Next Generation Performance Monitoring

Machine Learning Algorithms for Anomaly Detection

Susanne Greiner
How to monitor performance?

Data collection ≠ Problem solution

The right decision at each step is not trivial!
Performance Monitoring

Heart Rate

Can be influenced by
- Pathology
- Sport
- Breathing
- Drugs
- Temperature
- Dehydration
- Pressure
- Etc.

Monitoring & Alarms

Subject specific historical data

Expectation
- Time series
- Alarm thresholds

Population data
Performance Monitoring

Can be influenced by

- Batch requests
- Transactions
- Memory
- SAN
- Network
- Side Processes
- Etc.

Monitoring & Alarms

Machine/setting specific historical data

Expectation

- Time series
- Alarm thresholds

Experience, Data from similar machines/settings

Percentage Processor Time
Recent Trends

Reactivity → Proactivity

Standard Stats → Advanced Stats & Machine Learning

Combination of Performance Monitoring and User Experience
Agile Implementation of Solutions

Customer specific solutions with agile implementation
REATIVITY → PROACTIVITY
Visualization: Trend Detection

- Areas not to many points
- Smoothed signal
Historic Data

- Comparison time consuming
- Quantification complicated

- Historic data at hand
- Visualization of differences

=> Easy trend detection
STANDARD STATS → ADVANCED STATS & ML
Every time series is analyzed separately.
Thresholds are calculated on via baselining.
Alarms from separate time series are combined into a global alarm.
Relationships between time series are ignored.
Shape of time series is ignored.

Motivations:
- Separate Data Sources
- Different Precision
- Evolution of networks (complexity)
- Common practice was enough
Multi-variate Data Analysis

- All time series are analyzed on **together**
- Thresholds are calculated dynamically via **baselining and anomaly detection**
- **Risk estimation** in addition to **global alarm and specific alarms**
- Relationships between time series are used to create more reliable alarms and risks
- Shape of time series is **considered**

**Motivations**

- Common Data Source
- Grafana & InfluxDB
- Today we need more than common practice
- **Proactivity**
Anomaly vs. Threshold

Alarm quality improvement
Mathematical characterization of standard traffic
Anomaly vs. Threshold

Automatic detection of relevant changes
Risk: Anomaly Detection via Multivariate ML Analysis

Metrics

TRAIN DATA

MODEL STANDARD BEHAVIOUR

TEST DATA

• historical data of same metric
• historical data of similar metric
• historical data of similar machine

WHAT DO WE EXPECT?

• The farer away from expectation the higher the RISK
• RISK: different and rare

HOW FAR ARE WE FROM OUR EXPECTATION?

RISK SCORE

© Würth Phoenix 2017
Risk: Culprit Detection with Risk

IOs

• Which (set of) machine(s) is most probably causing the high risk
• Proactive analysis to prevent congestion

HIGH RISK PERIODS

AUTOMATED ANALYSIS

• historical data of same metric
• historical data of similar metric
• historical data of similar machine
• historical data of neighbours

Proactive search for potential future culprits

Faster Troubleshooting

• Check machines with high risk first, there might be no need to control the others
COMBINATION OF PERFORMANCE MONITORING AND USER EXPERIENCE
3 Levels of Dashboards

Overview

Multimeasure

Detailed
Level 1: Overview Dashboard

Server Overview

User Experience Overview
Level 2: Multimeasure - Troubleshooting
Detailed Dashboard (Alyvix)
GRAZIE!