Installing an SSL Certificate on AlmaLinux9 Running Nginx

Goal:

The goal of this project is to install a valid SSL Certificate on a AlmaLinux9 server running the Nginx web server.

We will be using Let's Encrypt to obtain a certificate for our domain. Let's Encrypt is an open-source Certificate Authority (CA) that issues SSL certificates for free.

Background and Prerequisites:

This tutorial assumes you are using an AlmaLinux 9 system on the public Internet with a valid DNS A or CNAME record. An A record simply maps a domain name to the IP address of the device hosting that domain. A CNAME, which stands for Canonical Name, is an alias for another domain.

In order to install an SSL certificate, you must have a Web Server installed on your system. In this tutorial, we will install Nginx as our Web Server.

NOTE: *This tutorial demonstrates the installation of an SSL certificate for the demo.linuxtrainingacademy.com domain. Even though this domain will be used throughout this tutorial,* ***you must use your own domain*** *when following along.*

Instructions:

Step 1: Connect to the Server as Root

Many of the commands you will be executing will require root privileges. Connect to your Linux server as the root user. If you log with another account, switch to the root account. You can switch to the root account with the "`su`" command:

```
su -
```

Step 2: Install and Configure the Nginx Web Server

The first step is to ensure that the system is up to date. Run the following command to install the latest updates:

```
dnf update -y
```

Now, install the Nginx Web Server:

```
dnf install -y nginx
```

Next, you need to replace a line in the `/etc/nginx/nginx.conf` file. Open it with your favorite editor.

```
nano /etc/nginx/nginx.conf
```

(NOTE: You can install nano with the "`dnf install -y nano`" command.)

Find the line that reads:

```
server_name _;
```

Change "_" to your domain name. Make sure to include the semicolon (;) after your domain at the end of the line:

```
server_name demo.linuxtrainingacademy.com;
```

Check for any syntax errors or typing mistakes with this command:

```
nginx -t
```

If you get a message such as "test failed", fix your edits in the `/etc/nginx/nginx.conf` file and try again.

You want to ensure that the web server starts on boot, so you need to enable it. Also, you will want to start it now, so you can use the following command to achieve both of those steps.

```
systemctl enable --now nginx
```

You can verify the web server started by checking its status.

```
systemctl status nginx
```

If Nginx is running properly, you will see something like this:

You can also use the "`is-active`" option to "`systemctl`" to see if it is running.

```
systemctl is-active nginx
```

