ASUG | SAP

Application Lifecycle Management Summit North America

#ALMSummit

Event Correlation and Anomaly Prediction with SAP Focused Run

Tomas Engelmann and Allam Drebes, SAP

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions..

Agenda

Intelligent Alerting

Alert Correlation

Anomaly Prediction

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 SAP 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

What is 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

Evolution of event and alert correlation

SAP Netweaver

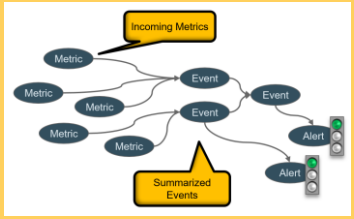
CCMS

single Metric time correlation

SAP Solution Manager

Monitoring and Alerting Infrastructure (MAI)

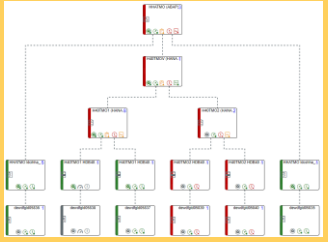
Event correlation for multiple metrics of same category



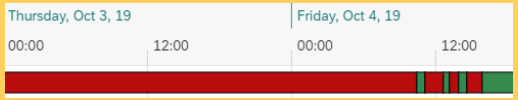
SAP Focused Run

Alert Correlation

Horizontal and vertical correlation of events from different managed objects, categories and monitoring use cases



