TECHNISCHES MERKBLATT

LogIQ Fleets: Anschluss an die Leitsteuerung

Für Administratoren der Anlage

Dieses Dokument beschreibt, welche Verbindung der Analyzer braucht, was in der Firewall dafür geöffnet werden muss und welche Angaben wir zum Verbinden benötigen.

Kurzfassung: **eine ausgehende MQTT-Verbindung zum Broker, lesend.** Der Analyzer verhält sich wie ein weiterer MQTT-Client, der Nachrichten abonniert. Er sendet nichts, solange der Proxy-Modus nicht ausdrücklich eingeschaltet ist.

1. Wie der Analyzer angeschlossen wird

VDA5050 läuft über MQTT. Fahrzeuge und Leitsteuerung sprechen nicht direkt miteinander, sondern über einen Broker. Der Analyzer hängt sich als zusätzlicher Client an diesen Broker.

Die Betriebsformen wirken sich in der Firewall unterschiedlich aus:

A · Analyzer im eigenen Netz (dediziert)

Der Analyzer läuft als Docker-Container in Ihrem Netz, typischerweise auf demselben Segment wie die Leitsteuerung.

```
[ Fahrzeuge ] ──► [ MQTT-Broker ] ◄── [ Leitsteuerung ]
                        ▲
                        │  MQTT, lesend (Subscribe)
                  [ Analyzer ]
```

Firewall: nur eine interne Regel, vom Analyzer-Host zum Broker, TCP 1883 oder 8883, wenn Ihr Broker TLS spricht. Nach außen muss nichts geöffnet werden. Das ist die einfachste und datensparsamste Variante und für Anlagen ohne Internetzugang die einzige.

B · Gehosteter Analyzer

Der Analyzer läuft bei uns unter `logiq-fleets.com`. Dann muss Ihr Broker von außen erreichbar sein oder es wird ein Tunnel gelegt.

```
[ MQTT-Broker in Ihrem Netz ] ◄── VPN / SSH-Tunnel ── [ Analyzer, gehostet ]
```

Empfehlung: VPN oder SSH-Tunnel, nicht die direkte Freigabe. Der Analyzer spricht MQTT über TLS (siehe Abschnitt 4), die Verbindung selbst lässt sich also absichern. Einen Broker mit Anlagendaten offen ins Internet zu stellen, ist dennoch unabhängig von diesem Werkzeug keine gute Idee; ein Tunnel hält ihn aus jedem Scanner heraus.

Wollen Sie den Broker dennoch direkt freigeben, nennen wir Ihnen auf Anfrage die feste Quell-IP-Adresse für Ihre Regel. Sie gehört zum gehosteten Analyzer und ändert sich nicht.

C · Analyzer als transparenter Proxy

Optional kann der Analyzer zwischen Fahrzeugen und Broker sitzen: Er nimmt Verbindungen entgegen und spiegelt alles auf den echten Broker weiter.

```
[ Fahrzeuge ] ──▶ [ Analyzer ] ──▶ [ MQTT-Broker ] ◀── [ Leitsteuerung ]
```

Firewall: zusätzlich eingehend auf den Analyzer-Host, TCP 1883, von den Fahrzeugen. Diese Betriebsart ändert den Nachrichtenweg und wird nur nach Absprache eingesetzt. Für eine Analyse ist sie nicht nötig.

2. Firewall-Regeln in Tabellenform

Betriebsform	Richtung	Quelle	Ziel	Port	Protokoll
A · dediziert	ausgehend	Analyzer-Host	MQTT-Broker	1883 oder 8883/TCP	MQTT (TLS)
B · Gehostet, über VPN	ausgehend	VPN-Endpunkt	MQTT-Broker	1883 oder 8883/TCP	MQTT (TLS)
B · Gehostet, direkt	eingehend	feste IP des Analyzers	MQTT-Broker	8883/TCP	MQTT über TLS
C · Proxy (optional)	eingehend	Fahrzeuge	Analyzer-Host	1883/TCP	MQTT
C · Proxy (optional)	ausgehend	Analyzer-Host	MQTT-Broker	1883 oder 8883/TCP	MQTT (TLS)
A · dediziert, Testbench (optional)	eingehend	Fahrzeuge, Leitsteuerung	Analyzer-Host	18900–18919/TCP	MQTT (TLS möglich)

Die letzte Zeile gilt nur, wenn Fahrzeuge oder eine Leitsteuerung auf der Testbench gegen einen Broker des Analyzers fahren: Der Broker-Dienst einer dedizierten Installation startet je Flotte einen eigenen Broker in diesem Portbereich, unter der Adresse `LOGIQ_BROKER_HOST`.

Port 8883 ist der übliche TLS-Port; der Analyzer folgt dem, worauf Ihr Broker tatsächlich lauscht.

