Docker Certified Associate

Mutually Authenticated TLS (MTLS)

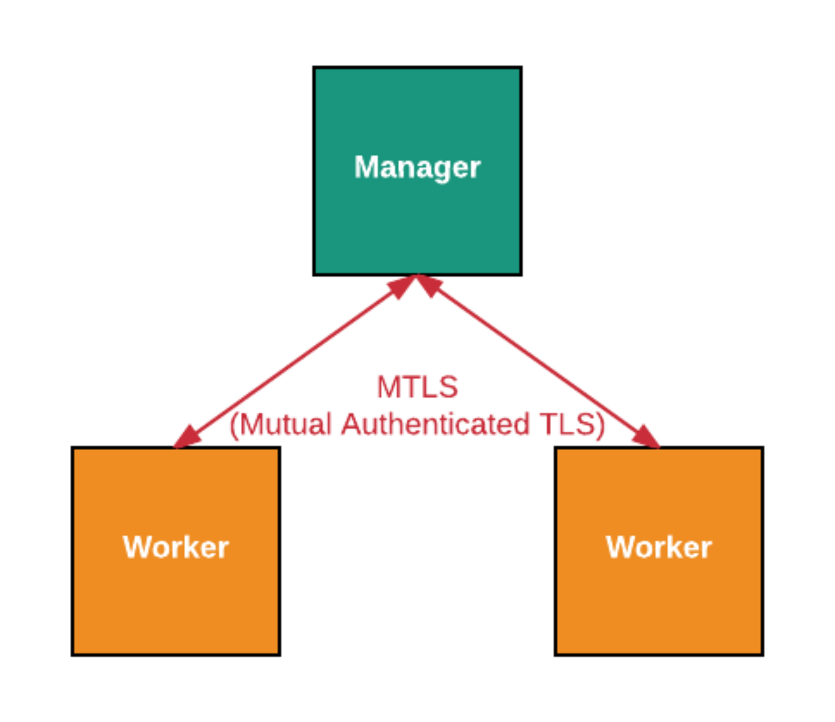
What is Mutually Authenticated TLS?

One of the primary goals of Docker Swarm is to be ‘secure by default’; a method to ensure communication within the swarm is implemented.

Mutually Authenticated TLS is the implementation that was chosen to secure that communication. Any time a swarm is initialized, a self-signed Certificate Authority (CA) is generated and issues certificates to every node (manager or worker) to facilitate those secure communications.

TLS (Transport Layer Security) was born from the Secure Sockets Layer (SSL) whose name is more well known. However, TLS has since superseded its use. Although their names are often used interchangeably, TLS provides greater security through message authentication, key material generation, and supported cipher suites.

Mutual Authentication TLS



Using the temporary certificates that are generated during a swarm initialization, workers and managers can register themselves with the swarm for communication.

Using TLS (Transport Layer Security) provides both privacy and data integrity in communications within the swarm.

The transaction consists of a two-layer (Record and Handshake) protocol that provides both security and authentication.