Checking Security Configuration and Authorization

... or how best to protect your data and keep the availability of your SAP solutions

SAP CoE Security Services
January 2020
Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document 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. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Abstract

Software security remains a critical topic of interest to all companies and to the information technology industry.

The security of a specific system thereby also significantly depends on the secure installation and operation of this system. SAP gained a lot of experience from its support for and engagement with numerous customers. It uses the resulting best practices not only for further improvements and enhancements of its support offering but also makes them available as recommendations, services and tools directly to its customers.

In this presentation you will learn about the self services and tools available for security, centered around the “Security” section in the EarlyWatch Alert report.

And you will get additional information about the Security Optimization Service and the Configuration Validation which can be used to analyze the security configuration for single systems as well as for the complete system landscape.

Finally you will see how to show the results of security reporting in Dashboards and how to trigger Alerts or pass results of change reporting or configuration validation to GRC Process Control.
Agenda

- Best Practices-based Services

Security Tools and Services
- EarlyWatch Alert (EWA) – Security Chapter
- Security Optimization Service (SOS)
- Configuration Validation

Security in Operations
- Dashboards & Alerts
- Integration with GRC Process Control
Security Management – continuous process along a Quality Circle

Analyze the differences and determine their root cause. Determine where to apply changes that will lead to improvements and the expected results.

Measure the new processes and compare the results via indicators (KPIs) against the expected results in order to identify possible differences.

Establish the objectives and processes necessary to deliver results in accordance with the expected output.

Implement the new processes and procedures.

The security plans (Plan) are implemented (Do) and the implementation is then evaluated (Check). After the evaluation both plans and implementation of the plan are carried out (Act).
Develop an implementation plan covering the missing IT Security measures according to the criticality of the related risk to be mitigated.

Implement the security measures.

Evaluate the operational risk resulting from the identified gaps.

Report the results of the risk assessment according to the defined operational IT Risk Management process.

For each IT organization:

- Collect and document all systems maintained/operated.
- Monitor changes in processes, infrastructure, and risk situations.

- All systems have to be assigned to a category of systems according to the criticality of the data/information stored/processed on the system.

- The IT security measures based on the system classification have to be aligned with the business requirements. Compromises might have to be made on both sides.

- Remaining risks have to be identified and addressed with respective business owners.

- Compare implemented security measures vs. security requirements and identify existing gaps.
Analysis+Reporting
Company wide consolidation of security settings.

Authentication
Prove who you are. Passwords, SSO, Federation.

User Management
Maintain accounts. Identity Management and more.

Authorizations
Who’s allowed to do what? Privilege management.

System+Infrastructure Security
Code security, RFC gateway, network and interfaces.

- Develop an implementation plan covering the missing IT Security measures according to the criticality of the related risk to be mitigated.
- Implement the security measures.
- Evaluate operational risk resulting from the identified gaps.
- Report and document all systems maintained/operated.
- Monitor changes in processes, infrastructure, and risk situations.

Investment on authorizations and user management (“putting locks on doors”) often endangered by negligent handling of baseline security measures (“leaving open the windows”).

The IT security measures based on the system classification have to be aligned with the business requirements. Compromises might have to be made on both sides. Remaining gaps have to be identified and addressed with respective business owners.

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Analysis+Reporting
Company wide consolidation of security settings.

- Develop an implementation plan covering the missing IT Security measures according the criticality of the related risk to be mitigated.
- Implement the security measures.
- Evaluate the operational risk resulting from the identified gaps.
- Report the results of the risk assessment according the defined operational IT Risk Management process.
- Collect and document all systems maintained/operated.
- Monitor changes in processes, infrastructure and risk situation.
- All systems have to be assigned to a category of systems according the criticality of the data/information stored/processed on the system.
- The IT security measures based on the system classification have to be aligned with the business requirements. Compromises might have to be made on both sides.
- Remaining risks have to be identified and addressed with respective business owners.
- Compare implemented security measures vs. security requirements and identify existing gaps.
- Internal and external auditors are “discovering” these topics at the moment!

System+Infrastructure Security
Code security, RFC gateway, network and interfaces.

IT Risk & Security Lifecycle - for each single IT organization
Transparency and Mitigation
Empowering on available tools and content

Comparison against SAP recommendations
Security in EarlyWatch Alert (EWA)

Overview

Comparison against company's security policy

Detail

Security Optimization Service System Recommendations

Company's SAP Security Baseline

Configuration Validation

Target System

Management Dashboard

Service delivery example:

A Automated services indicate security gaps

Recommendation: Detailed look into gaps through experts

Service – Part 1:
- Root cause analysis for security gaps
- SAP Security Baseline maintenance

Service – Part 2:
- Security patch deployment cycle
- Configuration setup
- Proactive threat identification

Service – Part 3:
- Security control via dashboard

Overview

Comparison against company's security policy

Detail

Security Optimization Service System Recommendations

Company's SAP Security Baseline

Configuration Validation

Target System

Management Dashboard

Service delivery example:

A Automated services indicate security gaps

Recommendation: Detailed look into gaps through experts

Service – Part 1:
- Root cause analysis for security gaps
- SAP Security Baseline maintenance

Service – Part 2:
- Security patch deployment cycle
- Configuration setup
- Proactive threat identification

Service – Part 3:
- Security control via dashboard

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Agenda

➔ Best Practices-based Services

Security Tools and Services
➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

Security in Operations
➔ Dashboards & Alerts
➔ Integration with GRC Process Control
The Role of EarlyWatch Alert (EWA) for Security

SAP EarlyWatch Alert (EWA) (see https://support.sap.com/ewa)

SAP EarlyWatch Alert is an important part of making sure that your core business processes work. It is a tool that monitors the essential administrative areas of SAP components and keeps you up to date on their performance and stability. SAP EarlyWatch Alert runs automatically to keep you informed, so you can react to issues proactively, before they become critical.

Security in the EarlyWatch Alert:

- The EWA Report includes selected information on critical security observations for
  - SAP Application Server ABAP
  - SAP Application Server Java
  - SAP HANA

- More detailed and additional information can be found with the help of the Security Optimization Service (SOS) – either as Guided Self Service (GSS) for AS ABAP or as remote or onsite SOS for all technologies.
During this EarlyWatch Alert session, we detected issues that could potentially affect your system. We recommend that you take corrective action as soon as possible.

**Alert Overview**

- **High** Standard users have default password.
- **High** Secure password policy is not sufficiently enforced.
- **High** A high number of users has critical authorizations.
- **High** Gateway Access Control List (req_info/sec_info) contains trivial entries.
Based on these findings it is recommended that you perform the following Guided Self Services.

**Guided Self Service**

<table>
<thead>
<tr>
<th>Security Optimization Service</th>
<th>FAQ SAP Note</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>696478</td>
</tr>
</tbody>
</table>

For more information about Guided Self-Services, see [SAP Enterprise Support Academy](https://support.sap.com).

Register for an Expert-Guided Implementation Session for the Guided Self-Service at [SAP Enterprise Support Academy - Learning Studio - Calendar](https://support.sap.com).

<table>
<thead>
<tr>
<th>Topic Rating</th>
<th>Topic</th>
<th>Subtopic Rating</th>
<th>Subtopic</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt=" " /></td>
<td>Security</td>
<td><img src="image" alt=" " /></td>
<td>SAP HANA System Privilege DATA ADMIN</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td></td>
<td><img src="image" alt=" " /></td>
<td>SAP HANA Password Policy</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td></td>
<td><img src="image" alt=" " /></td>
<td>SAP HANA Audit Trail</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td></td>
<td><img src="image" alt=" " /></td>
<td>SAP HANA SQL Trace Level</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td></td>
<td><img src="image" alt=" " /></td>
<td>SAP HANA Network Settings for Internal Services</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td></td>
<td><img src="image" alt=" " /></td>
<td>SAP HANA SSFS Master Encryption Key</td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>System Recommendations (ABAP)</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Default Passwords of Standard Users</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Control of the Automatic Login User SAP*</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Protection of Passwords in Database Connections</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>ABAP Password Policy</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Gateway and Message Server Security</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt=" " /></td>
<td>Users with Critical Authorizations</td>
<td><img src="image" alt=" " /></td>
<td></td>
</tr>
</tbody>
</table>
Critical security issues were found in your system. See the information in the following sections.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SAP HANA System Privilege DATA ADMIN</td>
</tr>
<tr>
<td></td>
<td>SAP HANA Password Policy</td>
</tr>
<tr>
<td></td>
<td>SAP HANA Audit Trail</td>
</tr>
<tr>
<td></td>
<td>SAP HANA SQL Trace Level</td>
</tr>
<tr>
<td></td>
<td>SAP Security Notes: ABAP and Kernel Software Corrections</td>
</tr>
<tr>
<td></td>
<td>Default Passwords of Standard Users</td>
</tr>
<tr>
<td></td>
<td>Control of the Automatic Login User SAP*</td>
</tr>
<tr>
<td></td>
<td>ABAP Password Policy</td>
</tr>
<tr>
<td></td>
<td>Gateway and Message Server Security</td>
</tr>
<tr>
<td></td>
<td>Users with Critical Authorizations</td>
</tr>
</tbody>
</table>
10.1 SAP HANA Database HDB

10.1.1 SAP HANA System Privilege DATA ADMIN

10.1.1.1 Users with DATA ADMIN Privilege

Users in your SAP HANA database have the DATA ADMIN system privilege. The count considers direct grants to the users as well as indirect grants using roles. Users are counted as activated if the validity time range matches the time of the evaluation and the user is not deactivated. The SYSTEM and _SYS_REPO users are not considered, because these users have the DATA ADMIN privilege by design and the privilege cannot be revoked from these users.

| Number of Additional Users with DATA ADMIN Privilege | 5 |

DATA ADMIN provides the authorization to modify and delete every object in every schema.

**Recommendation:** Remove the DATA ADMIN privilege from all user accounts except the SYSTEM and _SYS_REPO users.
10.1.1.2 Role DBA_COCKPIT with DATA ADMIN Privilege

The DATA ADMIN system privilege was granted to the DBA_COCKPIT role, probably based on the SAPINST installation procedure or on a former version of SAP Note 1640741.

**Recommendation:** Remove the DATA ADMIN privilege from the DBA_COCKPIT role also according to the updated version of SAP Note 1640741, points 5 and 12.

**Note:** The DBA_COCKPIT role is usually granted to the users DBACOCKPIT, DBA_COCKPIT_<calling_sid>, and/or SAP_<sid>. If you revoke the DATA ADMIN privilege from the DBA_COCKPIT role, therefore, the number of users in the 'Users with DATA ADMIN Privilege' section may be reduced.

10.1.1.3 Roles with DATA ADMIN Privilege

The DATA ADMIN system privilege is granted to the following roles.

<table>
<thead>
<tr>
<th>Name of Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASIS_ADMIN</td>
</tr>
<tr>
<td>DBA_COCKPIT</td>
</tr>
</tbody>
</table>

The DATA ADMIN privilege provides the authorization to modify and delete every object in every schema. It must not be granted to any user in a production environment. Therefore, it should not be assigned to any particular role since it is not required and is at risk of being misused.

**Recommendation:** Remove the DATA ADMIN privilege from all the above roles or delete these roles.
10.1.2 SAP HANA Password Policy

The following table provides an overview of the current values of the password policy and the corresponding values recommended by SAP. A yellow rating indicates a setting that is weaker than recommended, while a green rating indicates a recommended or stronger setting. This section only appears in the EWA report if at least one of the following parameters is rated yellow.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Parameter</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>force_first_password_change</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>![Yellow]</td>
<td>maximum_unused_initial_password_lifetime</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>![Green]</td>
<td>minimal_password_length</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

- If one of these three parameters gets a non-green rating – i.e. there is a severe finding regarding the password policy enforcement – then additional password complexity parameters are shown for information and recommendation (see next slide).
EarlyWatch Alert – HANA Security Checks
Password Policy – Additional Parameters

- The following list of password complexity parameters, current values and recommendations is shown only, if one of the three critical password parameters (see previous slide) received a non-green rating.
- These optional parameters listed on this slide never trigger an EWA HANA Password Policy entry on their own.

The following table provides an overview of the remaining password policy parameters.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Parameter</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>last_used_passwords</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>✔️</td>
<td>maximum_unused_productive_password_lifes</td>
<td>365</td>
<td>365</td>
</tr>
<tr>
<td>✔️</td>
<td>minimum_password_lifetime</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>✔️</td>
<td>password_expire_warning_time</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>✔️</td>
<td>password_layout</td>
<td>A1a</td>
<td>A1a</td>
</tr>
<tr>
<td>✔️</td>
<td>password_lock_time</td>
<td>1440</td>
<td>1440</td>
</tr>
<tr>
<td>✔️</td>
<td>maximum_invalid_connect_attempts</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>✔️</td>
<td>maximum_password_lifetime</td>
<td>182</td>
<td>182</td>
</tr>
</tbody>
</table>

**Recommendation:** Adapt all values to the recommended or stronger settings.
10.1.3 SAP HANA Audit Trail

Sources of information for the SAP HANA audit trail:
- SAP HANA Security Guide
- SAP HANA Administration Guide
- SAP HANA Audit Trail Best Practice in the SCN

10.1.3.1 Auditing Status
Auditing is disabled in the security settings of your SAP HANA database.

Recommendation: Activate the SAP HANA audit trail and define appropriate audit policies.

10.1.3.2 Audit Trail Target
The audit trail target is currently set to "CSV Text File". This is not secure enough and should only be used for test purposes. CSV text files are not sufficiently protected against unauthorized modifications.

Recommendation: Use the "Syslog" (default) or (as of SPS07) "Database Table" target.

Note: If you use the "Syslog" option, you also need to configure the operation system syslog accordingly so that you will not receive error messages in the event of issues with the OS syslog.

10.1.3.3 Audit Policies
No customer-defined audit policies are enabled.

Recommendation: Define audit policies according to your needs.
10.1.4 SAP HANA SQL Trace Level

**Current SQL Trace Parameter Values**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>trace</td>
<td>off</td>
</tr>
<tr>
<td>level</td>
<td>all_with_results</td>
</tr>
</tbody>
</table>

The SQL trace level is currently set to 'ALL_WITH_RESULTS'. This setting will force the trace to write all result sets from SQL statements in the trace file. Persons who are not authorized to see this information may still be able to read these trace files.

