



# MQTT in the Enterprise

How to successfully run an MQTT Message Broker

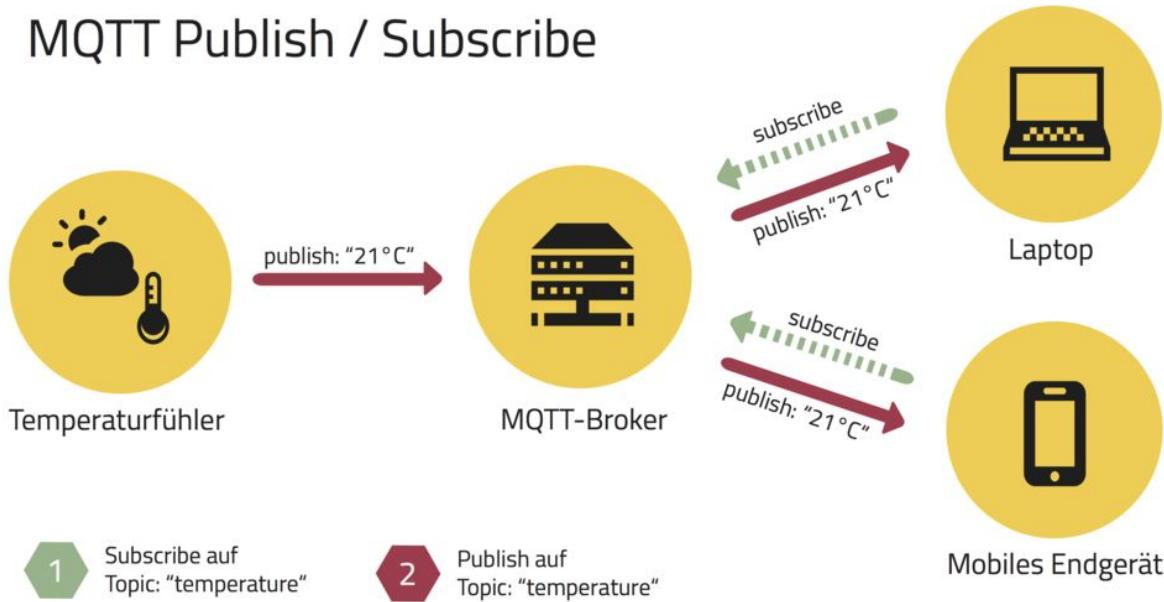
Arnold Bechtoldt  
@arnisoph

5 Learnings from 2+ years of  
solving challenges!

?

