TLS Persistence

Avi Technical Reference (v17.1)

TLS Persistence

view online

The TLS mode of persistence may be applied to any virtual service configured to terminate HTTPS. With this persistence method, Vantage embeds the client-to-server mapping within the TLS ticket ID, which is sent to the client, much the same way HTTP cookies behave. The data is embedded in an encrypted format that can be read by a Service Engine should a client reconnect to a different SE.

Note: This persistence method is often confused for an older, broken method of persistence called SSL Session ID. While both are used for secure connections, these methods are unrelated.

See also Overview of Server Persistence for descriptions of other persistence methods and options.

Persist Table

The TLS ticket ID is automatically mirrored to all Service Engines supporting the virtual service, regardless of this persistence mode. If this persistence is enabled, it adds no additional overhead to the SEs or the automated TLS ticket mirroring.

As with any SSL/TLS concurrency, additional memory is beneficial for increasing the maximum size of concurrent connections, and therefore TLS persistence mappings.

Configuration Options

- Name: A unique name for the persistence profile.
- Description: An optional, custom description for the profile.
- Type: TLS. Changing the type will change the profile to another persistence method.
- Select New Server When Persistent Server Down: If a server is marked down, such as by a health monitor or when it has reached a connection limit, should existing persisted users continue to be sent to the server, or load balanced to a new server?
    - Immediate: Vantage will immediately select a new server to replace the one marked down and switch the persistence entry to the new server.
    - Never: No replacement server will be selected. Persistent entries will be required to expire normally based upon the persistence type