**Recommendation:** Use SQL trace with results in exceptional cases only. Change the trace level to ALL or a lower trace level. Even if the SQL trace is switched off (trace=off), the trace level should not be set to ALL_WITH_RESULTS because someone could activate this critical trace level unintentionally by switching on the SQL trace.
EarlyWatch Alert – HANA Security Checks
Internal Network Settings / SSFS Master Encryption Key

10.1.5 SAP HANA Network Settings for Internal Services

<table>
<thead>
<tr>
<th>Rating</th>
<th>File Name</th>
<th>Layer</th>
<th>Section</th>
<th>Key</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Red Check]</td>
<td>global.ini</td>
<td>SYSTEM</td>
<td>communication</td>
<td>listeninterface</td>
<td>.global</td>
</tr>
<tr>
<td>![Green Check]</td>
<td>global.ini</td>
<td>DEFAULT</td>
<td>internal_hostname_resolution</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Your system internal network configuration is not secured against unauthorized access. Immediate action is required.

**Recommendation:** Follow the instructions in the [SAP Note 2183363](https://support.sap.com/).

10.1.6 SAP HANA SSFS Master Encryption Key

The parameter `ssfs_key_file_path` is not set in the section `[cryptography]` of the `global.ini` file. Most likely your SSFS Master Encryption Key has not been changed from its default value.

**Recommendation:** Change your SSFS Master Encryption Key as described in [SAP Security Note 2183624](https://support.sap.com/) and [SAP HANA Administration Guide, Section ‘Change the SSFS Master Key’](https://support.sap.com/).
11.1 ABAP Stack of XXX

11.1.1 System Recommendations (ABAP)

System Recommendations is not used for this system.

**Recommendation:** SAP strongly recommends applying important security fixes as soon as possible. The 'System Recommendations' application provides a detailed recommendation regarding which SAP security notes (ABAP and non-ABAP) should be implemented based on the actual status of the system and the notes already implemented. This is a mandatory prerequisite for setting up a strong security patch process. For more information, refer to [http://service.sap.com/sysrec](http://service.sap.com/sysrec).
11.1.2 Default Passwords of Standard Users

Standard users, including SAP* and DDIC, have default passwords.

**Recommendation:**
Run report RSUSR003 to check the usage of default passwords by standard users.

Ensure that:
- User SAP* exists in all clients
- Users SAP*, DDIC, SAPCPIC, and EARLYWATCH have non-default passwords in all clients
- Profile parameter login/no_automatic_user_sapstar is set to 1.

For more information, see "Protecting Standard Users" and "Profile Parameters for Logon and Password (Login Parameters)" either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

Make sure that the standard password for user TMSADM has been changed in client 000 and delete this user in any other client. SAP Note 1414256 describes a support tool to change the password of user TMSADM in all systems of the transport domain. SAP Note 1552894 shows how to update the report RSUSR003 to show the status of user TMSADM.
11.1.3 Control of the Automatic Login User SAP*

The profile parameter login/no_automatic_user_sapstar is set to 0 on at least one instance.

If the user SAP* user master record is deleted, it is possible to log on again with SAP* and the initial password. SAP* then has the following attributes:
- The user has all authorization, as authorization checks cannot be executed.
- You cannot change the standard password.
You can deactivate the special attributes of SAP* using profile parameter login/no_automatic_user_sapstar.

**Recommendation:** Set profile parameter login/no_automatic_user_sapstar to 1. For further information, see SAP Note 68048.
11.1.4 ABAP Password Policy

If password login is allowed for specific instances only, the password policy is checked only for these instances.

11.1.4.1 Password Complexity

**PARAMETER: LOGIN/MIN_PASSWORD_LNG**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Current Value(s)</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>iwdfvm2444_C70_01</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

The current system settings allow a minimum password length less than 8 characters. This allows weak passwords. Attackers may successfully recover these passwords and exploit this to gain unauthorized access to the system.

**Recommendation**: Use a minimum value of 8 for the profile parameter login/min_password_lng.
In addition, SAP provides options to enforce complex passwords. Find the current settings of the corresponding profile parameters in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Instance</th>
<th>Current Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_digits</td>
<td>iwdfvm2444_C70_01</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td>iwdfvm2444_C70_01</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_lowercase</td>
<td>iwdfvm2444_C70_01</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_uppercase</td>
<td>iwdfvm2444_C70_01</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td>iwdfvm2444_C70_01</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recommendation:** Enforce a minimum of 3 independent character categories using the corresponding profile parameters. For more information, see SAP Note [862989](https://support.sap.com/cn/862989) and the section Profile Parameters for Logon and Password (Login Parameters) either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.
### 11.1.4.2 Validity of Initial Passwords

<table>
<thead>
<tr>
<th>Rating</th>
<th>Parameter</th>
<th>Instance</th>
<th>Current Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚡</td>
<td>login/password_max_idle_initial</td>
<td>iwdfvm2444_C70_01</td>
<td>0</td>
</tr>
</tbody>
</table>

There is no time restriction on the validity of initial passwords.

**Recommendation:** Proceed as follows:

-- Handle users of type C (Communication) with initial passwords, because they will be locked if the profile parameter above is set.

Use transaction SUIM/report RSUSR200 in each client to find users of type C (Communication). If these users are active and in use, switch the user type to B (System). This has no negative effect.

-- Restrict the password validity to 14 days or less.

-- For more information, see SAP Note [862989](https://support.sap.com/notes/862989) and the section *Profile Parameters for Logon and Password (Login Parameters)* either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.
7.4 Gateway and Message Server Security

7.4.1 Kernel Patch Level

<table>
<thead>
<tr>
<th>Rating</th>
<th>Kernel Release</th>
<th>Current Kernel Patch Level</th>
<th>Minimal Required Kernel Patch Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️</td>
<td>701</td>
<td>89</td>
<td>98</td>
</tr>
</tbody>
</table>

To enable certain Gateway and Message Server security functionality, a minimum patch level of the kernel is required. Your system currently misses this requirement.

**Recommendation:**
Update the kernel of your system to the newest kernel patch level available. At least update to a kernel patch level equal or higher than the minimal required kernel patch level given above. Additional information can be found in SAP Note 1298433.
7.4.2 Gateway Security

Gateway Security Properties

**PARAMETER: gw/reg_no_conn_info**

The parameter gw/reg_no_conn_info controls the activation of certain security properties of the SAP Gateway. It is defined as a bit mask with one bit per property.

On your system the following properties were identified:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Value Name</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Warning]</td>
<td>Bypassing security in reg_info &amp; sec_info</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>![Checkmark]</td>
<td>Bypassing sec_info without reg_info</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>![Warning]</td>
<td>CANCEL registered programs</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>![Warning]</td>
<td>Uppercase/lowercase in the files reg_info and sec_info</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

**Recommendation:**
Enable the missing properties by adding the respective recommended values to the current value of gw/reg_no_conn_info.

More information regarding gw/reg_no_conn_info can be found in SAP Note [1444282](https://support.sap.com).
### Enabling an Initial Security Environment

**Parameter:** gw/acl_mode

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>All instances</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Recommendation:** Parameter gw/acl_mode can be set to 1 to activate a more secure default behavior if either of the access control lists defined by gw/sec_info and gw/reg_info does not exist. SAP recommends setting gw/acl_mode to 1 to establish an additional line of defense should any of the access control lists be missing. For more information, see SAP Note 1480644.
### Gateway Access Control Lists

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>All instances</td>
<td>gw/reg_info and gw/sec_info are defined</td>
</tr>
</tbody>
</table>

### REG_INFO

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Error Condition</th>
<th>File does not exist (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>All instances</td>
<td>P TP=*</td>
<td></td>
</tr>
</tbody>
</table>

### SEC_INFO

<table>
<thead>
<tr>
<th>Rating</th>
<th>Instance</th>
<th>Error Condition</th>
<th>File does not exist (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠</td>
<td>All instances</td>
<td>P TP=* USER=* USER-HOST=* HOST=*</td>
<td></td>
</tr>
</tbody>
</table>

**Recommendation:** The profile parameters gw/sec_info and gw/reg_info provide the file names of the corresponding access control lists. These access control lists are critical to controlling RFC access to your system, including connections to RFC servers. You should create and maintain both access control lists, which you can do using transaction SMGW. For more information, see "Configuring Connections between SAP Gateway and External Programs Securely" on SAP Help Portal.
7.4.3 Message Server Security

Separation of Internal and External Message Server Communication

**Parameters:** rdisp/msserv rdisp/msserv_internal

<table>
<thead>
<tr>
<th>Rating</th>
<th>Error Condition</th>
<th>Value of rdisp/msserv</th>
<th>Value of rdisp/msserv_internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>![ ]</td>
<td>rdisp/msserv_internal is not defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td>![ ]</td>
<td>rdisp/msserv_internal points to the same port as rdisp/msserv</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommendation:**

Communication with the message server should be separated into SAP system internal communication (TCP/IP port defined by rdisp/msserv_internal) and communication e.g. from user SAPGUIs to the system (TCP/IP port defined by rdisp/msserv). Network firewalls should block access to the port given in rdisp/msserv_internal from outside the SAP system.

Set parameter rdisp/msserv_internal to a TCP/IP port number different to the port number given in rdisp/msserv and additionally protect access to the internal message server port by appropriate firewalls. More information can be found in SAP Note 821875.
Message Server Administration Allowed for External Clients

Parameter: MS/MONITOR MS/ADMIN_PORT

<table>
<thead>
<tr>
<th>Rating</th>
<th>Parameter</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ms/monitor</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ms/admin_port</td>
<td>12345</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recommendation:**
SAP recommends to block external administration of the message server by setting the profile parameters `ms/monitor` and `ms/admin_port` both to the value 0.
More information can be found in SAP Note 821875.
The profile parameter `ms/admin_port` can be set dynamically via transaction SMMS -> Goto -> Security Settings.

Message Server Access Control List

Parameter: MS/ACL_INFO

<table>
<thead>
<tr>
<th>Rating</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ms/acl_info is not defined or empty</td>
</tr>
</tbody>
</table>

**Recommendation:**
The profile parameter `ms/acl_info` provides the file name of the message server's access control list. This list controls, which application servers are allowed to log on to the message server.
SAP recommends to define and properly maintain this list to prohibit rogue application servers to join the system. More information can be found in SAP Note 821875.
11.1.6 Users with Critical Authorizations

For more information about the following check results, please refer to SAP Note 863362. [...] 

11.1.6.1 Super User Accounts  

11.1.6.2 Users Authorized to Change all Tables

Unauthorized access to sensitive data is possible if too many users are granted authorization. The number of users with this authorization is stated for each client.

<table>
<thead>
<tr>
<th>Client</th>
<th>No. of Users Having This Authorization</th>
<th>No. of Valid Users</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>592</td>
<td>713</td>
<td>![ ]</td>
</tr>
<tr>
<td>999</td>
<td>227</td>
<td>285</td>
<td>![ ]</td>
</tr>
</tbody>
</table>

Authorization objects:
Object 1: $_TCODE with TCD=SE16, TCD=SE16N, TCD=SE17, TCD=SM30, or TCD=SM31  
Object 2: $_TABU_DIS with ACTVT = 03 or 02 and DICBERCLS = *

11.1.6.3 Users Authorized to start all Reports  
11.1.6.4 Users Authorized to Debug / Replace  
11.1.6.5 Users Authorized to Display Other Users Spool Request  
11.1.6.6 Users Authorized to Administer RFC Connections  
11.1.6.7 Users Authorized to Reset/Change User Passwords
My SAP EarlyWatch Alert Reports: You can read the EWA report in a complete new format that can be personalized with favorite systems and favorite topics. All details on alerts and recommendations are provided. The EWA Chapter about Security is included!

SAP EarlyWatch Alert – Analytical Dashboard: You can gain an overview on the system status with the most important KPIs from your SAP ABAP system and the SAP HANA database. KPI history of up to 12 months is available in drill-downs. (No security specific KPIs)

You require the SAP ONE Support Launchpad authorization “Service Reports & Feedback” to see data in these applications for the systems of the customer numbers to which your S-user is assigned. To request it, contact one of your company’s user administrators.

Either add the two new tiles to your SAP One Support Launchpad or use these direct links to the applications:
- https://launchpad.support.sap.com/#/ewaviewer
- https://launchpad.support.sap.com/#/ewadashboard
The application **My SAP EarlyWatch Alert Reports** provides the complete SAP EarlyWatch Alert report for ABAP on SAP HANA systems (and systems having an additional database connection to a separate SAP HANA database). You can easily monitor the alerts and find out how to improve the system stability, performance or security.

- Check the ratings for those systems for which an SAP EarlyWatch Alert service is active.
- Check the SAP EarlyWatch Alert report for a system and the ratings of its topic or subtopic.
- In a topic or subtopic, view detailed information.
- Use favorites to keep track of the systems you want to monitor frequently, or of the topics and subtopics you visit often.
- Customize your views through a variety of sorting, grouping and filter criteria, e.g. the rating or the reports' generation date.
SAP Support Portal
My SAP EarlyWatch Alert Reports

My SAP EarlyWatch Alert Reports (1)

<table>
<thead>
<tr>
<th>Favorite</th>
<th>System ID</th>
<th>Rating</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PR9</td>
<td>Very Critical</td>
<td>03.04.2017</td>
</tr>
<tr>
<td></td>
<td>Installation Number: 1234567890</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Number:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SAP EarlyWatch Alert Report for PR9

Date: 03.04.2017
Language: English

<table>
<thead>
<tr>
<th>Favorite</th>
<th>Topic</th>
<th>Topic Rating</th>
<th>Subtopic</th>
<th>Subtopic Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Software Configuration</td>
<td>Very Critical</td>
<td>Support Package Maintenance - ABAP</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HANA Database Version</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SAP Kernel Release</td>
<td>Very Critical</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>Critical</td>
<td>SAP HANA Database</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ABAP Stack</td>
<td></td>
</tr>
</tbody>
</table>
Security
System ID: Date: 03.04.2017

ABAP Stack of PR9

Standard users have default password.

Default Passwords of Standard Users

Standard users have default passwords.

Recommendation:
Run report RSUSR003 to check the usage of default passwords by standard users.