# MQTT in a Nutshell

## MQTT Publish / Subscribe





Background



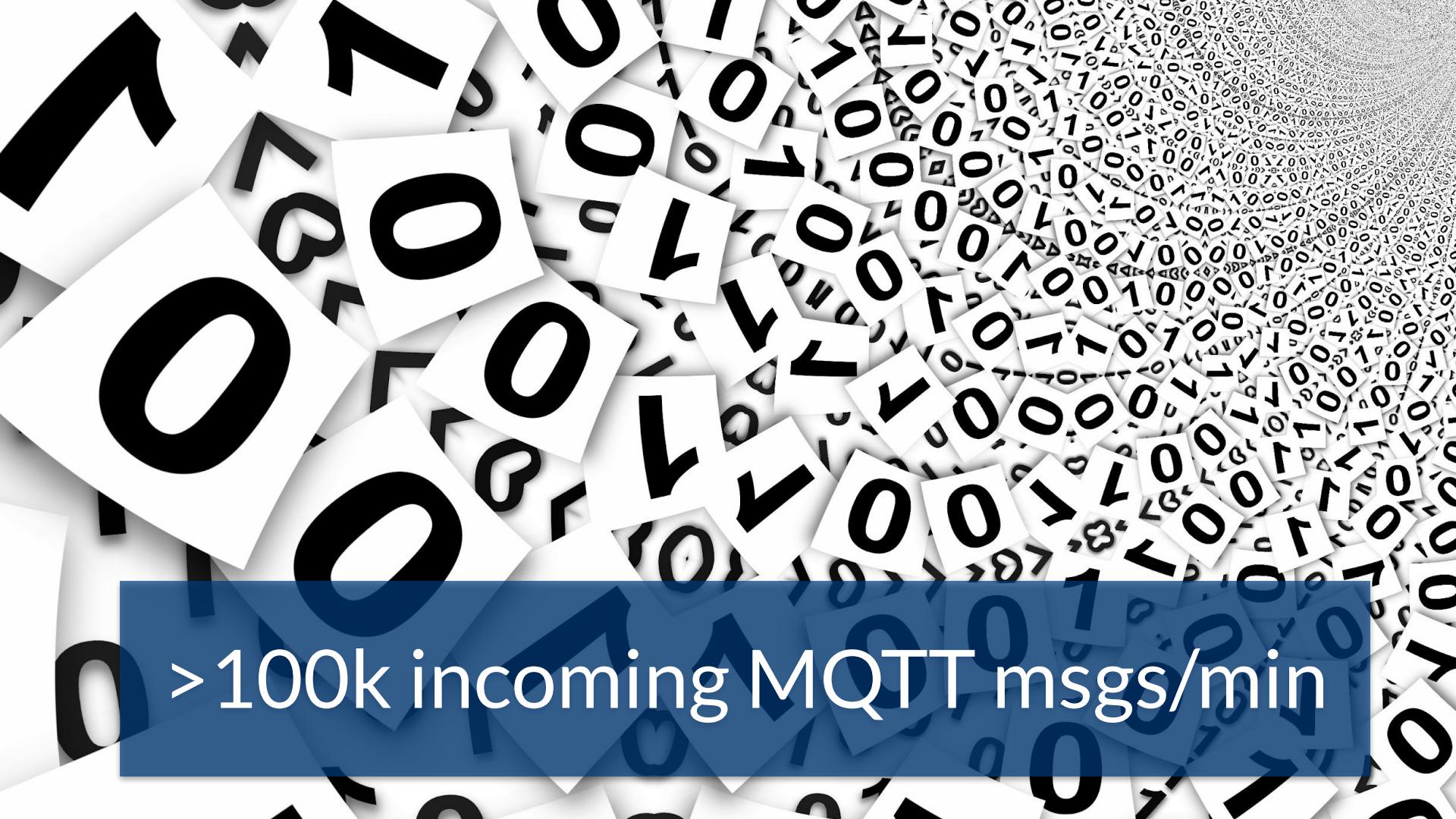
>30k MQTT Sessions



>140k MQTT Subscriptions



>200k Queued Messages



>100k incoming MQTT msgs/min



# Nodes in Prod: 3

# HiveMQ: Our Message Broker

hivemq / hivemq-community-edition

Watch 24 Star 166 Fork 32

Code Issues 3 Pull requests 2 Wiki Security Insights

HiveMQ CE is a Java-based open source MQTT broker that fully supports MQTT 3.x and MQTT 5. It is the foundation of the HiveMQ Enterprise Connectivity and Messaging Platform <https://www.hivemq.com>

mqtt-broker hivemq mqtt iot java messaging pubsub m2m iot-middleware broker mqtt-protocol mqtt-server

6 commits 3 branches 1 release 4 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find File Clone or download

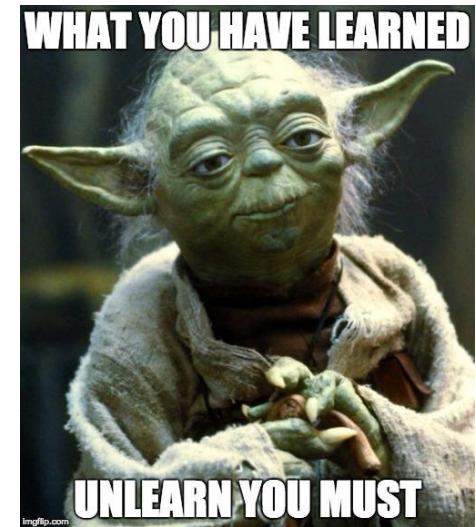
fraschbi	Develop (#12)	Latest commit e8c007e on 29 Apr
.github	Added issue and pull request templates (#2)	this year
.idea	Initial commit of HiveMQ Community Edition	this year
gradle	Initial commit of HiveMQ Community Edition	this year
src	Develop (#12)	last month
.gitignore	Initial commit of HiveMQ Community Edition	this year
.travis.yml	Develop (#12)	last month
CONTRIBUTING.adoc	Develop (#12)	last month
HEADER	Initial commit of HiveMQ Community Edition	this year
LICENSE	Initial commit of HiveMQ Community Edition	this year
README.adoc	Develop (#12)	last month

## Lesson #1

# MQTT: Things are different!

# MQTT: Things are different!

- Rules from HTTP world won't apply
- Lack of MQTT tooling (load testing, monitoring)
- Simple protocol vs. misbehaving clients
- HiveMQ is a stateful app, deal with it!



A Siemens cordless phone is positioned in the foreground on the left, its keypad clearly visible. Behind it, a vintage black rotary phone lies on its side, its circular dial and handset partially visible against a blurred background of green foliage.

## Lesson #2 The “I” in IoT

# The “I” in IoT

- Clients with bad internet connection (GSM/UMTS)
- MQTT clients lack of (network) fault tolerance
- Most support tickets caused by network issues (clients/ISP)
- Seek & Destroy with Monitoring!

# Lesson #3

## Monitor your (MQTT) clients...



# HiveMQ Webinterface

 **HIVEMQ**  
ENTERPRISE MQTT BROKER

[beekeeper](#) | [Logout](#)

[Dashboard](#)

[Clients](#)

[License](#)

[Plugins](#)

[Trace Recordings](#)

[Analytics](#)

Dropped Messages

Help

HiveMQ 3.4.3

## Dashboard

Connections: 9,642   Inbound Publish Rate: 467 / s   Outbound Publish Rate: 2,068 / s   Subscriptions: 144,326   Retained Messages: 67,464   Queued Messages: 203,360   Cluster Nodes: 3

### Connections per Cluster Node (stacked)

Cluster Nodes: Node 0959H, Node xt2c3, Node zwF9B

### Notifications

- 2019/05/27 19:27:19.227 Dropped Message: Client not connected
- 2019/05/07 14:19:42.208 Dropped Message: QoS 0 channel not writable
- 2019/05/03 15:44:34.099 Dropped Message: Full inflight message queue
- 2019/05/02 21:07:38.839 Dropped Message: QoS 0 queue not empty

### Active License Information

Connections: 9,642 / Unlimited  
License Type: Valid, Commercial License  
Maximum Connections: Unlimited  
Cluster License: ✓  
Filename: hivemq.lic

