Motivation – Typical Issues in today‘s SAP HANA systems

User SYSTEM is not de-activated or it is even in daily use for administration and support tasks

Sensitive data is written to diagnosis files directory and kept for months

Security audit log is not configured at all

Communication via insecure connections

Obsolete technical users and other users

Insecure network configuration that allows to access HANA internal communication from outside

Secure default configuration overwritten with modifications from earlier releases

Users allowed to read all data

Several users with various critical authorizations (development and/or administration privileges) in productive system

How to define, implement and monitor the security of your SAP HANA Platform?
Classification of Security Services

Overview

Comparison against SAP recommendations
- Security in EarlyWatch Alert (EWA)

Comparison against company’s security policy
- Management Dashboard

Detailed Services

Company Security Policy

Company’s SAP Security Baseline

Target System

Configuration Validation

Detail

Security Optimization Service (SOS)
- System Recommendations
- Security Notes in the SAP Support Portal

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Public
Classification of Security Services

Comparison against SAP recommendations

Security in EarlyWatch Alert (EWA)

Overview

EWA: Productive (10 Checks)

Detailed Services

SOS: Productive (27 checks)

Company Security Policy

SAP Security Baseline Template: (8 requirements)

Target System

Comparison against company’s security policy

Management Dashboard

Configuration Validation

Configuration Validation:
Stores available covering 20 SOS checks

NEW

HANA Security Checklist / Security Mini Check (28 Checks)

System Recommendations:
also checks Security Notes relevant for SAP HANA
Agenda

1. Security Optimization Service (SOS)
2. SAP EarlyWatch Alert (EWA) Report
3. SAP HANA Security Baseline Template and Configuration Validation
4. Monitoring and Alerting Infrastructure in SAP Solution Manager
5. System Recommendations
Security Optimization Service (SOS)

SOS remote service for SAP HANA currently based on 27 checks
Security Optimization Service (SOS) for SAP HANA

**Service Goal:**

*Keep the security of your SAP system at a high level by verifying critical security properties, identifying potential security issues and benefitting from recommendations on how to improve the security of your system.*

*Enable Customers to run SAP HANA in a secure manner no matter if HANA is used as a database of a traditional ABAP or JAVA system or as a platform for IoT or other innovative scenarios.*

*Source: [https://support.sap.com/sos](https://support.sap.com/sos)*

**Facts**

- Remote service delivered by an SAP Support Engineer.
- Up to 27 manual checks delivered through standard remote connection.
- Short Questionnaire to capture custom specific information.
- Primary focus: SAP HANA Database
- Expert checks available for non-standard scenarios.
- Approach is consistent with SOS for ABAP and JAVA

**How to order**

- Standard procedures for ordering an SAP Remote Service apply

**Scope**

- [Standard delivery – 1 Day]
  - Maintenance of SAP Code
  - Configuration Parameters
  - Encryption Master Keys
  - Auditing
  - Diagnosis Files
  - Users and Authorizations
- [Custom tailored expert delivery – 2 Days]
  - To be defined in scoping call
### Security Optimization Service (SOS)

**When to book?** Consider to book a Security Optimization Service for one or multiple SAP HANA Systems if at least one of the following statements is true for you!

<table>
<thead>
<tr>
<th>You are ...</th>
<th>You want to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• New to SAP HANA.</td>
<td>• Verify critical security properties.</td>
</tr>
<tr>
<td>• Deploying new HANA capabilities like Multi Tenancy, XS Advanced Engine,</td>
<td>• Identify potential security issues.</td>
</tr>
<tr>
<td>Smart Data Integration, Streaming, ...</td>
<td>• Learn about options to further improve the security of your system.</td>
</tr>
<tr>
<td>• Increasing the security level of your system due to new requirements</td>
<td>• Discuss customer-specific requirements directly with an SAP security expert</td>
</tr>
<tr>
<td>from business or compliance side.</td>
<td>• Analyze the security level of your SAP HANA as basis for a Security</td>
</tr>
<tr>
<td>• In the process of bringing your SAP HANA platform operation to a higher</td>
<td>Engagement with SAP or for your internal project</td>
</tr>
<tr>
<td>maturity level.</td>
<td></td>
</tr>
</tbody>
</table>
SOS Delivery Procedure

Standard booking and service preparation procedures apply.