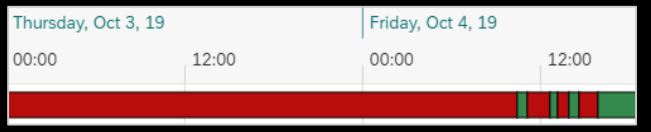
Robust Outlier Handling

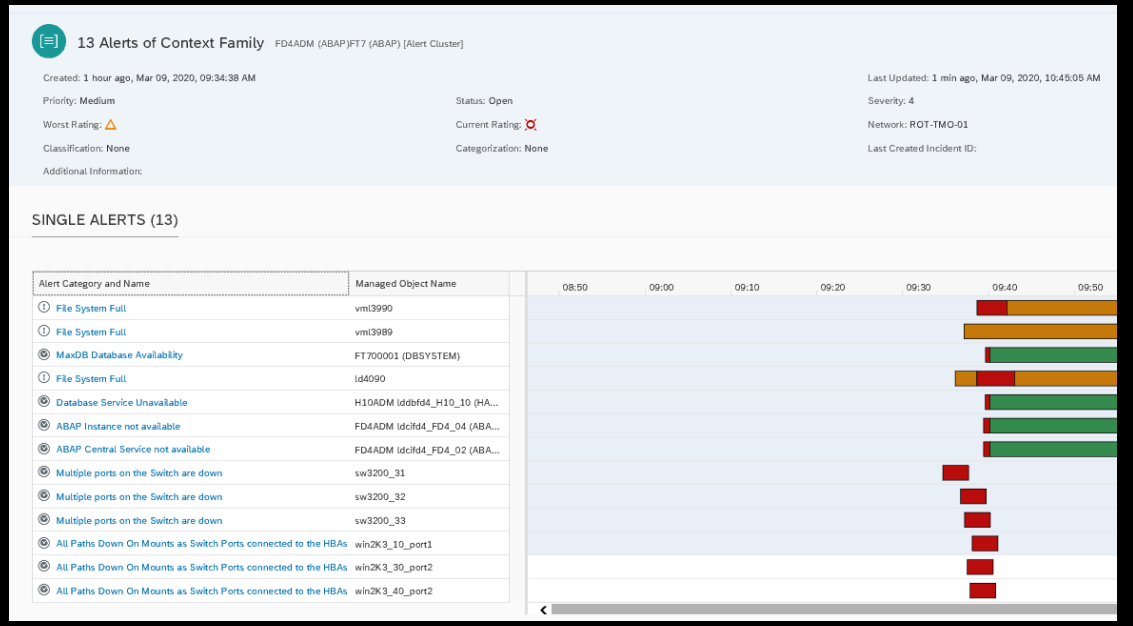


Concept of Horizontal Alert Correlation

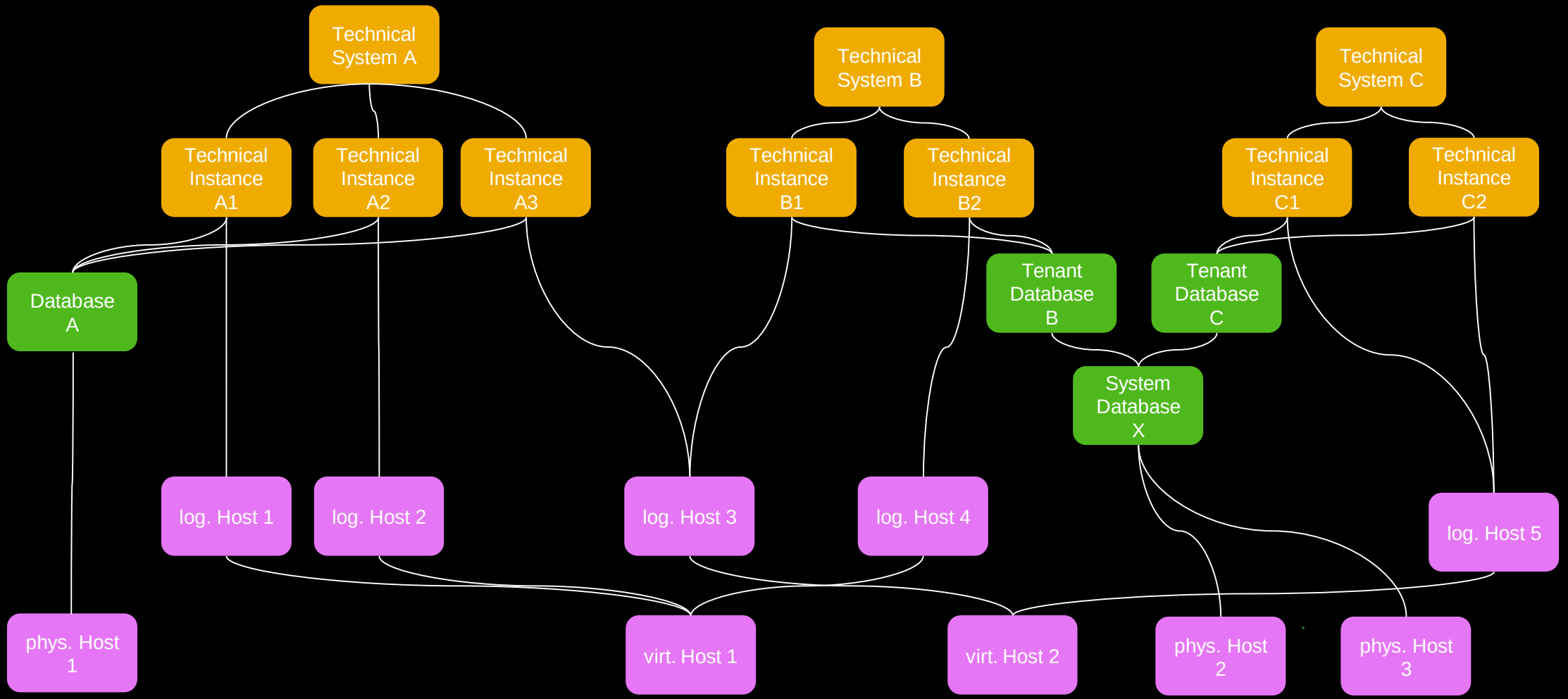
Combine alerts for the same managed object by:

- **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:

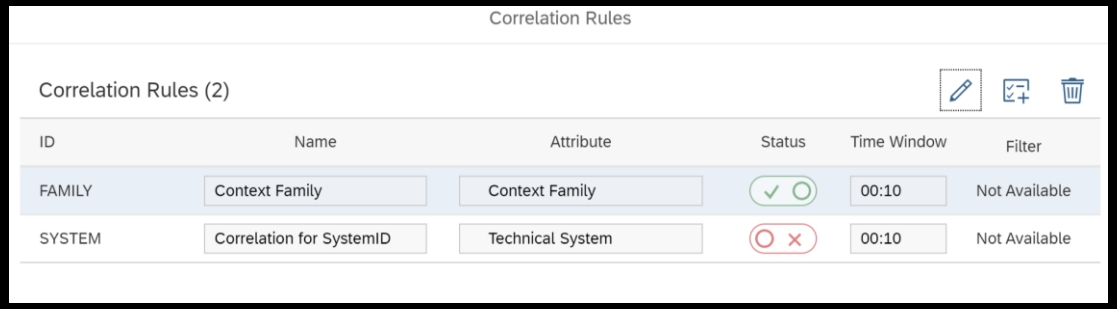
- Database unavailability will cause also instance and system unavailability
- Instance unavailability can cause performance issues on other instances or on system level due to load re-distribution