### Statistics per Cluster Node

Node	JVM Memory	Total Inbound Publish Messages	Total Outbound Publish Messages	HiveMQ Version	Total Inbound Volume	Total Outbound Volume	Inbound Network Traffic	Outbound Network Traffic
O959H*	5.83 GB / 22.80 GB	376,638,709	995,237,568	3.4.3	50.39 GB	131.47 GB	20.23 KB/s	20.29 KB/s
xt2c3								
zwF9B								

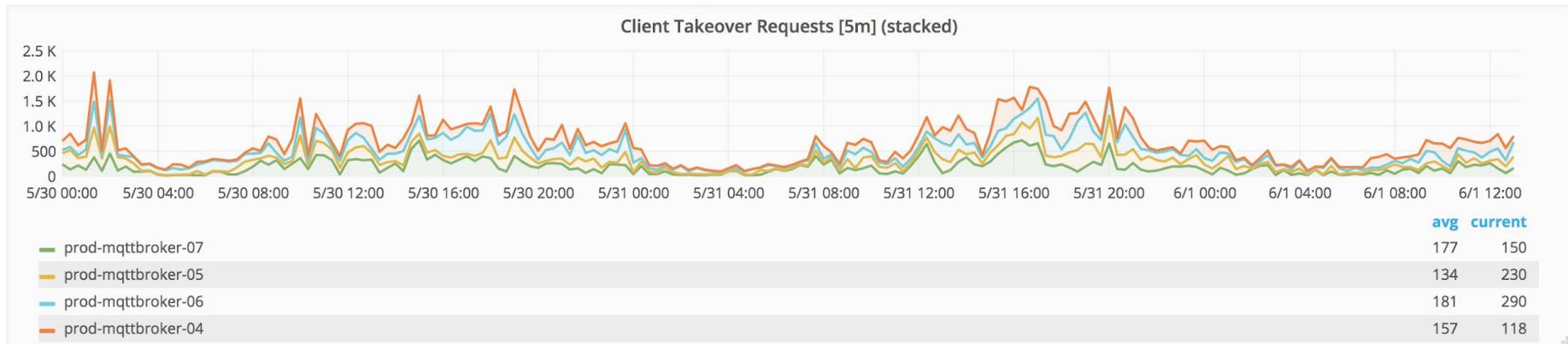
16

# HiveMQ Prometheus Metrics (> 1800)

```
metrics_com_hivemq_messages_dropped_before_publish_send_count_count 0.0
metrics_com_hivemq_messages_dropped_count_count 6092213.0
metrics_com_hivemq_messages_dropped_in_flight_window_count_count 835421.0
metrics_com_hivemq_messages_dropped_internal_error_count_count 0.0
metrics_com_hivemq_messages_dropped_not_connected_count_count 1238.0
metrics_com_hivemq_messages_dropped_not_writable_count_count 4775796.0
metrics_com_hivemq_messages_dropped_qos_0_queue_not_empty_count_count 479758.0
metrics_com_hivemq_messages_dropped_queue_full_count_count 0.0
metrics_com_hivemq_messages_dropped_rate_count 6092213.0
metrics_com_hivemq_messages_dropped_rate_fifteenminuterate 0.0026798488064779242
metrics_com_hivemq_messages_dropped_rate_fiveminuterate 0.003673811334623905
metrics_com_hivemq_messages_dropped_rate_meanrate 1.1690383860629943
metrics_com_hivemq_messages_dropped_rate_oneminuterate 0.0024693484286362477
metrics_com_hivemq_messages_incoming_connect_count_count 1.0997633E7
metrics_com_hivemq_messages_incoming_connect_rate_count 1.0997633E7
metrics_com_hivemq_messages_incoming_connect_rate_fifteenminuterate 2.695426446661923
metrics_com_hivemq_messages_incoming_connect_rate_fiveminuterate 2.846849980596273
metrics_com_hivemq_messages_incoming_connect_rate_meanrate 2.110342385291968
metrics_com_hivemq_messages_incoming_connect_rate_oneminuterate 2.890580707427736
metrics_com_hivemq_messages_incoming_disconnect_count_count 3926444.0
metrics_com_hivemq_messages_incoming_disconnect_rate_count 3926444.0
metrics_com_hivemq_messages_incoming_disconnect_rate_fifteenminuterate 0.8603151573544764
metrics_com_hivemq_messages_incoming_disconnect_rate_fiveminuterate 0.8937906297328476
metrics_com_hivemq_messages_incoming_disconnect_rate_meanrate 0.7534476952336496
metrics_com_hivemq_messages_incoming_disconnect_rate_oneminuterate 0.848894289974284
metrics_com_hivemq_messages_incoming_pingreq_count_count 1.6680187E8
```