Questionnaire
- System handover date
- Technical users
- Special users

Remote Analysis
- Usage scenarios
- Manual checks (27 checks)
- Rating of vulnerabilities
- Expert check on non-standard scenarios

Report & Wrap-up Call
- Service report
- Wrap-up call
- Results and recommendations
- Explanation
- Discussion of customer requirements and related capabilities in SAP HANA and SAP Solution Manager
<table>
<thead>
<tr>
<th><strong>Check Group</strong></th>
<th><strong>Check</strong></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></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>Secure Data Persistence</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>Auditing</strong></td>
<td>Traces configured on debug level</td>
</tr>
<tr>
<td><strong>Diagnosis Files</strong></td>
<td>SQL trace including results configured</td>
</tr>
<tr>
<td></td>
<td>Runtime dumps older than 42 days</td>
</tr>
<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>User SYSTEM is activated</strong></td>
<td></td>
</tr>
<tr>
<td><strong>User SYSTEM has recently been used</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Users</strong></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>Authorization</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.
### System User

**Activation Status and Validity of User SYSTEM**
- **User SYSTEM is currently active and valid.**
- **User SYSTEM is currently active but out of validity date.**

**Recent use of user SYSTEM**
- **Use within last 7 days**
- **Use within in last 8 to 30 days**

**Confidentiality of SYSTEM user password**
- **PASSWORD_CHANGE_TIME < Communicated Handover Date**

### Evaluated Risk – High

- **Active standard users are an easy target for hacking attacks due to being available in every system. Furthermore the user SYSTEM is like a super user with very powerful user authorizations that cannot be revoked.**

- **If the user SYSTEM is used, then user activity in the system can hardly be traced back to a unique identity.**

- **If the date of last password change is before system handover or if date of password change cannot be determined, the password of user SYSTEM might be known outside your organization. This could lead to unauthorized access.**
Critical Authorizations

**Users with critical privileges or with roles that must not be assigned in productive systems**
- Number of users having critical privileges
- List of users

<table>
<thead>
<tr>
<th>Rating</th>
<th>Authorization</th>
<th>Object Type</th>
<th>Number of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>DATA ADMIN</td>
<td>System Privilege</td>
<td>0</td>
</tr>
<tr>
<td>✓</td>
<td>DEBUG</td>
<td>System Privilege</td>
<td>0</td>
</tr>
<tr>
<td>✓</td>
<td>ATTACH DEBUGGER</td>
<td>System Privilege</td>
<td>0</td>
</tr>
<tr>
<td>✓</td>
<td>sap.hana.xs.debugger:Debugger</td>
<td>Application Privilege</td>
<td>0</td>
</tr>
<tr>
<td>✓</td>
<td>_SYS_BICP_ALL</td>
<td>Analytic Privilege</td>
<td>5</td>
</tr>
<tr>
<td>✓</td>
<td>SAP_INTERNAL_HANA_SUPPORT</td>
<td>Role</td>
<td>0</td>
</tr>
<tr>
<td>✓</td>
<td>DEVELOPMENT</td>
<td>System Privilege</td>
<td>2</td>
</tr>
</tbody>
</table>

**Evaluated Risk – High**
These authorizations allow users to access or change any data without further authority check or authorize users to execute activities that are only allowed to be used by SAP Development.

**Recommendation:**
Make sure that the authorizations listed above are not granted to users in a productive environment.
Review the users listed in the table below and revoke authorizations unless they are required for a documented, approved reason.

**Users with critical system privileges**
- Number of users having critical system privileges
- List of users

**Evaluated Risk – Medium**
Critical authorizations can enable users to perform actions that compromise the security of the system or its data. The more users are assigned the higher is the risk.

