$SYS

By Naveen PS

MAKERDEMY
LEARN EXPLORE MAKE

$SYS

Monitoring your systems is extremely important for production environments. When deploying an MQTT broker or a cluster of MQTT brokers, the operation team needs to know the health of the MQTT servers and uses monitoring data to circumvent foreseeable future problems. During the past few years, a feature of many MQTT brokers, the so-called SYS-Topics, has gained popularity not only for debugging and developing MQTT systems but also for monitoring. This blog post discusses the use of SYS-Topics for monitoring and explains when to use - and more importantly - when NOT to use SYS-Topics.

Many MQTT brokers implement SYS-Topics. These topics are special meta topics that the broker can use to publish information about the broker itself and its MQTT client sessions. All SYS-Topics start with $SYS and are read-only for MQTT clients. The MQTT broker should prevent clients from using such topic names to publish messages.

Brokers publish SYS-Topics periodically, the default period on most brokers is 60 seconds. All MQTT clients that subscribe to one or more SYS-Topics receive the current value on the SYS topics as soon as they subscribe. After the subscription was successful, the client will receive metrics on periodical basis. Some static SYS-Topics (e.g. broker version) are only published upon subscription.

SYS-Topics can be used for developing and debugging MQTT applications. Developers can quickly monitor the current state of the broker and calculate and verify metrics such as message amplification rate or network metrics.

Although SYS-Topics have use-cases for development and debugging, SYS-Topics are not suitable for monitoring broker instances in production. If you need to rely on the availability guarantees of your MQTT broker, use an actual monitoring system, SYS-Topics do not replace monitoring applications.

5 reasons SYS-Topics are not suitable for production monitoring:

1. Metric resolution is not good enough

The metric publishing interval for most MQTT brokers is 60 seconds by default. So, the broker does not dictate the monitoring system how the resolution should be. The monitoring system can decide how often new data should be collected, without modifying any configuration on the MQTT broker.

2. SYS-Topics provide only a subset of the available metrics

While the metrics provided by SYS-Topics can be useful, they are only a small subset of all available metrics. The SYS-Topic Metrics usually are more focused on MQTT session monitoring and thus don't provide metrics that can give you an overview of the brokers health at a quick glance. The most interesting metrics for operation teams are usually product dependant, so it's unlikely that a common SYS-Topic standard will cover these in the future.

3. SYS-Topics expose internal information to potential attackers

To make it more difficult for an attacker to use exploits that target a specific software version, it is a common best practice to conceal the actual software version that is used in a deployment. Frequently, you also want to hide the actual software that is used from attackers. While you should never rely on 'Security by Obscurity' as your primary security measure, it's still important to hide this deployment information. SYS-Topics expose key information such as the Broker Software Used and the Version Number to every subscriber. This information can be valuable for attackers but is seldom useful to legitimate subscribers.

4. It's hard to monitor broker clusters with SYS-Topics

If someone wants to build a custom monitoring solution based on SYS-Topics, MQTT connections to all cluster nodes need to be established. Typically, MQTT clusters are behind a load balancer, so often it's not even possible to connect to a specific cluster node. That's much harder to achieve with SYS-Topics.

5. The monitored channel should be separated from the monitoring channel

A good monitoring practice is to use a dedicated monitoring channel instead of using the same channel you are monitoring. With MQTT brokers, this means that if you are monitoring the MQTT communication, you shouldn't use MQTT (SYS-Topics) to monitor the MQTT communication. It's the same as: Don't use e-mail alerts for monitoring e-mail servers. If the MQTT communication is not available for any reason, you won't get any monitoring data. The monitoring data may be most valuable especially when unexpected occurs. If you rely on this data for the alert, you may have a problem.

THE END