Generate And Install A Let's Encrypt SSL Certificate For A Bitnami Application

Introduction

Let's Encrypt (https://letsencrypt.org) is a free Certificate Authority (CA) that issues SSL certificates. You can use these SSL certificates to secure traffic to and from your Bitnami application host.

This guide walks you through the process of generating a Let's Encrypt SSL certificate for your domain and installing and configuring it to work with your Bitnami application stack.

Assumptions And Prerequisites

This guide assumes that:

- You have deployed a Bitnami application and the application is available at a public IP address.
- You have the necessary credentials to log in to the Bitnami application instance.
- You own a domain name.
- You have configured the domain name's DNS record to point to the public IP address of your Bitnami application instance.

Step 1: Install The Certbot Client

The Certbot (https://certbot.eff.org) client simplifies the process of Let's Encrypt certificate generate. To use it, follow these steps:

- Log in to the server console as the *bitnami* user.
- Run the following commands to install the Certbot client:

```
$ sudo mkdir /opt/bitnami/letsencrypt
$ cd /opt/bitnami/letsencrypt
$ sudo wget https://dl.eff.org/certbot-auto
$ sudo chmod a+x ./certbot-auto
$ sudo ./certbot-auto
```

The *certbot-auto* script will download all the necessary dependencies and also request root privileges to run the client. During this process, you may see an error message similar to the following:

```
Failed to find executable apache2ctl in PATH...
Certbot doesn't know how to automatically configure the web server on this system. However, it can still get a certificat
e for you. Please run "certbot-auto certonly" to do so. You'll need to manually configure your web server to use the resu
lting certificate.
```

This message can be safely ignored.

Step 2: Generate A Let's Encrypt Certificate For Your Domain

NOTE: Before proceeding with this step, ensure that your domain name points to the public IP address of the Bitnami application host.

The next step is to generate a Let's Encrypt certificate for your domain.

- Turn off all Bitnami services:

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

- Change to the directory containing the Certbot client.

```
$ cd /opt/bitnami/letsencrypt
```

- Request a new certificate for your domain as below. Remember to replace the DOMAIN placeholder with your actual domain name, and the APPNAME placeholder with the path to your application.

```
$ sudo ./certbot-auto certonly --standalone -d DOMAIN
```