Ensure that users SAP* (must exist in all clients), SAPCPIc, and EARLYWATCH have non-default passwords in all clients. For more information, see "Protecting Standard Users"; either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

Make sure that the standard password for user TMSADM has been changed in client 000, and delete this user in any other client. SAP Note 1414256 describes a support tool to change the password of user TMSADM in all systems of the transport domain. SAP Note 1552894 shows how to update the report RSUSR003 to show the status of user TMSADM.
EarlyWatch Alert Workspace in Support Portal Launchpad
https://launchpad.support.sap.com/#/ewaworkspace

SAP EarlyWatch Alert Workspace – gain an overview on your system landscape health

Note 2517661 - How to include EWA Fiori Cloud apps into customer launchpads
You can view the EWA Alerts in Support Portal Launchpad, i.e. you can search for “Security”

- **4 Systems** Gateway Security (Security ➡ ABAP Stack ➡ Gateway and Message Server Security )
  Gateway access control list (reg_info/sec_info) contains trivial entries (P TP=* USER=* USER-HOST=* HOST=*).

- **6 Systems** Default Passwords of Standard Users (Security ➡ ABAP Stack)
  Standard users including SAP* or DDIC have default password.

- **14 Systems** SAP HANA Network Settings for Internal Services (Security ➡ SAP HANA Database HPJ)
  SAP HANA internal network configuration is insecure.

- **2 Systems** SAP HANA Network Settings for System Replication Communication (listeninterface) (Security ➡ SAP HANA Database P22)
  SAP HANA network settings for system replication is insecure.

- **22 Systems** ABAP Password Policy (Security ➡ ABAP Stack)
  Secure password policy is not sufficiently enforced (login/min_password_lng and login/password_max_idle_initial).

- **6 Systems** Gateway Security (Gateway and Message Server Security )
  Gateway Access Control List (reg_info/sec_info) contains trivial entries (P TP=*).

- **22 Systems** Users with Critical Authorizations (Security ➡ ABAP Stack)
  A high number of users has critical authorizations.

- **15 Systems** Default Passwords of Standard Users (Security ➡ ABAP Stack)
  Standard users other than SAP* or DDIC have default password.

- **3 Systems** Protection of Passwords in Database Connections (Security ➡ ABAP Stack)
  Protection of passwords in database connections (note 1823566).

- **3 Systems** SAP HANA SSFS Master Encryption Key (Security ➡ SAP HANA Database)
  SAP HANA SSFS master encryption key is not changed (note 2183624).
EarlyWatch Alert Workspace and Solution Finder
Prerequisites

➢ SAP Solution Manager sends EWA data

or

➢ Monitored System sends EWA data directly

Note 207223 - SAP EarlyWatch Alert processed at SAP

➢ SAP ONE Support Launchpad:
   Authorization:  “Service Reports & Feedback” (English),
   “Zugriff auf Servicemeldungen” (German)

If you don't want to have HANA Checks in your EarlyWatch Alert of a HANA Database which is connected via DBCON, then create an entry in DBACOCKPIT with this connection and add in the description field NON_EWA_... Note 1985402.
Agenda

- Best Practices-based Services

Security Tools and Services
- EarlyWatch Alert (EWA) – Security Chapter
- Security Optimization Service (SOS)
- Configuration Validation

Security in Operations
- Dashboards & Alerts
- Integration with GRC Process Control
Value Proposition

The SAP Security Optimization Service is designed to verify and improve the security of the SAP systems of customers by identifying potential security issues and giving recommendations on how to improve the security of the system.

Keeping the security and availability of customer SAP solutions high is a tremendous value to customers' businesses - a value delivered by the SAP Security Optimization Service. Analysis is the key to this value, which is necessary to:

- Decrease the risk of a system intrusion
- Ensure the confidentiality of business data
- Ensure the authenticity of users
- Substantially reduce the risk of costly downtime due to wrong user interaction

More information can be found under the alias SOS in the SAP Service Market Place

- https://support.sap.com/sos
SAP Security Optimization Service – Overview

- The SAP Solution Manager offers the possibility to locally execute the SAP Security Optimization Service

SAP Security Optimization Self Service
- All completely automated checks in ABAP systems
- No additional costs for this service

SAP Security Optimization Remote Service
- Broad range of security checks extending the Self-Service checks
- Performed by experienced service engineers
- Part of CQC service offering

SAP Security Optimization Onsite Service
- Individual range of security checks, e.g. for the SAP Enterprise Portal
- Performed by specialists
- Additional costs for this service

Create Self-Service

Service | Session | Processing
---|---|---
SAP GoingLive Check | GoingLive Verification Session | Automated
SAP Technical Performance Optim | Technical Performance Optim |
SAP Technical Project Evaluation | Technical Project Evaluation Session |
SQL Statement Tuning | SQL Statement Tuning Session |
Security Optimization Service | Security Optimization Service Session |
Setup EWA for HANA Platform | Setup EWA for HANA Platform Session |
Scope of the Security Optimization Service for the SAP NetWeaver Application Server ABAP

- Basis administration check
- User management check
- Super users check
- Password check
- Spool and printer authorization check
- Background authorization check
- Batch input authorization check
- Transport control authorization check
- Role management authorization check
- Profile parameter check
- SAP GUI Single Sign-On (SSO) check
- Certificate Single Sign-On (SSO) check
- External authentication check

Types of checks in SOS NW AS ABAP

- Authorization checks: 116
- Non authorization checks: 110
  - Configuration checks: 66
  - Other security checks: 44
## Scope of the Security Optimization Service for SAP HANA

### Check Group Check

<table>
<thead>
<tr>
<th>Check Group</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maintenance of SAP Code</strong></td>
<td>Maintenance status of current HANA database revision</td>
</tr>
<tr>
<td><strong>Network and Communication</strong></td>
<td>SAP HANA network settings for internal communication between HANA services (“listeninterface”)</td>
</tr>
<tr>
<td></td>
<td>SAP HANA network settings for communication between replication sites (“listeninterface”)</td>
</tr>
<tr>
<td></td>
<td>TLS protection of JDBC / ODBC client connections</td>
</tr>
<tr>
<td><strong>Secure Data Persistence</strong></td>
<td>Change of Encryption Root Keys (as of SPS 12)</td>
</tr>
<tr>
<td></td>
<td>Change of SSFS Master Keys</td>
</tr>
<tr>
<td><strong>Auditing</strong></td>
<td>SAP HANA Auditing Status</td>
</tr>
<tr>
<td></td>
<td>Valid SAP HANA Audit Policies exist</td>
</tr>
<tr>
<td></td>
<td>Default audit trail is not set to System Log or Column Store table</td>
</tr>
<tr>
<td></td>
<td>Policy specific audit trails are not set to System Log or Column Store table</td>
</tr>
<tr>
<td><strong>Diagnosis Files</strong></td>
<td>Traces configured on debug level</td>
</tr>
<tr>
<td></td>
<td>SQL trace including results configured</td>
</tr>
<tr>
<td></td>
<td>Runtime dumps older than 42 days</td>
</tr>
</tbody>
</table>

### Check Group Check

<table>
<thead>
<tr>
<th>Check Group</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>Password Policy is weaker than SAP recommendation</td>
</tr>
<tr>
<td></td>
<td>No protection against trivial passwords (Password Blacklist)</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>User SYSTEM is activated</td>
</tr>
<tr>
<td></td>
<td>User SYSTEM has recently been used</td>
</tr>
<tr>
<td></td>
<td>Multiple invalid connection attempts for user SYSTEM</td>
</tr>
<tr>
<td></td>
<td>Several users with multiple invalid connection attempts</td>
</tr>
<tr>
<td></td>
<td>Users with disabled password lifetime</td>
</tr>
<tr>
<td></td>
<td>Users with last password change before system handover</td>
</tr>
<tr>
<td></td>
<td>No use of Restricted Users</td>
</tr>
<tr>
<td></td>
<td>Potentially obsolete users</td>
</tr>
<tr>
<td><strong>Authorizations</strong></td>
<td>Users with privileges that must not be assigned in productive systems</td>
</tr>
<tr>
<td></td>
<td>Critical privileges assigned to many users</td>
</tr>
<tr>
<td></td>
<td>Users with directly granted privileges</td>
</tr>
</tbody>
</table>

**Red** = Checks decisive for an overall red rating of the SOS report.
In order to determine the actual risk, the vulnerabilities are ranked using a rating logic. The rating is based on the severity and probability of each vulnerability. A report is created containing the identified vulnerabilities of the analyzed SAP system. The report contains recommendations to eliminate or reduce the vulnerabilities found during the Security Optimization Service.

The implementation of the recommended security measures can be done:
- By the customer
- By SAP security consulting
- By certified SAP partners
Questionnaire

The questionnaire is filled out by the customer to prepare the service.
The questionnaire contains about 25 questions.
Specification of known users with critical authorizations in the questionnaire skips them from the report.
This helps to keep the report readable and to do a correct risk analysis.
Customize the look of the report.
Selection of the tested clients.
Guided Self-Service for Security Optimization
Create new Session
Guided Self-Service for Security Optimization

Execute Session

Security Optimization Service

Session Number: 200000032204  User Name: BUCHHOLZF

1. Prepare
   1.1 Select System
   1.2 Select Logon to Managed System
   1.3 Assign Questionnaire
   1.4 Choose/Schedule Data Collection
   1.5 Generate Report

2. Analyze

3. Report

Help

In this step you will prepare your session.

It is divided in several substeps, in which you’ll find detailed description.

Choose always ‘Next’ to continue and to go through the session.

Below ‘Steps’ you’ll find an overview of the substeps with additional information like status, changed date and time,…

In the ‘Log’ section you’ll find useful information if an activity generates a log message.

Steps

<table>
<thead>
<tr>
<th>Status</th>
<th>Updates Needed</th>
<th>Description</th>
<th>Last Changed at</th>
<th>Last Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td></td>
<td>Select System</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td></td>
<td>Select Logon to Managed System</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td></td>
<td>Assign Questionnaire</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td></td>
<td>Choose/Schedule Data Collection</td>
<td>00.00.0000 00.00.00</td>
<td></td>
</tr>
</tbody>
</table>
Guided Self-Service for Security Optimization
Maintain Questionnaire

Security Optimization Service

Session Number 200000032204  User Name BUCHHOLZF

1  Prepare
   1.1  Select System
   1.2  Select Login to Managed System
   1.3  Assign Questionnaire
   1.4  Choose/Schedule Data Collection
   1.5  Customize Report Output
2  Analyze
3  Report

Help
Assign Questionnaire
Prerequisites
SAP GUI is required to be able to maintain the questionnaire.

Assign Questionnaire

Automatic Rating (Green)  Maintain Questionnaire  Save & Refresh Timestamps

Questionnaire Assignment

<table>
<thead>
<tr>
<th>Selected</th>
<th>Solution Name</th>
<th>System</th>
<th>Last Changed by</th>
<th>Change Da...</th>
<th>Change Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AM_Q_01 (plea...</td>
<td>SID = Q1P</td>
<td></td>
<td></td>
<td>00:00:00</td>
</tr>
<tr>
<td></td>
<td>AM_Q_01 (ple... System indepe...</td>
<td></td>
<td></td>
<td>00:00:00</td>
<td></td>
</tr>
</tbody>
</table>
Customer Report: Service Rating

The Security Optimization Self Service results in a report which contains all identified findings, enhanced with corresponding recommendations.

If very critical issues are found, then the overall SOS rating will be red. In this case, the chapter “Service Rating” will list those checks that triggered the overall red rating.

### 3 Service Rating

Severe critical security issues were found in your system. See the information in the following sections.

The following list provides an overview of the selected checks that are decisive for the severe critical ("RED") rating of this service.

**CHECKS DECISIVE FOR SEVERE CRITICAL ("RED") RATING**

<table>
<thead>
<tr>
<th>Check Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User SAP* has the default password in some clients (0041)</td>
<td></td>
</tr>
<tr>
<td>User DDIC has the default password in some clients (0048)</td>
<td></td>
</tr>
<tr>
<td>Security Audit Log is not active (0170)</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Length (0126)</td>
<td></td>
</tr>
<tr>
<td>Additional Super User Accounts Found (0022)</td>
<td></td>
</tr>
<tr>
<td>Users Authorized to Debug / Replace (0308)</td>
<td></td>
</tr>
<tr>
<td>Users Authorized to Maintain All Tables (0514)</td>
<td></td>
</tr>
<tr>
<td>Users Authorized to Execute All Function Modules (0520)</td>
<td></td>
</tr>
<tr>
<td>System Change Option (0301)</td>
<td></td>
</tr>
</tbody>
</table>
The action items list on top of the report gives a good overview about the complete system status. The action items are created automatically of all checks rated with high risk. The list can be individually adapted. We use the red traffic light as “high risk” and the yellow traffic light as “medium risk.” “Green” results are normally skipped in order to reduce the size of the report. All checks have a four-digit identifier which allows to find the detailed description in the report easily.
Customer Report: Example of an Authorization Check

Information in the checks:

Explanation of the vulnerability
Some “Unexpected” users having this authorization
The number of unexpected users
A recommendation how to handle this situation
All checked authorization objects

6.3.7 Users - Other Than the Spool Administrators - Are Authorized to Print on all Devices (0197)
Output of sensitive data can be sent accidentally to a wrong printer and could be accessed by an unauthorized employee.

<table>
<thead>
<tr>
<th>Client</th>
<th>User</th>
<th>Type</th>
<th>Last Name</th>
<th>First Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>AARONF</td>
<td>A</td>
<td>Aaron</td>
<td>Frank</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>ANTONOVI</td>
<td>A</td>
<td>Antonov</td>
<td>Igor</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>AUTUMW</td>
<td>A</td>
<td>Autum</td>
<td>Wallis</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BARCANI</td>
<td>A</td>
<td>Barcan</td>
<td>Ivory</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BLACKBEARD</td>
<td>A</td>
<td>Blackbeard</td>
<td>Christ</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BLUEBERRYA</td>
<td>A</td>
<td>Blueberry</td>
<td>Agneta</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BLUMBERGH</td>
<td>A</td>
<td>Blumberg</td>
<td>Harald</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>BRAUERM</td>
<td>A</td>
<td>Brauer</td>
<td>Michael</td>
<td>OFFICE</td>
</tr>
<tr>
<td>300</td>
<td>BUSHH</td>
<td>A</td>
<td>Bush</td>
<td></td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>FERRYG</td>
<td>A</td>
<td>Ferry</td>
<td>Greg</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>HENGSTNERJ</td>
<td>A</td>
<td>Hengstner</td>
<td>Joan</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>KINGD</td>
<td>A</td>
<td>King</td>
<td>David</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>KINGF</td>
<td>A</td>
<td>King</td>
<td>Frank</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>LANDISG</td>
<td>A</td>
<td>Landis</td>
<td>George</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>ROBERTA</td>
<td>A</td>
<td>Robert</td>
<td>Alexander</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>VOLKOVIC</td>
<td>A</td>
<td>Volkov</td>
<td>Chris</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>WINTERN</td>
<td>A</td>
<td>Winter</td>
<td>Natalsha</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>WINTERN</td>
<td>A</td>
<td>Winter</td>
<td>Natascha</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>XERTAMY</td>
<td>A</td>
<td>Xertam</td>
<td>Yanis</td>
<td></td>
</tr>
</tbody>
</table>

Count: 220

Evaluated result:
More than 20% of your users, of at least one client, can print on all devices.

