Event Correlation and Anomaly Prediction with Focused Run for SAP Solution Manager

New Town Square: Janko Budzisch, SAP // Heidelberg: Frank Wenzke, SAP
December, 2019
Agenda

Overview Run Market

Focused Run for SAP Solution Manager

Intelligent Alerting

Alert Correlation

Anomaly Prediction
Overview Run Market
Operations for hybrid landscapes

**HEC, Hosting, AMS and IaaS Service Providers**
- Focused Run operated by Service Providers and used by Service Providers and/or Customers

**Customer On Premise Landscape**
- SAP Solution Manager and/or Focused Run operated and used by Customers

**SAP Solution Manager**: On Premise based operation platform for hybrid landscapes operated and used by Customers

**Focused Run**: On Premise based operation platform for hybrid landscapes operated by Service Providers or Customers and used by Service Providers and/or Customers

**SAP Cloud ALM**: SAP Cloud Platform based operation platform for hybrid landscapes operated as SaaS Service by SAP and used by Customers

- SAP C/4HANA
- SAP Fieldglass
- SAP Customer Experience
- SAP Cloud Platform
- SAP Ariba
- SAP SuccessFactors
- SAP S/4HANA Cloud
- SAP Concur

**SAP SaaS Cloud / SAP Cloud Platform**
- System, Application and Business Process Management Data
- Application and Business Process Management Data
## Different Operation Platforms for different target groups

### SAP Solution Manager
**Target group:**
- Medium and large hybrid customers
- Customers, who are satisfied with the currently provided functional scope

**Available**

### Focused Run for SAP Solution Manager
**Target group:**
- Service Providers
- Large and very large hybrid customers
- Customers with advanced needs, which go beyond SAP Solution Manager

**Available**

### SAP Cloud ALM for Operations
**Target group:**
- Cloud-centric customer
- Small and medium hybrid customers
- Customers, who are requesting cloud based Operation Platform

**Beta**

---

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
Focused Run for SAP Solution Manager
Focused Run – Mission statement

• Is a **powerful solution for customers & partners** to operate their solution **centralized and highly automated with minimal TCO impact**

• **Addresses advanced customer needs** in scalability, data volumes, security, automation, openness, dashboarding & artificial intelligence

• Uses the **full power of SAP HANA as a platform**, including replication, partitioning, predictive analytics, and compression

• Is a **separate installation**, which can run **side-by-side with an existing SAP Solution Manager**

• Provides feature rich and powerful **functionality dedicated to operations of IT solutions**

• Isn’t covered by maintenance fee, but **needs to be licensed separately from SAP**
Focused Run – Use cases in scope
Intelligent Alerting
What is intelligent alerting?

Raise **one alert per problem** instead of one alert per symptom

Alerting based on **overall system state** instead of single KPIs

Knowing about **critical anomalous situations in advance** and avoiding the same

Raise alert on **anomalous system behavior** instead of static threshold

Automatic alert reaction with **auto healing**
Approaches for intelligent alerting considered by Focused Run

Machine Learning

Use collected data to derive intelligent decisions e.g. distinguish normal from not normal situations automatically without manual interaction or interpretation.

Prediction

Predict behavior in the future based on the collected data concerning the past. Example is forecasting of single metrics. More important is the capability to predict from a certain set of symptoms consequences regarding the overall status of a managed object.

Impact Analysis

Events and metrics are measured for different managed objects at different layers. Necessary is to understand the impact of a symptom on one layer to other layers e.g. impact of hypervisor shutdown.

