Usando Let's Encrypt con Pandora FMS

El año pasado publicamos un tutorial **no oficial** sobre la instalación de Pandora FMS sobre CentOS 8 Stream y en esta oportunidad vamos a utilizar el popular emisor de certificados gratuitos de **Let's Encrypt**.

¡Recuerden todas y todos el donar a la EFF para que Let's Encrypt pueda sufragar sus gastos de mantenimiento de servidores!

Configurando VirtualHosts en Apache

Pandora FMS utiliza Apache como servidor web y de manera dedicada, es decir, dicho servidor web atiende única y exclusivamente a la Consola web PFMS.

Por lo tanto, y para que sea compatible con **Let's Encrypt**, debemos configurar el uso de anfitriones virtuales. Esencialmente el servidor web lo que hará es analizar la URL que recibe y redirigir al directorio respectivo (cada VirtualHost tiene su propia carpeta). Si desea conocer más acerca de este proceso, visite el siguiente artículo "ENCRYPTED SERVER NAME INDICATION".

> **¡Atención!** Emplearemos la variable $URL para que coloquen su propio dominio web. Debe estar correctamente configurado con 24 horas de anticipación (a veces menos) en los **DNS públicos respectivos** para que Let's Encrypt pueda reconocer el dominio y otorgar un certificado.

Primero crearemos el directorio para el VirtualHost que albergará a Pandora FMS *y luego lo redireccionaremos a la instalación por defecto de PFMS.*

?Pandora FMS siempre trabaja con usuario **root**.?

```
URL="su_dominio_web"
mkdir -p /var/www/$URL
chown -R apache:apache /var/www/$URL
ln -f -s -v /var/www/html/ /var/www/$URL/
chmod -R 755 /var/www
```

Habilitamos los sitios destinados a albergar el VirtualHost:

```
mkdir /etc/httpd/sites-available /etc/httpd/sites-enabled
```

Con su editor de texto favorito edite /etc/httpd/conf/httpd.conf y modifique la siguiente línea (recuerde sustituir $URL por el nombre de su dominio):

```
ServerName $URL:80
```

También agregue al final del fichero esta línea:

```
IncludeOptional sites-enabled/*.conf
```

Guarde y cierre. Edite /etc/httpd/sites-available/$URL.conf y agregue este contenido:

```
    ServerName www.$URL
    ServerAlias $URL
    DocumentRoot /var/www/$URL/html
    ErrorLog /var/www/$URL/html/pandora_console/log/error.log
    CustomLog /var/www/$URL
/html/pandora_console/log/requests.log combined
```

Guarde y cierre. Ahora haga un enlace simbólico de esta configuración (todo esto se hace en el supuesto caso que decida agregar más VirtualHosts, **rogamos dedique siempre un servidor exclusivo para Pandora FMS**):

```
ln -s /etc/httpd/sites-available/$URL
.conf /etc/httpd/sites-enabled/$URL.conf
```

Asegúrese de que solamente PFMS tenga acceso a config.php:

```
chmod 600 /var/www/$URL/html/pandora_console/include/config.php
```

Ya casi para finalizar reinicie el servicio Apache:

```
systemctl restart httpd
```

Comprobación:

Si ha hecho todo correctamente, Apache creará los *logs* respectivos, revise rápidamente con:

```
ls -lZ /var/www/$URL/html/pandora_console/log/
```

Para ver la configuración completa de manera resumida:

apachectl -D DUMP_VHOSTS

Instalando Let's Encrypt

Esto es un truco extraño:

- Pandora FMS al ser instalado con los valores por defecto **deja sin configurar el SSL en el puerto 443, carece de configuración alguna en ese aspecto.**
- Por eso cuando instalemos **Let's Encrypt** lo primero que hará dicho programa es habilitar SSL para un certificado autofirmado **el cual no hemos generado y fallará al tratar de obtener un certificado SSL proporcionado por Let's Encrypt.**
- Pues entonces crearemos nuestro propio certificado digital SSL autofirmado, lo agregaremos a la configuración, instalaremos de nuevo Let's Encrypt, obtendremos un nuevo certificado emitido por una CA de confianza y luego con este nuevo certificado lo pondremos en vez de nuestro certificado autofirmado.
- Lean como se instala y luego vuelven a leer estos párrafos ?.

```
dnf install epel-release
dnf install -y certbot python3-certbot-apache mod_ssl
certbot --apache -d $URL
```

¡Y aquí es donde fallará la instalación de Let's Encrypt!

Genere un certificado autofirmado y cópielo:

```
openssl req -x509 -out localhost.crt -keyout localhost.key \
    -newkey rsa:2048 -nodes -sha256 \
    -subj '/CN=localhost' -extensions EXT -config
```

Aún no hemos terminado, ahora nuestro sitio tiene HTTPS pero todavía está usando el certificado autofirmado.

Edite /etc/httpd/conf.d/ssl.conf y busque las siguientes dos líneas que contengan SSLCertificateFile y SSLCertificateKeyFile y sustituya con lo siguiente:

SSLCertificateFile /etc/letsencrypt/live/$URL/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/$URL/privkey.pem

Reinicie el servidor Apache:

```
systemctl restart httpd
```

De nuevo examine la configuración:

```
apachectl -D DUMP_VHOSTS
```

Fuentes consultadas

- https://pandorafms.com/manual/es/documentation/02_installation/01_installing
- https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-8
- https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-centos-8
- https://letsencrypt.org/docs/certificates-for-localhost/