Advanced Configuration Monitoring with Focused Run for SAP Solution Manager

New Town Square: Janko Budzisch, SAP // Heidelberg: Dr. Hendrik Müller, Reinhard Kirchner, SAP
November, 2019
Agenda

Overview Run Market

Focused Run for SAP Solution Manager

Configuration & Security Analytics - Overview

Configuration & Security Analytics - Policy handling

Configuration & Security Analytics - Content

Configuration & Security Analytics - Integration aspects

Configuration & Security Analytics - New features with Focused Run 2.0
Overview Run Market
Operations for hybrid landscapes

- **HEC, Hosting, AMS and IaaS Service Providers**
  - 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 Solution Manager: On Premise based operation platform for hybrid landscapes operated and used by Customers

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

- **SAP Cloud ALM**
  - SAP Cloud ALM operated 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**

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
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

**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

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

Available
Available
Beta
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

**On Premise**
- Gateway
- SAP Fiori/SAPUI5
- SAPGUI/DIAG
- Enterprise Portal
- CRM
- Business Suite
- BW
- SCM
- SCP Cloud Platform
- SRM
- SAP S/4 HANA
- Hybris
- SAP Process Integration
- Non-SAP (WebMethods, Tibco, …)

**Cloud**
- Fiori-as-a-Service
- SAP Cloud Platform
- Mobile Services
- SAP Cloud Analytics Cloud
- SuccessFactors
- ByD/G4C
- Concur
- IBP
- S/4 HANA Cloud Edition
- Ariba
- Fieldglass
- SCP Cloud Integration
- SCP Cloud Connector

**Presentation Layer**

**Application Layer**

**Integration Layer**
## Focused Run – Use cases in scope

### Advanced Analytics & Intelligence

<table>
<thead>
<tr>
<th>Advanced Event &amp; Alert Management</th>
<th>Advanced Configuration Monitoring</th>
<th>Advanced System Management</th>
<th>Advanced Integration Monitoring</th>
<th>Advanced Root Cause Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>SAP Fiori/SAPUI5</td>
<td>SAPGUI/DIAG</td>
<td>Fiori-as-a-Service</td>
<td>Presentation Layer</td>
</tr>
<tr>
<td>SAP GUI/DIAG</td>
<td>Enterprise Portal</td>
<td>Mobile Services</td>
<td>Mobile Services</td>
<td>Presentation Layer</td>
</tr>
<tr>
<td>SAP Cloud Platform</td>
<td>s/4 HANA Cloud Edition</td>
<td>Integration</td>
<td>Integration</td>
<td>Application Layer</td>
</tr>
<tr>
<td>Advanced Event &amp; Alert Management</td>
<td>Advanced Configuration Monitoring</td>
<td>Advanced System Management</td>
<td>Advanced Integration Monitoring</td>
<td>Advanced Root Cause Analysis</td>
</tr>
<tr>
<td>SAP Process Integration</td>
<td>Non-SAP (WebMethods, Tibco, …)</td>
<td>SAP Process Integration</td>
<td>SAP Process Integration</td>
<td>SAP Process Integration</td>
</tr>
<tr>
<td>SCP Cloud Integration</td>
<td>SCP Cloud Integration</td>
<td>SCP Cloud Integration</td>
<td>SCP Cloud Integration</td>
<td>SCP Cloud Integration</td>
</tr>
</tbody>
</table>

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
Configuration & Security Analytics
Overview
What is Configuration & Security Analytics?

Enable central governance of software levels and configuration settings

- Enforces validation of configuration & security settings by automated comparison of **TO-BE** with **AS-IS** situation
- **TO-BE** situation is defined in so-called **policies** which are derived from **configuration templates** or security hardening guides
- Policy maintenance via intuitive management tool and distributions of policy templates via github
- Efficient browsing and searching within high volumes of configuration items
- Analysis of software and parameter changes which maybe the root cause for critical issues
- Support of configuration items at system, database and operating system level ➔ Continuous delivery of new content based on customer feedback
Which capabilities are provided by Configuration & Security Analytics?

**Validation**
- checks items against a policy
- values must follow configuration and security policies

**Changes**
- provides which items changed
- values may change over time

**Configuration Item**
- has a name, has a type, has value(s), belongs to an object

**Search**
- searches for items and values

**Store Browser**
- references items to landscape objects, shows content and history
Validation of configuration items per systems, checks or system/checks
Identification of changes per system

1. Changes displays for a technical system in scope the number of detected changes and allows to drill down on changes (sum) or on the number of changes per day.