# Grafana Dashboard

▼ Publishments/Queues/Monitoring



Graph

General

Metrics

Axes

Legend

Display

Alert

Time range

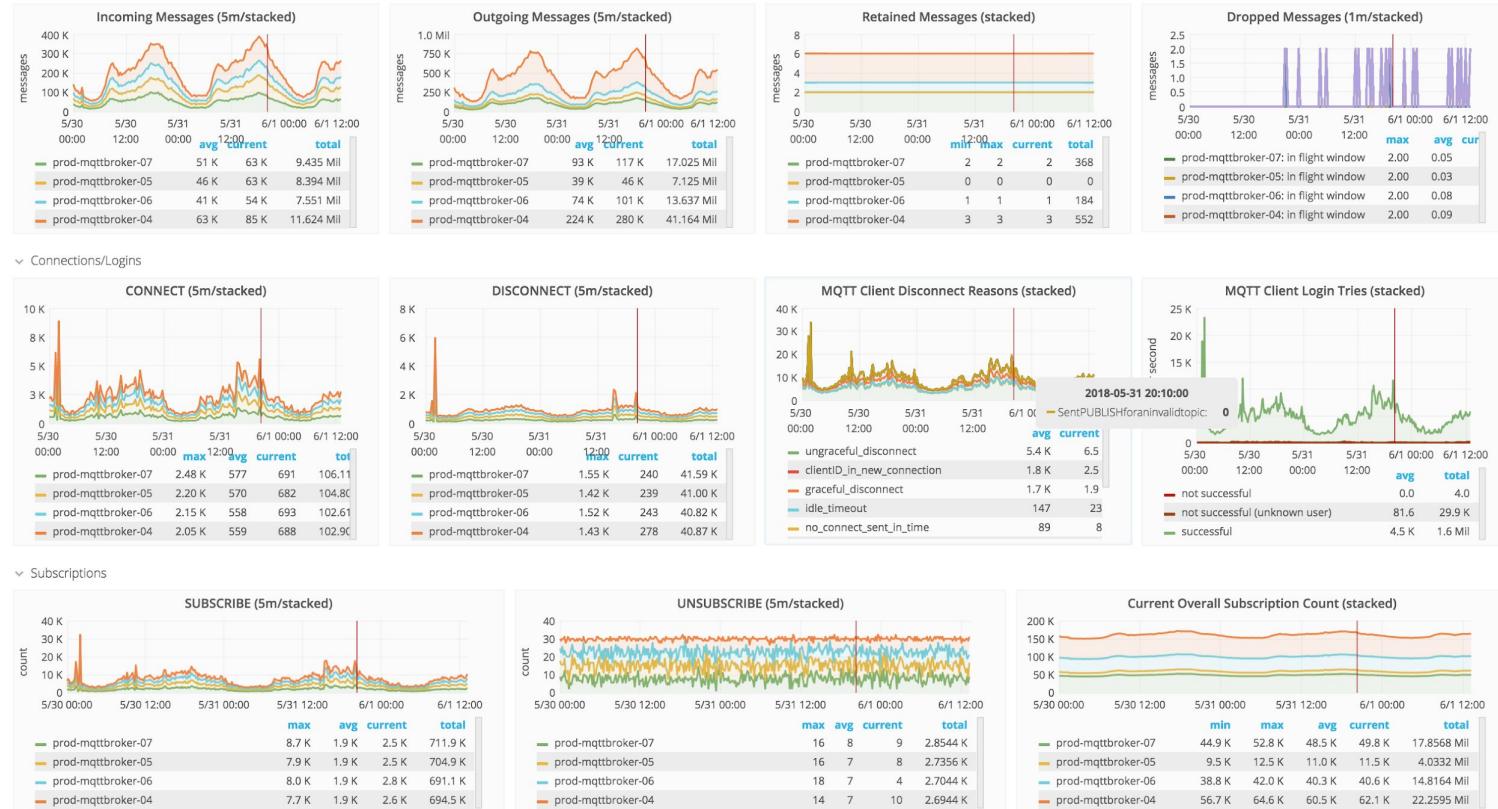
x

▲ A Query `increase(metrics_com_hivemq_cluster_sent_clienttakeoverrequest_count{group=\"$group",inst:`