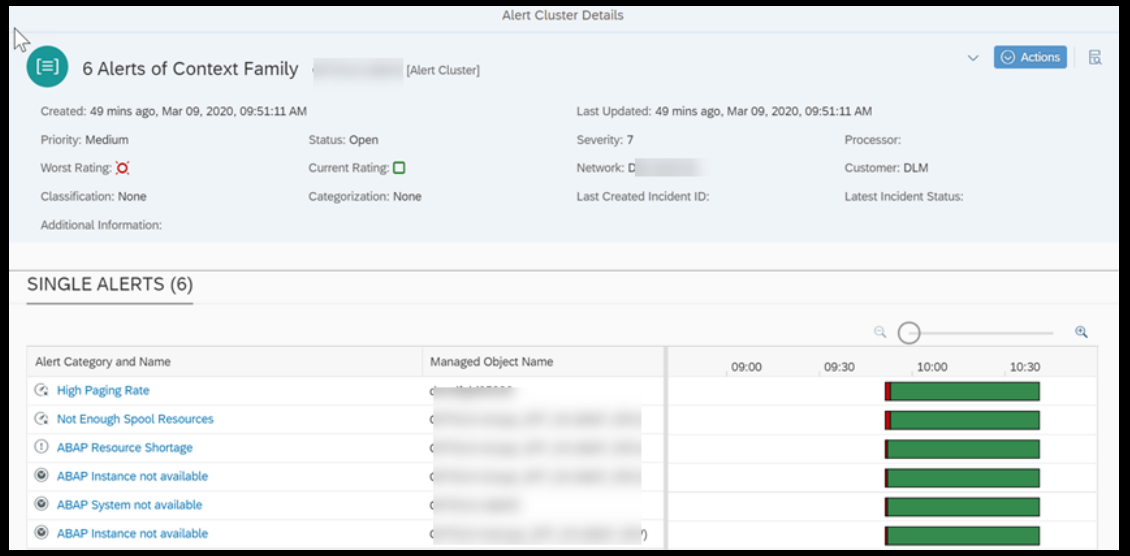
Available approaches:

