Poulain

- Statut changé de Nouveau à Fermé

#8 - 01/02/2018 11:30 - François Poulain

```
$ for url in https://www.libre-en-fete.net/ https://2017.libre-en-fete.net/ https://libre-en-fete.net/2017 htt
ps://2016.libre-en-fete.net/ ;do  curl -I $url; done
HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Thu, 01 Feb 2018 10:30:19 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive
Location: http://www.libre-en-fete.net/2018/

HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Thu, 01 Feb 2018 10:30:19 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive
Location: https://libre-en-fete.net/2017/

HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Thu, 01 Feb 2018 10:30:19 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive
Location: http://libre-en-fete.net/2017/

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 01 Feb 2018 10:30:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
```