### anomalies

이상탐지 포레스트 모델(Isolation Forest, 일부 데이터를 샘플링하여 의사결정 나무 모델을 생성하는 방식)을 사용하여 이상치를 예측하는 데이터를 출력합니다.

#### 문법

사전에 준비된 학습 모델에 기반한 이상치 예측

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

서브쿼리를 통해 이상탐지 포레스트 분석을 실행

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

필수 매개변수

**FIELD, ...**

이상탐지 포레스트 분석에서 사용할 필드 목록. 필드 구분자로 쉼표(,)를 사용합니다.

**model=MODEL**

이상탐지 포레스트 분석 모델의 이름을 입력합니다. 로그프레소 엔진에 CLI로 접속하여 학습 모델을 생성하고 학습을 진행할 수 있습니다.

**[ SUBQUERY ]**

이상탐지 포레스트 분석에서 사용할 트레이닝셋 데이터 조회 쿼리를 입력합니다.

선택 매개변수

**sample=INT**

이상탐지 포레스트에서 학습에 사용할 샘플 갯수(기본값: 샘플 개수의 제곱근).

**size=INT**

이상탐지 포레스트를 구성하는 트리 갯수(기본값: 100)

#### 설명

이상치 값은 **\_score** 필드에 출력되고, 0 ~ 1 사이의 값으로 표시됩니다.

1. 값이 1에 가까울수록 이상치일 확률이 높습니다.
2. 0.5보다 훨씬 작은 값은 정상적인 관측값입니다.
3. 모든 점수가 0.5에 가까우면 이상치가 없을 확률이 높습니다.

#### 사용 예

이름이 anomal\_stock인 학습 모델을 사용한 이상치 예측

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

서브쿼리로 트레이닝 셋을 사용하는 경우

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