SECURITY

How to install and use Let's Encrypt on a Ubuntu Server for SSL security

If you're looking for an easy way to install SSL certificates on your Ubuntu Server, follow this incredibly simple process to use Let's Encrypt.

By Jack Wallen | February 16, 2017, 12:20 PM PST

Image: Jack Wallen

It's a pain to add an SSL certificate to a web server. Fortunately, on the LAMP platform, you can make this IT task significantly easier with the help of Let's Encrypt (https://letsencrypt.org/). Once this tool is installed, you can make short shrift of adding SSL certificates to your websites.

Let's walk through the process of installing and using Let's Encrypt. I'll demonstrate the process on a Ubuntu Server 16.04 and assume you already have your LAMP server running and serving up websites.

SEE: Job description: Security Architect (http://www.techproresearch.com/downloads/job-description-security-architect/) (Tech Pro Research)

More about IT Security

- Video: Top 5 cybercrime vectors (http://www.techrepublic.com/article/top-5-cybercrime-vectors/)
- IoT security: What you should know, what you can do (free PDF) (http://www.techrepublic.com/resource-library/whitepapers/iot-security-what-you-should-know-what-you-can-do-free-pdf/)
- Cybersecurity in 2017: A roundup of predictions (http://www.techproresearch.com/article/cybersecurity-in-2017-a-roundup-of-predictions/)

How to install Let's Encrypt

First, we must install Let's Encrypt. Before we issue the installation command, let's update apt with this command:

```
sudo apt-get update
```

After that completes, we'll issue the following command to install Let's Encrypt:

```
sudo apt-get install python-letsencrypt-apache
```

Depending upon your setup, you might see a number of dependencies to be installed; if you do, okay those installations and allow the process to complete. Once it's finished, you're ready to continue.