Weitere Öffnungen sind nicht nötig. Insbesondere:

- **Keine Verbindung zu den Fahrzeugen.** Der Analyzer spricht ausschließlich mit dem Broker.
- **Kein Zugriff auf die Leitsteuerung**, weder auf deren API noch auf deren Datenbank.
- **Kein ausgehender Internetzugang** aus der Anlage. Einzige Ausnahme sind die E-Mail-Berichte: Dafür braucht der Analyzer-Host Ihren SMTP-Server (üblicherweise 587/TCP, intern).
- **Das Kundenportal ist freiwillig.** Online fragt eine dedizierte Installation unser Portal über HTTPS (443/TCP, ausgehend) nach neuen Releases, schickt ihren Verbrauchsbericht und tauscht Freigaben mit anderen Installationen. Offline geht all das als Datei: das Release aus dem Kundenportal heruntergeladen, der Austausch von Hand exportiert und importiert.

Die Weboberfläche des Analyzers erreichen Ihre Anwender über HTTPS (443/TCP) bzw. auf einer dedizierten Installation über den Port, den Sie beim Aufsetzen wählen (Vorgabe 8000/TCP).

3. Was der Analyzer auf dem Broker tut

Damit Sie eine Freigabe begründen können, hier genau, was auf der Verbindung passiert:

- **Verbindungsaufbau:** MQTT 3.1.1/5, Keepalive 60 Sekunden. Bricht die Verbindung ab, baut der Client sie selbstständig wieder auf.
- **Abonnement:** nur die Topics, die im Mitschnittprofil eingetragen sind, üblicherweise `uagv/#` oder enger, etwa `uagv/v2/<Hersteller>/<Seriennummer>/#`. QoS 0.
- **Senden:** nichts. Der Analyzer publiziert keine Nachricht auf den Broker, solange der Proxy-Modus (Betriebsform C) nicht eingeschaltet ist. Es gibt keinen versteckten Steuerkanal, keine instantActions, keine Orders.
- **Last:** ein zusätzlicher Subscriber. Bei einer üblichen Anlage sind das wenige hundert Kilobit pro Sekunde, verursacht durch die State-Nachrichten, die ohnehin fließen.
- **Speicherung:** die aufgezeichneten Nachrichten und die Befunde landen in der Datenbank des Analyzers. Auf einer dedizierten Installation verlassen sie Ihr Netz nicht.

Ein Benutzerkonto auf dem Broker mit **ausschließlich Leserechten** genügt und ist die empfohlene Einrichtung.

4. Verschlüsselung und was heute nicht geht

MQTT über TLS wird unterstützt. Ein Mitschnittprofil hat dafür drei Einstellungen. Sie decken ab, was ein Anlagennetz braucht:

- **TLS an oder aus**: üblicherweise Port 8883 statt 1883. Das Zertifikat des Brokers wird gegen den Systemspeicher geprüft.
- **Eigenes CA-Zertifikat**: der Normalfall in der Anlage, wo das Broker-Zertifikat von Ihrer eigenen Stelle signiert ist und keine öffentliche Wurzel davon weiß. Das PEM wird ins Profil eingefügt, bleibt dort und gilt nur für diese Verbindung.

- **Prüfung aus**: für ein selbstsigniertes Zertifikat, das niemand für einen zweiwöchigen Test neu ausstellt. Der Verkehr bleibt verschlüsselt; wer am anderen Ende sitzt, ist damit nicht belegt und das Profil sagt das auch so. Eine bewusste Entscheidung, kein stiller Rückfall.

Das Proxy-Ziel eines Profils (Betriebsform C) hat denselben Schalter, damit die Weiterleitung nicht unbemerkt schwächer abgesichert ist als die Verbindung, die sie spiegelt.

Ehrlichkeitshalber, damit Sie nicht danach suchen:

- **Client-Zertifikate** (mTLS) noch nicht: der Analyzer weist sich mit Benutzername und Passwort aus, nicht mit einem Zertifikat.
- **Websocket-Transport** (Port 9001 bei vielen Brokern) noch nicht; es muss der native MQTT-Port sein.

Broker-Zugangsdaten werden im Analyzer verschlüsselt gespeichert, nicht im Klartext. Ein Mitschnitt muss sich nach einem Neustart selbst wieder verbinden können.

5. Was wir von Ihnen brauchen

Diese Angaben genügen, um eine Verbindung einzurichten. Am einfachsten kopieren Sie den Block, füllen ihn aus und schicken ihn zurück.

```
Broker
  Host / IP-Adresse ......:
  Port ...................:  (1883 unverschlüsselt, 8883 TLS)
  TLS ....................:  nein / ja, öffentliche CA / ja, eigene CA
  CA-Zertifikat ..........:  (PEM, wenn von Ihrer eigenen Stelle signiert)
  Benutzername ...........:  (leer, wenn anonym erlaubt)
  Passwort ...............:  (bitte getrennt vom Rest übermitteln)
  Nur-Lese-Konto? ........:  ja / nein

Topics
  Zu beobachtende Topics .:  z. B. uagv/#
  Interface-Name .........:  z. B. uagv
  Major-Version im Topic .:  z. B. v2

Anlage
  VDA5050-Version ........:  2.1.0 / 3.0
  Anzahl Fahrzeuge .......:
  Hersteller / Serien ....:  z. B. Balyo / QA_BALYO_REACHY0001
  Leitsteuerung ..........:  Hersteller und Version
  M2X-Peripherie? ........:  ja / nein  (Lastaufnahme, Türen, Aufzüge …)

Betrieb
  Betriebsform ...........:  A dediziert / B gehostet / C Proxy
  Bei B: Zugangsweg ......:  VPN / SSH-Tunnel / direkte Freigabe
  Ansprechpartner IT .....:
```