Step 3: Allow Inbound HTTP and HTTPS Traffic

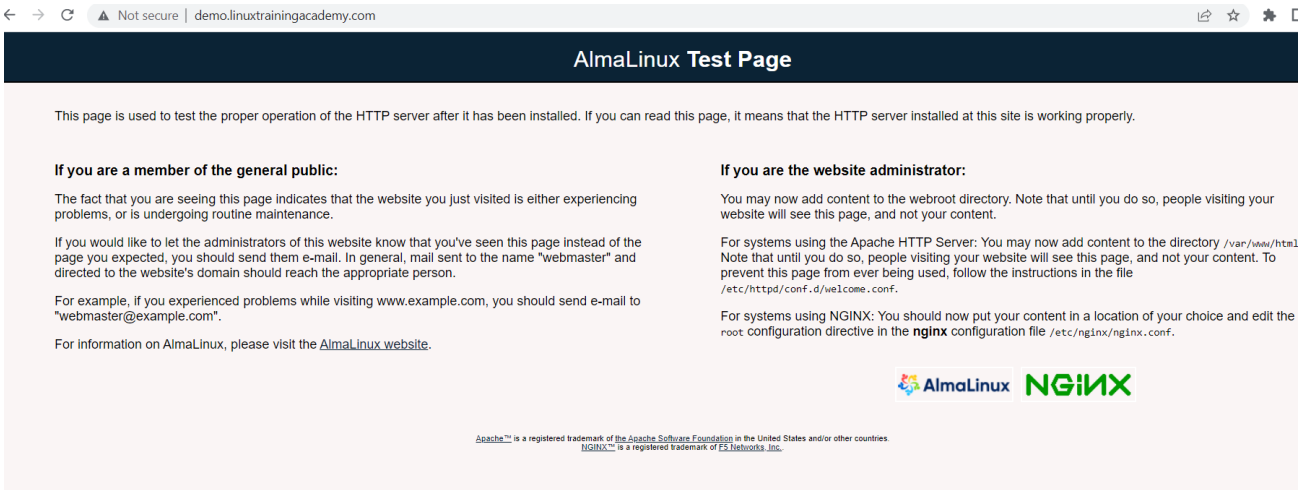
If you are using the local Linux firewall, run the following commands to allow HTTP and HTTPS traffic:

```
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

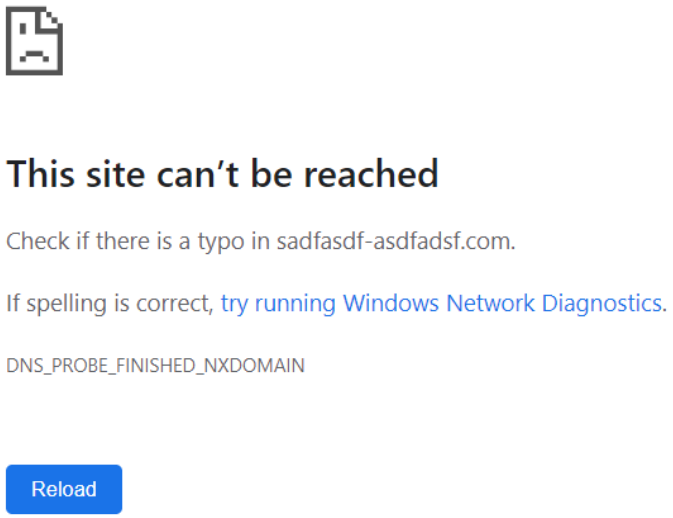
Step 4: Test the Web Server

Open up a web browser and connect to your domain name. In this example, I am using http://demo.linuxtrainingacademy.com, but use your domain.

At this point, you should see a test page:



If you type your domain name with https, for example https://demo.linuxtrainingacademy.com , you will see that the web page will not open. This is because Nginx is only configured to allow HTTP traffic by default.



Step 8: Install snapd

Snapd is not available in the default repository, so we need to add the EPEL repository with the following command:

```
dnf install -y epel-release
```

Now you can install the `snapd` package:

```
dnf install -y snapd
```

Next, enable the `systemd` unit that manages the main snap communication socket:

```
systemctl enable --now snapd.socket
```

Now, enable classic snap support:

```
ln -s /var/lib/snapd/snap /snap
```

Step 9: Install the Certbot Application

Use snap to install certbot:

```
snap install --classic certbot
```

When you run certbot, it will configure nginx for HTTPS traffic, tell nginx to use the newly generated cert for that traffic, and set up the auto-renewal of your certificate.

```
/snap/bin/certbot --nginx
```

(NOTE: The certbot tool will not be in your $PATH unless you log out and log back in again. This is why we are using the absolute path of `/snap/bin/certbot` to run it.)

During the installation, enter your email address when prompted. Also, answer "yes" to the questions by pressing "y" when prompted.

On the following page is an example execution of the Certbot application including the output it generated. The characters in bold were typed in as input.

```
[root@ssl-demo ~]# /snap/bin/certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security
notices)
 (Enter 'c' to cancel): you@example.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.
pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
(Y)es/(N)o: y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
Would you be willing, once your first certificate is
successfully issued, to
share your email address with the Electronic Frontier
Foundation, a founding
partner of the Let's Encrypt project and the non-profit
organization that
develops Certbot? We'd like to send you email about our work
encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
(Y)es/(N)o: y
Account registered.

Which names would you like to activate HTTPS for?
We recommend selecting either all domains, or all domains in a
VirtualHost/server block.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
1: demo.linuxtrainingacademy.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
Select the appropriate numbers separated by commas and/or
spaces, or leave input
```

```
blank to select all options shown (Enter 'c' to cancel):
Requesting a certificate for demo.linuxtrainingacademy.com

Successfully received certificate.
Certificate is saved at:
/etc/letsencrypt/live/demo.linuxtrainingacademy.com/fullchain.p
em
Key is saved at:
/etc/letsencrypt/live/demo.linuxtrainingacademy.com/privkey.pem
This certificate expires on 2023-04-13.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this
certificate in the background.