**Users with directly granted privileges**
- Number of Users
- List of users by number of directly granted privileges

**Evaluated Risk – Medium**
Privileges, that are granted directly to a user, can hardly be related to a specific role in the organization and the respective set of tasks. As result it is difficult to limit a user's authorizations according to the need-to-know principle.
Auditing on database level gets a must when there are end-users and project resources accessing HANA DB directly (e.g. web applications with XS (Classic) / XSA Engine)

SAP HANA Auditing Status
- Parameter `global_auditing_state` does not exist or is other than true

Valid SAP HANA Audit Policies exist
- No valid policy is active

Inappropriate Default Audit Trail Type
- Parameter `default_audit_trail_type` is CSVFILE rather than CSTABLE or SYSLOGPROTOCOL

Policies with inappropriate Audit trail type
- Rating when at least 1 policy with audit trail type CSVFILE is defined

**Evaluated Risk - High**
If auditing is disabled, then the execution of critical activities including unauthorized access or changes may stay undetected. Information that is required for the analysis of security incidents might be missing.

**Evaluated Risk – High**
If no valid Audit Policies are configured, then only changes to the audit configuration itself will be tracked. The execution of critical activities including unauthorized access or changes will not be audited and may stay undetected. Information that is required for the analysis of security incidents might be missing.

**Evaluated Risk – High / Medium**
With the use of CSVFILE, the Audit Trail can be accessed by users who are authorized to view diagnosis files. Unauthorized access and manipulations to the audit trail cannot be traced back to the user.
Details
Network Settings

Evaluated Risk - High
If parameters are set incorrectly, the SAP HANA service ports used for internal / system replication communication are exposed to a public network and can be used to attack the SAP HANA system.

Recommendation:
- Configure separate networks on infrastructure level
- Set the parameter “listeninterface” to recommended value (e.g. “.internal” for distributed system)
- Add parameters with appropriate mapping of IP address to hostname for all hosts of the SAP HANA system.
- Follow the detail instructions in SAP Note 2183363 and KBA 2222200.

SOS checks the parameter settings for internal communication and for system replication communication and validates the specified IP addresses.
Customers can use the Security Checklist provided as part of the SAP HANA documentation or Security MiniChecks provided with SAP Note 1969700 for analyzing the system on their own.
HANA Security in SAP EarlyWatch Alert

10 checks
Service Goal:

Provide automated weekly check on most critical security findings (including newly detected vulnerabilities) that should be fixed as soon as possible.

Provide an out-of-the-box means for assuring a secure configuration.

Facts

1. Implemented Checks

<table>
<thead>
<tr>
<th>SAP HANA-related checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SAP HANA System Privilege DATA ADMIN</td>
</tr>
<tr>
<td>• Users with DATA ADMIN privilege</td>
</tr>
<tr>
<td>• Roles with DATA ADMIN privilege</td>
</tr>
<tr>
<td>• SAP HANA password policy</td>
</tr>
<tr>
<td>• SAP HANA Audit Trail</td>
</tr>
<tr>
<td>• Auditing status</td>
</tr>
<tr>
<td>• Audit trail target</td>
</tr>
<tr>
<td>• Audit policies</td>
</tr>
<tr>
<td>• SAP HANA SQL Trace Level</td>
</tr>
<tr>
<td>• SAP HANA Network Settings for Internal Services</td>
</tr>
<tr>
<td>• SAP HANA SSFS Master Encryption Key</td>
</tr>
</tbody>
</table>

Source: SAP Note 863362

How to order

SAP EarlyWatch Alert is included in SAP Maintenance. Only its configuration in SAP Solution Manager is required.
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

- Standard users have default password
- Secure password policy is not sufficiently enforced
- A high number of users has critical authorizations
- Gateway Access Control List (reg_info/sec_info) contains trivial entries
- ...
EWA Summary

Perform the following Guided Self Services.

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

For more information about Guided Self Services, see [SAP Enterprise Support Academy](https://www.sap.com). Register for an Expert Guided Implementation Session for the Guided Self Service at [SAP Enterprise Support Academy - Learning Studio - Calendar](https://www.sap.com).

