NAME

SSL_CTX_set_session_cache_mode, SSL_CTX_get_session_cache_mode - enable/disable session caching

SYNOPSIS

```
#include <openssl/ssl.h>

long SSL_CTX_set_session_cache_mode(SSL_CTX ctx, long mode);
long SSL_CTX_get_session_cache_mode(SSL_CTX ctx);
```

DESCRIPTION

SSL_CTX_set_session_cache_mode() enables/disables session caching by setting the operational mode for **ctx** to <mode>.

SSL_CTX_get_session_cache_mode() returns the currently used cache mode.

NOTES

The OpenSSL library can store/retrieve SSL/TLS sessions for later reuse. The sessions can be held in memory for each **ctx**, if more than one SSL_CTX object is being maintained, the sessions are unique for each SSL_CTX object.

In order to reuse a session, a client must send the session's id to the server. It can only send exactly one id. The server then either agrees to reuse the session or it starts a full handshake (to create a new session).

A server will look up the session in its internal session storage. If the session is not found in internal storage or lookups for the internal storage have been deactivated (SSL_SESS_CACHE_NO_INTERNAL_LOOKUP), the server will try the external storage if available.

Since a client may try to reuse a session intended for use in a different context, the session id context must be set by the server (see **SSL_CTX_set_session_id_context**(3)).

The following session cache modes and modifiers are available:

SSL_SESS_CACHE_OFF

No session caching for client or server takes place.

SSL_SESS_CACHE_CLIENT

Client sessions are added to the session cache. As there is no reliable way for the OpenSSL library

to know whether a session should be reused or which session to choose (due to the abstract BIO layer the SSL engine does not have details about the connection), the application must select the session to be reused by using the **SSL_set_session**(3) function. This option is not activated by default.

SSL_SESS_CACHE_SERVER

Server sessions are added to the session cache. When a client proposes a session to be reused, the server looks for the corresponding session in (first) the internal session cache (unless SSL_SESS_CACHE_NO_INTERNAL_LOOKUP is set), then (second) in the external cache if available. If the session is found, the server will try to reuse the session. This is the default.

SSL_SESS_CACHE_BOTH

Enable both SSL_SESS_CACHE_CLIENT and SSL_SESS_CACHE_SERVER at the same time.

SSL_SESS_CACHE_NO_AUTO_CLEAR

Normally the session cache is checked for expired sessions every 255 connections using the **SSL_CTX_flush_sessions**(3) function. Since this may lead to a delay which cannot be controlled, the automatic flushing may be disabled and **SSL_CTX_flush_sessions**(3) can be called explicitly by the application.

SSL_SESS_CACHE_NO_INTERNAL_LOOKUP

By setting this flag, session-resume operations in an SSL/TLS server will not automatically look up sessions in the internal cache, even if sessions are automatically stored there. If external session caching callbacks are in use, this flag guarantees that all lookups are directed to the external cache. As automatic lookup only applies for SSL/TLS servers, the flag has no effect on clients.

SSL_SESS_CACHE_NO_INTERNAL_STORE

Depending on the presence of SSL_SESS_CACHE_CLIENT and/or SSL_SESS_CACHE_SERVER, sessions negotiated in an SSL/TLS handshake may be cached for possible reuse. Normally a new session is added to the internal cache as well as any external session caching (callback) that is configured for the SSL_CTX. This flag will prevent sessions being stored in the internal cache (though the application can add them manually using **SSL_CTX_add_session**(3)). Note: in any SSL/TLS servers where external caching is configured, any successful session lookups in the external cache (i.e. for session-resume requests) would normally be copied into the local cache before processing continues - this flag prevents these additions to the internal cache as well.

SSL_SESS_CACHE_NO_INTERNAL

Enable both SSL_SESS_CACHE_NO_INTERNAL_LOOKUP and SSL_SESS_CACHE_NO_INTERNAL_STORE at the same time.

SSL_SESS_CACHE_UPDATE_TIME

Updates the timestamp of the session when it is used, increasing the lifespan of the session. The session timeout applies to last use, rather then creation time.

The default mode is SSL_SESS_CACHE_SERVER.

RETURN VALUES

SSL_CTX_set_session_cache_mode() returns the previously set cache mode.

SSL_CTX_get_session_cache_mode() returns the currently set cache mode.

SEE ALSO

ssl(7), **SSL_set_session**(3), **SSL_session_reused**(3), **SSL_CTX_add_session**(3), **SSL_CTX_sess_number**(3), **SSL_CTX_sess_set_cache_size**(3), **SSL_CTX_sess_set_get_cb**(3), **SSL_CTX_set_session_id_context**(3), **SSL_CTX_set_timeout**(3), **SSL_CTX_flush_sessions**(3)

COPYRIGHT