Online Performance Anomaly Detection
with Kieker

Tillmann Bielefeld

empuxa GmbH, Kiel

KoSSE-Symposium Application Performance Management (Kieker Days 2012)
November 29, 2012 @ Wissenschaftszentrum Kiel
Agenda

1. Monitoring at XING
2. OPAD’s Architecture
3. Evaluation
4. Results
5. Conclusion
Thesis Goals

1. Design of online performance anomaly detection concept (ΘPAD)
2. ΘPAD implementation as Kieker plugin
3. ΘPAD integration with case study system
4. Evaluation @ XING

Tillmann C. Bielefeld:
“Online performance anomaly detection for large-scale software systems”
Logjam-based monitoring already in place @ XING
Integration of ΘPAD in XING’s Architecture

Monitoring at XING

Servers

App
Support
XWS (API)
DB
Background

Importer

Log Database

Logjam

XING’s logging/monitoring architecture
Integration of $\Theta$PAD in XING’s Architecture

Monitoring at XING

Servers

- App
- Support
- XWS (API)
- DB
- Background

$\Theta$PAD

Importer

Log Database

Logjam

$\Theta$PAD w/ Kieker

Nov. 29, 2012 @ Kiel
Example JSON Logging Message

Monitoring at XING

{ 
    "count": 5204.903527993169,
    "memcache_time": 6505.196318140181,
    "api_time": 2207.0271495891297,
    "db_time": 5004.8727338680155,
    ...
    "view_time": 3936.1623304929153,
    "total_time": 1586.8188192888886,
    "api_calls": 5546.250545491678
} 

Input data received via AMQP and processed by ΘPAD
Chapter 4. Design and Implementation of the ΘPAD System

High-Level ΘPAD Architecture

OPAD’s Architecture

4.4.1 Integration into Kieker

ΘPAD uses the Kieker monitoring framework written in Java as a base for its implementation. The connection to the anomaly detection code is made by a plugin container Kieker offers. The plugin pattern is used when certain behavior is based on different implementations that have to be configured in a central runtime environment [Fowler 2003, p. 500]. To start ΘPAD in a Kieker environment, all necessary depending libraries, the kieker.jar and the plugin code have to be accessible in the same class path. ΘPAD gets instantiated at startup of the Kieker server. Both main architectural components of Kieker, Monitoring and Analysis are used to route the measurements to the plugin. The data flow from input to output is illustrated in Figure 4.4.

Figure 4.4: The coarse-grained architecture follows the linear data flow of the approach (see Chapter 3). The AMQPBridge adapter translates the monitored system’s measurements to Kieker records and therefore makes ΘPAD reusable in other environments (NFR4).

This graphic uses the AMQP notation of Figure 2.19.

Raw measurements, encoded as JSON strings, are sent to the measurement queue by the system under monitoring in a temporal sequence fashion as described in Section 3.4. The Kieker Monitoring component, then deserializes these strings and transforms them into measurement records as defined in Equation 3.4. Subsequently, these records are put into a Java Pipe forwards data in memory according to the FIFO principle. Figure 4.5 shows the corresponding class instantiation.

1. AMQP messages transformed into Kieker monitoring records
2. ΘPAD: pipes-and-filters processing of records
3. ΘPAD results passed to alerting queue and time-series storage
PAD Processing Steps

OPAD’s Architecture

- Time Series Extraction
- Time Series Forecasting
- Anomaly Score Calculation
- Anomaly Detection
- Alerting (e.g., AMQP)
Step 1: Time Series Extraction

ΘPAD Processing Steps (cont’d)

OPAD’s Architecture

Time Series Extraction
↓
Time Series Forecasting
↓
Anomaly Score Calculation
↓
Anomaly Detection
↓
Alerting (e.g., AMQP)

Continuous Time

Discrete Time Series

select sum(value) as aggregation
from MeasureEvent.win:time_batch( 1000 msec )
Step 2: Time Series Forecasting

ΘPAD Processing Steps (cont’d)

OPAD’s Architecture

- Time Series Extraction
- Time Series Forecasting
- Anomaly Score Calculation
- Anomaly Detection
- Alerting (e.g., AMQP)

ΔW

1 2 3 4 5 6
Step 3: Anomaly Score Calculation

ΘPAD Processing Steps (cont’d)

ΘPAD’s Architecture

- Time Series Extraction
- Time Series Forecasting
- Anomaly Score Calculation
- Anomaly Detection
- Alerting (e.g., AMQP)

Tillmann Bielefeld (empuxa GmbH)
ΘPAD w/ Kieker
Nov. 29, 2012 @ Kiel
Step 4: Anomaly Detection

ΘPAD Processing Steps (cont’d)

OPAD’s Architecture

- Time Series Extraction
- Time Series Forecasting
- Anomaly Score Calculation
- Anomaly Detection
- Alerting (e.g., AMQP)

Abnormal Score
Normal Score
Anomaly Threshold
Anomaly Detected
ΘPAD Web Interface

OPAD's Architecture

Time Series Graphs from OPAD

Query MongoDB:
DB: opad_development  Collection: evaluation_2w2011_2
Sort: {"time": 1}  Limit: 2000
From - to: 1324285440000 - 1324317000000
Zoom: out left right

Anomaly Score
0.75
0.5
0.25
0

Measures
81697367
72619882
63542396
54464911
45387426
36309941
27232456
18154970
9077485

Measure: 32274036.4
Forecast: 72931402.17
Anomaly Score: 0.3057
2011-12-19 15:15:00

1 2 3 4

Tillmann Bielefeld (empuxa GmbH)  ΘPAD w/ Kieker  Nov. 29, 2012 @ Kiel 13 / 27
Goal
Assess Practicality of Approach

Questions
How precise is the detection?
How accurate is the detection?

Metric
Number of true positives
Number of false negatives

Goal/Question/Metric (GQM) plan (excerpt)
Manual detection using the visualization tool

8 anomalies were detected
ΘPAD Results

Evaluation

Results

aptt.Fses.D1min.L15min
aptt.Fets.D1min.L1h
aptt.Fmean.D5min.L1h

Tillmann Bielefeld (empuxa GmbH)

ΘPAD w/ Kieker

Nov. 29, 2012 @ Kiel
ROC Curves (Introduction)
Evaluation (cont’d)

Results

\[ TPR = \frac{TP}{TP + FN} = \frac{TP}{F} \quad \text{FPR} = \frac{FP}{FP + TN} = \frac{FP}{NF} \]  

(1)
ROC Curves (ΘPAD Results)

Evaluation (cont’d)

Results

- mean.D1min.L1h
- ses.D1min.L15min
- mean.D20min.L2h
- aptt.Fws.D1h.L24h
Accuracy and Precision
Evaluation (cont’d)

Results

\[
\text{PREC} = \frac{TP}{\text{POS}} = \frac{TP}{TP + FP} \quad \cdot (2)
\]

\[
\text{ACC} = \frac{TP + TN}{N} = \frac{TP + TN}{TP + FP + FN + TN} \quad \cdot (3)
\]
Outlook

- ΘPAD to be released as part of Kieker
- Follow-up theses on ΘPAD

Contact Us

- till@empuxa.com
Win a free empuxa Hoodie!
http://freebies.tielefeld.com