2. It’s possible to drill down into changes for a system.

3. It’s possible to drill down into changes for a config store.

4. It’s possible to drill down into change history of an item.
Intelligent search for configuration items

1. Searching for configuration item names and values in CCDB ➔ Search output can be filtered per config store

2. The result provides a common view for all items. A column view of a single config store is possible. It is supported to use OR, to combine pattern and to use wildcard *.
Browsing of configuration stores

1. Store Browser displays all technical systems having config stores

2. Store Browser displays for a technical system all available config stores

3. It’s possible to drill down into the config store content and into the item history

- Timestamp shows the last extraction date. “Valid since” shows since when item is unchanged

- A config store is always referenced to a landscape element

---

**Systems Overview**

**Stores of a System**

**Store Content**

**Item History**

---

**Config Stores of FT4ADM type Application Server ABAP - Items: 66 - displayed: 66**

<table>
<thead>
<tr>
<th>Description</th>
<th>Config Store Name</th>
<th>Landscape</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC destinations type H</td>
<td>RFCDES_TYPE_H</td>
<td>FT4 on idds84</td>
</tr>
<tr>
<td>RFC destinations type L</td>
<td>RFCDES_TYPE_L</td>
<td>FT4 on idds84</td>
</tr>
<tr>
<td>RFC destinations type T</td>
<td>RFCDES_TYPE_T</td>
<td>FT4 on idds84</td>
</tr>
<tr>
<td>SAINI/SPAM level</td>
<td>SPAM_VERSION</td>
<td>FT4 on idds84</td>
</tr>
<tr>
<td>SAP Kernel</td>
<td>SAP_KERNEL</td>
<td>AppServer 04 of FT4 on idds84</td>
</tr>
</tbody>
</table>

**SAP Kernel (SAP KERNEL) - Items: 6 - displayed: 6**

<table>
<thead>
<tr>
<th>ConfigurationKey</th>
<th>Value</th>
<th>Type of event</th>
<th>Switch table view</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME = KERN_COMP_ON</td>
<td>VALUE = Linux OSU/ES-11-86C_12d00d0f-3.4.1-109122</td>
<td>INITIAL</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_COMP_TIME</td>
<td>VALUE = 2016-12-22</td>
<td>INITIAL</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_DBLB</td>
<td>VALUE = SQLDBC 1.0.0.120.091.1510763291</td>
<td>UPDATED</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_DBLLEVEL</td>
<td>VALUE = 32G</td>
<td>INITIAL</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_KERL</td>
<td>VALUE = T45_KERL</td>
<td>INITIAL</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_DBLIB</td>
<td>VALUE = SQLDBC 1.0.0.120.091.1510763291</td>
<td>UPDATED</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_DBLIB</td>
<td>VALUE = SQLDBC 1.0.0.120.091.1510763291</td>
<td>UPDATED</td>
<td></td>
</tr>
<tr>
<td>NAME = KERN_DBLIB</td>
<td>VALUE = SQLDBC 1.0.0.120.091.1510763291</td>
<td>INITIAL</td>
<td></td>
</tr>
</tbody>
</table>
Configuration & Security Analytics
Policy handling
Usage of SAP baseline policies for configuration validation

1. SAP Baseline Security Policy Document

2. Policy Definition as XML file

3. Validation Result
Define your own policies based on SAP baseline policies

(*) For the Configuration and Security Analytics in Focused Run the SAP Baseline Policies are available at the GIT: https://github.com/SAP/frun-csa-policies-best-practices/
Further features for policy handling

**SAP Patch Day Policies**

- SAP Security Patch Day ➔ *Monthly publication of Security Notes*
- Security Note Policies are *published via GitHub* for measurable ABAP and HANA notes
- Via Policy Catalog a patch day check *within five minutes can be setup* for whole landscape

**Hiding policies for certain customers / networks**

- It is possible to *restrict the visibility of policies* to certain customers / networks (per default disabled)
- Service Provider can switch it on by policy naming and authorization (high maintenance effort), assign individual policies to customer network or *maintain assignment group* (Policy – Group – Customer Network)

**Exemptions for policies**

- Exemptions are only taken into account by the validation, if the *checkbox ‘Apply exemption’* is enabled
- Each exemption does refer to a *single check item of a single policy and can be timely restricted*
Configuration & Security Analytics

