**Renew LetsEncrypt SSL Certificate on LightSail Instance**

To renew the LetsEncrypt certificates, run the original command used to obtain them.

**Step 1**: Before Renewing SSL certificate, stop all the services running in the instance by using following command.

***sudo /opt/bitnami/ctlscript.sh stop***

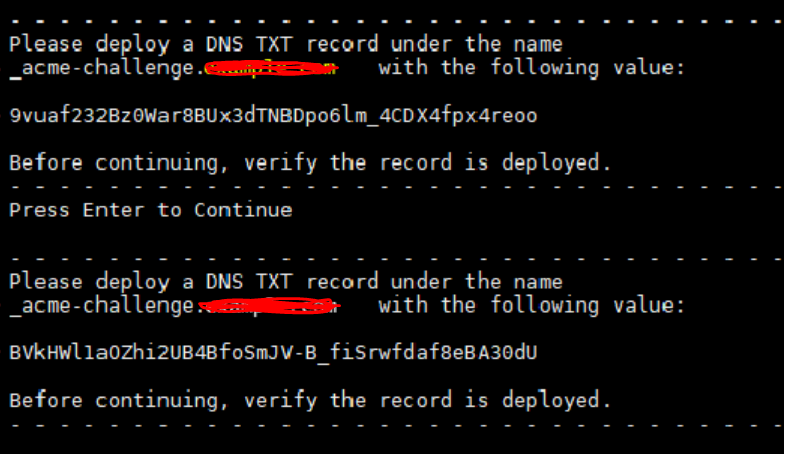
**Step 2**: Enter the following commands to set an environment variable for your domain.

***DOMAIN=indeez.eu***

***echo $DOMAIN***

***sudo certbot -d $DOMAIN --manual --preferred-challenges dns certonly***

Let’s Encrypt now prompts you to verify that you own the domain specified. You do this by adding TXT records to the DNS records for your domain.

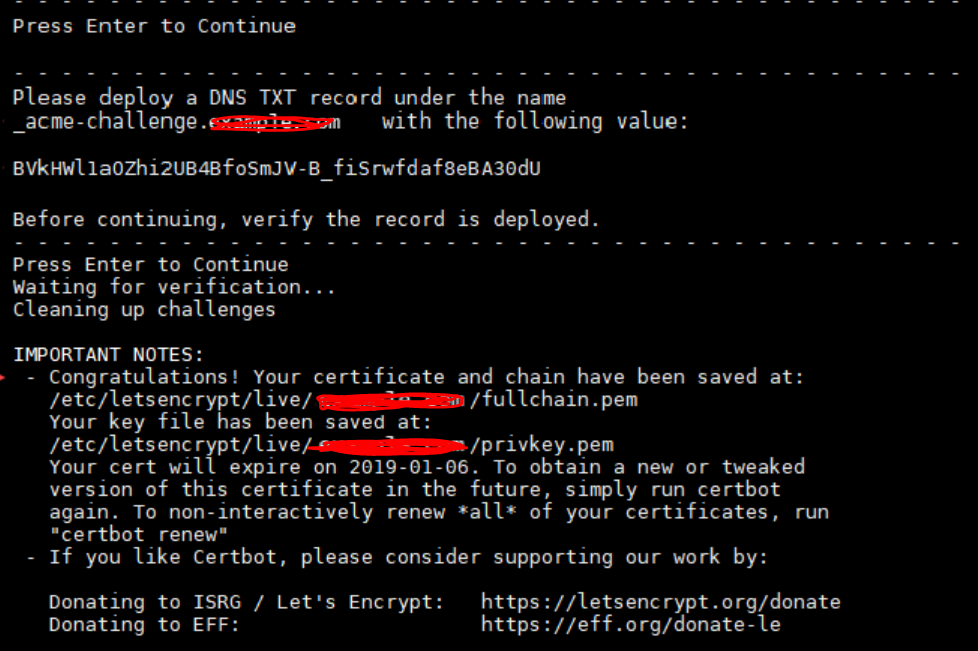


**Step 3**: Adding a TXT record in AWS Route 53 for the hosted Zone “Indeez.eu”.

**\_acme-challenge.indeez.eu à TXT à “Value”**

**Step 4**: Confirm that the TXT records have propagated. Use the MxToolbox utility to confirm that the TXT records have propagated to the internet’s DNS.

**Step 5**: Go back to the Lightsail browser based SSH session for your WordPress instance and complete the LetsEncrypt certificate request. Certbot saves your SSL certificate, chain, and key files to a specific directory on your WordPress instance.



**Step 6**: Create links to the Let’s Encrypt SSL certificate files in the Apache server directory on WordPress instance.

***sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/server.crt.old***

***sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/server.key.old***

***sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/server.key***

***sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/conf/server.crt***

***sudo /opt/bitnami/ctlscript.sh start***