Metric lookup metric name ☰ ⚡ 🗑

Legend format `{{instance_name}}` Step 10m ⓘ Resolution 1/2 ▾ ⟳

# Grafana Dashboard (2)

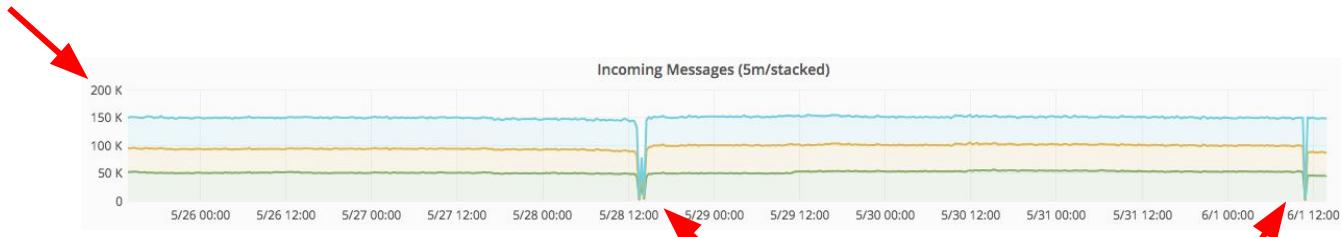


# Grafana Dashboard (3)



# Problem: Dev/Prod Parity

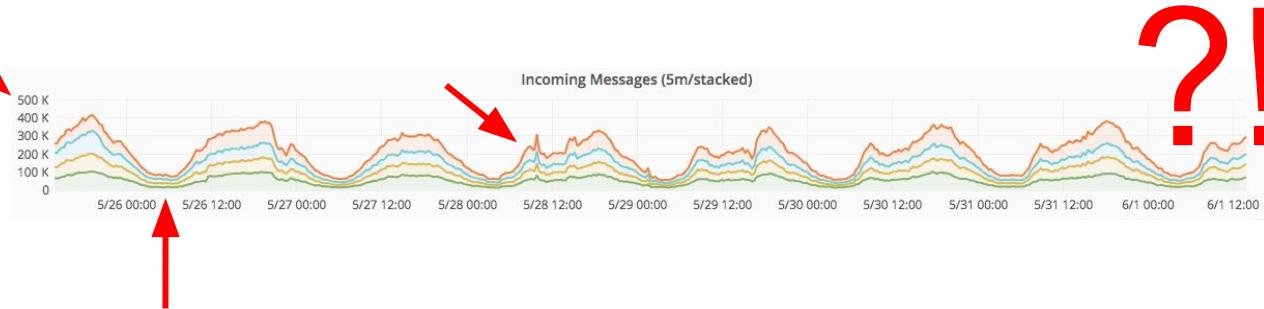
Testing



Integration



Production



# Lesson #4

## Log everything

\*GDPR/DSGVO Disclaimer ...

## Unstructured logs as base ...

2018-06-01T18:25:30,737Z [hivemq-native-eventloop-child-15] DEBUG event.client-connected - Client ID: mqttlinkstatusaggregator, IP: , Clean  
2018-06-01T18:25:31,452Z [hivemq-native-eventloop-child-3] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungracefull  
2018-06-01T18:25:31,788Z [hivemq-native-eventloop-child-5] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:31,829Z [single-writer-9] DEBUG event.client-disconnected - Client ID: mqttlinkstatusaggregator, IP: was disconnected. re  
2018-06-01T18:25:31,830Z [hivemq-native-eventloop-child-15] DEBUG event.client-disconnected - Client ID: mqttlinkstatusaggregator, IP: l dis  
2018-06-01T18:25:33,453Z [hivemq-native-eventloop-child-7] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungracefull  
2018-06-01T18:25:33,790Z [hivemq-native-eventloop-child-9] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:34,016Z [hivemq-native-eventloop-child-10] DEBUG event.client-connected - Client ID: mqttlinkstatusaggregator, IP: , Clean  
2018-06-01T18:25:35,124Z [single-writer-9] DEBUG event.client-disconnected - Client ID: mqttlinkstatusaggregator, IP: : was disconnected. re  
2018-06-01T18:25:35,125Z [hivemq-native-eventloop-child-10] DEBUG event.client-disconnected - Client ID: mqttlinkstatusaggregator, IP: dis  
2018-06-01T18:25:35,455Z [hivemq-native-eventloop-child-15] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungraceful  
2018-06-01T18:25:35,791Z [hivemq-native-eventloop-child-1] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:36,218Z [hivemq-native-eventloop-child-2] DEBUG event.client-connected - Client ID: mqttlinkstatusaggregator, IP: , Clean  
2018-06-01T18:25:37,347Z [single-writer-14] DEBUG event.client-disconnected - Client ID: mqttlinkstatusaggregator, IP: ! was disconnected. r  
2018-06-01T18:25:37,348Z [hivemq-native-eventloop-child-2] DEBUG event.client-disconnected - Client ID: mqttlinkstatusaggregator, IP: disc  
2018-06-01T18:25:37,457Z [hivemq-native-eventloop-child-7] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungracefull  
2018-06-01T18:25:37,795Z [hivemq-native-eventloop-child-9] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:38,700Z [hivemq-native-eventloop-child-11] DEBUG event.client-connected - Client ID: test-mqttdbrokerlb-03-haproxy-healthchecker, IP:10  
2018-06-01T18:25:38,706Z [hivemq-native-eventloop-child-11] DEBUG event.client-disconnected - Client ID: test-mqttdbrokerlb-03-haproxy-healthchecker, IP  
2018-06-01T18:25:39,459Z [hivemq-native-eventloop-child-15] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungraceful  
2018-06-01T18:25:39,797Z [hivemq-native-eventloop-child-1] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:40,221Z [hivemq-native-eventloop-child-2] DEBUG event.client-disconnected - Client ID: vehicel eMockListener1521022427024, IP ;  
2018-06-01T18:25:41,460Z [hivemq-native-eventloop-child-5] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungracefull  
2018-06-01T18:25:41,798Z [hivemq-native-eventloop-child-7] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:43,462Z [hivemq-native-eventloop-child-9] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungracefull  
2018-06-01T18:25:43,807Z [hivemq-native-eventloop-child-11] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull  
2018-06-01T18:25:44,521Z [hivemq-native-eventloop-child-13] DEBUG event.client-connected - Client ID: test-mqttdbrokerlb-04-haproxy-healthchecker, IP:10  
2018-06-01T18:25:44,529Z [hivemq-native-eventloop-child-13] DEBUG event.client-disconnected - Client ID: test-mqttdbrokerlb-04-haproxy-healthchecker, IP  
2018-06-01T18:25:44,978Z [hivemq-native-eventloop-child-1] DEBUG event.client-connected - Client ID: mqttlinkstatusaggregator, IP: , Clean  
2018-06-01T18:25:45,464Z [hivemq-native-eventloop-child-5] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.25 disconnected ungracefull  
2018-06-01T18:25:45,808Z [hivemq-native-eventloop-child-7] DEBUG event.client-disconnected - Client ID: UNKNOWN, IP:10.9.54.31 disconnected ungracefull