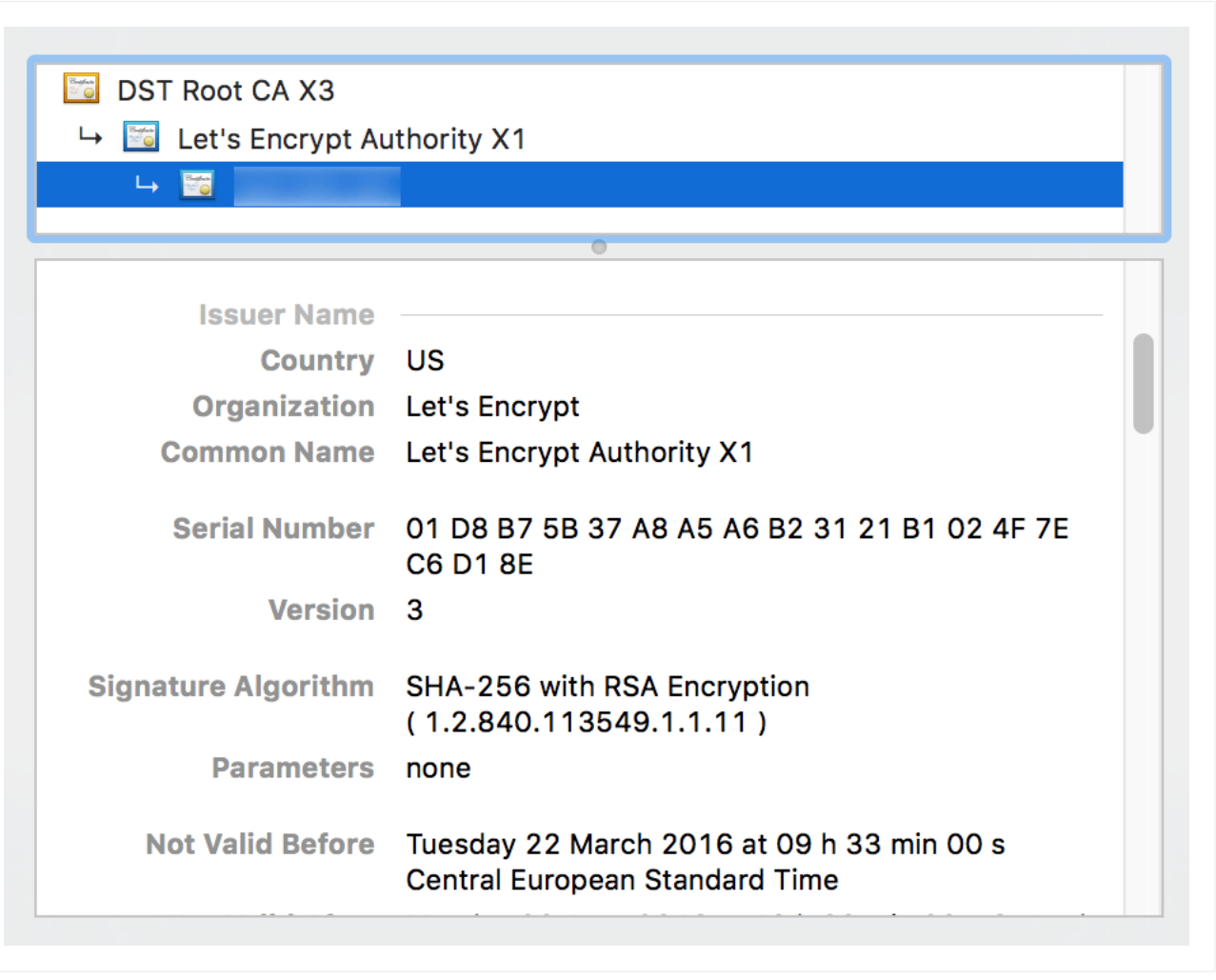
> TIP: Let's Encrypt has an issuance limit of 5 certificates per domain per week. To create a test certificate, add the *--test-cert* option to the previous command.

- Enter basic information, including your email address, and agree to the terms of service.

A set of certificates will now be generated, typically in the */etc/letsencrypt/live/DOMAIN* directory. This set includes the server certificate file *cert.pem* and the server certificate key file *privkey.pem*.

An output message will provide some information, including the expiry date of the certificate. Note this expiry date carefully as you will need to renew your certificate before that date in order for it to remain valid.

An example certificate is shown below:



(/images/img/how_to_guides/generate-install-lets-encrypt-ssl/lets-encrypt-1-8c5a8b36.png)

Step 3: Configure The Web Server To Use The Let's Encrypt Certificate

Next, tell the Web server about the new certificate, as follows:

- Link the new SSL certificate and certificate key file to the correct locations, depending on which Web server you're using. Update the file permissions to make them readable by the root user only. Remember to replace the DOMAIN placeholder with your actual domain name.

  For Apache:

  ```
  $ 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 mv /opt/bitnami/apache2/conf/server.csr /opt/bitnami/apache2/conf/server.csr.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 chown root:root /opt/bitnami/apache2/conf/server*
  $ sudo chmod 600 /opt/bitnami/apache2/conf/server*
  ```

  For nginx:

  ```
  $ sudo mv /opt/bitnami/nginx/conf/server.crt /opt/bitnami/nginx/conf/server.crt.old
  $ sudo mv /opt/bitnami/nginx/conf/server.key /opt/bitnami/nginx/conf/server.key.old
  $ sudo mv /opt/bitnami/nginx/conf/server.csr /opt/bitnami/nginx/conf/server.csr.old
  $ sudo ln -s /etc/letsencrypt/live/DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/server.crt
  $ sudo ln -s /etc/letsencrypt/live/DOMAIN/privkey.pem /opt/bitnami/nginx/conf/server.key
  $ sudo chown root:root /opt/bitnami/nginx/conf/server*
  $ sudo chmod 600 /opt/bitnami/nginx/conf/server*
  ```

  > TIP: To find out if your Bitnami stack uses Apache or nginx, check the output of the command *sudo /opt/bitnami/ctlscript.sh status*.