**CHECK OVERVIEW**

<table>
<thead>
<tr>
<th>Topic Rating</th>
<th>Topic</th>
<th>Subtopic Rating</th>
<th>Subtopic</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td>Security</td>
<td><img src="attachment" alt="Score" /></td>
<td><a href="https://www.sap.com">SAP HANA System Privilege DATA ADMIN</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td><img src="attachment" alt="Score" /></td>
<td><a href="https://www.sap.com">SAP HANA Password Policy</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td><img src="attachment" alt="Score" /></td>
<td><a href="https://www.sap.com">SAP HANA Audit Trail</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td><img src="attachment" alt="Score" /></td>
<td><a href="https://www.sap.com">SAP HANA SQL Trace Level</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td></td>
<td><a href="https://www.sap.com">System Recommendations (JAVA)</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td></td>
<td><a href="https://www.sap.com">SAP Security Notes: ABAP and Kernel Software Corrections</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td></td>
<td><a href="https://www.sap.com">System Recommendations (ABAP)</a></td>
</tr>
<tr>
<td><img src="attachment" alt="Score" /></td>
<td></td>
<td></td>
<td><a href="https://www.sap.com">Default Passwords of Standard Users</a></td>
</tr>
</tbody>
</table>
## 10 Security

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 und _SYS_REPO users.
EarlyWatch Alert – HANA Security Checks
DATA ADMIN Privilege (2/2)

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.
EarlyWatch Alert – HANA Security Checks
Password Policy – Critical Parameters

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>✓</td>
<td>maximum_unused_initial_password_lifetime</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>✓</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>Parameter</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_used_passwords</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>maximum_unused_productive_password_lifetime</td>
<td>365</td>
<td>365</td>
</tr>
<tr>
<td>minimum_password_lifetime</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>password_expire_warning_time</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>password_layout</td>
<td>A1a</td>
<td>A1a</td>
</tr>
<tr>
<td>password_lock_time</td>
<td>1440</td>
<td>1440</td>
</tr>
<tr>
<td>maximum_invalid_connect_attempts</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<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. |
EarlyWatch Alert – HANA Security Checks
SQL Trace Level

### 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>☢️</td>
<td>global.ini</td>
<td>SYSTEM</td>
<td>communication</td>
<td>listeninterface</td>
<td>.global</td>
</tr>
<tr>
<td>✔️</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.

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 and SAP HANA Administration Guide, Section 'Change the SSFS Master Key'.
SAP HANA in Security Baseline Template and Configuration Validation
Classification of Security Services

Comparison against SAP recommendations
Security in EarlyWatch Alert (EWA)

Overview

Company Security Policy

SAP Security Baseline Template: (8 requirements)

Target System

Comparaison against company’s security policy
Management Dashboard

Configuration Validation:
Stores available covering 20 SOS checks

Detailed Services

Security Optimization Service (SOS)
System Recommendations
Security Notes in the SAP Support Portal

Detail

© 2016 SAP SE or an SAP affiliate company. All rights reserved.
The SAP Security Baseline Template Package

“The SAP Security Baseline Template is a template document provided by SAP on how an organization specific SAP Security Baseline could be structured. It is prefilled with selected baseline relevant requirements and corresponding concrete values as recommended by SAP.” (see SAP Knowledge Base Article 2253549 – “The SAP Security Baseline Template”)

The SAP Security Baseline Template Package contains

- SAP Knowledge Base Article 2253549 – providing overview and introduction
- The SAP Security Baseline Template (October 2016: version 1.9)
- A package for customizing the Configuration Validation to verify baseline template requirements, which can technically be checked. (October 2016: version 1.9 CV-2)

It consists of

- Data files and transports to customize Configuration Validation
- Documentation on how to upload/transport these data files and transports
- Documentation on the customizing, target systems and reporting options of this package
# SAP Secure Operations Map

<table>
<thead>
<tr>
<th>Security Compliance</th>
<th>Security Governance</th>
<th>Audit</th>
<th>Cloud Security</th>
<th>Emergency Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Setup</td>
<td>Secure Configuration</td>
<td>Communication Security</td>
<td>Data Security</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td>Network Security</td>
<td>Operating System and Database Security</td>
<td>Frontend Security</td>
<td></td>
</tr>
</tbody>
</table>
The 16 Secure Operation Tracks cover the following topics:

**Security Governance:** Adopt security policies for your SAP landscape, create and implement an SAP Security Baseline

**Audit:** Ensure and verify the compliance of a company’s IT infrastructure and operation with internal and external guidelines

**Cloud Security:** Ensure secure operation in cloud and outsourcing scenarios

**Emergency Concept:** Prepare for and react to emergency situations

**Users and Authorizations:** Manage IT users and authorizations including special users like administrators

**Authentication and Single Sign-On:** Authenticate users properly – but only as often as really required

**Support Security:** Resolve software incidents in a secure manner

**Security Review and Monitoring:** Review and monitor the security of your SAP systems on a regular basis

**Secure Configuration:** Establish and maintain a secure configuration of standard and custom business applications

**Communication Security:** Utilize communication security measures available in your SAP software

**Data Security:** Secure critical data beyond pure authorization protection

**Security Maintenance of SAP Code:** Establish an effective process to maintain the security of SAP delivered code

**Custom Code Security:** Develop secure custom code and maintain the security of it

**Network Security:** Ensure a secure network environment covering SAP requirements

**Operating System and Database Security:** Cover SAP requirements towards the OS and DB level

**Frontend Security:** Establish proper security on the frontend including workstations and mobile devices
What is Configuration Validation?
The Idea behind Configuration Validation

**Goal:** 
A reporting on actual configurations against a pre-defined, custom-specific Reference System 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
    - ...

### Compliance with Reference System
- Software Packages
  - System 1: ✔️
  - System 2: ✔️
  - System N: ❌
- ABAP Notes
  - System 1: ✔️
  - System 2: ✔️
  - System N: ❌
- Transports
  - System 1: ✔️
  - System 2: ❌
  - System N: ❌

### 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?
## Content Deliverables – Configuration Items Overview

### Available Data Stores for SAP HANA
- HANA Revision
- HANA Parameter
- Audit Policies
- Users
- Special Privileges
- Critical Combinations of Privileges

### Table: Available Data Stores

<table>
<thead>
<tr>
<th>Store Name</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD8_LEVEL</td>
<td>HANA</td>
</tr>
<tr>
<td>HD8_PARAMETER</td>
<td>HANA</td>
</tr>
<tr>
<td>AUDIT_POLICIES</td>
<td>HANA-SECURITY</td>
</tr>
<tr>
<td>PUBLIC_USERS</td>
<td>HANA-SECURITY</td>
</tr>
<tr>
<td>SEREGATION_NATIVE_OBJECTS</td>
<td>HANA-SECURITY</td>
</tr>
<tr>
<td>SPECIAL_PRIVILEGES</td>
<td>HANA-SECURITY</td>
</tr>
</tbody>
</table>

### Diagram: Store Content

**History**

- SAPDLM Audt - Change System Configuration
- SAPDLM Audt - Create or Drop Role

**Element History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Mod_Type</th>
<th>AUDIT_POLICY_NAME</th>
<th>AUDIT_POLICY_OID</th>
<th>EVENT_ACTION</th>
<th>EVENT_STATUS</th>
<th>EVENT_LEVEL</th>
<th>IS_AUDIT_POLICY_ACTIVE</th>
<th>USER_NAME</th>
<th>EXCEPT_USER_NAME</th>
<th>OBJECT_TYPE</th>
<th>OBJECT_SCHEMA</th>
</tr>
</thead>
</table>
Big Picture: Reporting / Alerting / Management Dashboard

Configuration Validation Target Systems can be used in several areas

- Configuration Validation
- Management Dashboard
- Reporting
- System Monitoring / Alerting

Selected ConfigStores and Items - Only Non compliant Items with Value and Target Value
HANA Security in Monitoring and Alerting
HANA Security in Monitoring and Alerting

**Goal:**

*Provide automated notifications on security issues, non-compliant configuration or suspicious user activity / system behavior.*

**Facts**

1. **Infrastructure**
   - Matured infrastructure
   - Highly flexible
   - Easy extensibility

2. **Implemented Checks**
   - Currently very few security-related checks available.

