¿Qué es MQTT?

MQTT es un protocolo de mensajería basado en estándares, o un conjunto de reglas, que se utiliza para la comunicación de un equipo a otro. Los sensores inteligentes, los dispositivos portátiles y otros dispositivos de Internet de las cosas (IoT) generalmente tienen que transmitir y recibir datos a través de una red con recursos restringidos y un ancho de banda limitado. Estos dispositivos IoT utilizan MQTT para la transmisión de datos, ya que resulta fácil de implementar y puede comunicar datos IoT de manera eficiente. MQTT admite la mensajería entre dispositivos a la nube y la nube al dispositivo.

¿Por qué es importante el protocolo MQTT?

El protocolo MQTT se ha convertido en un estándar para la transmisión de datos de IoT, ya que ofrece los siguientes beneficios:

Ligero y eficiente

La implementación de MQTT en el dispositivo IoT requiere recursos mínimos, por lo que se puede usar incluso en pequeños microcontroladores. Por ejemplo, un mensaje de control MQTT mínimo puede tener tan solo dos bytes de datos. Los encabezados de los mensajes MQTT también son pequeños para poder optimizar el ancho de banda de la red.

Escalable

La implementación de MQTT requiere una cantidad mínima de código que consume muy poca energía en las operaciones. El protocolo también tiene funciones integradas para admitir la comunicación con una gran cantidad de dispositivos IoT. Por tanto, puede implementar el protocolo MQTT para conectarse con millones de estos dispositivos.

Fiable

Muchos dispositivos IoT se conectan a través de redes celulares poco fiables con bajo ancho de banda y alta latencia. MQTT tiene funciones integradas que reducen el tiempo que tarda el dispositivo IoT en volver a conectarse con la nube. También define tres niveles diferentes de calidad de servicio a fin de garantizar la fiabilidad para los casos de uso de IoT: como máximo una vez (0), al menos una vez (1) y exactamente una vez (2).

Seguro

MQTT facilita a los desarrolladores el cifrado de mensajes y la autenticación de dispositivos y usuarios mediante protocolos de autenticación modernos, como OAuth, TLS1.3, certificados administrados por el cliente, etc.

Admitido

Varios lenguajes, como Python, tienen un amplio soporte para la implementación del protocolo MQTT. Por lo tanto, los desarrolladores pueden implementarlo rápidamente con una codificación mínima en cualquier tipo de aplicación.

¿Qué historia hay detrás del protocolo MQTT?

El protocolo MQTT se inventó en 1999 para su uso en la industria del petróleo y el gas. Los ingenieros necesitaban un protocolo para un ancho de banda mínimo y una pérdida de batería mínima para supervisar los oleoductos vía satélite. Inicialmente, el protocolo se conocía como transporte de telemetría de Message Queue Server debido al producto de IBM MQ Series que admitió por primera vez su fase inicial. En 2010, IBM lanzó MQTT 3.1 como un protocolo gratuito y abierto para que cualquiera pudiera implementarlo, que después, en 2013, se envió al organismo de especificación de la Organización para el Avance de Estándares de Información Estructurada (OASIS) para su mantenimiento. En 2019, OASIS lanzó una versión 5 de MQTT actualizada. Ahora MQTT ya no es un acrónimo, sino que se considera el nombre oficial del protocolo.

¿Cuál es el principio en el que se basa MQTT?

El protocolo MQTT funciona según los principios del modelo de publicación o suscripción. En la comunicación de red tradicional, los clientes y servidores se comunican directamente entre sí. Los clientes solicitan recursos o datos del servidor, a continuación, el servidor procesa y envía una respuesta. Sin embargo, MQTT utiliza un patrón de publicación o suscripción para desacoplar el remitente del mensaje (editor) del receptor del mensaje (suscriptor). En lugar de ello, un tercer componente, denominado agente de mensajes, controla la comunicación entre editores y suscriptores. El trabajo del agente consiste en filtrar todos los mensajes entrantes de los editores y distribuirlos correctamente a los suscriptores. El agente desacopla los editores y suscriptores de la siguiente manera:

Desacoplamiento espacial

El editor y el suscriptor no conocen la ubicación de la red del otro y no intercambian información como direcciones IP o números de puerto.

Desacoplamiento de tiempo

El editor y el suscriptor no se ejecutan ni tienen conectividad de red al mismo tiempo.