Recommendation:
Use the Profile Generator (PFCG) to correct roles. Use the transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization info system (SUIM) to check the results. For this check examine the roles or profiles that include the authorization objects listed below.

Authorization object:
Object: S_SPO_DEV with SPODEVICE = *. 
Sample Questionnaire and Report
Deriving an Action Plan

Deriving an Action Plan is easy ... in theory.

The SOS report is designed to already contain everything you need for it:

- a general introduction
- the findings and explanations
- risk ratings
- recommendations
- technical background information

So just go ahead!

For each check in the SOS report:
- analyze the reason and validity of the finding
- maintain the questionnaire where appropriate
- take corrective action based on the recommendation
Deriving an Action Plan

... is not that easy when the report is huge

When the SOS report is huge

- working on it as described on the slide before takes a lot of time and resources
- ... and may even cause that nothing happens at all.

The goal of the SOS however is not to produce a nice report but to have impact and improve the security of the respective system!

Recommended solution:

- Identify „Top Issues“ – including those potentially listed in the “Service Rating” chapter – and solve them first!
- Identify „Systematic Issues“ (e.g. issues with the authorization concept) and trigger a solution
- Identify „Quick Wins“ and implement them
- Determine the remaining risk and
  - either address the next set of „Top Issues“
  - or get agreement, that the achieved level of security looks acceptable until the next scheduled run of the SOS
How to Identify „Top Issues“
Some Risk Management Basics

Consider external threats before internal threats

Consider intentional threats before unintentional threats

Consider the potential of a risk and go for higher risks first
How to Identify „Top Issues“
Candidate „Standard Users with Default Password“

- Candidate: „Standard Users with Default Passwords“
- Threat: Standard users with default passwords allow anyone, who is able to establish a network connection to your system, to anonymously enter it and execute code under potentially high authorizations.
- In the SOS report look for section „User Authorization“ – „Standard Users“. Check-ID 0041
- Action: Change the password. Use report RSUSR003 to show the critical users locally.
- Remark: Look for the other checks in this SOS section as well. They also contain valuable recommendations to protect your system from this threat!
How to Identify „Top Issues“
Candidate „Insufficient Password Policy“

- Candidate: „Insufficient Password Policy“
- Threat: Weak passwords may give unauthorized people access to potentially powerful accounts. This risks the confidentiality, integrity and availability of your data.
- In the SOS report look for section „Authentication“ – „Passwords“ Check-ID 0123
- Action: Carefully review the whole „Password“ section of the SOS. Decide on an appropriate password policy (if not already defined) and implement it with recommended settings as given suggested in the SOS report.
How to Identify „Top Issues“
Candidate „Users with authorization profile SAP_ALL“

- Candidate: „Users with authorization profile SAP_ALL“
- Threat: Users with SAP_ALL can completely compromise your system – intentionally or unintentionally. Moreover they can not only circumvent any authorization checks but any auditing as well.
- In the SOS report look for section „Special Focus Checks“ – „Additional Super User Accounts Found“ - Check-ID 0022
- Action: Avoid SAP_ALL as far as possible and try to restrict it to relevant emergency accounts which are only used in emergency situations under tight control. Add accepted SAP_ALL accounts to the questionnaire and closely monitor this section in future SOS runs.
How to Identify „Top Issues“
Candidate „Users authorized to start all reports“

- Candidate: „Users authorized to start all reports“
- Threat: These users can start all reports, potentially also bypassing certain S_TCODE checks.
- In the SOS report look for section „Change Management“ – „Data & Program Access“ Check-ID 0512
- Action: Limit users with this authorization to the unavoidable minimum
How to Identify „Top Issues“
Candidate „Users with full authorization for authorization object S_RFC“

 Candidate: „Users with full authorizations for authorization object S_RFC“
 Threat: These users can be used to call any RFC function from outside the system.
 In the SOS report look for section „Basis Authorization“ – „Incoming RFC“ Check-ID 0241
 Action: Replace authorizations for S_RFC with RFC_NAME = * with strongly restricted authorizations.
 Limit the RFC functions, for which a specific user (group) is authorized to the required set. Use the Workload Statistics, transaction ST03N, to identify required RFC functions.
How to Identify „Top Issues“
Candidate „Users authorized to debug / replace“

- Candidate: „Users authorized to debug / replace“
- Threat: These users can run all programs with debug / replace, e.g. replace an data value or bypass any authorization check.
- In the SOS report look for section „Change Management“ – „Change Control“ Check-ID 0308
- Action: Limit users with this authorization to the unavoidable minimum. Authorization for „Debug / Replace“ (authorization object S_DEVELOP with type DEBUG and activity 02=change) should only be assigned to emergency users in production systems.

<table>
<thead>
<tr>
<th>Client</th>
<th>User</th>
<th>Type</th>
<th>Last Name</th>
<th>First Name</th>
<th>Department</th>
<th>User Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>100441</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>Count 0001</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>100227</td>
<td>S</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>AC295-99</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to Identify „Top Issues“
Candidate „Users authorized to display all tables“

- Candidate: „Users authorized to display all tables“
- Threat: These users can view all tables, including technical information as well as any business or personal data
- In the SOS report look for section „Change Management“ – „Data & Program Access“
  Check-ID 0513
- Action: Limit users with this authorization (authorization object S_TABU_DIS with table group * and activity 03=display) to the unavoidable minimum. Use authorization object S_TABU_NAM to grant access to a short list of tables if required.
How to Identify „Top Issues“
Candidate „Users authorized to maintain all tables“

- Candidate: „Users authorized to change all tables“
- Threat: These users can change most tables, including technical information as well as any business or personal data
- In the SOS report look for section „Change Management“ – „Data & Program Access“
  Check-ID 0514
- Action: Limit users with this authorization (authorization object S_TABU_DIS with table group * and activity 02=change) to the unavoidable minimum. Use authorization object S_TABU_NAM to grant access to a short list of tables if required.
How to Identify „Top Issues“
Candidate „Users authorized to execute all function modules“

- **Candidate:** „**Users authorized to execute all function modules**“
- **Threat:** These users can execute any function modules, where several critical function modules do not contain any further authorization checks.
- **In the SOS report look for section „**Change Management“ – „**Data & Program Access“** Check-ID 0520
- **Action:** Limit users with this authorization (authorization object S_DEVELOP with type FUGR and activity 16=execute) to the unavoidable minimum
How to Identify „Top Issues“
Candidate „Security Audit Log Deactivated“

- Candidate: „Security Audit Log Deactivated“
- Threat: If the Security Audit Log is deactivated, security critical events are not recorded and are neither available for monitoring nor for the follow-up of any security incident.
- In the SOS report look for section „Authentication“ – „General Authentication“ Check-ID 0136
- Action: Switch on the Security Audit Log in all clients. The Security Audit Log is optimized for performance and space. So if logging is restricted to critical security violations only, activation of the Security Audit Log is possible on all systems including production systems.
How to Identify „Top Issues“
Candidate „System Change Option Not Appropriately Configured“

8.2.1 System Change Option Not Appropriately Configured in the Production System (0301)

Threats that arise with the possibility of development in production systems:
- Malfunction of system due to programs that have not been tested properly
- Unauthorized data access with modified or self-developed programs

**Evaluated Risk - High**

**Recommendation:**
Set the System Change Option to 'Not modifiable' in SE06.

- **Candidate:** „System Change Option Not Appropriately Configured“
- **Threat:** If the system is set to “modifiable”, then unintended or malicious changes may be possible which is especially critical for a production system. For production systems this even may endanger the auditability of the system or lead to critical audit findings.
- **In the SOS report look for section „Change Management“ – „Change Control“ Check-ID 0301**
- **Action:** Set the System Change Option to “not modifiable”
How to Identify „Top Issues“
Candidate „RFC destinations with login information“

- Candidate: „RFC destinations with login information“
- Threat: These RFC destinations allow access to remote systems with stored login information. Unauthorized usage will compromise the security of the remote system
- In the SOS report look for section „Basis Authorization“ – „Outgoing RFC“ Check-ID 0254
- Action: For each RFC connection with login information find a responsible persons, who knows about the need and purpose for this entry. Check the other entries whether they can be removed and remove all entries, that are not needed any longer. Use Report RSRFCCHK and Workload Statistics, transaction ST03N, to analyze RFC connectivity.
How to Identify „Top Issues“
Authorization checks with high numbers of users

- **Candidate:** Authorization checks with high numbers of users

- **Threat:** If a high number of users has a certain critical authorization, misuse of this authorization is more likely and the ability to audit usage or misuse is diminished.

- In the SOS report look for any authorization with a high „Count:“ in any of the clients. A high count means, there are many users with this authorization, that are not named in the questionnaire.

- **Action:** Limit users with the respective authorization to the unavoidable minimum
**Action Definition Template**

<table>
<thead>
<tr>
<th>Name / Identification of the Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Short summary of the issue</strong></td>
</tr>
<tr>
<td><strong>Required Actions</strong></td>
</tr>
<tr>
<td><strong>Who</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>tbd</strong></td>
</tr>
</tbody>
</table>

Use the standard procedure that works best in your environment for defining, assigning and tracking actions. This can be issues / top issues in the Solution Manager, some ticketing system or a manual process based on Word, PowerPoint, Outlook or something else.
Further Information and Contact

Contact address
SecurityCheck@sap.com

Public information
SAP Support Portal, using alias /sos
https://support.sap.com/sos

SAP Notes:
• Note 696478 - SAP Security Optimization: Preparation & Additional Info
• Note 863362 - Security Checks in the SAP EarlyWatch Alert
• Note 1484124 - Guided Security Optimization Self Service - Prerequisites

Related SAP education training opportunities
• http://www.sap.com/education
  Search for ADM960: Security in SAP system environments
Security Optimization Service: Expert Guided Implementation
“Training on the Job” at Its Best

Training, practical experience, remote consulting

Day 1

Empowering, Web session, 1-2 hours each morning
SAP expert explains step-by-step configuration using training materials

Day 2

Execution, 2-3 hours on the same day
Participants execute demonstrated steps within their own project, on their own SAP Solution Manager software

Day 3-5

Expertise on demand, during execution
Participants have direct access to an SAP expert who directly supports them remotely, if necessary, during the execution

More information on available EGI topics and booking information can be found here:
Agenda

➔ Best Practices-based Services

Security Tools and Services

➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

Security in Operations

➔ Dashboards & Alerts
➔ Integration with GRC Process Control
Change Diagnostics Capabilities

E2E Change Analysis

System

System

Extraction

SAP Solution Manager

Reporting

Configuration Items are stored in one repository within SAP Solution Manager

Configuration Validation

Compliance reporting on configuration items
Typical Questions

- Which database parameters were changed by the 24/7 support team last night?
- What was last month's content of the j2ee/cluster/instance.properties file?
- Is there one place where all changes in the system are listed?
- What are the configuration differences between server0 and server1?
- How many transports did we import last month?
- How many urgent corrections did we import last month?
- How many objects did we change last month?
- How many stabilization transports did we have after the last GoLive?

Challenges

For a large number of system in a complex SAP landscape we need to perform comparison of current configuration status against a defined target or standard configuration baselines with minimum effort and ASAP.
The Diagnostics Core
Diagnostic Infrastructure

The extraction of the data is scheduled as soon as a “Managed System Configuration” has been performed for a system.

1. E2E Change Analysis – Top-Down View on Changes

2. Change Reporting – Browse CCDB data

The Diagrams show the integration of various components:

- **Solution Manager**
  - BI Reporting
  - InfoCube: 0SMC_CA02
  - E2E Change Analysis II

- **Extractor Framework (EFWK)**
  - Hourly

- **Configuration and Change Database (CCDB)**

- **Managed System**
  - Non-ABAP based installations
    - Diagnostics Agents
  - ABAP based installations
    - Extractor Framework
    - once a day
    - Solution Tool Plugins (ST-A/PI)

- **Drilldown navigation**

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
What is a Config Store?

- The single configuration details are stored in containers of a defined type called **Configuration Store**

- There are different types of Configuration Stores depending on the structure of the data the Configuration Store contains

- The most important types are xml, txt, ini, properties (two column based container: parameter, value), table (more than two column based container: key1, key2,, value1 , value2 ,) and event (as table but event-based)
CCDB Administration – Overview

Transaction CCDB

CCDB Infrastructure
- Overview showing the relevant jobs and tasks status

CCDB Statistics
- Statistics provide an quick overview via categories about all Config Stores of all connect technical (managed) systems
Technical Systems provides

- E2E Alerting: Managed systems raises alert in case of an error
- Manual start of data collection
- Link to (EFWK) Administration
- Status Grouping
- Config Store list with status (error) categories per technical (managed) system
Configuration Validation
Architecture Overview

Solution Manager EHP1

Configuration Validation

Virtual InfoProvider
0SMD_VCA2

Function Module

Configuration and Change Database (CCDB)

DB Table

Copy

Configuration Validation Reporting

Interactive BI based Reporting

Manual maintenance of copied configuration data

Target System Maintenance

Existing system configurations

JAVA based installations

Diagnostics Agents

Extractor Framework (EFWK) Once a day

ABAP based installations

Solution Tool Plugins

Configuration Validation Reporting

Customer defined system configurations / baselines

Copy

Change Reporting

Existing system configurations

JAVA based installations

Diagnostics Agents

Extractor Framework (EFWK) Once a day

ABAP based installations

Solution Tool Plugins
# Content Deliverables – Configuration Items Overview

<table>
<thead>
<tr>
<th>Application</th>
<th>Software Release Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Support Package Stack</td>
</tr>
<tr>
<td></td>
<td>• Software Component Versions</td>
</tr>
<tr>
<td></td>
<td>• Implemented SAP Notes</td>
</tr>
<tr>
<td></td>
<td>• Imported ABAP Transports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kernel</th>
<th>Software Release Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Web AS ABAP Kernel Release</td>
</tr>
<tr>
<td></td>
<td>• Java VM version</td>
</tr>
<tr>
<td></td>
<td>• Web AS Java Release</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database</th>
<th>Parameter Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Database Release</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Parameter Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Operation System Release</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th>Parameter Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Standard Users</td>
</tr>
<tr>
<td></td>
<td>• Gateway Secinfo</td>
</tr>
<tr>
<td></td>
<td>• Gateway Reginfo</td>
</tr>
</tbody>
</table>

