Let’s Encrypt: Kostenloses SSL-Zertifikat auf Deinem Server nutzen

Version 2 vom 09.09.2020

Inhaltsverzeichnis

Einleitung

Eine unsichere HTTP-Verbindung wirkt abschreckend auf Besucher von Websites und Online-Shops. Ebenso auf Suchmaschinen. Entsprechend wichtig ist es, auf eine sichere HTTPS-Verbindung umzustellen. Eine kostenlose Möglichkeit bietet die Zertifizierungsstelle Let's Encrypt (letsencrypt.org) an – übersetzt „Lasst uns verschlüsseln". Let's Encrypt vertreibt seit Ende 2015 X.509-Zertifikate für das Verschlüsselungsprotokoll Secure Sockets Layer (SSL). Hinter dem Zertifikat steckt die gemeinnützige Organisation Internet Security Research Group (ISRG). Hauptsponsoren sind unter anderem die Electronic Frontier Foundation (EFF), die Mozilla Foundation, Akamai, Google Chrome und Cisco Systems.

Ziel der Organisation: die Verschlüsselung im Internet zum Normalfall machen. Um das zu erreichen, setzt die EFF auf einen automatisierten Prozess, der die meisten händischen Vorgänge bei der Erstellung, Validierung, Signierung, Einrichtung und Erneuerung von Zertifikaten automatisiert. Auf einem Linux-Webserver reichen einige Befehle, um innerhalb weniger Minuten ein Zertifikat anzufordern und zu installieren. Eine Einfachheit, die Website-Betreiber zu schätzen wissen. Im Februar 2020 stellte die Organisation das milliardste Zertifikat aus. Let's Encrypt zielt darauf ab, mit so vielen Systemen wie möglich kompatibel zu sein. Fast jeder moderne Browser und die meisten Betriebssysteme unterstützen das Zertifikat.

Am einfachsten gelingt die Installation mit der Verwaltungssoftware Plesk. Erweiterungen führen Dich automatisch durch die Installation. Falls Du die Installation manuell auf Debian-Basis mit installiertem Apache durchführen möchtest, reichen einige Zeilen Code. In dieser Anleitung zeigen wir Dir am Beispiel eines Testservers mit Ubuntu 18.04 LTS 64bit, wie Du Let's Encrypt auf einem STRATO V-Server Linux einrichtest.

Du benötigst für eine Installation von Let's Encrypt:

1. eine Domain und eine korrekt konfigurierte Website,
2. administrativen Zugriff auf die Domain,
3. einen laufenden Linux-Server

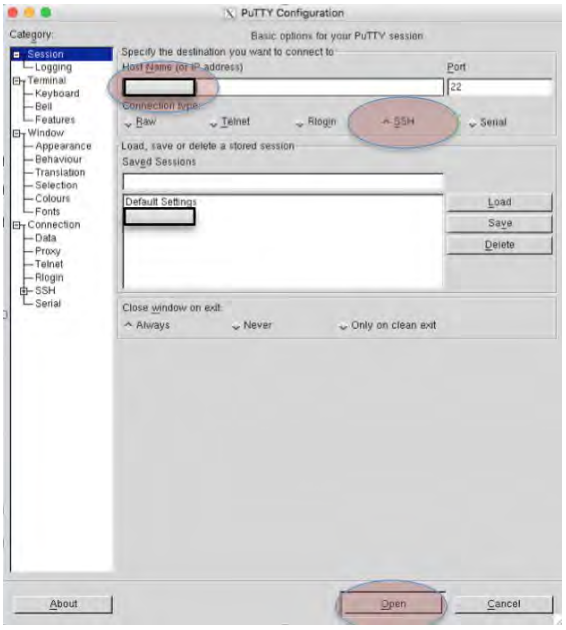
Wichtig: Backups sind immer ratsam. Bei STRATO legt die automatische Funktion BackupControl täglich Sicherungskopien an. Kunden müssen sich aber selbst um konsistente Datenbank-Backups kümmern. Deshalb: Sichere Deine Server-Daten, bevor Du mit der HTTPS-Konfiguration beginnst.

Schritt 1: Auf dem Server anmelden

Du benötigst als erstes einen Secure Shell Zugang (SSH), um eine verschlüsselte Verbindung zur Kommandozeile (Shell) auf dem Webserver herzustellen. Das funktioniert beispielsweise mit dem SSH-Client PuTTY, den Du unter putty.org downloaden kannst.