Content
Pre-defined content for managed ABAP systems

ABAP Database interface
ABAP Generic Whitelists Information
ABAP Notes
ABAP Scenario-Based Checks Information
ABAP Secure Storage Encryption Key status
ABAP UCON RFC Basic Scenario
ABAP UCON http white list Scenario
ABAP clients (T000)
Access to P_ABAP objects by role (CSTO-EXAMPLE)
Audit log (Configuration)
Audit log (CONFIGURATION_SLOT)
Audit log (Configuration XML)
BW administration settings (RSADMIN)
BW customizer control table (RSADMINA)
BW customizing table (RSADMINC)
BW frontend (RSFRONTENDINIT)
BW source system transfer
BW system settings (RSADMINS)
Clients - Change log
Component change settings
Component change settings - Change log
Crypto library version
Customizing settings for authorization process
Default profile
Display roles (CSTO-EXAMPLE)
Environment variables
Gateway proxy
Gateway registry
Gateway security
Global change setting
Global change setting - Change log
HTTP Whitelist
HTTP Whitelist (UCON Client dependent)
HTTP Whitelist (UCON)
Host - installed software packages
Host configuration
http services (SICF)
IGS Manifest
Installed software packages
Instance parameter
Instance profile
License
Maintenance areas for tables
Message server security
Namespace change settings
Namespace change settings - Change log
PSE certificates
Path for backup and authorization
Permitted trusted systems
RFC destinations
RFC destinations type '3'
RFC destinations type 'G'
RFC destinations type 'H'
RFC destinations type 'L'
RFC destinations type 'T'
Role User Relation (CSTO-EXAMPLE)
Role by authorization check (test)
Role by organisation element (CSTO-EXAMPLE)
Roles ZSAP
SAINT/SPAM level
SAP Kernel
SAPHostAgent: Version
SAPHostAgent: host_profile
SAPUI5 library
SAPUI5 version
SCS profile
SMLT Languages
SNC Access Control List (ACL)
SSO2 - Access control list
Security policy
Sensitive table access by role (CSTO-EXAMPLE)
Sensitive transaction access by role (CSTO-EXAMPLE)
Session management
Set Values for the Session Manager / Profile Generator
Software component level
Standard users
System Hosts
Transports
Usage of password hashing
User by authorization check
User with SAP_ALL profile
User with cust. profiles
Virus scan groups
Virus scan server
XMS: Integration Engine Config. Parameters (Client)
XMS: Integration Engine Configuration Parameters

Pre-defined other standard content & Integration of custom content

Further standard content

- Java Systems
- HANA Systems
- SAP Business Object Cluster
- Databases (Sybase, LiveCache,..)
- Host
- Operating Systems
- Others

Integration of custom content

- ABAP only: Custom function module
- Custom File System Extractor
- Custom Database SQL Statement
- Custom Operating System Script
- ABAP only: Customizable Stores for basic role and user authorization checks

Configuration & Security Analytics
Integration aspects
Integration in System Health Checks Reports

It is possible to **schedule** (daily, monthly, ad hoc) the **automatic execution of System Health Checks** based on the SAP Guided Procedure Framework.

The registered recipients will get a **email** which includes the **System Health Check document** in HTML format.

Some examples for included checks:

- **Availability** (System, Instance)
- **ABAP Performance** (Dialog Response time, HTTP Response Time, Long Running Jobs, …)
- **ABAP Exceptions** (Lock Entries, Short Dumps, …)
- **OS Level Checks** (Top CPU Processes, File System Free space)
- **HANA Checks** (HANA Space, HANA Used Memory, Database Growth)
- **ASE Checks** (Space, Long Running Transactions, …)

Integration in System Monitoring

- Metric and alerts based on non-compliant items
- Data collectors for CSA policy
- Data collectors for Store Changes
Configuration & Security Analytics
New features with Focused Run 2.0
New features with Focused Run 2.0 FP01

Check item restriction by LMDB attributes

- Customer specific LMDB attributes as landscape grouping option
- Validity of a check item can be restricted based on custom LMDB attributes
- Several attributes can be combined using a logical AND condition
- Avoids complex system scope selection

Transitioning of policies from Solution Manager 7.2

- Transforming of Solution Manager 7.2 Target Systems into Focused Run CSA Policies
- Automates the policy definition for common check types
- ABAP report delivered with Solution Manager 7.2 SP10 or via SAP note 2828567 (SP 07/08/09)
- Verification and manual post processing mandatory
New features with Focused Run 2.0 FP02

Cross Search and Change Reporting
• Cross landscape views on chosen config store data
• Allows flexible cross reporting on data as required
• Examples: Software Levels (e.g. SAP Host Agent Level, Security Parameter, ABAP Transports, …)

Certificate Alerting for SAP Cloud Platform Integration
• Saving CPI endpoint triggers CSA setup ➔ Certificates are automatically retrieved
• Alert is raised, if a certificate will expire

Enhanced Policy Maintenance
• Policy selection via table (filtering, sorting) & find policies by pattern search in definition and SQL
• Simplified copying of a policy
• Direct start of validation for testing
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

**Reinhard Kirchner**
Service Engineer
reinhard.kirchner@sap.com

**Dr. Hendrik Müller**
Service Engineer
hendrik.mueller@sap.com