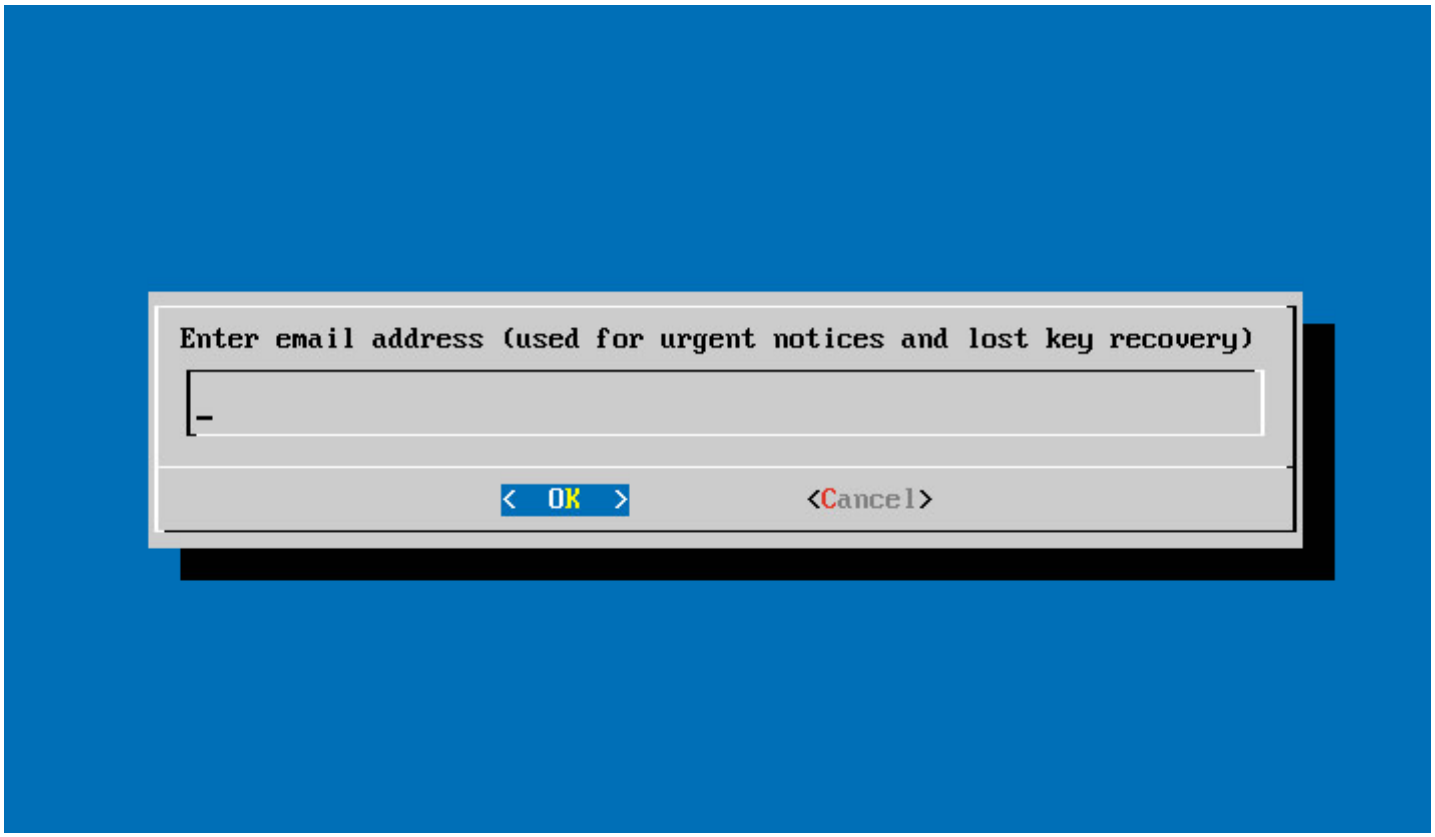
How to set up the SSL certificate

The next step is using letsencrypt to set up your certificate. Let's use the domain domain.com for our demonstration. (**Note:** You must have a public-facing domain for this process, and the domain must be owned by you, have a DNS A record, and have a publicly routable IP address; otherwise, the process will fail.) In order to launch the interactive certificate setup, go back to your terminal window and issue the command (DOMAIN.COM is your actual domain):

```
sudo letsencrypt --apache -d DOMAIN.COM
```

The first window in the setup will ask for an email address (for notices and lost key recovery) (**Figure A**). Enter your email address and tab down to OK.

Figure A



The Let's Encrypt interactive setup.

The next window you must agree to is the EULA. That's it—letsencrypt will do its thing and dump the original certificate files into */etc/letsencrypt/archive* and create links to the most recent certificate files in */etc/letsencrypt/live* (this is important after you've renewed your certificates...more on that in a bit). You can verify the status of the SSL certificate by pointing a browser to this link (DOMAIN.COM is your domain):

```
https://www.ssllabs.com/ssltest/analyze.html?d=DOMAIN.COM&latest
```

How to set up auto renewal of SSL certificates

By default, letsencrypt creates certificates that are valid for only 90 days; because of this, you need to set up a process that will auto renew those certificates. Since this is Linux, you can easily use cron for that job. To create a cronjob that will renew your certificates on the first day of every month at midnight, issue the command *sudo crontab -e* and then add the following:

```
0 0 1 * * /usr/bin/letsencrypt renew >> /var/log/letsencrypt-renew.log
```

Save and close that file. At this point, letsencrypt will automatically renew your certificate (by way of the letsencrypt-auto renew command) every month, so those certificates never expire.

Easy peasy

That's it—you just created SSL certificates for your domain with the help of an incredibly easy to use tool. After using this method, you'll never want to install a certificate in any other fashion.

Also see

- Ebook: Why Munich made the switch from Windows to Linux—and may be reversing course (PDF download) (http://www.techrepublic.com/resource-library/whitepapers/why-munich-made-the-switch-from-windows-to-linux-and-may-be-reversing-course/) (TechRepublic)
- How Mark Shuttleworth became the first African in space and launched a software revolution (PDF download) (http://www.techrepublic.com/resource-library/downloads/how-mark-shuttleworth-became-the-first-african-in-space-and-launched-a-software-revolution-pdf-download/) (TechRepublic)
- How to fix Apache 2 not executing PHP files (http://www.techrepublic.com/article/how-to-fix-apache-2-not-executing-php-files/) (TechRepublic)
- How to solve SELinux issues with ease using SELinux Alert Browser (http://www.techrepublic.com/article/how-to-solve-selinux-issues-with-ease-using-selinux-alert-browser/) (TechRepublic)
- How to harden MySQL security with a single command (http://www.techrepublic.com/article/how-to-harden-mysql-security-with-a-single-command/) (TechRepublic)
- How to harden Ubuntu Server 16.04 security in five steps (http://www.techrepublic.com/article/how-to-harden-ubuntu-server-16-04-security-in-five-steps/) (TechRepublic)
- Linux Foundation releases business open source basics ebook (http://www.zdnet.com/article/linux-foundation-releases-business-open-source-basics-ebook/) (ZDNet)

About Jack Wallen

Jack Wallen is an award-winning writer for TechRepublic and Linux.com. He's an avid promoter of open source and the voice of The Android Expert. For more news about Jack Wallen, visit his website jackwallen.com.