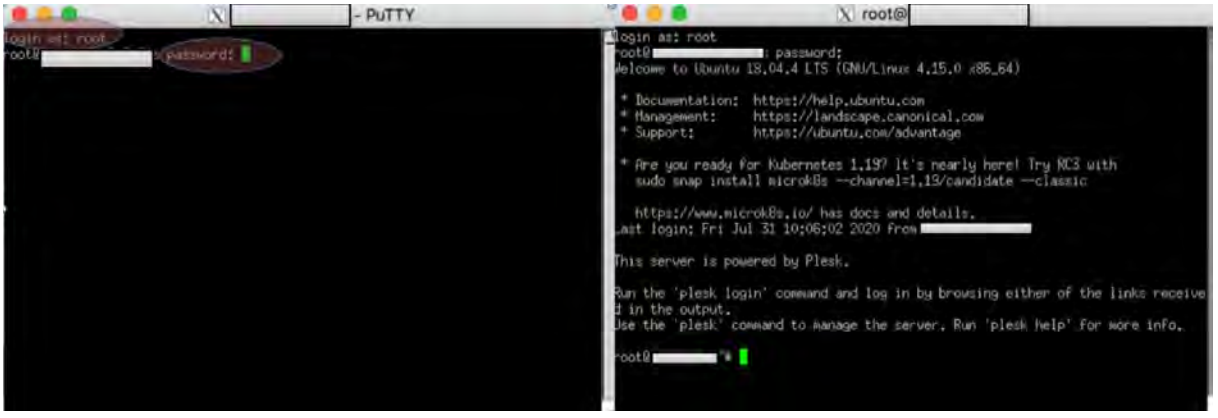
Nutzer von Linux oder OS X benötigen die Software nicht, da ein Befehlszeile-SSH-Client (Terminal) Teil des Betriebssystems ist. Willst Du dennoch PuTTY nutzen, benötigst Du eine Software wie XQuartz (xquartz.org), die das Installieren und Starten von X11-basierten Anwendungen unter Mac OS X ermöglicht.

Wenn Du PuTTY verwenden möchtest, musst Du die Software zunächst konfigurieren. Öffne das Programm und trage Deine IP-Adresse ein. Du findest sie im Server-Login unter „Mein Server" → „Serverdaten". Wähle als Verbindungsart SSH und klicke auf Open. Das Terminalfenster öffnet sich.



Konfiguration der Client-Software PuTTY: Du benötigst Deine IP-Adresse, die Du im Server-Login von STRATO findest.

Nachdem sich das Terminalfenster geöffnet hat, meldest Du Dich auf dem Server an. Dafür gibst Du hinter der Aufforderung „login as:“ den Namen „root“ ein. Anschließend gibst Du als Admin-Passwort Dein root-Passwort ein. Falls Du es noch nicht geändert hast, findest Du es – genau wie die IP-Adresse – in Deinen Serverdaten. **Achtung:** Aus Sicherheitsgründen siehst Du das Passwort im Terminal nicht. Du tippst quasi ins Dunkle.



Melde Dich als „root“ mit Deinem initialen root-Passwort auf dem Server an (links); nach dem Login (rechts).

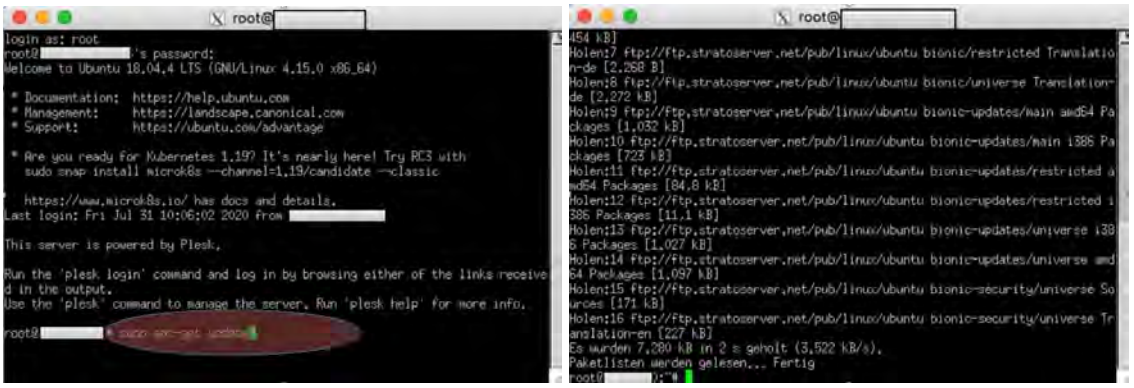
Schritt 2: ACME-Client Certbot zu Programmen hinzufügen