- **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

Alert correlation with SAP Focused Run

- **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

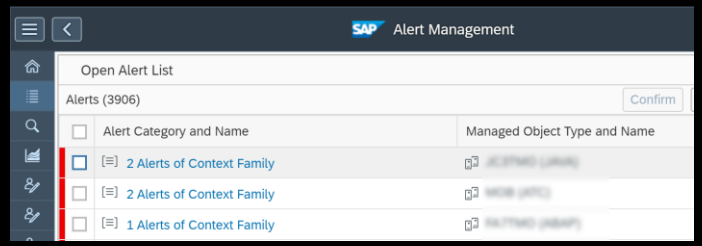




Demo of Alert Correlation

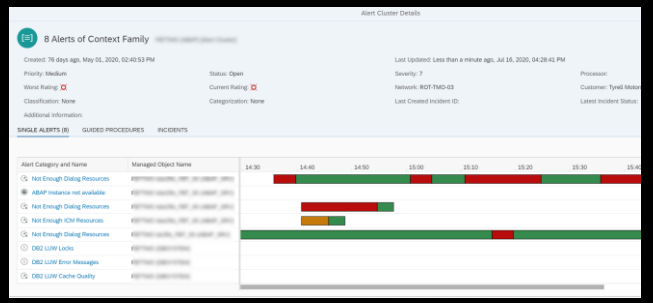
Usage scenario for alert correlation

1 **Identify relevant alert cluster in Alert Inbox**



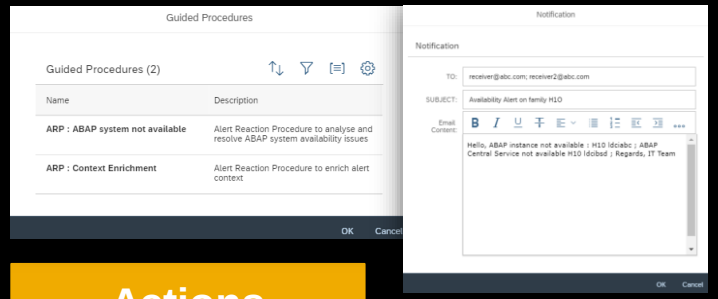
Alert Inbox

2 **Drill-down into Alert Cluster to analyze contributing single alerts**



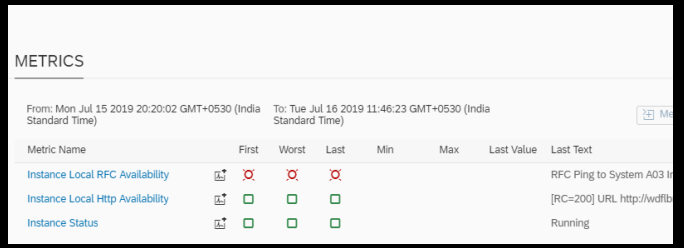
Alert Cluster

3 **Work on Alert resolution direct within Alert Cluster**



Actions

4 **Drill-down from Alert Cluster to single alert for metric detail**



Metric Monitoring

Roadmap for alert correlation

Lab Preview

- Enhance **analytics possibilities** for alert clusters
- Provide possibilities for **manual clustering / de-clustering**
- Provide **Root Cause prediction** for alert clusters
- 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 …"