Operation Automation

Reduce dramatically the amount of manual operation tasks. This starts with the initial setup and maintenance of the Operation Platform itself, but it touches also automatic alert resolution and regular health checks.
Alert Correlation
Problem: Alert flooding

- High number of events regarding health status of the managed objects are generated
- Problems on central data center components raises following events for different components
- To many single events are flooding the IT service desk team

Resolution: Alert correlation

- All events or symptoms belonging to the same problem shall be summarized to alert clusters, even if events are caused in multiple components
- Reduction of alerts occurrences, which are processed manually
- Focus on most important problems without distraction by parallel workstreams
- Avoid double work and associated costs
- Save 2nd and 3rd level resources by providing standardized alert response procedures on alert cluster level to be executed by 1st level resources

What is alert correlation?
Evolution of event and alert correlation

- SAP Netweaver
- CCMS
  - single Metric time correlation
- SAP Solution Manager
  - Monitoring and Alerting Infrastructure (MAI)
    - Event correlation for multiple metrics of same category
  - Alert Correlation
    - Horizontal and vertical correlation of events from different managed objects, categories and monitoring use cases
- Focused Run for SAP Solution Manager
  - Robust Outlier Handling
  - Time-based analysis for events
Concept of Horizontal Alert Correlation

Combine alerts for the same managed object by:

- **Robust Outlier Handling**: Alert flickering shall be prevented by summarization of **re-occurring events with short breaks**

- **Grouping of different sources**: Alerts from different monitoring use cases e.g. System Monitoring and Integration Monitoring including external alerts imported via inbound adapter will be grouped together

- **Grouping of different alerts**: Grouping of the different alerts for the same managed object e.g. Sybase Database availability will cause also alerts for the availability of the Job Scheduler and the Backup Server
Concept of Vertical Alert Correlation (1/2)
Concept of Vertical Alert Correlation (2/2)

Alerts from **different sources on different levels** will be correlated e.g. in case of a **network issue** on infrastructure layer, the **performance of systems** is affected as well as the **throughput of interfaces and business processes**. See the following examples:

- Database unavailability will cause also instance and system unavailability
- Instance unavailability can cause performance issues on other instances or on system level due to load re-distribution

**Available approaches:**

- **Top-down:** Correlation of alerts for instances and/or systems running on the host
- **Bottom-up:** Correlation of alerts belonging to the same system
- **Network:** Create **Context Families** to correlate alerts coming from different systems sharing common components e.g. disaster recovery scenarios
Outlook for alert correlation (Focused Run 2.0 FP02)

- **Pre-defined rules** based on customer specific alert analysis are **shipped as best practices** (inactive by default)
- **Multiple active rules are possible** ➔ First matching rule is used
- **Rule ordering can be influenced** by drag-n-drop during maintenance
- **Rule configuration options:**
  - **Vertical correlation** can be dependent on either Host (top-down), Technical System (bottom-up) or Context Family (network)
  - **Time based correlation** of flickering alert with configurable overlap time
Usage scenario for alert correlation

1. **Identify relevant alert cluster in Alert Inbox**
   - ![Alert Inbox](image1)

2. **Drill-down into Alert Cluster to analyze contributing single alerts**
   - ![Alert Cluster](image2)

3. **Work on Alert resolution direct within Alert Cluster**
   - ![Actions](image3)

4. **Drill-down from Alert Cluster to single alert for metric detail**
   - ![Metric Monitoring](image4)
Roadmap for alert correlation

- Allow **correlation on other alert attributes** (not managed object related), e.g.:
  - Correlate all alert from same **alert category**
  - Correlate all alerts in single **customer network**
  - Correlate all alerts of the same **alert type**
- Enhance **analytics possibilities** for alert clusters
- Provide possibilities for **manual clustering / de-clustering**
- Apply reinforcement machine learning to learn from manual cluster actions
Anomaly Prediction
What is anomaly prediction?

