Các bước lấy chứng chỉ SSL với certbot standalone mode trên Ubuntu 20.04

Dưới đây là chi tiết các bước hướng dẫn cách lấy chứng chỉ SSL với Certbot Standalone Mode trên Ubuntu 20.04, bạn có thể tham khảo và thực hiện theo nhé!

### **Cài đặt Certbot**

Certbot đề xuất bạn nên sử dụng gói snap mà họ cung cấp để cài đặt. Những gói snap có thể sử dụng trên hầu hết các phiên bản **Linux**, nhưng trước tiên bạn cần cài đặt snap để quản trị. Ubuntu 20.04 đã tích hợp sẵn snap, vì vậy,  bạn có thể kiểm tra việc cập nhật snap core bằng cách chạy lệnh dưới đây:

**sudo snap install core; sudo snap refresh core**

Nếu bạn đã từng cài đặt phiên bản cũ của Certbot trên máy chủ  và muốn nâng cấp nó, thì lúc này bạn nên gỡ bỏ phiên bản cũ trước khi tiến hành cài đặt cerbot mới:

**sudo apt remove certbot**

Bước tiếp theo, bạn có thể cài đặt gói certbot thông qua sử dụng lệnh sau đây:

**sudo snap install --classic certbot**

Sau cùng, bạn có thể tạo liên kết giữa lệnh certbot trong thư mục cài đặt snap với đường dẫn chung của hệ thống, để bạn có thể chạy lệnh bạn chỉ cần nhập  lệnh “**certbot**“. Điều này không cần thiết cho tất cả các gói, nhưng việc sử dụng snap thường an toàn hơn và ít gây xung đột với các gói hệ thống khác:

**sudo ln -s /snap/bin/certbot /usr/bin/certbot**

1. Chạy certbot

Certbot lúc này cần phải thực hiện một phần thách thức mật mã (cryptographic challenge) mà API của Let’s Encrypt đặt ra để chứng minh rằng bạn có quyền quản lý tên miền của mình. Để thực hiện điều này, Cerbot sử dụng cổng 80 ([**HTTP**](https://lanit.com.vn/http-co-an-toan-khong.html)) hoặc 443 ([**HTTPS**](https://lanit.com.vn/giao-thuc-bao-mat-https-ssl-tam-quan-trong-https-doi-voi-doanh-nghiep.html)). Và lúc này bạn cần mở các cổng phù hợp trên tường lửa của bạn để thực hiện chúng. Bạn có thể nhập lệnh như dưới đây:

**sudo ufw allow 443**

Khi đã chuẩn bị các bước xong, bạn có thể chạy Certbot để lấy chứng chỉ. Bằng việc sử dụng tùy chọn **–standalone** để yêu cầu Certbot xử lý cryptographic challenge và sử dụng máy chủ web riêng biệt của nó. Cuối cùng, bạn có thể sử dụng  -d để chỉ định tên miền mà bạn muốn yêu cầu chứng chỉ. Bạn có thể thêm nhiều tùy chọn -d nếu bạn muốn bao gồm nhiều tên miền một lúc trong một chứng chỉ.

**sudo certbot certonly --standalone -d your\_domain**

Sau khi chạy lệnh trên, bạn sẽ được yêu cầu cung cấp địa chỉ email và bạn cần đồng ý với các điều khoản dịch vụ. Sau khi bạn hoàn thành, bạn sẽ nhận thấy thông báo xác nhận rằng quá trình đã thành công và chứng chỉ của bạn được lưu tại:

**IMPORTANT NOTES:**

**Successfully received certificate.**

**Certificate is saved at: /etc/letsencrypt/live/your\_domain/fullchain.pem**

**Key is saved at: /etc/letsencrypt/live/your\_domain/privkey.pem**

**This certificate expires on 2022-02-10.**

**These files will be updated when the certificate renews.**

**Certbot has set up a scheduled task to automatically renew this certificate in the background.**

Sau khi bạn đã sở hữu chứng chỉ, bước tiếp theo, chúng ta sẽ kiểm tra một số tệp mà bạn đã tải xuống và tìm hiểu về chức năng của chúng.