Monitoring Dashboards

Anomaly Prediction

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

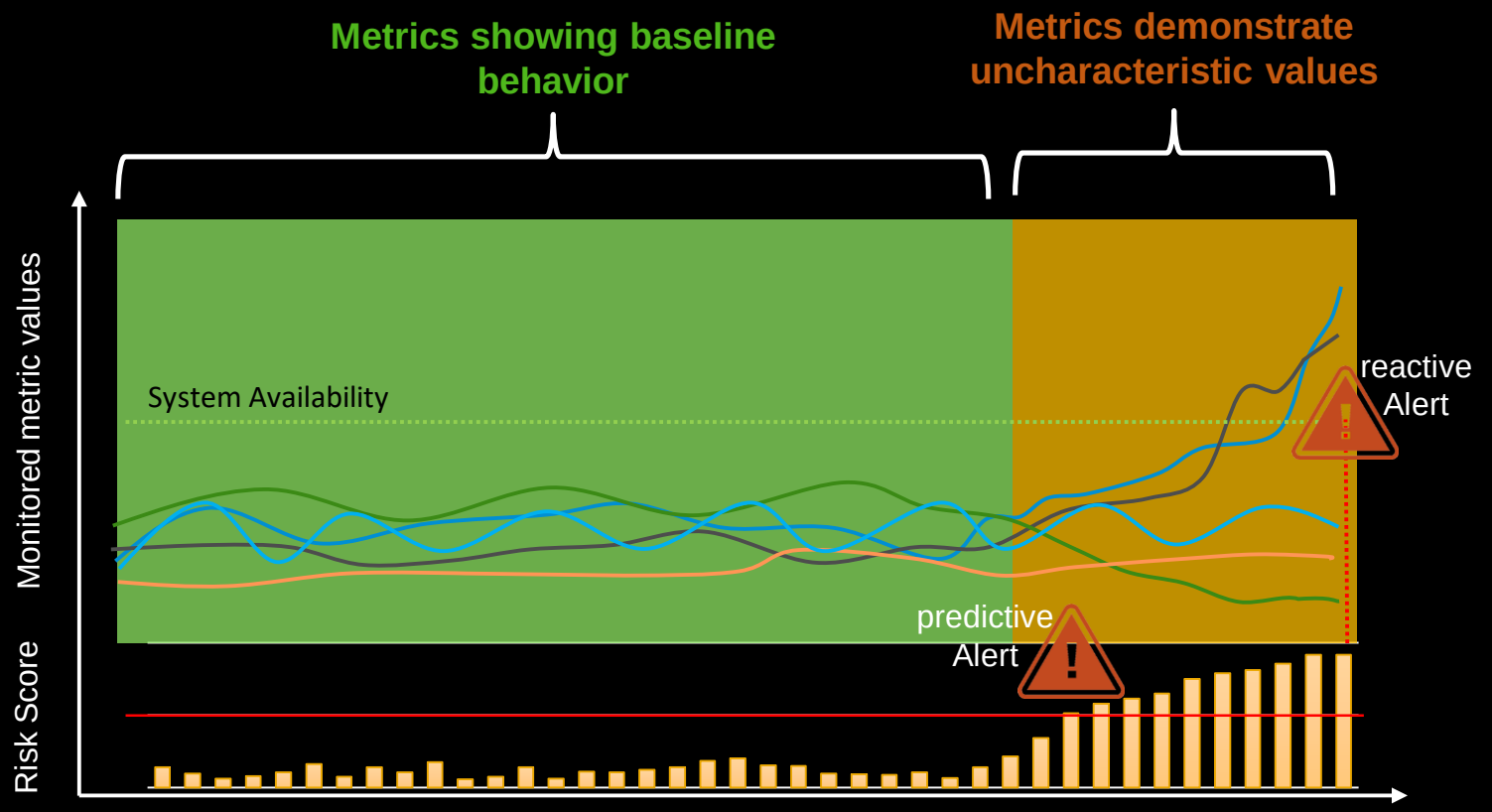
Reactive

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

Proactive

Concept of system anomaly prediction

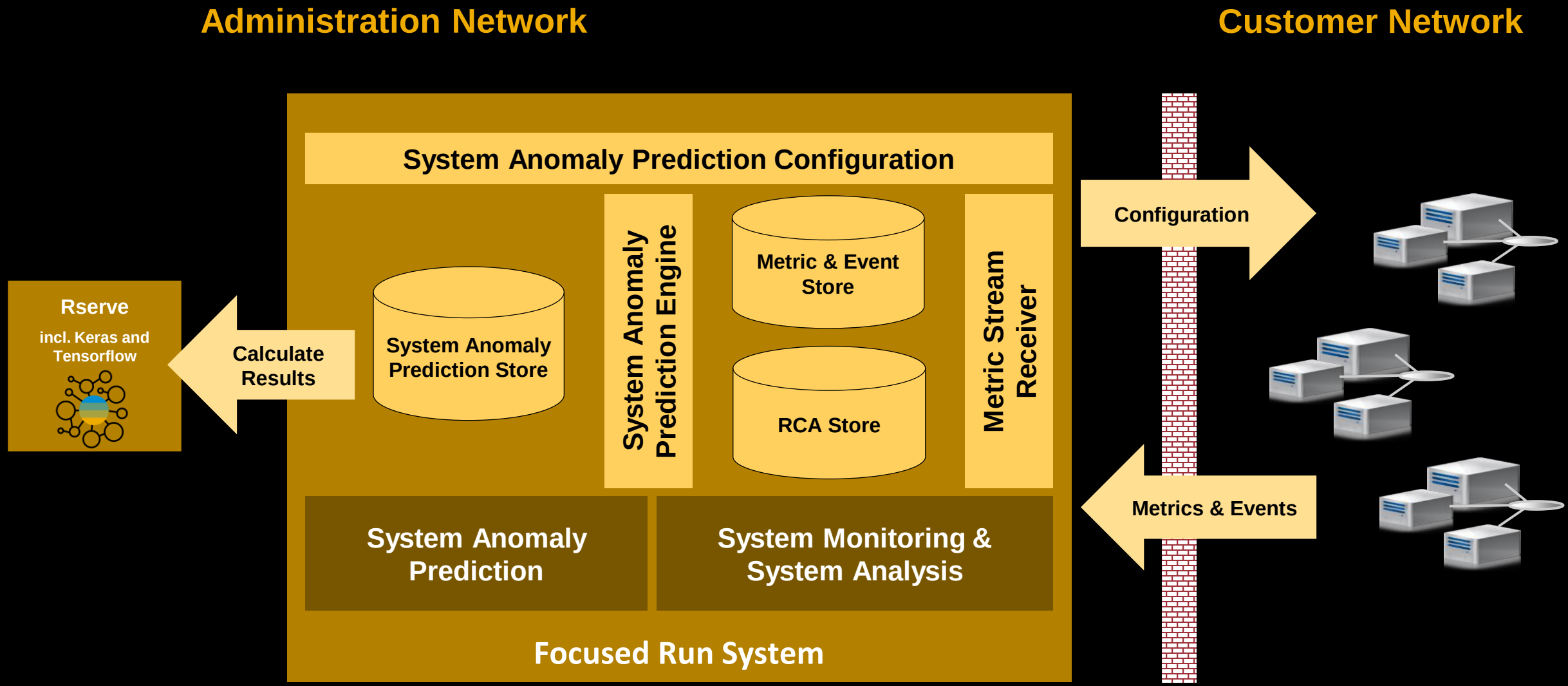
Target: Predict critical anomalies in a system **30-60 minutes in advance** with **high confidence**



