How to install a LetsEncrypt SSL certificate in VoipNow

Applies to VoipNow 5.5.0 and higher installed on CentOS Linux 8!

Let's Encrypt is a free, open initiative to provide SSL certificates for websites with the purpose of enabling the adoption of encrypted communications. It's completely free (for now, at least) and you can use it with VoipNow following the steps described below.

Please note, however, that this is a domain-validated certificate. The only criteria to get a valid SSL certificate is the proof of some form of control over that domain. It could be a custom DNS TXT record, a response to an administrative email for that domain and so on.

This type of certificate **does not ensure** that a particular legal entity is connected to that domain (i.e. somebody can register the m1crosoft.com domain, request a SSL certificate and everything will be technically correct, while in real life an Extended Validation certificate wouldn't be granted). Basically, this article helps you get rid of the "insecure page" warning displayed by browsers.

Step-by-step guide

Before you start, make sure you know your VoipNow server's DNS hostname and IP address. Also, check that your DNS is correctly configured and pointing to your VoipNow server's IP address.

This guide will use `sip.voipnowserver.com` and `172.173.174.175` as place holders for your VoipNow host name and IP address. Make sure to replace them with the correct values.

Download the required files

This KB article will assume the EPEL repo is not installed and enabled on the current machine. For installing Certbot, you need the EPEL repo and for that run the following command. In case EPEL is already installed, you can skip to the second step and install Certbot.

```
# yum -y install epel-release
```

Install the Certbot rpm file.
yum -y install certbot
Let's start

For the sake of simplicity, we will export an environment variable that will hold the actual name of the domain for which a SSL certificate will be generated. This can be easily, done by running the following command:

DOMAIN='sip.voipnowserver.com'
Now we are ready to run Certbot and create the SSL certificate for the domain contained in the ${DOMAIN} variable defined above. Here is the command:

```
certbot --standalone certonly --pre-hook='systemctl stop crond && service httpsa stop && cp -p /etc/voipnow/certs
/http.pem /etc/voipnow/certs/http.pem.bkp' --post-hook="cat /etc/letsencrypt/live/${DOMAIN}/privkey.pem /etc
/letsencrypt/live/${DOMAIN}/fullchain.pem > /etc/voipnow/certs/http.pem && service httpsa start && systemctl
start crond" -d ${DOMAIN}
```

You might be prompted to provide a valid email address and accept the legal terms. Proceed as required and the script should continue. At the end, you will see something like this:

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/sip.voipnowserver.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/sip.voipnowserver.com/privkey.pem
   Your certificate will expire on 2021-06-14. To obtain a new or
   tweaked version of this certificate in the future, simply run
   certbot again. To non-interactively renew *all* of your
   certificates, run "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

The above command has two important sections defined by the pre-hook and post-hook parameters. In order to generate a certificate you must stop the web interface of the server making sure that it doesn't get started by the monitoring script. This is achieved in the pre-hook section:

```
systemctl stop crond
service httpsa stop
cp -p /etc/voipnow/certs/http.pem /etc/voipnow/certs/http.pem.bkp
```

There are 3 actions that are executed before the actual certificate generation starts. These are:

- Stop the crond daemon for being sure that the srvmonitor script will not start the web interface service during the certificate generation.

- Stop the web interface, httpsa process.
- Make a backup copy of the existing SSL certificate.

At the end of the process we have a valid SSL certificate that must be installed before starting the web interface. These steps are done in the post-hook section, as follows:

```
cat /etc/letsencrypt/live/${DOMAIN}/privkey.pem /etc/letsencrypt/live/${DOMAIN}/fullchain.pem > /etc/voipnow/certs/http.pem
service httpsa start
systemctl start crond
```

The same as the pre-hook section, we have 3 actions that are automatically executed at the end of the process. These are as follow, in this order:

- Assemble the SSL certificate by copying the generated files, private key and SSL certificate, in the file used by the VoipNow web interface for loading the SSL certificate.
- Start the web interface, the httpsa process like in the previous section.
- Start the crond daemon.

Let's check the SSL certificates

This can be easily done by running the following command:

```
certbot certificates
```

The output of the above command contains all the information about the existing certificate, including the expiry date. This way, we know when we have to renew the SSL certificate:

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Found the following certs:
  Certificate Name: sip.voipnowserver.com
    Serial Number: 34c43ee6cf18b9dd868fd5316f2d92176ca
    Key Type: RSA
    Domains: sip.voipnowserver.com
    Expiry Date: 2021-06-14 08:52:43+00:00 (VALID: 89 days)
    Certificate Path: /etc/letsencrypt/live/sip.voipnowserver.com/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/sip.voipnowserver.com/privkey.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Let's renew the expired SSL certificate

The free SSL certificates are valid for 90 days. In order to renew the existing certificates, just run the following command:

certbot renew
In case the process succeeds, you will end up having a valid certificate, the pre-hook and post-hook actions will be also executed automatically by the renewal process.

Related articles

- How to install a LetsEncrypt SSL certificate in VoipNow
- How to change the SSL certificate in VoipNow
- How to change my 4PSA DNS Manager HTTP server SSL certificate
- Where can I find the VoipNow certificates
- Fail2Ban for Kamailio on VoipNow