

SSL 证书- Apache

优化加密算法

(cipher)



优化加密算法 (cipher)

1. 通过 https 方式访问您的站点，测试站点证书的安装配置。

<https://cryptoreport.websecurity.symantec.com/checker/views/certCheck.jsp>

2. 在提高网络服务器的 SSL 证书部署优化方面，我们通常建议系统管理员使用更加安全的加密套件，对于这一点，我们提出对常见的服务器支持的方案。

打开 apache 安装目录下 /etc/httpd/conf/ssl.conf 文件在配置文件中加入：

```
SSLProtocol All -SSLv2 -SSLv3 -TLSv1
SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-
AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-
AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-
SHA:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-
SHA256:AES256-SHA:AES128-SHA:DES-CBC3-
SHA:HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4
SSLHonorCipherOrder on
```