Let’s Encrypt arbeitet mit Automatic Certificate Management Environment (ACME) – ein Protokoll, das automatisch die Inhaberschaft einer Internet-Domain bestätigt und die Ausstellung von

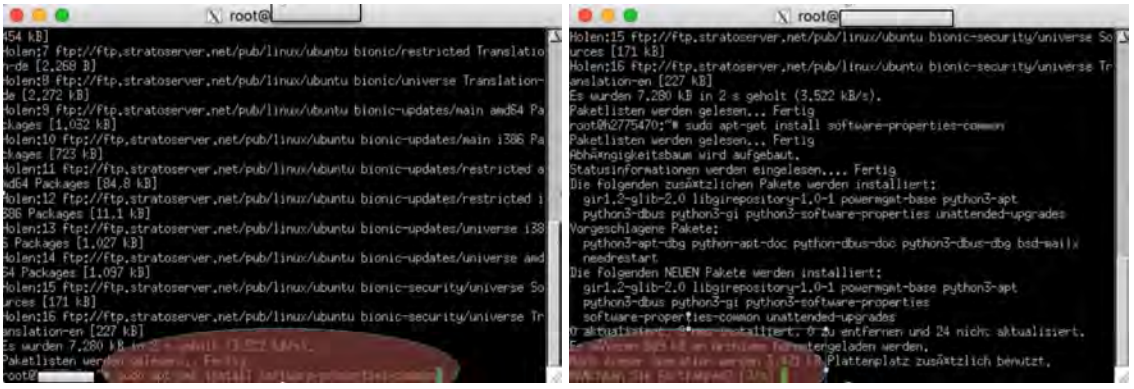
SSL-Zertifikaten vereinfacht. Zahlreiche ACME-Clients sind mit Let's Encrypt kompatibel, sofern sie ACMEv2-API (RFC 8555) unterstützen (**Achtung:** Die Unterstützung für ACMEv1 ist bald eingestellt).

Let's Encrypt empfiehlt die Nutzung eines ACME-Clients namens Certbot. Möchtest Du mit diesem kleinen Helfer arbeiten, musst Du den Update-Manager-Cache aktualisieren und Certbot zur Programmliste (Repositorys) hinzufügen. Die Befehle, die Du nacheinander ausführen musst, lauten:

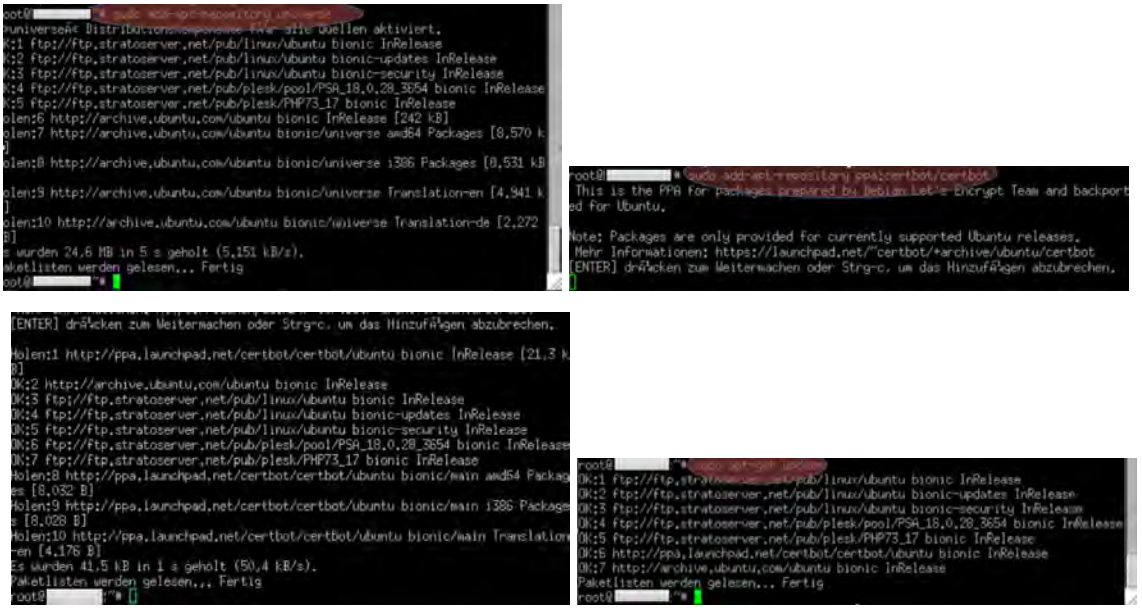
```
sudo apt-get update
sudo apt-get install software-properties-common
sudo add-apt-repository universe
sudo add-apt-repository ppa:certbot/certbot
```