### Parameter Validation

- SAP Product specific settings
  - PI/ XI specific configuration
  - BI specific configuration
  - BIA specific configuration
- ABAP Instance Parameters
- Java VM parameters for J2EE
- Critical auth. profiles
- Critical authorizations
CCDB Content Overview of an ABAP system

Software Configuration
ABAP Instance Parameter
Database Configuration
Operating System Configuration
Business Warehouse Configuration
RFC Destinations Configuration
System Change Option Configuration
Security Configuration
Critical user authorizations
CCDB Content Overview of a J2EE system

ADOBE DOCUMENT SERVICES
ADS
BOOTSTRAP
DBPOOL
HTTP
ICM
IGS
J2EE
J2EE Engine
J2EE Software
J2EE Transports
JSTARTUP
JVM Parameters
KERNEL
LIBRARY
LOG
LV
OS
SDM
SECURITY
SERVICE
SLD
START Parameters

SAP J2EE ENGINE

J2EE ENGINE SERVERCORE
What is Configuration Validation?
The Idea behind Configuration Validation

A reporting to understand how homogeneous the configuration of systems is

**Reference System**

- Configuration Items
  - Software Packages
  - ABAP Notes
  - Kernel level
  - Transports
  - Parameters

**Compared Systems**

- System 1
  - Configuration Items
  - ABAP Notes
  - Software Packages
  - Transports
  - Parameters

- System N
  - Configuration Items
  - ABAP Notes
  - Software Packages
  - Transports
  - Parameters

**Typical questions are:**

- All systems on a certain OS level or DB level?
- Template configuration (SAP or DB parameter) applied on all systems?
- No kernel older than 6 month on all systems?
- Security policy settings applied? Security defaults in place?
- Have certain transports arrived in the systems?
Configuration Validation
Target System Maintenance
# Configuration Validation

## Drilldown Reporting

**Formatting**

Drilldown → Instance Name

### Reference System

Reference System: SMX 0020253565

### Comparison Systems

- B35 0020144209
- B70 0020213988
- C35 0020108503
- C60 0020182324
- C70 SAP-INTERN
- ESU 0120021077

### Config Store

- ASAP_INSTANCE_RAH1

### Configuration Item

- logon/log_to_user_block
- logon/log_in_password
- logon/log_to_user_sap_user

---

<table>
<thead>
<tr>
<th>System</th>
<th>Instance Name</th>
<th>Configuration Item</th>
<th>Config Item Value</th>
<th>Target Value</th>
<th>Last Check [UTC]</th>
<th>Compliant (1=yes, 0=no)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMX 0020253565</td>
<td>D00</td>
<td>logon/log_to_user_block</td>
<td>5</td>
<td>#</td>
<td>2010/09/20/03:01</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>6</td>
<td>#</td>
<td>2010/09/20/03:01</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>1</td>
<td>#</td>
<td>2010/09/20/03:01</td>
<td>1</td>
</tr>
<tr>
<td>B35 0020144209</td>
<td>DVEBMS500</td>
<td>logon/log_to_user_block</td>
<td>12</td>
<td>5</td>
<td>2010/03/22/06:08</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>3</td>
<td>6</td>
<td>2010/03/22/06:08</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2010/03/22/06:08</td>
<td>0</td>
</tr>
<tr>
<td>B70 0020213988</td>
<td>DVEBMS500</td>
<td>logon/log_to_user_block</td>
<td>5</td>
<td>5</td>
<td>2010/09/20/03:02</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>6</td>
<td>6</td>
<td>2010/09/20/03:02</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2010/09/20/03:02</td>
<td>1</td>
</tr>
<tr>
<td>C35 0020108503</td>
<td>DVEBMS500</td>
<td>logon/log_to_user_block</td>
<td>10</td>
<td>5</td>
<td>2003/10/19/08:05</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>6</td>
<td>6</td>
<td>2003/10/19/08:05</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2003/10/19/08:05</td>
<td>0</td>
</tr>
<tr>
<td>C60 0020182324</td>
<td>DVEBMS500</td>
<td>logon/log_to_user_block</td>
<td>5</td>
<td>5</td>
<td>2010/09/19/13:25</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>6</td>
<td>6</td>
<td>2010/09/19/13:25</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2010/09/19/13:25</td>
<td>0</td>
</tr>
<tr>
<td>C70 SAP-INTERN</td>
<td>DVEBMS501</td>
<td>logon/log_to_user_block</td>
<td>5</td>
<td>5</td>
<td>2010/09/19/13:29</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>6</td>
<td>6</td>
<td>2010/09/19/13:29</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2010/09/19/13:29</td>
<td>0</td>
</tr>
<tr>
<td>ESU 0120021077</td>
<td>D58</td>
<td>logon/log_to_user_block</td>
<td>12</td>
<td>5</td>
<td>2010/02/25/14:36</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_in_password</td>
<td>3</td>
<td>6</td>
<td>2010/02/25/14:36</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2010/02/25/14:36</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>logon/log_to_user_sap_user</td>
<td>0</td>
<td>1</td>
<td>2010/02/25/14:36</td>
<td>0</td>
</tr>
</tbody>
</table>

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Introducing operators offers a greater flexibility to define a fitting target system
Operators and Target Systems

All rules are transparent and no rules are hardcoded

Operators available for all types of Config Stores: property, table, text, and xml

Operators comprise the rule used for validation for a Config Item
The SAP Notes relevant for the source system can be restricted via:

- Data Range
- Note Group – for example only Security and Hotnews

SAP Notes can be inserted:

Option b) all notes based on System Recommendations
New option to paste note numbers into the selection screen of the reporting as of SolMan 7.1 SP 9 for the query showing results of System Recommendations.

1. Step: Activate the new option

2. Step: Paste the system names or the note numbers into the new popup
Critical User Authorizations: Config Stores in CCDB

- **AUTH_CHECK_USER**
  User authority check store

- **AUTH_PROFILE_USER**
  User profile check store

- **AUTH_TRANSACTION_USER**
  User transaction check store

**Example:** Store Content of AUTH_PROFILE_USER

<table>
<thead>
<tr>
<th>History</th>
<th>USER</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_ALL</td>
<td>ADSUSER</td>
<td>USER IS AUTHORISED</td>
</tr>
<tr>
<td></td>
<td>AGRAVALKA</td>
<td>USER IS AUTHORISED</td>
</tr>
<tr>
<td></td>
<td>ALEREMOTE</td>
<td>USER IS AUTHORISED</td>
</tr>
<tr>
<td></td>
<td>AMRAM</td>
<td>USER IS AUTHORISED</td>
</tr>
</tbody>
</table>
Critical User Authorizations: Customizing Store Content

CCDB Administration tool allows to customize those store contents

- Call transaction **CCDB** to start CCDB Administration tool
- Navigate to tab “**Technical Systems**”
- Select system and display stores relevant for user critical authorizations

- Navigate to tab “**Customizing**”
- Create new customizing variant and adjust it accordingly (by default only users with SAP_ALL role are tracked)
Critical User Authorizations: Analysis of user profiles

**AUTH_PROFILE_USER**: User profile check store in the Target System (reference) defines that no user is allowed to have SAP_ALL profile

**Validation Output**: The Users which have critical authorizations in the system SI7 (compared system)
Critical User Authorizations: Analysis of user authorizations

**AUTH_CHECK_USER**: User authorizations check store in the Target System (reference) defines that only certain admin users are allowed to have debug authorizations.

Validation Output: Users which have the critical debug authorizations in the system SD7 (compared system) can be easily found.
Critical User Authorizations: Analysis of user transactions

**AUTH_TRANSACTION_USER:** User transaction check store in the Target System (reference) defines that only admin users are allowed to have authorizations for the transaction SM59

![Comparison Store: SD7 / 18A0054 AUTH_TRANSACTION_USER](image)

**Validation Output:** The Users which are not allowed to have the authorizations for Configuration RFC in the system SD7 (compared system) can be easily found

![Configuration Items](image)
RFC Hopping: Overview

Risk of RFC Hopping with RFC Destinations
Privilege Escalation
User impersonation
Bypass Network Firewalls
Hop through the whole system landscape (e.g. jump to a central system like the SolMan)

Countermeasure
Identify critical RFC Destinations across systems
Identify RFC Destinations to critical systems
RFC Hopping: Store RFCDES_TYPE_3_CHECK

RFCDES_TYPE_3_CHECK: For each RFC Destinations it is checked if the user provided in this RFC Destination has critical authorizations and/or can be used for login.

Result of RFC Destination Analysis

- **CRITICAL_USER_PROFILE**: User provided exists in destination System and has critical authorizations
- **OK_USER_NOT_IN_PROFILE_STORE**: User provided exists in destination System but does not have critical authorizations
- **OK_NO_USER_OR_PW_IN_RFCDEST**: No user and/or no pw is stored in the destination

CV_USER_PROFILE_RESULT

- **CRITICAL_USER_PROFILE** – User provided exists in destination System and has critical authorizations
- **OK_USER_NOT_IN_PROFILE_STORE** - User provided exists in destination System but does not have critical authorizations
- **OK_NO_USER_OR_PW_IN_RFCDEST** - No user and/or no pw is stored in the destination
RFC Hopping: Target System to find all critical RFC Destinations

RFCDES_TYPE_3_CHECK: This Store has been reduced up to one record and defines the pattern to search all RFC Destinations with critical status.

![Image of RFC hopping diagram]

Field Values and Operators:

<table>
<thead>
<tr>
<th>Field Role</th>
<th>Field Name</th>
<th>Operator</th>
<th>Value Low</th>
<th>Value High</th>
<th>Comparison Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RFCDEST</td>
<td>Contains</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>LOGON_CLIENT</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>LOGON_USER</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>PASSWORD_STATUS</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>HOST_NAME</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>SYSTEM_IDENTIFIER</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>SYSTEM_NUMBER</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>TRUSTED_SYSTEM</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>CV_USER_PROFILE_RESULT</td>
<td>Not equal</td>
<td></td>
<td>CRITICAL_USER_PROFILE</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>CV_CONFIG_DEST_LONG_SID</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>CV_REMARK</td>
<td>Ignore</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
0TPL_0SMD_VCA2_NCOMPL_CI_REF: This report shows all the RFC Destinations with critical status. The critical user authorizations could be customized via the AUTH_PROFILE_USER Store (by default the users with the profile “SAP_ALL” is checked).

**Validation Details:** In the column “Comparison Value” you can find all the details on the critical RFC Destination. In our example for the RFC Destination “PMIB4X001” which is created in the system B4X the user “PIRWBUSER” and the password saved in the logon data. This user has the profile “SAP_ALL” assigned in the system B4X.
RFC Hopping: Find all RFC Destinations pointing to a critical System

RFCDES_TYPE_3_CHECK: This Store has been reduced up to one record and defines the pattern to search all RFC Destinations pointing to the System SI7.
0TPL_0SMD_VCA2_CITEMS_REF: This Report displays validation results for all RFC Destinations.

Filter: Select filter value “Yes” for column “Compliance” to display only the RFC Destinations pointing to the critical system.
The Security Template:

- Supports customer to have a head start when starting with configuration validation towards security. It contains suggestions for rules and values for a number of Config Stores and can be used to create a target system.

- It’s possible to add or remove Config Stores and to change rules and values.
The definition means that the entry HOST=* which is the default entry used in a system in case no message server ACL is defined is validated as NON compliant.

This definition is to validate all lines that use only parameters with the * as non compliant which would be the same result as the validation of EhP1, see SAP note 1234799.

In a SAP system only the really needed services for the SAP Internet Communication Framework (ICF) should be active.
The Password status should not be DEFAULT. The user SAP* must exist in all clients and its password must be changed. For the other users there is no need to be existent in all clients.

The definition covers parameters that are validated also by the security optimization services (SOS). The Regex for login/ticket_expiration_time means less than 12 hours would be compliant.
Target System Maintenance

Save versions of compliance rules

Rule Repository

It's possible to save versions of a compliance rule to track what has been changed over the time.

It supports to create a rule repository for reuse in other target systems.
Weighted Validation
Target System Maintenance - Maintain weight and description

Weight and Description
It possible (but not necessary) to set a Weight per config item (Very High, High, Medium, and Low). Additional a description for a item may be maintained. The description is also available in reporting.
Weighted Validation
Reporting Templates

Reference system and comparison systems

Operator validation | Consistency validation | Configuration reporting

Weighted validation

Choose a weighted report

<table>
<thead>
<tr>
<th>Weighted report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0TPL_0SMD_VCA2_SY_WDOC_NC_ITEM</td>
<td>Weighted Validation - Elements with Description and Weighting</td>
</tr>
<tr>
<td>0TPL_0SMD_VCA2_SYS_WEIGHTED</td>
<td>Weighted Validation - Cumulated Risk Factors per System</td>
</tr>
<tr>
<td>0TPL_0SMD_VCA2_SYS_WEIGHT_NC_N</td>
<td>Weighted Validation - Number of Elements per Weighting (Initial View: Non-Compli...</td>
</tr>
</tbody>
</table>
## Weighted Validation Reporting - items with weight and description

<table>
<thead>
<tr>
<th>System</th>
<th>Config/Store Name</th>
<th>Client</th>
<th>Instance</th>
<th>Config Item Value</th>
<th>Compliance</th>
<th>Description/Action</th>
<th>Weight</th>
<th>% of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIT 002070862</td>
<td>STANDARD_USERS</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
<tr>
<td>SIT 002070862</td>
<td>ABAP_INSTANCE_PA1</td>
<td>#</td>
<td>#</td>
<td>CLIENT:000_USER:SAPOPC; PASSWORD_STATUS:DEFAULT; EXISTS:XL; LOCKED;</td>
<td>No</td>
<td>Please change default password</td>
<td>Very high</td>
<td>1</td>
</tr>
</tbody>
</table>

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Weighted Validation
Number of elements per weight

Example
Distribution of non-compliant items per weights per technical system (Initial View: Non-Compliant)
**Weighted Validation**  
**Cumulated risk factors per System Validation**

**Factors**  
If weights are not enough, you can combine it with factors to get to an overall result.

If the cumulative weighting is greater than 1 then the system is rated red.

