SSL Certificate renewals in HAProxy based Load-Balancer

- Login to HAProxy VM
- Execute certbot --dry-run command
  `sudo certbot renew --dry-run --cert-name <domain_name>`

  Fix errors if you receive any issues apart from Port Binding errors

```
[bala@argoid-saas-prod1-host-043 ~]$ sudo certbot renew --dry-run --cert-name prod.azadea.saas.argoid.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Processing /etc/letsencrypt/renewal/prod.azadea.saas.argoid.com.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Cert not due for renewal, but simulating renewal for dry run
Plugins selected: Authenticator standalone, Installer None
Starting new HTTPS connection (1): acme-staging-v02.api.letsencrypt.org
Simulating renewal of an existing certificate for prod.azadea.saas.argoid.com
Performing the following challenges:
http-01 challenge for prod.azadea.saas.argoid.com
Cleaning up challenges
Failed to renew certificate prod.azadea.saas.argoid.com with error: Problem binding to port 80: Could not bind to IPv4 or IPv6.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
All simulated renewals failed. The following certificates could not be renewed:
  /etc/letsencrypt/live/prod.azadea.saas.argoid.com/fullchain.pem (failure)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1 renew failure(s), 0 parse failure(s)
[bala@argoid-saas-prod1-host-043 ~]$
```

- Stop HAProxy service(docker container) if HAProxy has acquired Port 80
- Install new certificates
  `sudo certbot renew --cert-name <domain_name>`
- Start back the HAProxy service
- Check for SSL certificate volume mounts of HAProxy container by using command
  `sudo docker inspect <container_name> | jq .[0] | jq .HostConfig.Binds`

Usually, SSL certificate will be mounted with option `"/etc/letsencrypt/live/:/etc/letsencrypt/live/"` OR `"/etc/ssl:/etc/ssl"`

```
[bala@argoid-saas-prod1-host-043 ~]$ sudo docker inspect haproxy-container | jq .[0] | jq .HostConfig.Binds
[
  "/etc/haproxy:/usr/local/etc/haproxy:ro",
  "/etc/letsencrypt/live/:/etc/letsencrypt/live/"
]
[bala@argoid-saas-prod1-host-043 ~]$
[bala@argoid-saas-prod1-host-043 ~]$
```

OR

```
[manjunath@argoid-saas-prod1-host-015 ~]$ sudo docker inspect haproxy | jq .[0] | jq .HostConfig.Binds
[
  "/etc/haproxy:/usr/local/etc/haproxy:ro",
  "/etc/ssl:/etc/ssl"
]
[manjunath@argoid-saas-prod1-host-015 ~]$
```

- Check for SSL config setting in `haproxy.cfg` config file using command
  `grep -r "ssl crt" /etc/haproxy/haproxy.cfg`

```
[bala@argoid-saas-prod1-host-043 ~]$ grep -r "ssl crt" /etc/haproxy/haproxy.cfg
   bind *:443 ssl crt /etc/letsencrypt/live/prod.azadea.saas.argoid.com/prod.azadea.saas.argoid.com.pem
[bala@argoid-saas-prod1-host-043 ~]$
```

  OR

```
[manjunath@argoid-saas-prod1-host-015 ~]$ grep -r "ssl crt" /etc/haproxy/haproxy.cfg
   bind *:8443 ssl crt /etc/ssl/prod.rarerabbit.saas.argoid.com.pem
```

- Create new certificate file `<domain_name>.pem` by merging `fullchain.pem` and `privkey.pem` certificates
  Login as root user (not with sudo)

```
[root@argoid-saas-prod1-host-043 ~]#cat /etc/letsencrypt/live/prod.
azadea.saas.argoid.com/fullchain.pem /etc/letsencrypt/live/prod.
azadea.saas.argoid.com/privkey.pem  > /etc/letsencrypt/live/prod.
azadea.saas.argoid.com/prod.azadea.saas.argoid.com.pem
```

OR

```
[root@argoid-saas-prod1-host-015 ~]#cat /etc/letsencrypt/live/prod.
rarerabbit.saas.argoid.com/fullchain.pem /etc/letsencrypt/live/prod.
rarerabbit.saas.argoid.com/privkey.pem  > /etc/ssl/prod.rarerabbit.saas.
argoid.com.pem
```

- Restart HAProxy Docker conatiners
- To check whether the certificate has been renewed or not..

```
echo | openssl s_client -servername <domain_name>  -connect
<domain_name>:443 2>/dev/null | openssl x509 -noout -dates ; echo -e ""
```

This will give the cert expiry date..