Knowing about **critical anomalous situations in future** to avoid potential outages or resource bottlenecks ➔ Come to statements like “… with 98 % confidence, the system XYZ will not be available or in a very critical state within the next 1 hour …”

Enabled end users to detect and analyze a certain situation reactively, meaning after a certain problem is already occurred

Predicts a situation in advance with certain confidence level based on past data ➔ Confidence level is automatically recalculated on regular basis

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
Concept of system anomaly prediction (1/2)

Target: Predict critical anomalies in a system **30-60 minutes in advance** with **high confidence**

**Hypothesis:**
Some metrics are likely to demonstrate uncharacteristic values few minutes before the outage.

**Model:**
Values of “target variable” as a function of values of other metrics indicating anomalies before an outage.
Concept of system anomaly prediction (2/2)

Supervised multivariate time-series anomaly prediction based on deep learning approach:

- Model training based on real outages in large landscape (>20,000 systems) with data from multiple customers over a longer period of time (>2 years)
- Risk score calculation based on multiple metrics leads to better prediction hit ratio and earlier indication of issues, than forecast based on single metrics
- Specialized models for different critical situation, based on the model with the highest risk score, the error handling can already start focused on a special situation

Advantages for selected approach:

- Only critical anomalies are alerted
- As anomalous situation is known, countermeasures can be started to avoid the critical system situation from being happen
Collaboration between customer and development

**SAP HANA Enterprise Cloud (HEC): Zero Outage Project team**

- **Objective:** Zero Downtime of HEC systems
- **Tasks:**
  - Collect metric data for all outages
  - Analyze outages and update the RCA in master downtime list
  - Perform Trend Analysis and makes effort to ensure that the issue doesn’t happen in other systems
  - Retrain Prediction Models
  - Re-deploy prediction models

**Focused Run Development Team**

- **Tasks:**
  - Run SAP delivered prediction models, provide feedback on results
  - Collect metric data in case of unexpected results

**Other Focused Run customers e.g. SAP IT**

- **Objective:** Stable system operation

**Common Objective:** prevent system outages
Architecture for system anomaly prediction

**Focused Run System**

**System Anomaly Prediction**
- System Anomaly Prediction Store
- System Anomaly Prediction Engine
- RCA Store

**System Monitoring & System Analysis**
- Metric & Event Store

**Administration Network**
- System Anomaly Prediction Configuration
- Calculate Results

**Customer Network**
- Configuration
- Metrics & Events

Rserve incl. Keras and Tensorflow
Usage scenario for system anomaly prediction

1. Receive and react to Anomaly Prediction Alert

2. Identification of critical systems including problems area/category

3. Detailed analysis of specific model versions associated with system

4. Identification of critical metrics within a system contributing to anomaly

5. Detailed analysis of metrics associated with metric forecasting
Bring your own model

Enable the creation and training of **own models** based on Focused Run data collection and Anomaly Prediction Engine. **Seamless integration** in alerting capabilities.

Adoption to customer specific situations and **system specific models** for systems with high priority

**Enhancement of prediction scope** to system types not supported by standard models
Roadmap for system anomaly prediction

Trend Based Alerting
- Enable alerting based on trends of single metrics

Models
- ABAP Resource Exhaustion model
- Java Out of Memory model

Preventive Measures for Zero Outage approach
- Provide guided procedure content to structure the analysis of the issue
- Provide activities to prevent the system standstill based on the analysis results

Build & Test models on lower granularity e.g. 1 minute
- Required for further quality improvement expected

Evaluation of Semi-Supervised Learning approach
- Per system / group of systems based automated (re-)training based on SAM based outage classification
- Automated model validation based on SAM unplanned outages
Join our social media family

Follow us on **Twitter** (#solman and #CloudALM), get the latest news, learn about support offerings and events!

Search for “SAP Cloud ALM” on **YouTube** for product demos, expert interviews and event insights!

Subscribe to **WhatsApp** SAP Product Support channels and receive updates including KBAs, wiki's, guided answers, SAP Notes and “hot tips”.

Join the SAP Digital Business Services **LinkedIn** group for networking and updates!
Thank you.

Contact information:

**Janko Budzisch**  
Chief Product Owner  
janko.Budzisch@sap.com

**Frank Wenzke**  
Product Owner  
frank.wenzke@sap.com