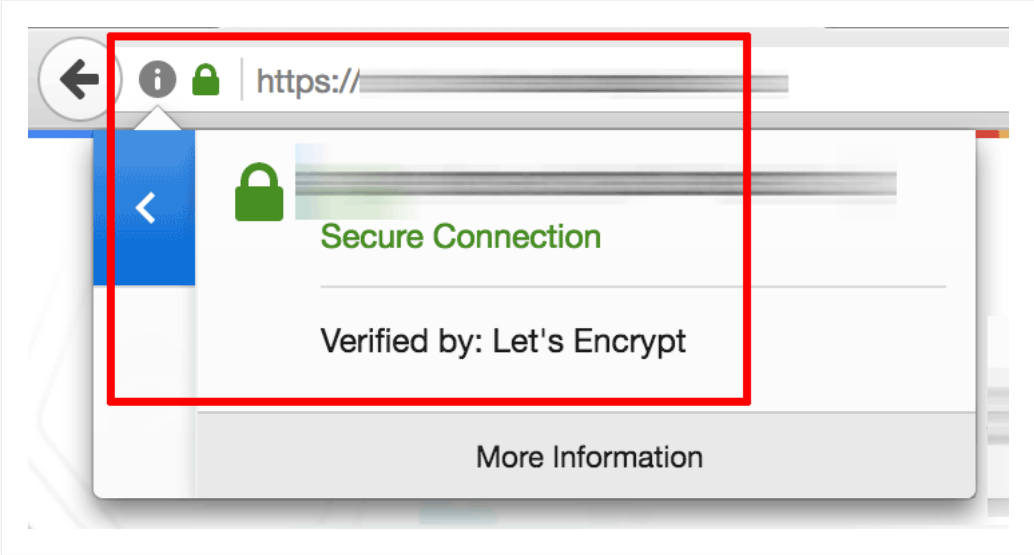
- Restart all Bitnami services:

  ```
  $ sudo /opt/bitnami/ctlscript.sh start
  ```

Step 4: Test The Configuration

After reconfirming that your domain name points to the public IP address of the Bitnami application instance, you can test it by browsing to *https://DOMAIN* (replace the DOMAIN placeholder with the correct domain name).

This should display the secure welcome page of the Bitnami application. Clicking the padlock icon in the browser address bar should display the details of the domain and SSL certificate.



(/images/img/how_to_guides/generate-install-lets-encrypt-ssl/lets-encrypt-2-21489962.png)

Step 5: Renew The Let's Encrypt Certificate

Let's Encrypt certificates are only valid for 90 days. To renew the certificate before it expires, run the following command from the server console as the *bitnami* user:

```
$ cd /opt/bitnami/letsencrypt
$ sudo ./certbot-auto renew
```

To automatically renew your certificates before they expire, schedule a *cron* job. The Certbot documentation (https://certbot.eff.org/all-instructions/) recommends running the *cron* job twice a day, at a random minute within the hour. To do this:

- Execute the following command to open the crontab editor:

```
$ sudo crontab -e
```

- Add the following lines to the crontab file and save it:

```
24  0 * * * /opt/bitnami/letsencrypt/certbot-auto renew
16 12 * * * /opt/bitnami/letsencrypt/certbot-auto renew
```

To learn more about the topics discussed in this guide, consider visiting the following links:

- Certbot documentation (https://certbot.eff.org/docs/)
- Let's Encrypt documentation (https://letsencrypt.org/docs/)
- Bitnami documentation for Apache (/general/components/apache)
- Bitnami documentation for nginx (/general/components/nginx)