# ... manipulated with Logstash

```
# fix a few inconsistencies in the original log format before offering the log line to kv for parsing
mutate {
    gsub => [
        "LOGMESSAGE", "connected\.$", "",
        "LOGMESSAGE", "\swas disconnected\.", "",",
        "LOGMESSAGE", "disconnected gracefully\?", ", reason: graceful_disconnect",
        "LOGMESSAGE", "disconnected ungracefully\?", ", reason: ungraceful_disconnect",
        "LOGMESSAGE", "An other client connected with the same client id.$", "clientID_in_new_connection",
        "LOGMESSAGE", "Another client connected with the same clientId.$", "clientID_in_new_connection",
        "LOGMESSAGE", "Client was idle for too long.$", "idle_timeout",
        "LOGMESSAGE", "Outgoing publish message was dropped\.", "",
        "LOGMESSAGE", "reason: Internal error\.$", "reason: internal_error",
        "LOGMESSAGE", "reason: No CONNECT sent in time.$", "reason: no_connect_sent_in_time",
        "LOGMESSAGE", "reason:", "event_reason:",
        "LOGMESSAGE", "\.$", ""
    ]
}

kv {
    source => "LOGMESSAGE"
    prefix => "mqtt_"
    field_split => ","
    value_split => ":"
    remove_char_value => " "
    remove_char_key => " "
    transform_key => "lowercase"
}
```

