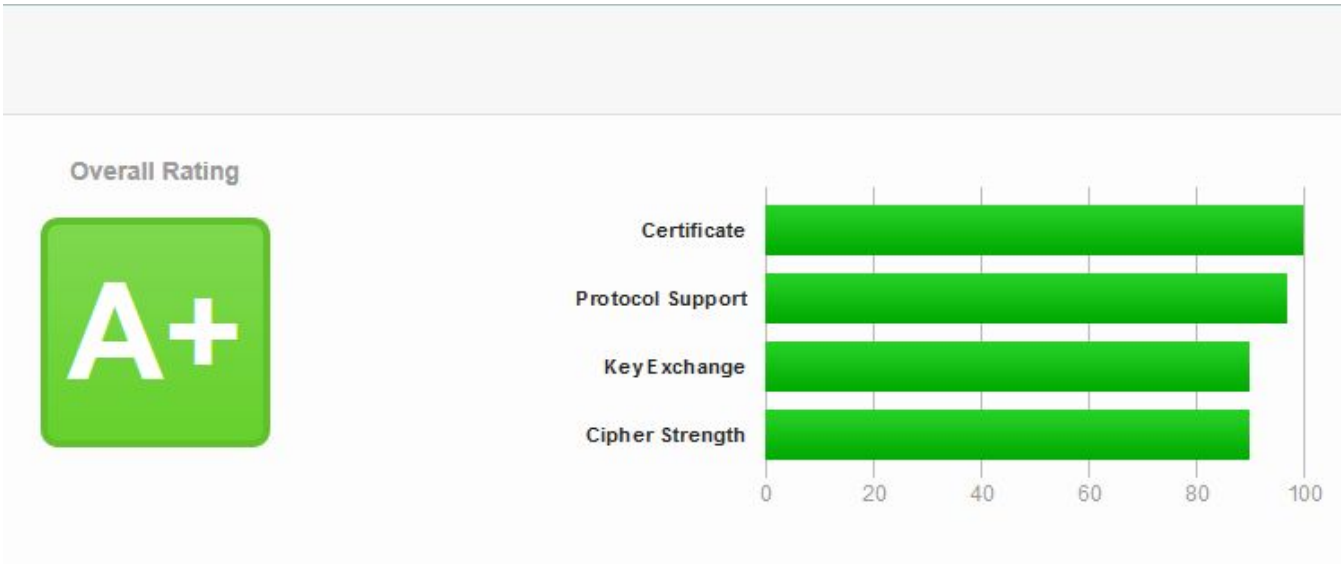
C?u hình Nginx ?? Qualys SSL Labs x?p h?ng A

admin Sun, Apr 14, 2019 Chứng Chỉ Số SSL Certificates 0 1599



L?u ý: Các tiêu chu?n ?ánh giá c?a Qualys SSL Labs thay ??i theo th?i gian, do ?ó bài vi?t này c?ng s? ???c c?p nh?t th??ng xuyên

?? Qualys SSL Labs x?p h?ng A, b?n c?n ph?i c?p nh?t c?u hình c?a Nginx th?a mãn m?t s? tiêu chí nh?t ??nh. B?n có th? tham kh?o bài vi?t này ?? th?c hi?n c?p nh?t cho máy ch? c?a mình.

1. Ch? h? tr? TLS 1.0, TLS 1.1 và TLS 1.2, vô hi?u hóa SSL 2.0 và SSL 3.0

B?n c?n ph?i nâng c?p phiên b?n OpenSSL lên phiên b?n m?i nh?t không b? v??ng l? h?ng b?o m?t và h? tr? TLS 1.2 và TLS 1.2. Ví d?: các phiên b?n 0.9.x và 1.0.0 tr? v? tr??c không h? tr? TLS 1.2.
Sau khi nâng c?p OpenSSL, b?n c?n ph?i build l?i ho?c nâng c?p Nginx lên phiên b?n m?i nh?t. K? t? phiên b?n 1.1.13 tr? lên, Nginx ?ã h? tr? TLS 1.1 và TLS 1.2.
?? vô hi?u hóa SSL 2.0, SSL 3.0 và ch? h? tr? TLS 1.0, TLS 1.1 và TLS 1.2, b?n c?n ch?nh l?i tham s? sau:

```
ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
```

2. Poodle and TLS-FALLBACK-SCSV

SSL 3.0 là nguyên nhân quan tr?ng nh?t gây ra l? h?ng Poodle. B?ng cách vô hi?u hóa SSL 3.0, b?n ?ã kh?c ph?c l? h?ng Poodle cho máy ch?.

?? vô hi?u hóa l? h?ng "protocol downgrade attack", extension TLS FALLBACK SCSV ph?i ???c kích ho?t trong OpenSSL. Các phiên b?n sau ?ây ?ã bao g?m extension này:

- OpenSSL 1.0.1j ho?c cao h?n
- OpenSSL 1.0.0o ho?c cao h?n
- OpenSSL 0.9.8zc ho?c cao h?n

3. Heartbleed

L? h?ng Heartbleed là m?t l? h?ng khá nghiêm tr?ng, có th? ?nh h??ng ??n m?i máy ch? s? d?ng th? vi?n OpenSSL. ?? kh?c ph?c l?i này, cách duy nh?t là b?n ph?i ki?m tra phiên b?n OpenSSL ?ang s? d?ng và nâng c?p n?u n?m trong danh sách sau ?ây:

- OpenSSL 1.0.1 ??n 1.0.1f b? ?nh h??ngg
- OpenSSL 1.0.1g không b? ?nh h??ng
- OpenSSL 1.0.0 không b? ?nh h??ng
- OpenSSL 0.9.8 không b? ?nh h??ng

4. Cipher suites

Luôn luôn áp d?ng các cipher suites an toàn nh?t và yêu c?u server l?a ch?n ?u tiên theo th? t? mà b?n ?ã thi?t l?p.

```
ssl_prefer_server_ciphers on;
ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4
EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK
!SRP !DSS !RC4";
```

5. Strong DH (Diffie-Hellman)

Ch?y l?nh:

```
openssl dhparam -out /usr/local/ssl/dhparams.pem 2048
```

B? sung dòng sau ?ây vào file c?u hình:

```
ssl_dhparam /usr/local/ssl/dhparams.pem;
```