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

Architecture for system anomaly prediction

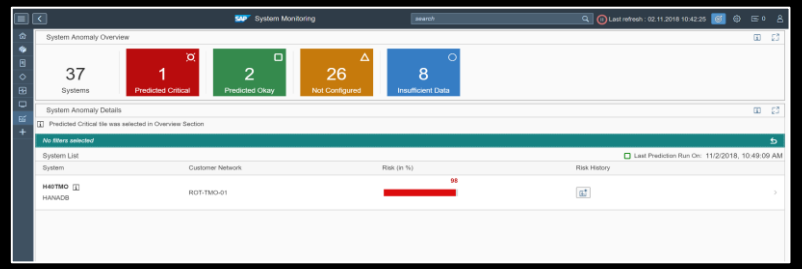


Usage scenario for system anomaly prediction

1 **Receive and react to Anomaly Prediction Alert**

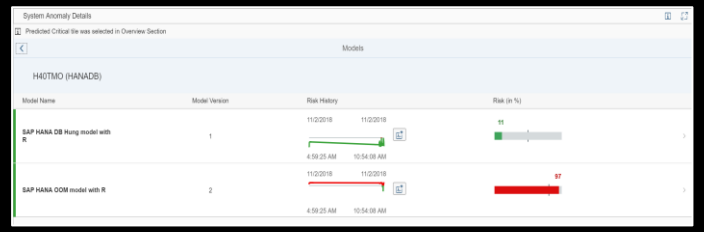
Alert Inbox

2 **Identification of critical systems including problems area / category**



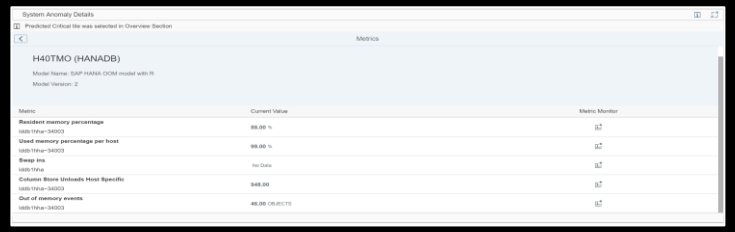
System Anomaly Prediction

3 **Detailed analysis of specific model versions associated with system**



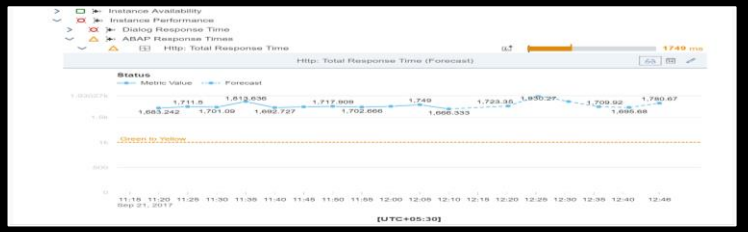
Model analysis

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



Metric identification

5 **Detailed analysis of metrics associated with metric forecasting**



Metric analysis

Roadmap for system anomaly prediction

Lab Preview

Trend-Based Alerting

- Enable alerting based on trends of single metrics

Semi-supervised training of custom models

- Provides system specific models to predict abnormal system behavior
- Based on system health classification of System Availability Management
- Guided data preprocessing, analysis and model training

Models

- Generalized anomaly model for SAP HANA (based on 1 minute data frequency using RCA data store)
- ABAP Resource Exhaustion model
- Java Out of Memory model

Preventive Measures for Zero Outage

- Provide guided procedure content to structure the analysis of the issue
- Provide activities to prevent the system standstill based on the analysis results

Ask your questions today!

Use the Q&A panel in the Zoom webinar to ask your questions.

Further Questions?

For questions after this session, please send to tomas.engelmann@sap.com or allam.drebes@sap.com.

Thank you!

Stay connected. Share your SAP experiences anytime, anywhere. Join the ASUG conversation on social media: **@ASUG365 #ASUG**

ASUG | SAP

Application Lifecycle Management Summit North America