Nützlich, aber nicht nötig zum Start:

- Das **Factsheet** jedes Fahrzeugs als JSON-Datei. Damit prüft der Analyzer nicht nur gegen den Standard, sondern gegen das, was Ihr Fahrzeug zusagt. Wenn die Fahrzeuge ihr Factsheet auf dem Broker veröffentlichen, holt der Analyzer es sich selbst.
- Das **LIF-Layout** der Anlage (VDMA LIF 1.0.0). Damit werden Aufträge über dem echten Fahrkurs dargestellt und gegen das Layout abgeglichen.

Passwörter bitte nicht per E-Mail im Klartext. Ein zweiter Kanal genügt: Telefon, Signal, ein Passwort-Link. Für einen befristeten Test reicht ein eigens angelegtes Konto, das Sie danach wieder löschen.

6. Verbindung vorab selbst prüfen

Bevor wir uns verbinden, können Sie den Weg von dem Rechner aus testen, auf dem der Analyzer laufen soll. Mit den Mosquitto-Werkzeugen:

```
mosquitto_sub -h <broker-host> -p 1883 -t 'uagv/#' -v -C 5 -u <benutzer> -P <passwort>

# mit TLS und eigener CA:
mosquitto_sub -h <broker-host> -p 8883 --cafile ca.pem -t 'uagv/#' -v -C 5 -u <benutzer> -P
<passwort>
```

Kommen fünf Nachrichten, ist alles offen, was der Analyzer braucht. Kommt nichts:

Meldung	Bedeutung
`Connection refused`	Port zu oder der Broker hört nicht auf dieser Adresse
Zeitüberschreitung, keine Meldung	Firewall verwirft die Pakete stillschweigend
`Connection Refused: not authorised`	Netzweg steht, Zugangsdaten oder ACL stimmen nicht
Verbindung steht, keine Nachrichten	Topic-Filter passt nicht oder das Konto darf dieses Topic nicht lesen

7. Lizenz im eigenen Netz

Eine Installation in Ihrem Netz trägt eine signierte Lizenzdatei. Sie ist ein kleines Textdokument: was gekauft wurde, lesbar, mit einer Signatur darunter.

- **Kein Anruf nach Hause.** Die Lizenz wird lokal geprüft, gegen einen Schlüssel in der Anwendung. Ein Netz ohne Weg nach draußen ist ein unterstütztes Netz.
- **Einspielen in der Oberfläche.** Administration → Lizenz, einfügen oder hochladen. Eine Datei, die nicht verifiziert, wird abgewiesen, bevor sie eine funktionierende ersetzen kann.

- **Binnen drei Tagen aktiviert.** Die Seite zeigt einen Instanzcode; er wird im Kundenportal eingetragen und die Aktivierung, die zurückkommt, auf derselben Seite eingefügt. Ohne sie wird die Installation nach drei Tagen schreibgeschützt.
- **Updates mit Rückweg.** Administration → Updates nimmt ein Release aus dem Portal oder als Datei und behält es nur, wenn seine Signatur stimmt. Der Updater, ein eigener Dienst neben der Installation, sichert vor dem Umschalten die Datenbank und rollt zurück, wenn die neue Version nicht antwortet.
- **Vierzehn Tage Karenz** nach Ende der Laufzeit, danach eine schreibgeschützte Installation: alles Aufgezeichnete, jeder Bericht und jeder Export bleibt erreichbar, nur neue Arbeit wartet auf eine gültige Lizenz.

8. Datenschutz und Rückwirkungsfreiheit

- Der Analyzer liest **Maschinendaten**: Aufträge, Zustände, Positionen, Fehlermeldungen. Personenbezogene Daten enthält VDA5050-Verkehr nicht.
- Der Betrieb ist **rückwirkungsfrei**: ein Subscriber verändert weder den Nachrichtenfluss noch das Verhalten der Fahrzeuge. Nur die Betriebsform C (Proxy) liegt im Weg und die wird ausdrücklich vereinbart.
- Auf einer dedizierten Installation verlassen Mitschnitte und Berichte Ihr Netz nicht. Im gehosteten Betrieb liegen sie auf einem Server in Deutschland; Berichte und Läufe sind nur über nicht erratbare Adressen und nach Anmeldung erreichbar.

Fragen zum Anschluss: **support@logiq-fleets.com** LogistiXpert · logistixpert.com