Mit dem Befehl „sudo apt-get update" aktualisierst Du den Update-Manager-Cache.



Vorbereitung der Installation mit dem Befehl „sudo apt-get install software-properties-common".

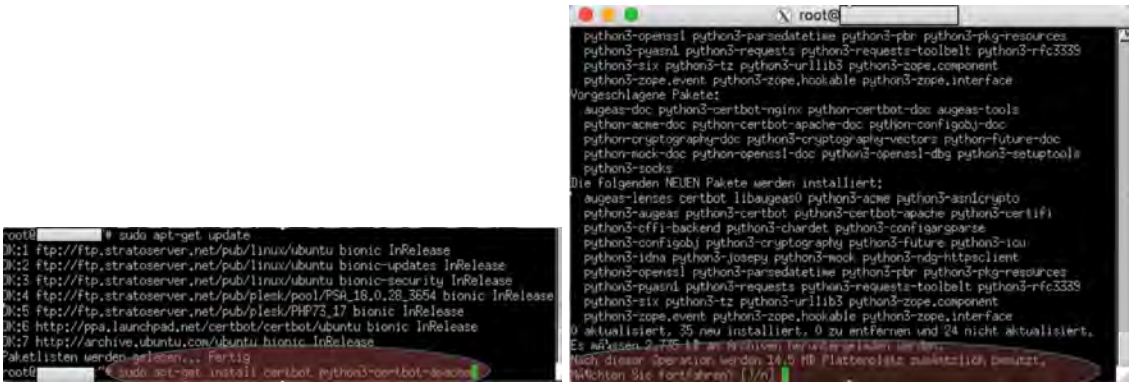


Mit den Befehlen „sudo add-apt-repository universe“, „sudo add-apt-repository ppa:certbot/certbot“ und „sudo apt-get update“ fügst Du Certbot zur Programmliste hinzu.

Schritt 3: Certbot installieren

Als Nächstes folgt die Installation des ACME-Client Certbot. Folgenden Befehl musst Du dafür ins Terminal eingeben:

```
sudo apt-get install certbot python3-certbot-apache
```

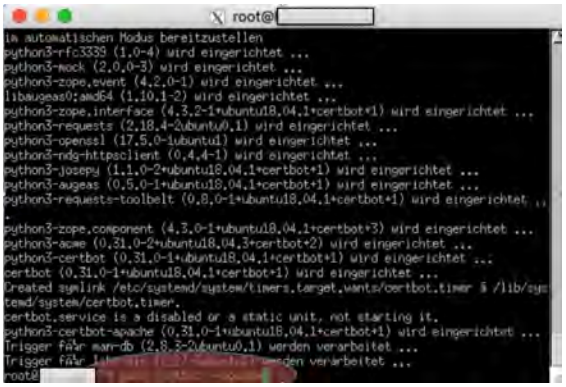


Mit dem Befehl „sudo apt-get install certbot python3-certbot-apache“ installierst Du den ACME-Client.

Schritt 4: SSL-Zertifikat holen

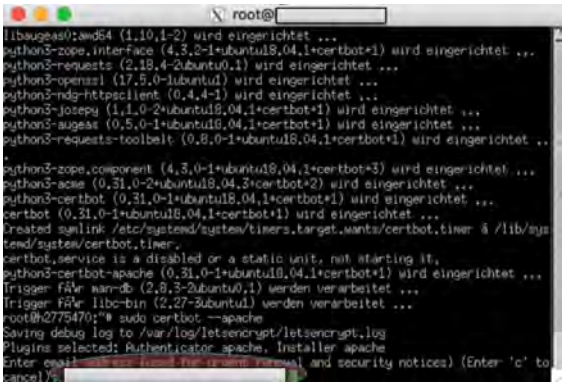
Ein Zertifikat anfordern und aktivieren, ist dank des Certbot denkbar einfach. Es reicht folgender Befehl:

```
sudo certbot --apache
```