### **Cấu hình ứng dụng**

Việc cấu hình SSL cho ứng dụng tùy vào mỗi ứng dụng sẽ có những yêu cấu hình riêng biệt nên sẽ có những cách khác nhau. Tuy nhiên, bạn nên kiểm tra các tệp mà Certbot đã tải về bằng cách sử dụng lệnh ls. Lệnh ls sẽ hiển thị danh sách các thư mục chứa khóa (key) và chứng chỉ (certificate), bạn hãy nhập lệnh sau đây:

**sudo ls /etc/letsencrypt/live/your\_domain**

Kết quả hiện ra sẽ như sau:

cert.pem chain.pem fullchain.pem privkey.pem README

Tệp README trong thư mục này bao gồm những thông tin cần thiết về từng tệp. Tuy nhiên, hầu hết trong các tệp, bạn chỉ cần quan tâm đến hai tệp sau đây, đó là:

* **privkey.pem**: Tệp này chứa khóa riêng tư (private key) và cần được bảo mật tuyệt đối. Đó chính là lý do thư mục /etc/letsencrypt thường có quyền truy cập hạn chế và chỉ có người dùng root mới có thể truy cập vào được. Trong một số phần mềm, tệp này có thể sử dụng tên khác như ssl-certificate-key hoặc ssl-certificate-key-file.
* **fullchain.pem**: Tệp này bao gồm chứng chỉ trung gian (Intermediate Certificate). Hầu hết phần mềm sẽ sử dụng tệp này cho chứng chỉ thực và sẽ tham chiếu đến nó trong cấu hình dưới tên đó là  ‘SSL-certificate’.

Một số phần mềm sẽ lưu chứng chỉ SSL bằng một số định dạng khác hoặc một thư mục khác với nhiều quyền người dùng.  Lúc này, bạn nên giữ nguyên các file trong thư mục letsencrypt và không được thao tác bất cứ thay đổi về quyền nào. Trong trường hợp bắt buộc bạn muốn thay đổi quyền thì lúc bạn sẽ cần tới các đoạn script để thực hiện các quyền thay đổi quyền đối với từng file.

### **Gia hạn chứng chỉ tự động**

Chứng chỉ của Let’s Encrypt chỉ có giá trị trong vòng 90 ngày, và để khuyến khích người dùng tự động gia hạn, gói certbot sẽ tự động thực hiện gia hạn. Cerbot sẽ thêm một số đoạn mã vào thư mục /etc/cron.d và thực hiện gia hạn chứng chỉ tự động 2 lần/ ngày.

Sau khi thực hiện tự động gia bạn, bạn cần khởi động lại máy chủ hoặc tải lại nó để áp dụng chứng chỉ mới. Certbot cung cấp một tùy chọn là “**renew\_hook**” để giải quyết vấn đề này.

Để thêm **renew\_hook**, bạn cần thao tác một số thay đổi đối với file cấu hình gia hạn của Certbot. Lúc này, Certbot đã ghi lại toàn bộ các chi tiết trong lần nạp chứng chỉ đầu tiên và sẽ thực hiện lại các tuỳ chọn đã được ghi lại này trong quá trình này.

Để mở file config bạn có thể sử dụng câu lệnh sau:

**sudo nano /etc/letsencrypt/renewal/your\_domain.conf**

Tiếp theo, bạn có thể thêm “hook” vào dòng cuối cùng để thao tác lại bất kỳ dịch vụ nào cần cập nhật chứng chỉ sau khi gia hạn:

**renew\_hook = systemctl reload your\_service**

Tuỳ vào những tình huống cụ thể mà có thể thay đổi nội dung của câu lệnh. Đối với hệ điều hành Ubuntu, bạn nên sử dụng lệnh **systemctl**để tái khởi động một dịch vụ. Bước tiếp theo, bạn hãy lưu rồi thoát file. Và sử dụng lệnh sau đây để đảm bảo mọi thứ vẫn hoạt động bình thường:

**sudo certbot renew --dry-run**

Làm theo các bước trên bạn đã lấy chứng chỉ SSL với certbot Standalone Mode trên Ubuntu 20.04 thành công.

Bạn cần [**mua SSL**](https://lanit.com.vn/chung-chi-ssl.html) ở một nơi uy tín? LANIT chính là một lựa chọn không thể bỏ qua với bạn. Bất kể bạn cần một giải pháp mua chứng chỉ SSL cho dự án cá nhân nhỏ hay một hệ thống phức tạp để phục vụ hàng triệu khách hàng, chúng tôi đều có khả năng cung cấp cho bạn một giải pháp phù hợp nhất.

1. Cấu hình nginx

listen 443 ssl default\_server;

listen [::]:443 ssl default\_server;

ssl\_certificate /etc/letsencrypt/live/vonhucong.id.vn/fullchain.pem;

ssl\_certificate\_key /etc/letsencrypt/live/vonhucong.id.vn/privkey.pem;

ssl\_session\_cache shared:SSL:1m;

ssl\_session\_timeout 5m;

ssl\_ciphers HIGH:!aNULL:!MD5;

ssl\_prefer\_server\_ciphers on;