OpenSSL - s_client

Programme client SSL/TLS qui peut se connecter à un hôte distant en utilisant SSL/TLS. Utilitaire de diagnostique très utile

OPTIONS

-connect host :port Hôte et port distant (défaut : localhost :4433)

-cert certname Le certificat à utiliser (défaut : n'utilise pas de certificat)

-certform format Format du certificat, DER ou PEM

-key keyfile La clé privée à utiliser

-keyform format Le format de la clé privée, DER ou PEM

-pass arg Source du mot de passe de la clé privée

-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

-purpose, -ignore_critical, -issuer_checks, -crl_check, -crl_check_all,

-policy_check, -extended_crl, -x509_strict, -policy -check_ss_sig Définir divers options de validation de la chaîne de certificat (voir verify)

-reconnect Se reconnecte au même serveur 5 fois avec le même session ID, utile pour tester le cache de session.

-pause effectue une pause d'une seconde entre chaque appel de lecture et d'écriture

-showcerts Affiche la chaîne entière de certificat (défaut : seul le certificat du serveur est affiché)

-prexit Affiche les informations de session quand le programme quitte.

-state Affiche les statistiques de session SSL

-debug Affiche des informations additionnelles, incluant un dump hexa de tout le traffic

-msg Affiche tous les messages de protocole avec un dump hexa

-nbio_test Tests IO non bloquant

-nbio Active l'I/O non bloquant

-crlf Traduit un line feed depuis le terminal en CR+LF

-ign_eof Inhibe la fin de connection quand la fon du fichier est atteind

-quiet N'affiche pas d'information de session et des certificats. active implicitement -ign_oef

-psk_identity identity Utilise l'identité PSK lors de l'utilisation de la suite de chiffrement PSK

-psk key Sépcifie la clé PSK lors de l'utilisation de la suite de chiffrement PSK. La clé est donnée en nombre hexa sans le 0x, par exemple : -psk 1a2b3c4d

-ssl2, -ssl3, -tls1, -no_ssl2, -no_ssl3, -no_tls1 Désactive l'utilisation de certains protocoles SSL ou TLS. Par défaut, le handshake utilise une méthode qui devrait être compatible avec tous les serveur 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.

-starttls protocol Envoie les messages spécifique au protocole pour passer en TLS pour les communications. le protocole est un mot clé pour le protocole (smtp, pop3, imap et ftp)

-tlsextdebug Affiche un dump hexa des extensions TLS reçues du serveur

-no_ticket Désactive le support de ticket de session RFC4507bis

-sess_out filename sort la session SSL dans le fichier

-sess_in sess.pem Charge la session SSL depuis le fichier. Le client va tenter de résumer une connection depuis cette session.

-engin id s_client va tenter d'obtenir une référence fonctionnelle du moteur spécifié.

-rand file(s) Le(s) fichier(s) contenant les données aléatoire utilisé par le générateur de nombre aléatoire.

Exemples

se connecter à un serveur SSL distant :
openssl s_client -connect servername :443