- **Very High Items**: $18 \times 1 = 18$
- **High Items**: $9 \times 0.1 = 0.9$
- **Medium Items**: $12 \times 0.05 = 0.6$
- **Sum**: $19.5$

$19.5 > 1 \rightarrow \text{Red}$

Factors can be customized.

### Weighted Configuration Validation - Non Compliance

<table>
<thead>
<tr>
<th>Configuration Items</th>
<th>Cumulative weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD7 0020270862</td>
<td>10.500</td>
</tr>
<tr>
<td>ABAP-PARAMETER</td>
<td>7.500</td>
</tr>
<tr>
<td>SECURITY</td>
<td>12.000</td>
</tr>
<tr>
<td>SD7 0020230702</td>
<td>15.500</td>
</tr>
<tr>
<td>ABAP-PARAMETER</td>
<td>7.500</td>
</tr>
<tr>
<td>SECURITY</td>
<td>12.000</td>
</tr>
<tr>
<td>SD7 0020270862</td>
<td>11.500</td>
</tr>
<tr>
<td>ABAP-PARAMETER</td>
<td>2.500</td>
</tr>
<tr>
<td>SECURITY</td>
<td>9.000</td>
</tr>
<tr>
<td>SW7 0020270862</td>
<td>0.850</td>
</tr>
<tr>
<td>ABAP-PARAMETER</td>
<td>1.000</td>
</tr>
</tbody>
</table>
Filtering notes provided by System Recommendation Reporting in SP10

Paste
Paste easily notes from the clipboard as filter for system recommendation output

System Recommendation Reporting for specific SAP Notes

Paste notes from clipboard
SolMan 7.2 SP 3: More ABAP Configuration Stores

Transactions
- LOCKED_TRANSACTIONS

Virus Scan Providers
- VSCAN_GROUP
- VSCAN_SERVER

ABAP Change Logs (*)
- GLOBAL_CHANGE_LOG
- COMPONENTS_CHANGE_LOG
- NAMESPACES_CHANGE_LOG
- AUTH_PROFILE
- USER_CHANGE_DOC
  (customizing possible, timestamps are extracted from the managed system log)

SAPUI5
- SAPUI5_LIBS
- SAPUI5_VERSION

System Timezone
- SYSTEM_TIMEZONE

*including integration into system monitoring and alerting
The Diagnostic Agent can now read user and role data from the J2EE engine using SPML

Configuration stores:
- sapGroupAllAssignedUsers:<group>
- sapRoleAllAssignedUsers:<role>
- sapRoleAssignedActions:<action>
- sapUserProperties:<user>

Documentation how to setup SPML based extractors for CCDB: Configuration Validation Wiki

Caution: You may need to repeat the configuration after a Support Package upgrade of the SAP Solution Manager
SolMan 7.2 SP 3: UI related features

Reporting directory
includes Bookmark now

Comparison Lists
Badi Implementation to build dynamic comparison list base on the BAdI enhancement DIAGCV_ES1_SYSTEM_LIST
For more information see note 2365039

BI Reporting
Larger Strings in columns (up to 250 chars instead of 60 chars)
SolMan 7.2 SP 5: Send Configuration Validation reports via email

BW Information Broadcasting is not longer supported in SAP BW 7.40 (Note 2020590)

Conclusion: You cannot schedule broadcast notifications for the System Recommendations BW report in SAP Solution Manager 7.2 anymore

New reports to send Configuration Validation results via email:

Configuration Validation
DIAGCV_SEND_CONFIG_VALIDATION

System Recommendation Report
DIAGCV_SEND_SYSREC
SolMan 7.2 SP 5: Merge Target Systems

Report to merge several target systems into a new one:
DIAGCV_MERGE_TARGET_SYSTEMS

Usage:
Create several small target systems representing individual KPIs.
Use these target systems e.g. to create a Dashboard.
Merge these target systems into one for reporting.
Example: Merge the SAP Security Baseline target systems into one combined target system
SolMan 7.2 SP 5: New key operator for table stores: regex

New key operator (regex) for table stores

Example: Configuration Store STANDARD_USERS:
The check rule for user TMSADM in other clients than client 000 should result in 'compliant' if…
a) The user does not exists or
b) PASSWORT STATUS=CHANGED and LOCKED=X
New interfaces to Dashboard Builder

Trend Analysis based on various queries:
Overview:
0SMD_CVA2_TR_SYSTEMS_DSH
Details:
0SMD_CVA2_TR_ITEMS_DSH
Last results:
0SMD_CVA2_TR_NC_ITEMS_LAST_DSH

Configuration Validation based on function
DIAGCPL_CV_DSH
New Configuration Store **ABAP_INSTANCE_PAHI_ENH**
allows to check if parameter icm/server_port_0 to 9 contains at least one entry about HTTPS

New Field **TRAIL_TYPE** in Configuration Store **AUDIT_POLICIES (HANA)**
with values **TABLE** | **SYSLOG** | **CSV**

<table>
<thead>
<tr>
<th>History</th>
<th>★ AUDIT_POLICY_NAME</th>
<th>★ AUDIT_POLICY_OID</th>
<th>★ EVENT_ACTION</th>
<th>TRAIL_TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>SAPDLM Audit - Change System Configuration</td>
<td>499099</td>
<td>SYSTEM CONFIGURATION CHANGE</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>5</td>
<td>SAPDLM Audit - Create or Drop Role</td>
<td>499101</td>
<td>CREATE ROLE</td>
<td>TABLE</td>
</tr>
<tr>
<td>5</td>
<td>SAPDLM Audit - Execution of Procedure 001_dlm_start_procedure</td>
<td>2283841</td>
<td>EXECUTE</td>
<td>TABLE</td>
</tr>
</tbody>
</table>

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
New Configuration Store (ABAP): Count of users per security policy
SECURITY_POLICY_USAGE

<table>
<thead>
<tr>
<th>History</th>
<th>SECURITY_POLICY</th>
<th>USER_COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td></td>
<td>2002</td>
</tr>
<tr>
<td>EMERGENCY</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>DDIC</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

New Field RFCTCDCHK for Configuration Store RFCSYSACL
Use this field to check if the transaction flag is active for Trusted RFC definitions.
See note [2413716 - Setup of Trusted RFC in GRC Access Control EAM](#)
SolMan 7.2 SP 5: New Configuration Stores for HANA XSA

The new Store Group XSA_STOREGROUP contains several Configuration Stores about the HANA XSA application configuration.

<table>
<thead>
<tr>
<th>Store Path</th>
<th>Store Name</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>audilog-broker</td>
<td>brokeruser</td>
<td>XSA_STOREGROUP</td>
</tr>
<tr>
<td></td>
<td>serviceurl</td>
<td>XSA_STOREGROUP</td>
</tr>
<tr>
<td>audilog-cdata</td>
<td>DEPLOY_ATTRIBUTES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_METADATA</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_MODULE_METADATA</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_MODULE_PROVIDED_DEPENDENCIES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_SERVICES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>TARGET_RUNTIME</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td>audilog-ui</td>
<td>DEPLOY_ATTRIBUTES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_METADATA</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_MODULE_METADATA</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_MODULE_PROVIDED_DEPENDENCIES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_SERVICES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>destinations</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td>component-registry-db</td>
<td>DEPLOY_ATTRIBUTES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>DEPLOY_ID</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_METADATA</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_MODULE_METADATA</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_MODULE_PROVIDED_DEPENDENCIES</td>
<td>XSA.StoreGroup</td>
</tr>
<tr>
<td></td>
<td>MTA_SERVICES</td>
<td>XSA.StoreGroup</td>
</tr>
</tbody>
</table>
Navigation within Validation to Trend Analysis (Items, Roles, and Query showing latest data)

Validation: Additional search indexes to improve performance for Configuration Stores with more than 4 key fields
SolMan 7.2 SP 7: Fiori based Reporting

The Fiori Launchpad tile “Configuration Validation Reporting” points to the new reporting app:
You select a Target System, a Comparison List and optionally a selection for a Configuration store.

You get a System Overview page.

The diagram shows a pie chart indicating compliance with certain technical systems. The chart includes a table with the following columns:

- System ID (E73, EB1, FA7, FBT, FN8, FQ7, FT7, GM6, MW5, NS2)
- TechSystType (ABAP)
- Compliance (Yes, No, Item not found)

The percentages shown are 39.5%, 52.6%, and 7.9%.
SolMan 7.2 SP 7: Fiori based Reporting

Drilldown into system specific details:

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Item Key</th>
<th>Item Value</th>
<th>Item Key Rule</th>
<th>Item Value Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>login/no_automatic_user_sapstar</td>
<td>0</td>
<td>= login/no_automatic_user_sapstar</td>
<td>= 1</td>
</tr>
<tr>
<td>No</td>
<td>CLIENT = 000 USER = SAP*</td>
<td>PASSWORD_STATUS = CHANGED EXISTS = X LOCKED = VALIDTO = USERGROUP = SUPER</td>
<td>CLIENT Contains * USER = SAP*</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>CLIENT = 000 USER = DDIIC</td>
<td>PASSWORD_STATUS = CHANGED EXISTS = X LOCKED = VALIDTO = USERGROUP = SUPER</td>
<td>CLIENT Contains * USER = DDIIC</td>
<td></td>
</tr>
</tbody>
</table>

Reference System: BL_O-1; System ID: E73; Data retrieval: Oct 23, 2018, 8:03:01 PM - Oct 23, 2018, 8:03:04 PM
Further Information
Configuration Validation

Change Diagnostics @ Support Portal (Overview & Capabilities)

➢ Change Reporting
➢ Change Analysis / Product Instance
➢ Change Analysis / Systems
➢ Configuration Validation
➢ Configuration Validation / Reporting

Configuration Validation @ WIKI (Technical Details)
https://wiki.scn.sap.com/wiki/display/TechOps/ConfVal_Home
Configuration Validation: Expert Guided Implementation
“Training on the Job” at Its Best

Training, practical experience, remote consulting

Day 1

Empowering, Web session, 1-2 hours each morning
SAP expert explains step-by-step configuration using training materials

Execution, 2-3 hours on the same day
Participants execute demonstrated steps within their own project, on their own SAP Solution Manager software

Day 2

Day 3-5

More information on available EGI topics and booking information can be found here:

Empowerment on demand, during execution
Participants have direct access to an SAP expert who directly supports them remotely, if necessary, during the execution
Agenda

➔ Best Practices-based Services

Security Tools and Services
➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

Security in Operations
➔ Dashboards & Alerts
➔ Integration with GRC Process Control
Management Dashboard

**Designed for:** IT Managers

**Answers the question:**
“What is the current status of my IT department?”
“Are there currently any major issues in the IT department?”

**Scope:**
- Easy and effortless usage of SAP dashboard apps
- Clear-cut overview of score zones in customer-tailored focus

**Technology:**
Management Dashboard Framework in SAP Solution Manager based on SAP BusinessObjects Dashboards

**Time horizon:** Near real-time

[https://support.sap.com/dashboards](https://support.sap.com/dashboards)
Security in Operations – The Big Picture (1/2)

Status Overview
Management View

- Management Dashboards (Big screens on the wall)

Input / Work Items

- Inbox / Alerts (Workplace)
- Reporting & Drill Down (Workplace)

Tools for analysis and deeper insight

- Workflows for Follow-Up

  - Incident Management Guided Procedures (Immediate Resolution)
  - Change Management (Change Projects)

Legend:
- Screens on the wall
- Workplace
- Follow-up Workflows
Security in Operations – The Big Picture (2/2)

Management Dashboards
- Provide an overview on system landscape status
- For Security could also include the progress of get-clean projects
- Mainly used for quick status overview as required by management and operations

Incident Management
Guided Procedures (Immediate Resolution)

Change Management
(Change Projects)

Inbox of Work Items – used as trigger for action
- For Security may contain
  - Snapshot spot checks (identified issues at time of check)
  - Security critical events (independent of time of check)
Dashboard Tile

Via Launchpad Designer and “App Launcher static” a tile could be added to the Launchpad to start directly the configuration validation dashboard from there.
Dashboard Builder for Configuration Validation
Available as of SAP Solution Manager 7.2 SP 5

New interfaces to Dashboard Builder

Trend Analysis based on various queries:
Overview:
0SMD_CVA2_TR_SYSTEMS_DSH
Details:
0SMD_CVA2_TR_ITEMS_DSH
Last results:
0SMD_CVA2_TR_NC_ITEMS_LAST_DSH

Configuration Validation based on function
DIAGCPL.CV_DSH
Dashboard Builder for Configuration Validation
Available as of SAP Solution Manager 7.2 SP 5

Online Help: Dashboard Builder
https://help.sap.com/viewer/82f6dd44db4e4518aad4dfce00116fcf/7.2.09/en-US/d0c91556d22c0033e10000000a44538d.html

Blog: SAP Solution Manager 7.2 – Dashboard Builder

Blog: SAP Solution Manager 7.2 – Dashboard Builder configuration

KPI Catalog
https://go.support.sap.com/kpicatalog

SAP Security Baseline Template Version 1.9 (including ConfigVal Package version 1.9_CV-%)
Dashboard Builder for Configuration Validation
Example: Dashboard

So far, two examples are part of the SAP Security Baseline Template.

These examples are based on following Target Systems:

BL_S-1  Password Policy
BL_O-1  Standard Users

The numbers on the tiles show the count of non-compliant systems.
The overview page shows partly consolidated results per system. You observe that some systems show compliant and non-compliant results. This is because we check for multiple configuration items and some of them produce a compliant result, others a non-compliant result.
The details page shows the result per configuration item.
Dashboard Builder for Configuration Validation
Example: Definition of Dashboard

The Dashboard uses a Global Filter to select the system list.

The Global Filter is used by all KPIs of the Dashboard.
Dashboard Builder for Configuration Validation
Example: Definition of Dashboard KPIs

A dashboard tile shows the consolidated result of a KPI.
You can drill-down into an overview view and to one or more detail views.
You define all views independently with similar settings as described on next page.

Various visualization types are available:
The definition of a view shows:

- The data source **DIAGCPL.CV.DSH (= Configuration Validation)**
- The selected visible fields in the rows
- The filter for the Target System
- The filters for the Configuration Stores and the Configuration Items (necessary if the Target System contains more rules than the ones which should be used here)
Note 2562089 - Directory Traversal vulnerability in ABAP

ABAP correction: Configuration Store \texttt{ABAP\_NOTES} for note 2562089

Configuration: Configuration Store \texttt{ABAP\_INSTANCE\_PAHI} with check rule for profile parameter \texttt{abap/path\_normalization = ext}
To define the rule set for ABAP notes you just enter the note number into configuration store ABAP_NOTES, select the line, and use the function “Get validity information for the selected notes” to populate the rule set.

