Guía de Seguridad

Guía Nro.: 2019-01
Fecha de Publicación: 19/03/2019
Tema: Instalación/Renovación de certificado Let's Encrypt en servidor de correo Zimbra

Let's Encrypt es una Autoridad de Certificación (AC, o CA por sus siglas en inglés) que proporciona certificados X.509 gratuitos para el cifrado de Seguridad de nivel de transporte (TLS) a través de un proceso automatizado diseñado para eliminar el complejo proceso actual de creación manual, la validación, firma, instalación y renovación de los certificados de sitios web seguros. Para obtener un certificado para su dominio de sitio web de Let's Encrypt, se debe demostrar control sobre ese dominio.

En esta guía se describe el procedimiento para instalar y/o renovar el certificado de Let's Encrypt en un servidor de correo Zimbra.

Condiciones

1. El servidor donde será instalado no tiene certificado o necesita renovación del certificado
2. Tiene que estar instalado el paquete **certbot**
3. No debe estar ejecutándose ningún servicio sobre el puerto **TCP/80**
4. Si el servidor está detrás de un cortafuegos (*firewall*) deberá realizarse un ***PAT*** *(Port Address Translation*) al puerto **TCP/80** del servidor de correo

Procedimiento

1. Detener los servicios involucrados **(**usuario**: zimbra):**

```
zmproxyctl stop
zmmailboxdctl stop
```

En caso de querer realizar una instalación de certificado:

2. Generar el certificado **(**usuario**: root):**

```
certbot certonly
```

En caso de querer realizar una Renovación de certificado:

3. Renovar el certificado (usuario: **root**):

```
certbot renew
```

4. Adicionar el CA_ROOT del Let's Encrypt (usuario: **root**) al archivo **chain.pem** (**/etc/letsencrypt/live/$HOSTNAME/chain.pem)**

   Archivo CA_ROOT

```
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVow
PzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD
Ew5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O
rz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq
OLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9b
xiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw
7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD
aeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG
SIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69
ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXr
AvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz
R8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5
JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo
Ob8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----
```

5. Copiar el certificado privado generado (usuario: **root**)

```
cp /etc/letsencrypt/live/$HOSTNAME/privkey.pem
                /opt/zimbra/ssl/zimbra/commercial/commercial.key
```

6. Aplicar el certificado al Zimbra (usuario:**zimbra**)

```
cd /etc/letsencrypt/live/$HOSTNAME
/opt/zimbra/bin/zmcertmgr deploycrt comm cert.pem chain.pem
```

7. Reiniciar el servicio del Zimbra (usuario:**zimbra**)

```
zmcontrol restart
```

letsencrypt-zimbra.sh

script **bash** que hace todo el procedimiento en forma desatendida

```
#!/usr/bin/bash

OS_RELEASE=`rpm -q centos-release | sed "s/\(^centos-release-[0-9]\)\-.*/\1/"`
no_centos () {
  echo "El SO actualmente soportado es el Centos Linux" ; exit
}

[ -z $OS_RELEASE ] && no_centos

case $OS_RELEASE in
    centos-release-6) ;;
    centos-release-7) ;;
    *) no_centos ;;
esac

CA_ROOT=/tmp/letsencrypt.$$


CA_ROOT=/tmp/letsencrypt.$$

#temporal para el certificado
cat > $CA_ROOT <<EOT
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVow
PzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD
Ew5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O
rz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq
OLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9b
xiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw
7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD
aeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG
SIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69
ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXr
AvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz
R8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5
JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo
Ob8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----
EOT

echo "1. Deteniendo los servicios involucrados (usuario: zimbra)"
$TEST su - zimbra -c "zmproxyctl stop"
$TEST su - zimbra -c "zmmailboxdctl stop"

echo "Instalar/Renovar el certificado Let's Encrypt (usuario:root"
echo "1. Instalar"
echo "2. Renovar"
read opt
```

```
case $opt in
  1) certbot certonly
     ;;
  2) certbot renew
     ;;
  *) exit
     ;;
esac

echo "3. Adicionar el CA_ROOT del Let's Encrypt (usuario: root) al archivo chain.pem"
cat $CA_ROOT >> /etc/letsencrypt/live/$HOSTNAME/chain.pem
rm $CA_ROOT

echo "4. Copiar el certificado privado generado (usuario: root)"
cp /etc/letsencrypt/live/$HOSTNAME/privkey.pem /opt/zimbra/ssl/zimbra/commercial/commercial.key

echo "5. Aplicar el certificado al Zimbra (usuario:zimbra)"
case $OS_RELEASE in
    centos-release-6)
        cd /etc/letsencrypt/live/$HOSTNAME ; /opt/zimbra/bin/zmcertmgr deploycrt comm cert.pem chain.pem
        ;;
    centos-release-7)
        su - zimbra -c "cd /etc/letsencrypt/live/$HOSTNAME ; /opt/zimbra/bin/zmcertmgr deploycrt comm
cert.pem chain.pem"
        ;;
    *) no_centos ;;
esac

echo "6. Reiniciar el servicio del Zimbra (usuario: zimbra)"
su - zimbra -c  "zmcontrol restart"

echo "7. Todo hecho"
```

Fuente:

https://www.jorgedelacruz.es/2015/12/09/zimbra-instalando-un-certificado-gratuito-ssl-lets-encrypt/