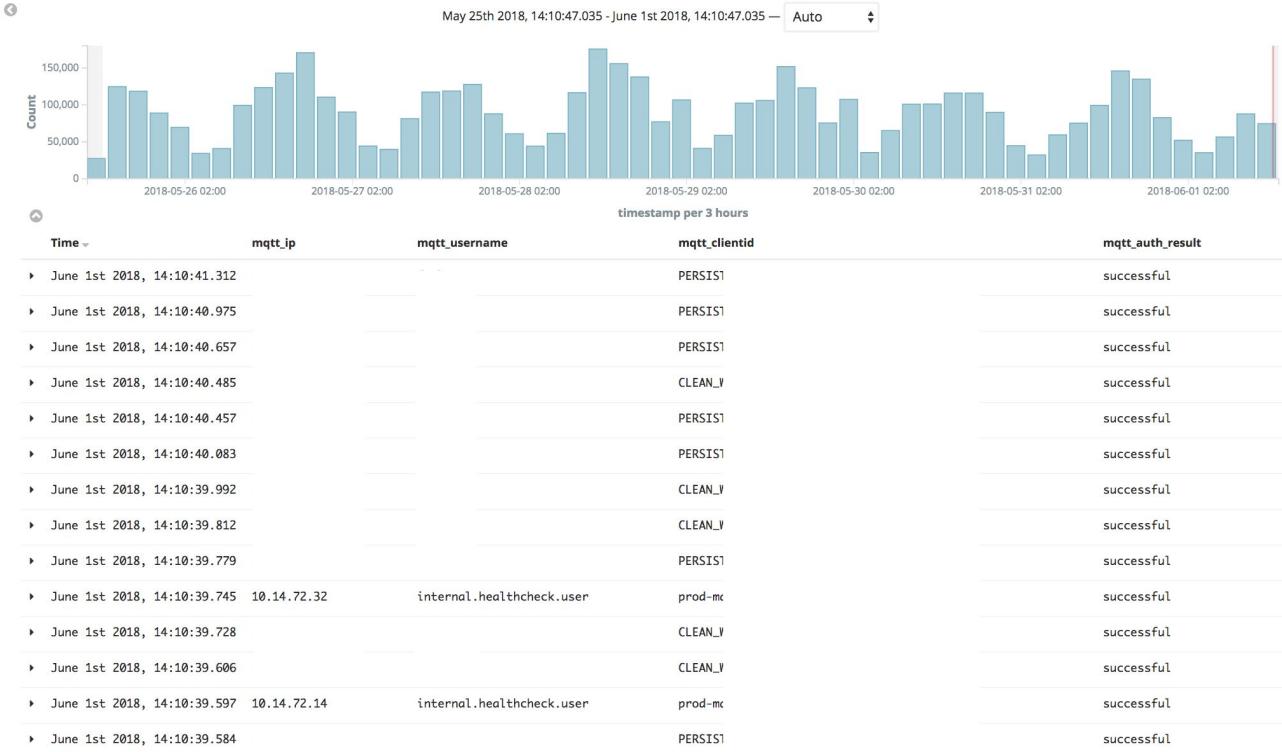
# Prepared for general use

## Quick Links

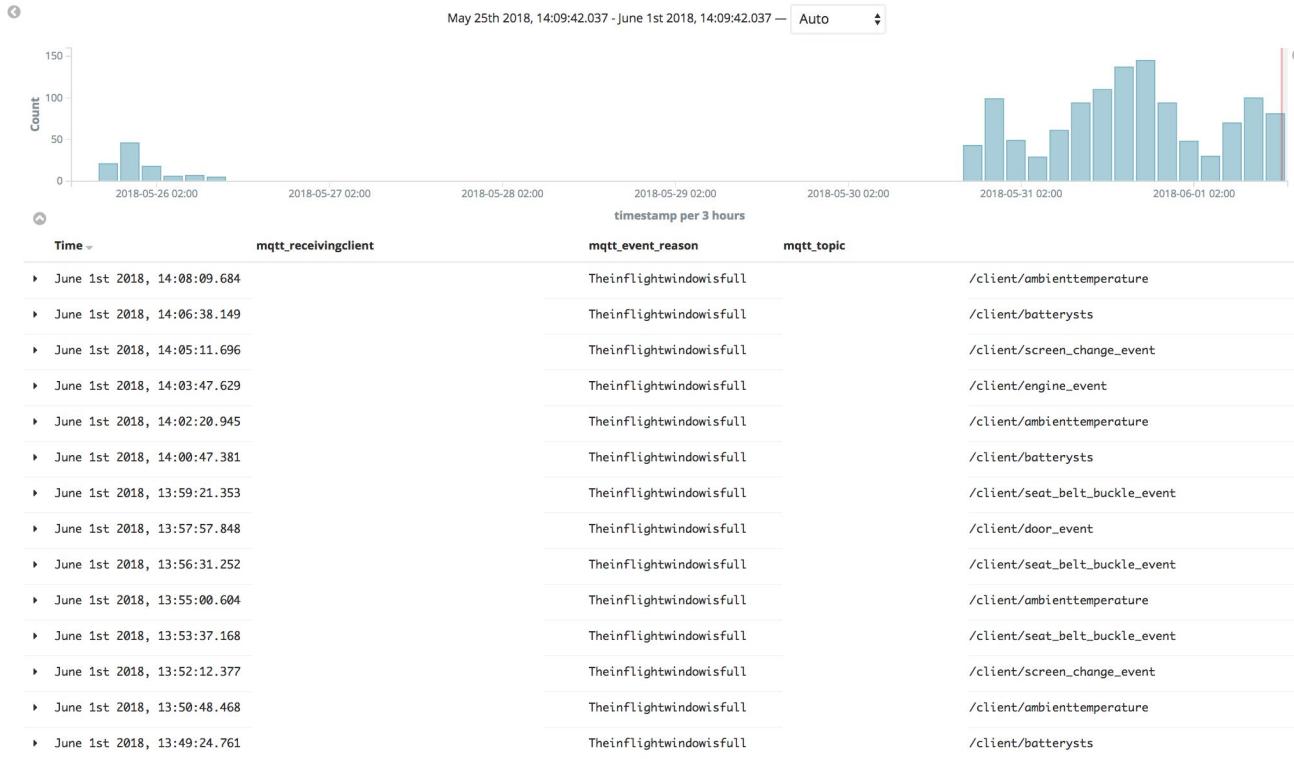
The following links help you to find some query examples. Open an example and modify to your own needs:

Use Case	Index	TEST	INT	PROD	Comment
Login details (after connect)	*-mqttbroker-authplugin-*	Kibana	Kibana	Kibana	(user abc)
Login details by VIN (after connect)	*-mqttbroker-authplugin-*	Kibana	Kibana	Kibana	(vehicle XYZ)
Connects/Disconnects by VIN	*-mqttbroker-events-*	Kibana	Kibana	Kibana	(vehicle XYZ)
Non-graceful disconnects	*-mqttbroker-events-*	Kibana	Kibana	Kibana	
MQTT Message Drops	*-mqttbroker-events-*		Kibana	Kibana	
HTTP IP Triggers	*-mqttbroker-restplugin-*	Kibana	Kibana	Kibana	
MQTT actions by VIN	*-mqttbroker-logs-*	Kibana	Kibana	Kibana	(vehicle XYZ)

# ... to show MQTT client login



# ... or dropped messages!



## Lesson #5

# Ain't Nobody Got Time for That: Security

# Kritische Lücken im Automatisierungs-Baustein Siemens LOGO!

Ein offener Port und alle Passwörter lassen sich darüber auslesen – aber Updates gibt es keine.

Von Jürgen Schmidt



(Bild: Siemens)

- Unsecured TCP port
- Hardcoded enc key
- Leaks passwords
- No firmware updates
- Vendor recommends: RTFM