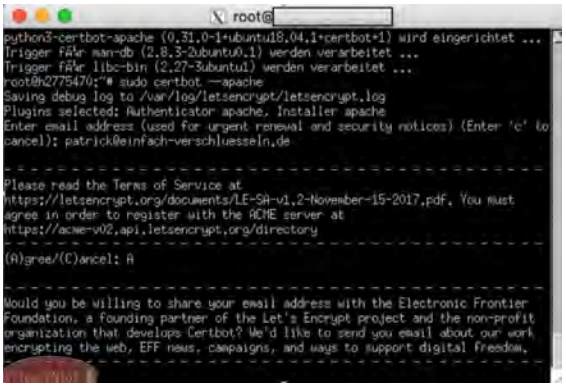
Mit dem Befehl „sudo certbot –-apache“ holt Certbot das Zertifikat.

Als Nächstes musst Du eine E-Mail-Adresse angeben, damit Let’s Encrypt Dich kontaktieren kann. Am besten eignet sich hier das Mailkonto, das der Webmaster für die Administration der Seite verwendet. Anschließend musst Du den Nutzungsbedingungen zustimmen.



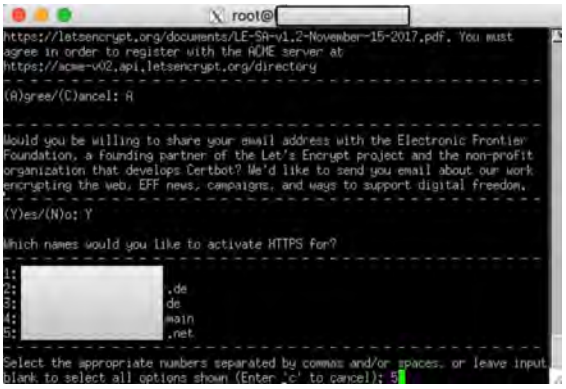
Eingabe Deiner E-Mail-Adresse

Mit „A“ stimmst Du den Nutzungsbedingungen zu.



Hier kannst Du mit „Y“ zustimmen, dass EFF dir News schickt. Oder Du lehnst mit „N“ ab.

Abschließend musst Du Dich entscheiden, für welche Seite Du HTTPS aktivieren möchtest. Trage einfach die entsprechende Zahl ins Terminal ein (mehrere Nummern mit Komma trennen). Falls Du HTTPS für alle Seiten aktivieren möchtest, trage keine Nummer ein und drücke einfach auf Enter.



Hier kannst Du HTTPS für Deine Seiten aktivieren.

Schritt 5: HTTPS-Verbindung prüfen

Herzlichen Glückwunsch, das SSL-Zertifikat sollte nun aktiv sein. Besuche Deine Website und prüfe, ob links neben dem Domainnamen ein Schlosssymbol auftaucht. Falls ja, ist das Zertifikat gültig und die Website sicher. Testen kannst Du die Verbindung auch mit einem Online-Tool unter ssllabs.com/ssltest.

Achtung: SSL-Zertifikate von Let’s Encrypt sind nur 90 Tage gültig. Du musst Dich allerdings nicht um eine Erneuerung kümmern. Das System hält die Zertifikate mittlerweile automatisch aktuell. Du kannst diese Funktion mit dem Befehl „sudo certbot renew --dry-run“ testen.

Fazit

Let’s Encrypt ist eine hervorragende Möglichkeit, um für den V-Server Linux von STRATO schnell und kostenlos ein SSL-Zertifikat zu erhalten. Let’s Encrypt ist aber nicht die einzige Möglichkeit, an ein SSL-Zertifikat zu kommen, und auch nicht immer der beste Weg: Wenn Du den Umstieg auf

eine SSL-verschlüsselte Website planst, lohnt sich auf alle Fälle ein Blick auf die Zertifikate, die STRATO kostenpflichtig anbietet. Für den geschäftlichen Einsatz empfehlen wir Dir dringend, identitätsvalidierte Zertifikate oder sogar eine erweiterte Validierung zu nutzen. Sie prüfen nicht nur technisch, ob die Domain zu Deinem Server gehört (wie Let's Encrypt es tut). Sie prüfen auch, ob die Domain tatsächlich zu Dir und Deinem Geschäft gehört.