Desacoplamiento de sincronización

Tanto los editores como los suscriptores pueden enviar o recibir mensajes sin interrumpirse entre sí. Por ejemplo, el suscriptor no tiene que esperar a que el editor envíe un mensaje.

¿Qué son los componentes MQTT?

MQTT implementa el modelo de publicación o suscripción mediante la definición de clientes y agentes, tal y como se muestra a continuación.

Cliente MQTT

Un cliente MQTT es cualquier dispositivo, desde un servidor hasta un microcontrolador, que ejecuta una biblioteca MQTT. Si el cliente envía mensajes, actúa como editor, y si recibe mensajes, actúa como receptor. Básicamente, cualquier dispositivo que se comunique mediante MQTT a través de una red puede denominarse dispositivo cliente MQTT.

Agente MQTT

El agente MQTT es el sistema de *back-end* que coordina los mensajes entre los diferentes clientes. Las responsabilidades del agente incluyen recibir y filtrar mensajes, identificar a los clientes suscritos a cada mensaje y enviarles los mensajes. También se encarga de otras tareas como:

- La autorización y autenticación de clientes MQTT
- Pasar mensajes a otros sistemas para su posterior análisis
- El control de mensajes perdidos y sesiones de clientes

Conexión MQTT

Los clientes y los agentes comienzan a comunicarse mediante una conexión MQTT. Los clientes inician la conexión al enviar un mensaje *CONECTAR* al agente MQTT. El agente confirma que se ha establecido una conexión al responder con un mensaje *CONNACK*. Tanto el cliente MQTT como el agente requieren una pila TCP o IP para comunicarse. Los clientes nunca se conectan entre sí, solo con el agente.

¿Cómo funciona MQTT?

A continuación, se proporciona una descripción general del funcionamiento de MQTT.

1. Un cliente MQTT establecer una conexión con el agente MQTT.
2. Una vez conectado, el cliente puede publicar mensajes, suscribirse a mensajes específicos o hacer ambas cosas.
3. Cuando el agente MQTT recibe un mensaje, lo reenvía a los suscriptores que están interesados.

Analicemos los detalles para una mayor comprensión.

Tema de MQTT

El término “tema” se refiere a las palabras clave que utiliza el agente MQTT a fin de filtrar mensajes para los clientes de MQTT. Los temas están organizados jerárquicamente, de forma similar a un directorio de archivos o carpetas. Por ejemplo, considere un sistema doméstico inteligente que opera en una casa de varios pisos que tiene diferentes dispositivos inteligentes en cada uno de ellos. En ese caso, es posible que el agente MQTT organice temas como:

ourhome/groundfloor/livingroom/light

ourhome/firstfloor/kitchen/temperature

Publicación MQTT

Los clientes MQTT publican mensajes que contienen el tema y los datos en formato de bytes. El cliente determina el formato de los datos, como datos de texto, datos binarios, archivos XML o JSON. Por ejemplo, es posible que una lámpara del sistema doméstico inteligente publique un mensaje sobre el tema *salón o luz*.

Suscripción MQTT

Los clientes MQTT envían un mensaje *SUBSCRIBE* (SUBSCRIBIRSE) al agente MQTT para recibir mensajes sobre temas de interés. Este mensaje contiene un identificador único y una lista de suscripciones. Por ejemplo, la aplicación de hogar inteligente en su teléfono quiere mostrar cuántas luces están encendidas en casa. Se suscribirá a la *luz* del tema y aumentará el contador para todos los mensajes *activados*.

¿Qué es MQTT sobre WSS?

MQTT sobre WebSockets (WSS) es una implementación de MQTT para recibir datos directamente en un navegador web. El protocolo MQTT define un cliente de JavaScript para proporcionar compatibilidad con WSS para navegadores. En este caso, el protocolo funciona como de costumbre, pero agrega encabezados adicionales a los mensajes MQTT para admitir también el protocolo WSS. Puede considerarlo como la carga útil del mensaje MQTT ajustada en un sobre WSS.

¿MQTT es seguro?

La comunicación MQTT utiliza el protocolo SSL para proteger los datos confidenciales que transmiten los dispositivos IoT. Puede implementar la identidad, la autenticación y la autorización entre los clientes y el agente mediante certificados SSL y contraseñas. El agente MQTT normalmente autentica a los clientes mediante sus contraseñas, así como los identificadores de cliente únicos que asigna a cada cliente. En la mayoría de las implementaciones, el cliente autentica el servidor con certificados o búsquedas de DNS. También puede implementar protocolos de cifrado con MQTT.