Risk-Analytics services

Created by John Haldeman, last modified by Shachaf Katz on May 16, 2023

There are 3 risk-analytics services involved in the risk event flow (owned by Tigers team) :

- Risk-analytics-engine
- Risk-analytics-classification
- Risk-analytics-controller

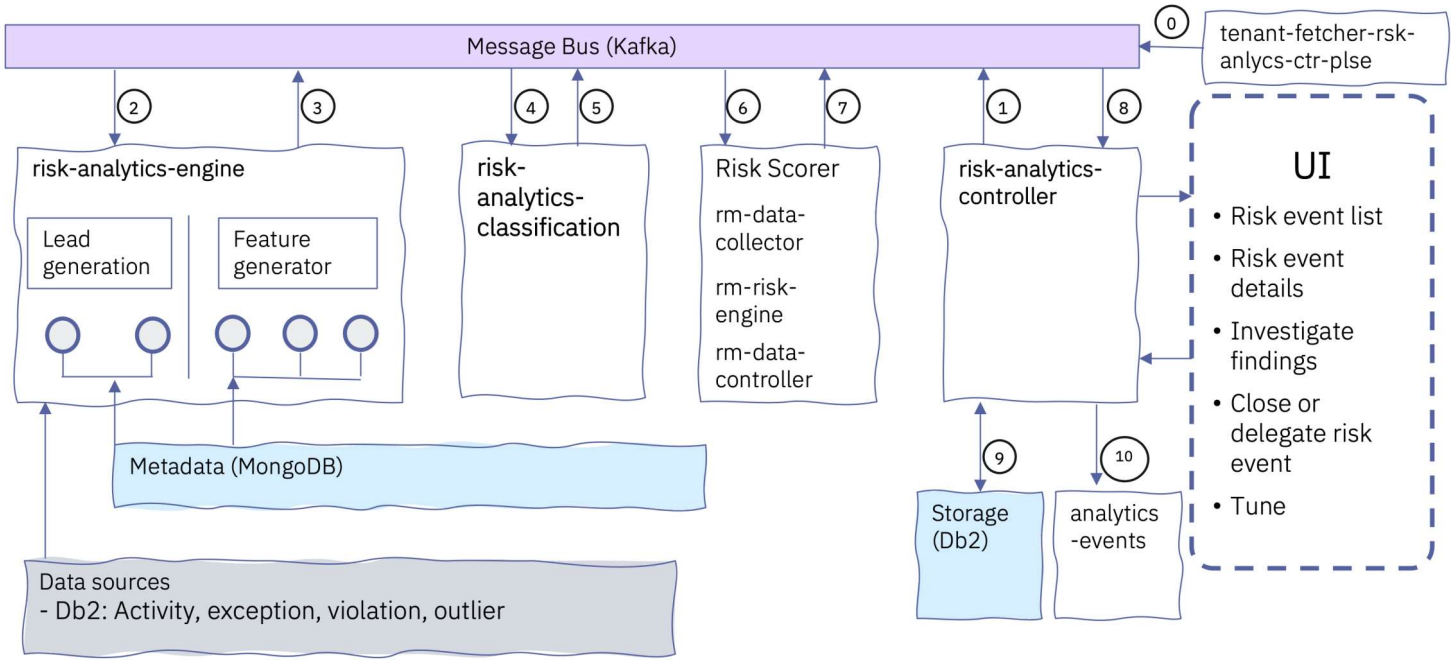
In addition, there are 3 rm services involved in the risk event flow - these services are responsible on calculating the risk score (owned by Varja team):

- rm-data-collector
- rm-risk-engine
- rm-data-controller

There is an additional service to process risk rules and send out notifications based on user defined rules (owned by Phoenix team) :

- analytics-events

Risk Event Architecture



Risk event flow:

0. once an hour tenant-fetcher-rsk-anlycs-ctr-plse cron job is triggered and send kafka msg to risk-analytics-controller service for each tenant in the environment (topic : risk_analytics_controller_pulse)

1. risk-analytics-controller check if the risk event process is enabled for this tenant. if enabled - it sends 4 Kafka msgs to risk-analytics-engine to start generate risks. 1 msg per each asset type - database, db user, os user, global. (topic: start_risk_analytics_engine)

2. risk-analytics-engine start generate leads, one done it sends the assets that were found in group of 50 assets per 1 Kafka msg. these assets are sent over the topic pivots_group which is also consumed by the risk-analytics-engine.
For the assets that arrived in pivots_group topic,

3. The risk-analytics-engine will generate features and will send each asset (with leads and features) as a separate Kafka msg to topic risk_with_featuresets.

4. risk-analytics-classification receives each risk and categorize the risk.

5. The categorized risk is then sent to risk_with_classification topic

6. The rm services receives the risk and calculate the risk score

7. The calculated risk is then sent to risk_with_score topic.

8. risk-analytics-controller receives the risk that incudes - leads features, classification, score.

9. The risk is then scored in DB2.

10. risk-analytics-controller checks if this is a new risk or existing risk that had different severity/classification before -
and sends the risk as a Kafka msg to topic risk_controller_notification.
analytics-events listen to risk_controller_notification topic and if the risk will match any of the response rules it will send a msg to notification service to create notification.

gi_sre