3. **Custom Adoption**
   - Custom specific Alerts e.g. based on HANA system views or Configuration Validation
Available Checks

HANA Statistics Server Alerts related to Security
(for triggering Operations Team - also available in SAP Solution Manager)

<table>
<thead>
<tr>
<th>Alert</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>Secure store file system (SSFS) consistency</td>
<td>Determines if the secure storage file system (SSFS) is consistent regarding the database.</td>
</tr>
<tr>
<td>62</td>
<td>Expiration of database user passwords</td>
<td>Identifies database users whose password is due to expire in line with the configured password policy. If the password expires, the user will be locked. If the user in question is a technical user, this may impact application availability. It is recommended that you disable the password lifetime check of technical users so that their password never expires (ALTER USER &lt;username&gt; DISABLE PASSWORD LIFETIME).</td>
</tr>
<tr>
<td>63</td>
<td>Granting of SAP_INTERNAL_HANA_SUPPORT role</td>
<td>Determines if the internal support role (SAP_INTERNAL_HANA_SUPPORT) is currently granted to any database users.</td>
</tr>
<tr>
<td>64</td>
<td>Total memory usage of table-based audit log</td>
<td>Determines what percentage of the effective allocation limit is being consumed by the database table used for table-based audit logging.</td>
</tr>
</tbody>
</table>

Configuration Mini Checks related to HANA Security
(for ad-hoc analysis – e.g. via Solution Manager DBA Cockpit)

<table>
<thead>
<tr>
<th>Check ID</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1310</td>
<td>Secure store (SSFS) status</td>
</tr>
<tr>
<td>1330</td>
<td>Number of users with expiration date</td>
</tr>
<tr>
<td>1335</td>
<td>Number of SAP users with password expiration</td>
</tr>
<tr>
<td>1340</td>
<td>CATALOG READ privilege granted to current user</td>
</tr>
<tr>
<td>1360</td>
<td>Size of audit log table (GB)</td>
</tr>
</tbody>
</table>

Checks that would trigger an Alert in Security team (rather than in Operations) are with very few exceptions not available. Custom specific metrics, alerts, reports and Dashboards are possible.
Architecture – Data Sources and Flow

Solution Manager

- Alert Inbox
- Regular alert metric + statistics data collection
  - Metric store
  - RCA infocubes

HANA DB

- Hostagent
- Diagnostic agent
- Regular statistics data historization & alerting
  - Statistics historization (_SYS_STATISTICS_HOST_)
  - Online monitoring views (_SYS_M_)

HANA host

Web service
(high frequency availability metrics)

SQL
(5 min or lower frequency metrics, statistics data)

Typical implementation effort: 1 day per Custom Alert
System Recommendations
**System Recommendations**

**Goal:**

Support an effective Security Patch Management Process by automatically identifying the applicable SAP Security Notes and by providing further means for implementation and tracking.

You have to apply various types of notes and patches to keep your SAP systems up-to-date and secure.

### Security notes
Advice from SAP experts regarding important actions and patches to ensure the security of your systems: [https://support.sap.com/securitynotes](https://support.sap.com/securitynotes)

### Performance relevant notes
SAP notes containing information and corrections for performance improvement of SAP systems

### Java patches
A patch is a code correction for a specific version of an SAP product.

### Legal Change notes
Respond to requirements caused by changes in legal regulation

### HotNews
SAP customer notes with priority 1 (very high priority) to resolve or avoid problems that can cause the SAP system to shut down or lose data

### General SAP notes
[https://support.sap.com/notes](https://support.sap.com/notes)

---

**Facts (on HANA):**

- System Recommendations runs in Solution Manager
- Notes already covered by current revision are automatically filtered out
- No need to filter all applicable components (currently not just HAN*)
- Automatic detection of Revision number from landscape data
- Coding corrections usually require a revision update via HANA LM Tools
- Workarounds usually require a (manual) Parameter Change
- Notes can be manually **confirmed** or marked **not relevant**
Thank you

Contact information:
AGS Security Services
securitycheck@sap.com