LET’S ENCRYPT SSL CERTIFICATE

Cognitive Assistant for Networks (CAN) Release 5.5

JULY 22, 2021

AVANSEUS TECHNOLOGY PVT. LTD.

REVISION HISTORY

Version	Date	Change description	Created by	Updated by	Reviewed by
V 1.0	July, 2021	Initial Release	Sunil	Sandeep Singh	Chiranjib

Table of Contents

1. Introduction

This document is generic and is applicable for all type of deployments i.e. VM based deployment and Kubernetes based deployment.

2. To install Let's Encrypt SSL certificate in RHEL Server

Follow the steps:

1. Install snapd

   For RHEL 7

   ```
   sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
   sudo yum -y upgrade
   sudo yum -y install snapd
   sudo systemctl enable --now snapd.socket
   sudo ln -s /var/lib/snapd/snap /snap
   ```

   For RHEL 8

   ```
   sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   sudo dnf -y upgrade
   sudo dnf -y install snapd
   sudo systemctl enable --now snapd.socket
   sudo ln -s /var/lib/snapd/snap /snap
   ```

2. Ensure that your version of snapd is up to date

   ```
   sudo snap install core; sudo snap refresh core
   ```

   Note: If this command is not working then enter the same command again. It will work for the second time.

3. Install certbot using the below command

   ```
   sudo snap install --classic certbot
   sudo ln -s /snap/bin/certbot /usr/bin/certbot
   ```

4. Install SSL certificate using the below command. During installation, it will ask for email and domain. It will ask again for sharing your email id to them. Deny the sharing option with entering no.

   ```
   sudo certbot certonly --apache  //This is for apache server.
   ```

5. SSL certificates will be stored under /etc/letsencrypt/live directory. Put the SSL certificates path in ssl.conf file for the required properties.

   ```
   vi   /etc/httpd/conf.d/ssl.conf
   SSLCertificateFile /etc/letsencrypt/live/<domain>/cert.pem
   SSLCertificateKeyFile /etc/letsencrypt/live/<domain>/privkey.pem
   SSLCertificateChainFile /etc/letsencrypt/live/<domain>/chain.pem
   ```

   Save the file.

6. After saving, restart the apachectl

   ```
   apachectl restart
   apachectl status
   ```

```
apachectl configtest  //Check this by logging into the root user
```

7. To test automatic renewal run this command

```
sudo certbot renew --dry-run
```

8. Check the expiry dates of the certificate using the below command

```
sudo openssl x509 -noout -dates -in /etc/letsencrypt/live/<domain>/cert.pem
```