---

**Target System**: N2562089 / **Store Name**: ABAP_NOTES

<table>
<thead>
<tr>
<th>Field Role</th>
<th>Field Name</th>
<th>Operator</th>
<th>Value Low</th>
<th>Value High</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>VERSION</td>
<td>&gt;=</td>
<td>#</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>TEXT</td>
<td>Ignore</td>
<td>#</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>PRSTATUST</td>
<td>Ignore</td>
<td>#</td>
<td></td>
</tr>
</tbody>
</table>

Field Values and Operators

Get validity information for the selected notes
## Dashboard Builder for Configuration Validation
### Example Note 2562089 : Edit Target System

**Target System : N2562089 / Store Name : ABAP_NOTES**

<table>
<thead>
<tr>
<th>Sel.</th>
<th>NOTE</th>
<th>VERSION</th>
<th>TEXT</th>
<th>PRSTATUS</th>
<th>PRSTATUS</th>
<th>COMPONENT</th>
<th>RELEASE</th>
<th>EXTRELEA...</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>( = ) 0002562089</td>
<td>( &gt;= ) 0008</td>
<td>(Ignore) #</td>
<td>(Ignore) Com...</td>
<td>( = ) E</td>
<td>( = ) SAP_B...</td>
<td>( = ) 752</td>
<td>( &lt;= ) 0001</td>
</tr>
<tr>
<td>☐</td>
<td>( = ) 0002562089</td>
<td>( &gt;= ) 0008</td>
<td>(Ignore) #</td>
<td>(Ignore) Com...</td>
<td>( = ) E</td>
<td>( = ) SAP_B...</td>
<td>( = ) 740</td>
<td>( &lt;= ) 0019</td>
</tr>
<tr>
<td>☐</td>
<td>( = ) 0002562089</td>
<td>( &gt;= ) 0008</td>
<td>(Ignore) #</td>
<td>(Ignore) Com...</td>
<td>( = ) E</td>
<td>( = ) SAP_B...</td>
<td>( = ) 750</td>
<td>( &lt;= ) 0010</td>
</tr>
<tr>
<td>☐</td>
<td>( = ) 0002562089</td>
<td>( &gt;= ) 0008</td>
<td>(Ignore) #</td>
<td>(Ignore) Com...</td>
<td>( = ) E</td>
<td>( = ) SAP_B...</td>
<td>( = ) 751</td>
<td>( &lt;= ) 0005</td>
</tr>
</tbody>
</table>

**Target System : N2562089 / Store Name : ABAP_INSTANCE_PAHI**

<table>
<thead>
<tr>
<th>Sel.</th>
<th>Operator</th>
<th>Parameter</th>
<th>Operator</th>
<th>Value Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>=</td>
<td>abap/path_normalization</td>
<td>=</td>
<td>ext</td>
</tr>
</tbody>
</table>

**Result for configuration store**

**ABAP_NOTES**

Enter a rule for the profile parameter for configuration store

**ABAP_INSTANCE_PAHI**
### Dashboard Builder for Configuration Validation

#### Example Note 2562089: Reporting

<table>
<thead>
<tr>
<th>Configuration Items</th>
<th>SAP System ID</th>
<th>Config. Item Value</th>
<th>Value of Target System</th>
<th>Compliance</th>
<th>Last Check [UTC]</th>
<th>Compliant (1=Yes, -1=No, 0=Not valuated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAP_INSTANCE_PAHI</td>
<td>abap/path_normalization</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321101712</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T1E</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321101710</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T1P</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321101810</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T1Z</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180316141526</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T41</td>
<td>on</td>
<td>ext</td>
<td>No</td>
<td>20180321104908</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T42</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321104908</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T4N</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321104908</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>T6N</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321104908</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>TKS</td>
<td>#</td>
<td>ext</td>
<td>Item not found</td>
<td>20180321102306</td>
<td>-1</td>
</tr>
<tr>
<td>ABAP_NOTES</td>
<td>0002562089</td>
<td>T1E</td>
<td>Version 0008 Completely implemented</td>
<td>No</td>
<td>20180320191611</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T1P</td>
<td>#</td>
<td>Version 0008 Completely implemented</td>
<td>No</td>
<td>20180320191100</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T1Z</td>
<td>#</td>
<td>Version 0008 Completely implemented</td>
<td>No</td>
<td>20180320191053</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T41</td>
<td>#</td>
<td>Version 0008 Completely implemented</td>
<td>No</td>
<td>20180315190113</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>T42</td>
<td>#</td>
<td>Version 0008 Completely implemented</td>
<td>No</td>
<td>20180320191313</td>
<td>-1</td>
</tr>
<tr>
<td></td>
<td>TKS</td>
<td>Version 0008 Completely implemented</td>
<td>Version 0008 Completely implemented</td>
<td>Yes</td>
<td>20180321102307</td>
<td>1</td>
</tr>
</tbody>
</table>

**Standard reporting using Configuration Validation with adjusted layout**

You can store the view as a “bookmark” for repeated reporting
Dashboard Builder for Configuration Validation
Example Note 2562089: Definition of corresponding Dashboard Tile

<table>
<thead>
<tr>
<th>KPI Type</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Name</td>
<td>Note 2562089</td>
</tr>
<tr>
<td>Subhead</td>
<td>Directory Traversal vulnerability in...</td>
</tr>
<tr>
<td>Description</td>
<td>ABAP Note + Configuration</td>
</tr>
<tr>
<td>Visualization</td>
<td>Number-based</td>
</tr>
<tr>
<td>Size</td>
<td>1 X 1</td>
</tr>
<tr>
<td>Unit</td>
<td>Systems</td>
</tr>
<tr>
<td>Data Source Type</td>
<td>Function Module</td>
</tr>
<tr>
<td>* Data Source Name</td>
<td>DIAGCPL.CV.DSH</td>
</tr>
<tr>
<td>Detail Page Template</td>
<td>Drill-Down views</td>
</tr>
</tbody>
</table>

**Filters**

- **Key Figures**
  - ! All

- **Aggregate on System Level**
  - X

- **Reference SID**
  - N2562089

- **Required for technical reasons**
- **For the tile we want to consolidate results on system level**
- **Target System**

Function module which implements the integration with Configuration Validation
Dashboard Builder for Configuration Validation
Example Note 2562089: Dashboard Tile and Drilldown View

- Dashboard Templates
- Application Operations
- IT Service Management
- Change Management
- Project Management
- Not Assigned Dashboards
- Business Process Operations
- Cross Applications
- Test Suite

- Security Baseline

Security Baseline ABAP

Security Notes with Configuration
E2E Alerting

It’s possible to add a target system to E2E Alerting. Non-compliant items could then cause an alert within the alert inbox (System alert: configuration validation)
Consolidated Alert Overview – Short Introduction

The following information is shown in the Alert Inbox overview screen:

- Basic information, e.g.
  - Issue Area, category, relevant system, current status etc.
- History information, e.g.
  - How many alerts have been raised / Worst rating in the past / No. of status changes etc.
- Processing information, e.g.
  - Processor name, current status (automatic confirmation, manual notification, incident etc.)
Technical Monitoring - Alert Inbox
Personalized query for Security Configuration
Technical Monitoring - Alert Inbox
Drill-Down Reporting

Alert Inbox

Unexpected Assignment of SAP_ALL

Reporting / Drill-Down (e.g. via Configuration Validation)
Alerting based on SAP EarlyWatch Alert
SAP EarlyWatch Alert Integration into Operation

**You want to...**
- Get all system alerts in one place
- Get access to SAP assistance

**Why integrate EWA into operation?**
- Optimize system behavior
- Reduce manual effort due to consolidated overview of critical EWA findings
- Start mitigating measures directly out of the reported issue

Continuous system improvement by leveraging EWA results
EWA Results Now Available in Alert Inbox

Advantages

• EWA results are in one place, with customizable views
• No need to check EWA reports manually every week
• Recommendations and guidelines for alert resolution are in the same place
• Processing of alerts in inbox supported by integration with incident management, alert assignment etc.
Alert Details and Metrics

Opening a specific alert displays the individual details of the alert

Mark a line to see how to resolve the issue
The handling of alerts is supported by...

- Sending mail or SMS notifications
- Integration of Issue Management
- Assigning a person responsible to an alert
Use Case for EWA Security Alerts

Red Alert

Security Alert appears in Alert Inbox

Actions & Recommendations

Alert Details recommends actions to resolve the alert, e.g. to implement a SAP Note, to change the passwords etc.

Resolution

Follow the recommendation. Assign alerts to processor for follow up and issue resolution

Green Rating

Problem is solved. Next set of Alerts in Inbox is green
Technical Details

Prerequisites

- Solution Manager system and connected managed systems with activated EWA
- Alert Inbox for EarlyWatch Alert

Activation

- EWA integration into Alert Inbox is activated automatically. No manual configuration steps are required
- Currently, updates to the EWA Alert Inbox template are shipped via Support Packages. New template content has to be activated manually. In the future it is planned that new content will be imported and activated dynamically
Alerting based on Security Audit Log
Overview

Prerequisites

• The Security Audit Log is activated on managed system using transaction SM19 respective RSAU_CONFIG
• The “Security” monitor within the monitor set “SAP CCMS Monitor Template” is activated using transaction RZ20
• Security Monitor

Activation

• System Monitoring - How-to Guides
• Activate the corresponding alerts in the SAP Solution Manager
  System and Application Monitoring
  https://help.sap.com/viewer/82f6dd44db4e4518aad4dfce00116fcf/7.2.09/en-US/c55d7a53ece90a2ce10000000a44538d.html
Recommended Filter settings for the Security Audit Log


1. Filter: Activate everything which is critical for all users "*" in all clients "*".
You may deactivate the messages of class “User master record change (32)” because you get change documents for users in transaction SUIM anyway.
Consider to add messages AUO, AUZ, BU5, BU6, BU7, BU9, BUA, BUB, BUC, BUH, AUP, AUQ.
If you maintain logical file names using transaction FILE (see note 1497003) than add messages CUQ, CUR, CUS, CUT.

2. Filter: Activate everything for special user SAP* in all clients "*".
You cannot use a filter 'SAP*' because this would include the virtual user. However, you can use the special filter value 'SAP#*' instead.

3+4. Filter: Activate everything for other support and emergency users, e.g. 'SAPSUPPORT*' (SAP Support users) respective 'FF*' (FireFighter) in all clients "*".

5. Filter: Activate all events for the dialog activities 'logon' and 'transaction' for user 'DDIC' in all clients.
This user should not be used in dialog mode. It's only required for specific activities while applying support packages or while importing transports (however in this case you can use another background user as well).

6. Filter: Activate everything for client '066'.
This client is not used anymore and can be deleted
(see http://scn.sap.com/community/security/blog/2013/06/06/how-to-remove-unused-clients-including-client-001-and-066 ).

7. Filter: Activate RFC events (AUL, AUK, AU6, AU5) for a short time for selected users to identity RFC connection problems easily
(see http://scn.sap.com/community/security/blog/2010/12/05/how-to-get-rfc-call-traces-to-build-authorizations-for-srfc-for-free ).

8.-10. Filter: free for other project specific purpose
“Security” monitor within the monitor set “SAP CCMS Monitor Template”
Alerting based on Configuration Validation
Setup – Configuration Validation
Example: Target System for critical authorization profile SAP_ALL

- Create target system based on template 0SECN
- Delete all other configuration stores besides AUTH_PROFILE_USER
- Check the rule:
  - for profile SAP_ALL
  - and any user ‘*’
  - the authorization assignment is classified as “non compliant”
Notification Management maintains and notifies system users, business partners, and external users.

Notification Management

Simple example, use „My Notification Settings“ to add my user to global recipient pool.

In recipient lists, create SAP_ALL_NOTIFICATION list and add my user to it.
Prerequisites: perform steps 1 – 3 which are not system specific
Setup – Technical Monitoring
Step 4: Template Maintenance: Deriving a template and adding a target system

Metric Number of non-compliant items is non active. It is necessary to active it.

Create template for the SAP basis version your system is running on
1. Mark Template
2. Create Custom Template
3. New template appears
Setup – Technical Monitoring
Step 4: Add target System SAP_ALL to metric number of non-compliant items

Tab Metrics
click on Number of non-compliant items

1. In tab data collection add target system
2. in tab Metrics Check Active
3. Save button is at the top
Setup – Technical Monitoring
Step 5: Define Scope

Choose a system

Next
Setup – Technical Monitoring

Step 6: Setup Monitoring

1. Assign Template for Technical System
2. Apply and activate it
3. Configuration Managed Object is the next step
Configuration of Managed Object – Notification

Notification setting can be done here
Technical Monitoring – Alert Inbox
Personalized query for Security Configuration
Guided Procedures for regular Tasks

- You can create Guided Procedures for **regular tasks**
- Option to **link** Guided Procedures to alerts
- Accessible from **Technical Administration Work Center** via Guided Procedure Browser

![Guided Procedures](image)
Agenda

➔ Best Practices-based Services

Security Tools and Services
➔ EarlyWatch Alert (EWA) – Security Chapter
➔ Security Optimization Service (SOS)
➔ Configuration Validation

Security in Operations
➔ Dashboards & Alerts
➔ Integration with GRC Process Control

Diagram:
- EWA
- SOS
- Configuration Validation
- Dashboards & Alerts

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Entering: SAP Process Control

SAP Process Control core features:

➢ Documentation of regulations (external) and create, review and publish policies (internal)

➢ Documentation of critical processes subject to regulations and policies

➢ Documentation of the organizational units that are handling those processes

➢ Documents control activities that are required to ensure that the processes are executed properly

➢ Provides issue handling on exceptions with remediation plans to get back on the path

➢ Provides automated monitoring for exceptions to target values

➢ **Goal:** Keep a firm grip on critical processes by making them and their applicable regulations and policies transparent, provide controls that are checking on proper conduct, test controls for effectiveness
SAP GRC Solutions
Overall Picture

GRC for Industries
- Banking
- Utilities
- Mfg
- Oil & Gas
- CPG
- ...