Deploying certificate
Successfully deployed certificate for
demo.linuxtrainingacademy.com to /etc/nginx/nginx.conf
Congratulations! You have successfully enabled HTTPS on
https://demo.linuxtrainingacademy.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - -
```

You can test the auto-renewal functionality of your SSL certificate by running this command:

```
/snap/bin/certbot renew --dry-run
```

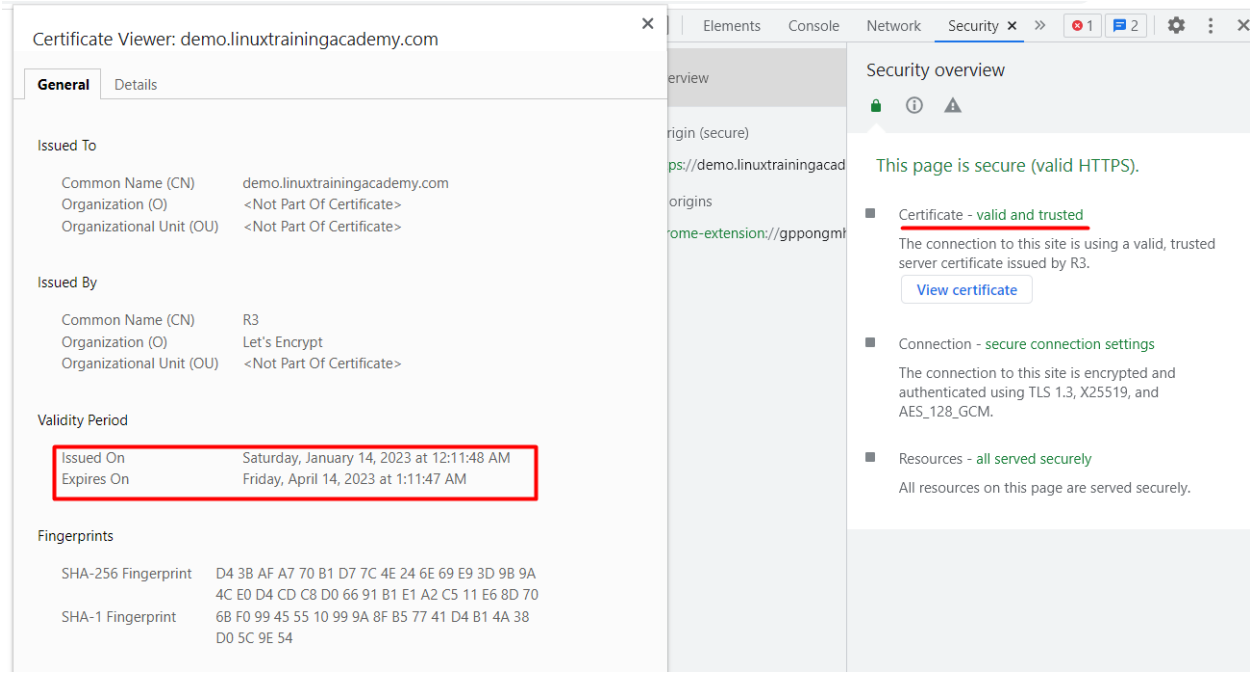
If the automatic renewal works, you will get a response: "Congratulations, all simulated renewals succeeded."

NOTE: If you want certbot to simply download the SSL certificate and leave the Nginx configuration up to you, use this command:

```
/snap/bin/certbot certonly --nginx
```

Step 10: Verify the SSL Certificate

Open up a web browser and connect to your domain over HTTPS. If the certificate installation was successful, you will not receive any errors or warnings about the SSL certificate from your web browser.



You can also check the web server from the command line using the curl utility:

```
curl https://demo.linuxtrainingacademy.com
```

If the certificate is valid, curl will return the contents of the website without any errors or warnings.

Congratulations!

At this point, you should have a valid SSL certificate that will be automatically renewed!

Additional Resources

If you enjoyed this tutorial, then you will also enjoy our courses, available at https://courses.linuxtrainingacademy.com.