OpenSSL - s_time

Programme de test de performance SSL/TLS

OPTIONS

-connect host :port Spécifie l'hôte :port distant

-www page Spécifie la page à GET. Sans cette options, s_time effectue simplement un handshake pour établir la connexion SSL, mais ne transfère pas de données payload.

-cert certname Certificat à utiliser (PEM)

-key keyfile Clé privée à utiliser

-verify depth Active la vérification du certificat du serveur et spécifie la longueur max de la chaine de certificat du serveur

-CApath directory Répertoire à utiliser pour la vérification du certificat du serveur. doit être un 'hash format'

-CAfile file Fichier contenant les certificats à truster

-new Effectue un test de temps en utilisant un nouvel ID de session pour chaque connexion.

-reuse Effectue un test de temps en utilisant le même ID de session.

-nbio Active l'I/O non bloquant

-ssl2, -ssl3 Désactive l'utilisation de certains protocoles SSL. Par défaut, le handshake utilise une méthode qui devrait être compatible avec tous les serveurs et permet d'utiliser SSLv3, SSLv2 ou TLS.

-bugs Il y'a de nombreux bugs connus dans les implémentations SSL et TLS. Cette option autorise diverses solutions.

-cipher cipherlist Permet d'envoyer la liste des chiffrements à modifier. Le serveur détermine quelle suite est utilisée et devrait prendre la première supportée dans la liste.

-time length Spécifie le temps en second que s_time devrait mettre pour établir les connections et optionnellement transférer les données payload du serveur.

Notes

s_time peut être utilisé pour mesurer les performances d'une connexion SSL. Pour se connecter à un serveur SSL HTTP et obtenir la page par défaut :

openssl s_time -connect servername :443 -www / -CApath yourdir -CAfile yourfile.pem -cipher commoncipher [-ssl3]