Let's Encrypt: Linux

Julian F. Latorre

22 de noviembre de 2024

Índice

1. Implementación Detallada de Let's Encrypt

1.1. Introducción a Let's Encrypt

Let's Encrypt es una Autoridad de Certificación (CA) gratuita, automatizada y abierta que proporciona certificados SSL/TLS para habilitar HTTPS en

sitios web. Su objetivo es hacer que HTTPS sea accesible para todos, simplificando el proceso de obtención y renovación de certificados.

1.2. Conceptos Clave

- **ACME (Automatic Certificate Management Environment)**: Protocolo utilizado por Let's Encrypt para verificar el control de un dominio y emitir certificados.
- **Certbot**: Cliente ACME de código abierto para automatizar la obtención y renovación de certificados Let's Encrypt.
- **Desafío HTTP-01**: Método de validación donde Let's Encrypt verifica el control del dominio solicitando un archivo específico a través de HTTP.
- **Desafío DNS-01**: Método de validación donde Let's Encrypt verifica el control del dominio mediante un registro TXT en el DNS.

1.3. Preparación del Servidor

Antes de comenzar, asegúrese de que su servidor cumpla con los siguientes requisitos:

- Sistema operativo compatible (Linux recomendado)
- Acceso root o sudo
- Puerto 80 (HTTP) accesible para la validación
- Puerto 443 (HTTPS) abierto para servir contenido seguro
- Servidor web instalado (Apache, Nginx, etc.)

1.4. Instalación de Certbot

1.4.1. En sistemas basados en Debian/Ubuntu

```
sudo apt update
sudo apt install certbot
```

1.4.2. En sistemas basados en CentOS/RHEL

```
sudo yum install epel-release
sudo yum install certbot
```

1.5. Obtención de Certificados

1.5.1. Para Apache

```
sudo certbot --apache -d ejemplo.com -d www.ejemplo.com
```

1.5.2. Para Nginx

```
sudo certbot --nginx -d ejemplo.com -d www.ejemplo.com
```

1.5.3. Obtención manual (sin modificar la configuración del servidor web)

```
sudo certbot certonly --standalone -d ejemplo.com -d www.ejemplo.
    com
```

1.6. Configuración del Servidor Web

1.6.1. Apache

Edite el archivo de configuración de su sitio virtual:

```
sudo nano /etc/apache2/sites-available/ejemplo.com.conf
```

Agregue o modifique las siguientes líneas:

```
<VirtualHost *:443>
    ServerName ejemplo.com
    DocumentRoot /var/www/ejemplo.com
    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/ejemplo.com/fullchain.
    pem
    SSLCertificateKeyFile /etc/letsencrypt/live/ejemplo.com/privkey
    .pem
</VirtualHost>
```

1.6.2. Nginx

Edite el archivo de configuración de su sitio:

```
sudo nano /etc/nginx/sites-available/ejemplo.com
```

Agregue o modifique las siguientes líneas:

```
server {
    listen 443 ssl;
    server_name ejemplo.com www.ejemplo.com;
    ssl_certificate /etc/letsencrypt/live/ejemplo.com/fullchain.pem
    ;
    ssl_certificate_key /etc/letsencrypt/live/ejemplo.com/privkey.
    pem;
    # Otras configuraciones...
}
```

1.7. Renovación Automática de Certificados

Let's Encrypt recomienda renovar los certificados cada 60 días. Para automatizar este proceso:

1.7.1. Crear un script de renovación

Cree un archivo llamado `renew-certs.sh`:

```
#!/bin/bash
certbot renew --quiet --no-self-upgrade
systemctl reload apache2  # O 'nginx' si usa Nginx
```

Haga el script ejecutable:

```
chmod +x renew-certs.sh
```

1.7.2. Configurar Cron Job

Edite el crontab:

```
sudo crontab -e
```

Agregue la siguiente línea para ejecutar el script dos veces al día:

```
0 0,12 * * * /ruta/al/renew-certs.sh
```

1.8. Solución de Problemas Comunes

- **Error de conexión**: Asegúrese de que los puertos 80 y 443 estén abiertos en su firewall.
- **Fallo en la validación del dominio**: Verifique que su servidor sea accesible públicamente y que el dominio apunte correctamente a su IP.
- **Errores de permisos**: Asegúrese de ejecutar Certbot con privilegios sudo.
- **Certificado no se renueva**: Verifique los logs de Certbot y asegúrese de que el cron job esté configurado correctamente.

1.9. Mejores Prácticas

- Implemente HSTS (HTTP Strict Transport Security) para forzar conexiones HTTPS.
- Configure la redirección de HTTP a HTTPS.
- Mantenga su sistema y Certbot actualizados.
- Monitoree regularmente la validez de sus certificados.
- Utilice el modo de prueba de Let's Encrypt para experimentar sin afectar los límites de tasa.

1.10. Implementación en Entornos Específicos

1.10.1. Servidores Virtuales Privados (VPS)

Siga los pasos generales mencionados anteriormente. Asegúrese de tener acceso root y de que su proveedor de VPS permita la modificación de la configuración del servidor web.

1.10.2. Plataformas de Alojamiento Compartido

Muchos proveedores de alojamiento compartido ofrecen integración con Let's Encrypt a través de su panel de control. Consulte la documentación de su proveedor para obtener instrucciones específicas.

1.10.3. Contenedores Docker

Para implementar Let's Encrypt en contenedores Docker, considere usar la imagen oficial de Certbot:

```
docker run -it --rm --name certbot \
    -v "/etc/letsencrypt:/etc/letsencrypt" \
    -v "/var/lib/letsencrypt:/var/lib/letsencrypt" \
    certbot/certbot certonly
```