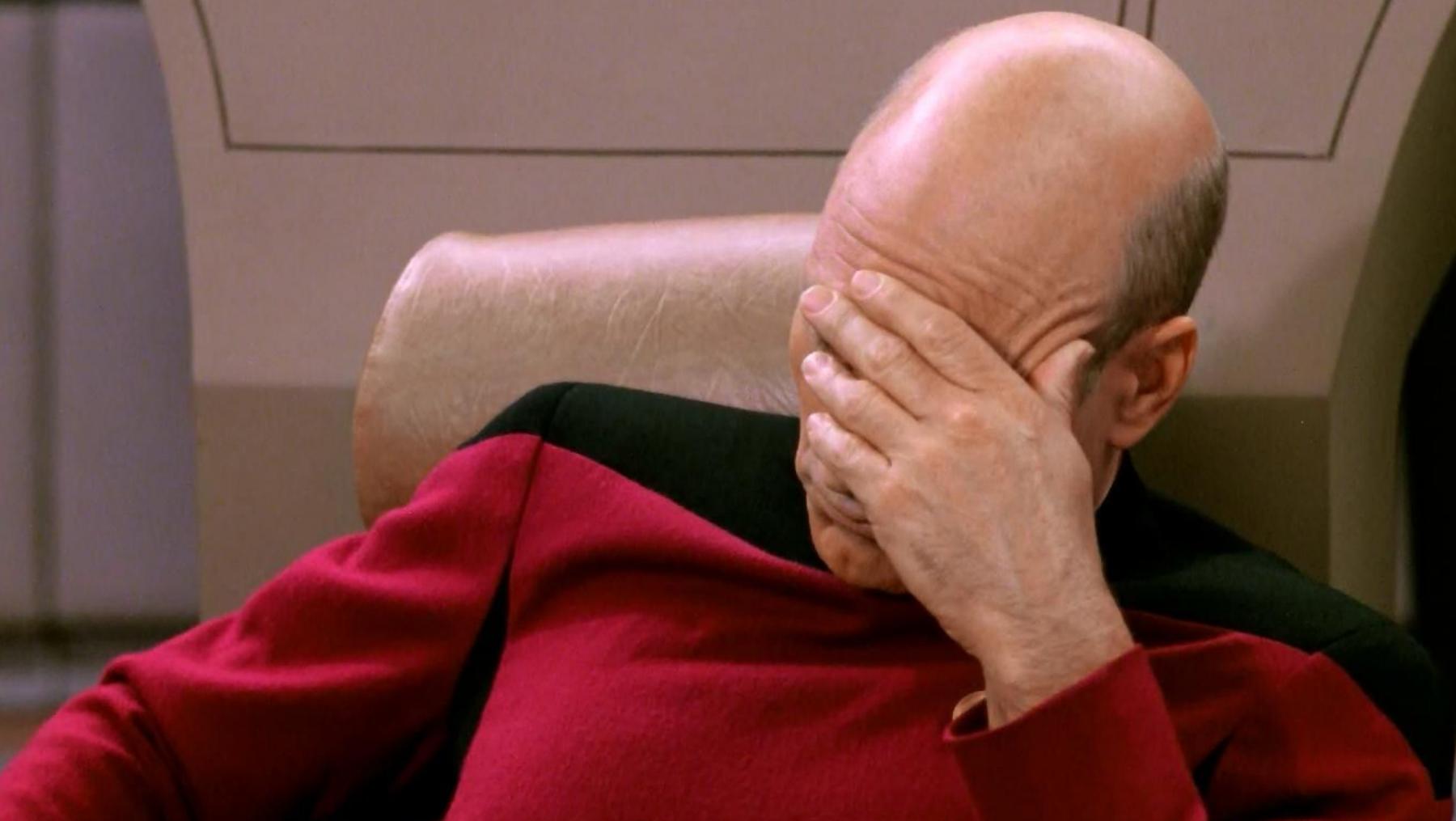
# Ain't Nobody Got Time for That: Security

*Problem Exists Between Chair And Keyboard (PEBCAK)*

# A PEBCAK example..

Do not ...

- forget authorization after implementing authentication (MQTT).
- use the password across ten thousands of clients.
- implement HW/SW with max password length of 8 chars.
- log them as plaintext into Elasticsearch.
- forget the firewall in front of your public Elasticsearch.
- publish *The Password™* on Github.



# Key Takeaways

- MQTT is different
- Share broker insights (Metrics, Logs)
- Keep in touch with your Devs
- Continuously improve broker and client security
- Choose your hosting provider wisely
- As broker team you'll be single point of contact

# Our MQTT tools on Github

- [github.com/inovex/mqtt-stresser](https://github.com/inovex/mqtt-stresser)
- [github.com/inovex/mqtt\\_blackbox\\_exporter](https://github.com/inovex/mqtt_blackbox_exporter)
- ... and more for beer!



# GitHub

WE'RE  
HIRING!  
[inovex.de/jobs](http://inovex.de/jobs)

## IT Engineering & Operations – Wir bauen Clouds

inovex ist seit vielen Jahren auf die Architektur, Realisierung und Betreuung von modernen IT-Infrastrukturen spezialisiert.

In unserer Unit „IT Engineering & Operations“ entstehen Cloud-Plattformen, die entweder komplett als Private Cloud oder als hybride Cloud im Zusammenspiel mit den großen Public Clouds (Amazon, Google, Microsoft) realisiert werden. Mit den „inovex Cloud Services“ unterhalten wir außerdem eine eigene Cloud-Plattform, auf der wir für Kunden digitale Lösungen im DevOps-Modus betreiben.

Für unser ITO-Team suchen wir *dich!* Du bist von Linux begeistert, hast einen Engineering Background und Lust, dich mit neuen Technologien zu beschäftigen? Dann bist du bei uns genau richtig! Was wir tun, wen wir suchen und wie es ist, bei uns zu arbeiten – das kannst du dir hier schon einmal ansehen. Und wenn du dann denkst, das könnte passen, freuen wir uns auf deine Bewerbung!

Dein ITO-Team bei inovex.

PS: Wir suchen für alle unsere Standorte neue Kolleg\*innen. Ganz besonders allerdings für unser [Office in München](#). Wenn dich das interessiert – hier gibt es mehr Infos zu inovex München.



Wir bauen Clouds  
Smarte Plattformen für die Digitale Transformation.



Engineeren statt administrieren  
Es geht immer noch ein bisschen automatischer.



Der inovex Spirit  
Wir machen unsere Kunden glücklich. Und uns selbst.



Wir leben DevOps  
Cloud Engineering ist agile Software-Entwicklung.



**WE'RE  
HIRING!**  
[inovex.de/jobs](http://inovex.de/jobs)



# Arnold Bechtoldt

inovex

[arnold.bechtoldt@inovex.de](mailto:arnold.bechtoldt@inovex.de)

---

[github.com/bechtoldt](https://github.com/bechtoldt)

@arnisoph

[youtube.com/inovexGmbH](https://youtube.com/inovexGmbH)

[arbe.io](https://arbe.io)

[inovex.de](https://inovex.de)

[inovex.de/blog](https://inovex.de/blog)