GRC for LoBs
<table>
<thead>
<tr>
<th>IT</th>
<th>Supply Chain</th>
<th>Sales and Marketing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

SAP GRC solutions
- Dashboards & Visualization
- Interactive Analysis
- Analyze
- Exploration
- Reports

- Manage
  - Risk
  - Compliance
  - Audit
  - Policy
  - Access
  - Exception

Monitor
- Enterprise Applications
  - SAP
  - PeopleSoft
  - Oracle
  - Greenlight Technologies
  - Legacy Apps

- IT Infrastructure
  - CA
  - loglogic
  - Novell
  - SAP NetWeaver
  - Sensage
  - ArcSight

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Integrated Governance Risk & Compliance – Example

**SAP Process Control**

**Enterprise Risks**
- Accept
- Avoid
- Transfer
- Control
- Reduce

**Fraud**

**Responses**

**Compliance Management**
- Process
  - IT Operations
  - Security Mgmt
  - Patching
- Process Risks
  - Patch proc. not followed
  - Valid invoices not entered

**Access Risks**
- User can enter vendor & PO
- User can enter invoices & payments

**Regulations**
- Review of new SAP Security Notes
- Review of system configuration
- Standard users & passwords

**Controls**
- Policies
  - Update and roll out strengthened security policy

**Policies**

**Access Risk Management**

**Mitigate Access Violations**

**Monitor Access Status**
#1: Policy Lifecycle Management

Key process steps in Policy Management

- **Create and Document the Policy**
  - Centrally documented and defined in the policy library

- **Review & Approve the Policy**
  - Workflow support to review and approve policies
  - Determine the relevant recipients per policy and organization

- **Publish & Distribute the Policy**
  - Workflow support to distribute policies across the organization
  - Receive confirmation on acknowledgement of policies
  - Optional: adjust policies to local needs

- **Monitor Policy Effectiveness**
  - Monitor policy acknowledgement
  - Measure policy understanding using quizzes and surveys
  - Monitor the policy effectiveness through policy “quizzes” and controls

- **Report on Policies**
  - “Out-of-the-box” online reports on policy and policy status
## Key features of Automated Monitoring Framework (AMF)

<table>
<thead>
<tr>
<th>Business-User Configurable Rules</th>
<th>Interactively Configured Queries</th>
<th>Change Analysis</th>
</tr>
</thead>
</table>
| - Arithmetic calculations on query results: date differences, amount %  
- Nested logical expressions — ANDs and ORs  
- Built-in currency conversion (leverages basic currency support)  
- Grouping and aggregation | - Define queries in GRC product front-end, no changes to backend content or code  
- Search for relevant backend tables, pick fields and conditions, join related tables, and so on | - Monitors configurations and master data  
- Reconstructs past settings over monitored timeframe from Basis logs → assurance to catch even fleeting changes  
- Fall back on snapshots of monitored settings (if not using Basis change logging) |

### Example

- **Process Control (PC) 10.0**
  - ($\text{Today} – \text{DateDue}) > 5
  - (\text{CreditCheck} = \text{True} \text{ AND } \text{CreditLimit} \text{ NULL})
  - (\text{NewAmt} – \text{OldAmt})/\text{OldAmt} < 0.1

- **Example**
  - Find sales to one-time customers grouped by sales person where the total exceeds the limit
  - SD credit checks can be configured in many different ways which are regularly fine-tuned by SAP customers. AMF should raise a red flag only if the overall configuration varies from the list of acceptable settings.
### Key features of Automated Monitoring Framework (AMF), cont.

<table>
<thead>
<tr>
<th>Process Control (PC) 10.0</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Leverage ABAP Report Content</strong></td>
<td>Find qualified ABAP reports, discover their parameters, schedule them, and pass parameter values at run-time (no variants in backend)</td>
</tr>
<tr>
<td>- Search for available reports in backend systems</td>
<td></td>
</tr>
<tr>
<td>- Bind values such as date ranges and company codes to report parameters</td>
<td></td>
</tr>
<tr>
<td>- Configure the invocation completely within GRC applications — no changes to backend systems or use of variants</td>
<td></td>
</tr>
<tr>
<td><strong>Inbound Events</strong></td>
<td>CISCO SONA can detect inappropriate use of corporate networks, security breaches, and so on</td>
</tr>
<tr>
<td>- Some systems such as CISCO’s SONA, ArcSight (HP) log analysis systems and Oversight’s fraud detection software offer more specialized monitoring capabilities</td>
<td></td>
</tr>
<tr>
<td>- Such systems can communicate problems to PC as they are detected, and PC can evaluate them via the rule engine</td>
<td></td>
</tr>
<tr>
<td>- Issues can be created, routed, and remediation documented</td>
<td></td>
</tr>
<tr>
<td><strong>Access to Other Query Engines</strong></td>
<td>Oversight can detect fraud patterns in ERP transactions</td>
</tr>
<tr>
<td>- Web-services-based query interface and integration enable connectivity to any query engine</td>
<td></td>
</tr>
<tr>
<td>- Partner or customer might need to adapt the web services interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use defined web service interface to invoke suitable queries in non-SAP systems, e.g. Greenlight</td>
</tr>
</tbody>
</table>
### Other features of Automated Monitoring Framework (AMF)

#### Process Control (PC) 10.0

<table>
<thead>
<tr>
<th><strong>SAP NetWeaver PI</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
</table>
| • SAP NetWeaver PI is SAP’s preferred integration platform  
• Can be used to query databases using ODBC/JDBC  
• Can connect to any application, but typically requires programming — at least to enable connectivity (but not necessarily for every rule/data source) | Monitoring legacy or proprietary systems is sometimes necessary, especially for very industry-specific or niche software |

<table>
<thead>
<tr>
<th><strong>BW Query</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
</table>
| • SAP Business Warehouse is used by many customers to extract and analyze transaction information in many dimensions  
• Sometimes monitoring risks and compliance on the basis of BI analysis is the optimal strategy | SAP SCPM delivers a lot of analytical content to measure supply chain performance. BW Queries on this content can quickly find problem areas such as sole-sourced supplies, stock-out durations, etc. |

<table>
<thead>
<tr>
<th><strong>Access Control Enhancement</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
</table>
| • Access Control API enables PC business rule to pass full criteria for access risk reporting  
• API enables reporting access permission violations, not just segregation of duties violations  
• Drill-down from PC to AC from evaluation details to access risk | Any access risk analysis criteria that can be defined directly in AC is now also available in the data source and business rule definition in PC |
Monitoring: query-driven and event-driven

- Process Control can extract data via queries or by waiting for events, triggering requests
- A scheduler can regularly check for changes
Monitoring security with SAP Process Control: overall architecture

- Checking compliance with security policies directly, such as SAP Security Patch status or recommended security settings, is inefficient and highly complex.

- Direct connections to all backend systems would be required with a Plug-In Add-On needed as well.
Monitoring security with SAP Process Control: overall architecture
Monitoring security with SAP Process Control: overall architecture

1. Policy Management
2. Control Testing & Workflows
3. Automated Monitoring
4. SAP Solution Manager
5. System Recommendations
6. Configuration Validation

- SAP Query, BW Query
- Tables, InfoCubes
- SAP OSS
- SAP Query
- SAP Portal, Legacy, DB, LDAP, OS
- SAP Process Control
- SAP Query, BW Query
- SAP Solution Manager
- System Recommendations
- Configuration Validation

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
GRC Process Control in the Business Client

http://<server>:8002/nwbc
Data Source: BW query of Configuration Validation

Copy of existing query with fixed values for mandatory parameters

Info provider of Configuration Validation
Business Explorer – Query Designer
BExQueryDesignerStarter.exe
Business Explorer – Query Designer
Set fixed values for mandatory parameters in copied query
Business Rule triggered by non-compliant item
Thank You!

Contact information:

SAP Active Global Support – Security Services
securitycheck@sap.com
Appendix

Sample ABAP content of Configuration Validation
Examples of content areas:

- Software Configuration
- ABAP Instance Parameter
- Database Configuration
- Operating System Configuration
- Business Warehouse Configuration
- RFC Destinations Configuration
- System Change Option Configuration
- Security Configuration
- Critical user authorizations

Change Reporting:
Content grouped by 'Alias / Subalias'
Configuration Stores dealing with Software Configuration

- **SAP_KERNEL**
  SAP Kernel release and patch information

- **ABAP_COMPRELEASE**
  Software component release information

- **ABAP_COMP_SPLEVEL**
  Software component and support package information

- **ABAP_NOTES**
  Notes applied via SNOTE

- **ABAP_PACKAGES**
  Installed ABAP software packages

- **ABAP_SWITCH_FRAMEWORK**
  Active switches

- **ABAP_TRANSPORT**
  Transports created and/or imported

Available with ST 710 SP12:

- **LANDSCAPE**
  Contains a few landscape information (product and product version)

- **MESSAGE_SERVER_PORT**
  Contains message server specific port information

- **SPAM_VERSION**
  Contains SPAM-Release with version and patch number
Configuration Stores dealing with ABAP Instance Parameter

- **ABAP_INSTANCE_PAHI**
  Active parameter of an ABAP instance

- **ABAP_DEFAULT_PROFILE, ABAP_INSTANCE_PROFILE, ABAP_START_PROFILE**
  Profile files used by an ABAP instance

- **TRANSPORT_TOOL**
  Contains the custom transport settings (available 710 ST SP10).
Configuration Stores dealing with Database Configuration

- **DB_INFO**
  DBSL release information of an SAP Kernel

- **Database dependent Config Stores**
Configuration Stores dealing with Operating System Configuration

- **ENV_VARIABLES**
  Shell environment variables of user <SID>ADM

- **PHYSICAL_HOST**
  Relation physical host to virtual host

- **saposcol**
  CPU, memory, and operating system patch information
Configuration Stores dealing with Business Warehouse Configuration

- **ROIDOCPRMS**
  BW request transfer parameters

- **RSADMIN, RSADMINA, RSADMINC, RSADMIN**
  Common BW configuration

- **UPC_DARK, UPC_DARK2**
  Specific BW configuration
Configuration Stores dealing with RFC Destinations Configuration

- **RFCDES**
  All RFC destinations of a system; all attributes in one column

- **RFC_TYPE_[3,G,H,L,T]**
  RFC destinations per type, each attribute is a column

- **RFC_DES_TYPE_3_CHECK** (Security)
  Is a user with critical authorizations used in an RFC destination?
Configuration Stores dealing with System Change Configuration

- **CLIENTS**
  System change settings per client

- **COMPONENTS**
  System change settings per component

- **GLOBAL**
  System change settings global

- **NAMESPACE**
  System change settings per namespace
Configuration Stores dealing with Security Configuration

- **GW_REGINFO, GW_SECINFO, MS_SECINFO**
  Gateway and message server access control lists

- **STANDARD_USERS**
  ABAP standard user with password and lock status

- **PSE_CERT**
  Certifications with validity information

- **TWPSSOACL, RFCSYSACL, SNCSYSACL**
  Trusted-RFC, Trusted-SNC and Trusted-“Logon Tickets“ information

- **SICF_SERVICES**
  Active Web Services

- **SESSION_MANAGEMENT**
  Contains the new ABAP session management setting

Available with ST 710 SP12:

- **USER_PASSWD_HASH_USAGE**
  Distribution of password hashes of different types

- **TDDAT and TDDAT_TABLES**
  Tables and assigned authorization classes

- **AUDIT_CONFIGURATION**
  Contains the audit log file configuration
Configuration Stores dealing with Critical User Authorizations

Examples:

- **AUTH_COMB_CHECK_[USER|ROLE]**
  Users or roles with special authorization combinations

- **AUTH_PROFILE_USER**
  User profile check store

- **AUTH_TRANSECTION_USER**
  User transaction check store

Additional in 7.10 ST10:

- **AUTH_ROLE_USER**
  Role to user relationship

- **AUTH_USER_TYPES**
  User to user type relationship

Most of these stores are customizable to adapt their content to the business needs.
Examples - CCDB Content for a J2EE system

ADOBE DOCUMENT SERVICES
ADS
BOOTSTRAP
DBPOOL
HTTP
ICM
IGS
J2EE
J2EE Engine
J2EE Software
J2EE Transports
JSTARTUP
JVM Parameters
KERNEL
LIBRARY
LOG
LV
OS
SDM
SECURITY
SERVICE
SLD
START Parameters
Configuration stores dealing with J2EE software components

Alias J2EE Software

- **J2EE_COMP_SPLEVEL**
  J2EE software components containing: Component, release, extended release, and patch level

- **SAP_J2EEDeployedSCService**
  Deployed object per component
  The content of those config stores is retrieved from SLD.
  Starting with SLD Release >= 7.10 the default setting has been changed in a way that these data is no longer processed. However, it's possible to turn on the processing of these data in newer releases.
Configuration stores dealing with J2EE parameters

Alias J2EE

- **SAP_J2EEClusterNode**
  Exists per server or dispatcher node. It’s based on MBean query containing: VM parameters, system properties, and system infos (type XML).

- **version.txt**
  Specifies the version of the system. It’s written at start up time of instance (type text).

- **instance.properties.vmprop**
  Contains VM parameter (type property)
  → overlaps with config store `instance.properties` at Alias JVM Parameters
New Config Stores for Technical System of type J2EE

- **J2EE_PSE_CERT**
  Contains the current certificates of the J2EE instances

- **Profile**
  Start and default profile

- **CTC config stores**
  CTC template changes at instances level now available as config stores
Configuration stores dealing with J2EE UME settings

**Alias J2EE ENGINE**

- **com.sap.security.core.ume.service**
  - Contains UME Properties for the Security Policy
  - (Example uses element search for parameter: ume.logon.security_policy.auto_unlock_time)
Further Configuration Stores impacting J2EE security

Source CTC
- servlet_jsp
- http
- authschemes.xml.file
Config Stores for Technical Systems supplied via CTS+

Transports & Transport Tool config stores for
- SAP HANA
- Business Object
Configuration Stores for SAP HANA

On Database Level
Store Groups
- HDB_LEVEL
- HDB_PARAMETER

On Host Level
Store Groups
- HANA_HW_VALIDATION
- HANA_IMDB_NAMESERVER
- HANA_INI_FILES
- HANA_SAPPROFILE_CONF
New Configuration Stores for SAP HANA

On Database Level
Store Group HANA-SECURITY

- **AUDIT_POLICIES**
  Contains HANA authentication policies

- **PASSWORD_BLACKLIST**
  Contains password patterns which couldn’t be used
  (only works with SYSTEM auth)

- **PUBLIC_USERS**
  HANA DB users and attributes

- **SEGREGATION_NATIVE_OBJECTS**
  Contains objects if the Segregation of Duties (SoD) constraint
  concerning native objects is not met

- **SPECIAL_PRIVILIGES**
  User having special privileges like TRACE ADMIN, DATA ADMIN,
  IMPORT, DELETE, INSERT, UPDATE