SysMon Logger Server

Process

The Windows client autorun data is sent via a HTTPS (TLS) service to the server. The client uses the **server.pem** file as a certificate pinning mechanism, this allows the use of a self signed TLS certificate.

The client connects to the HTTPS port and sends data to the server. The request URL takes the form of:

https://1.2.3.4:8000/domain/host/user

All data sent from the client is compressed using GZIP. When the server recieves a new client connection, it decompresses the data and sends the data to one of the worker threads. The number of worker threads can be set within the configuration file, or can be auto set by the server e.g. 1 thread per core. A good default value is the number of cores divided by 2.

When the processor thread receives a new set of data, the event type is parsed, and the XML is then marshalled into internal data specific structs.