### anomalies

Calculates the anomaly score using the Isolation Forest modeling (a way of creating a decision tree model by sampling some data).

#### Syntax

Calculate the anomaly score using a stored training model.

anomalies [sample=INT] [size=INT] model=MODEL

Calculate the anomaly score using a model trained based on subquery results.

anomalies [sample=INT] [size=INT] FIELD, ... [ SUBQUERY ]

Required Parameter

**FIELD, ...**

Fields to be used for the Isolation Forest modeling. Use a comma(,) as a separator.

**model=MODEL**

Name of the Isolation Forest model. You can generate and train the Isolation Forest model by connecting to the Logpresso engine via CLI.

**[ SUBQUERY ]**

Subquery that returns the data set for model training.

Optional Parameter

**sample=INT**

Number of samples to draw when training the Isolation Forest model (default: the square root of the number of samples).

**size=INT**

Number of trees within the Isolation Forest (default: 100).

#### Description

The anomaly score, ranging from 0 to 1, is assigned to the **\_score** field.

1. The higher the score, the more likely it is an anomaly.
2. A score much smaller than 0.5 indicates normal observations.
3. If all scores are close to 0.5, the entire sample does not seem to have clearly distinct anomalies.

#### Usages

Calculate the anomaly score using the anomal\_stock model.

# Download: https://raw.githubusercontent.com/logpresso/dataset/main/stocks.csv | table stocks | anomalies model=anomal\_stock | eval anom = if(\_score>0.7, stocks, null)

Calculate using a model trained based on the training data set returned from a subquery.

table stocks | anomalies sample=256 stocks [ csvfile /test/sam\_train.csv | eval \_time=date(date, "yyyyMMdd"), stocks = int (stocks) | fields \_time, stocks ] | eval anom = if(\_score>0.65, stocks, null) | fields \_time, anom, stocks