This document shows the description of all checks which are executed by the SAP Security Optimization Service for a HANA system.

Author: SAP Security Services
Contact: securitycheck@sap.com
Date: 01.04.2020

This report contains confidential customer data and may be viewed only by SAP Support employees, authorized SAP partners, and customer employees. Do not distribute it to other parties.
1 SC_HANA - SECURITY CHECKS FOR THE SAP HANA DATABASE

1.1 SAP HANA DATABASE .................................................................................................................. 5
  1.1.1 Landscape Overview ................................................................................................................. 5
  1.1.2 Maintenance of SAP Code ....................................................................................................... 6
    1.1.2.1 Maintenance Status of current SAP HANA Database Revision (SY146) ......................... 6
    1.1.2.2 System Recommendations (HANA) (SY133) ..................................................................... 7
  1.1.3 Communication ......................................................................................................................... 8
    1.1.3.1 SAP HANA Network Settings for Internal Services (SY128) ............................................. 8
    1.1.3.2 SAP HANA Network Settings for System Replication Communication (listeninterface) (SY132) .................................................................................................................. 9
    1.1.3.3 TLS protection of JDBC / ODBC Client Connections is not configured (HA023) .............. 12
  1.1.4 Data Persistence ....................................................................................................................... 12
    1.1.4.1 Change of SSFS Master Keys (HA026) ............................................................................ 12
    1.1.4.2 Change of Encryption Root Keys (HA058) .................................................................... 13
  1.1.5 Auditing ................................................................................................................................... 14
    1.1.5.1 SAP HANA Auditing Status (HA028) .............................................................................. 14
    1.1.5.2 No valid SAP HANA Audit Policies exist (HA057) ............................................................ 14
    1.1.5.3 Inappropriate Default Audit Trail Type (HA029) ............................................................ 15
    1.1.5.4 Policies with inappropriate Audit trail type (HA030) ....................................................... 15
  1.1.6 Diagnosis Files ....................................................................................................................... 16
    1.1.6.1 Database Trace set to debug level (HA032) .................................................................... 16
    1.1.6.2 SQL trace including results configured (HA033) ............................................................. 17
    1.1.6.3 Dump files older than 42 days (HA034) ....................................................................... 18
  1.1.7 Authentication ......................................................................................................................... 19
    1.1.7.1 SAP HANA Password Policy (SY115) ........................................................................... 19
  1.1.8 Users ........................................................................................................................................ 20
    1.1.8.1 Activation Status and Validity of User SYSTEM (SY134) .................................................. 20
    1.1.8.2 User SYSTEM has recently been used (HA040) ............................................................. 20
    1.1.8.3 Confidentiality of SYSTEM user password (HA065) ..................................................... 21
    1.1.8.4 Several users with multiple invalid connect attempts (HA042) ....................................... 21
    1.1.8.5 Users with disabled password lifetime (HA043) ............................................................ 23
    1.1.8.6 Age of last password change of users with disabled password lifetime (HA044) ................. 24
    1.1.8.7 No use of Restricted Users (HA045) ........................................................................... 24
    1.1.8.8 Potentially obsolete users (HA046) ............................................................................. 25
  1.1.9 Authorizations ......................................................................................................................... 26
    1.1.9.1 Users with highly critical privileges or with roles that must not be assigned in productive systems (HA048) ........................................................................................................... 26
      1.1.9.1.1 Users with critical System Privilege DATA ADMIN (HA073) ........................................ 26
      1.1.9.1.2 Users with critical System Privilege DEVELOPMENT (HA079) ................................ 28
      1.1.9.1.3 Users with critical Analytical Privilege _SYS_BI_CP_ALL (HA077) ....................... 29
      1.1.9.1.4 List of users with critical Object Privilege DEBUG (HA074) ....................................... 30
      1.1.9.1.5 List of users with critical Object Privilege ATTACH DEBUGGER (HA075) .............. 31
      1.1.9.1.6 Users with critical Application Privilege sap.hana.xs.debugger::Debugger (HA076) .... 33
      1.1.9.1.7 List of users with critical Role SAP_INTERNAL_HANA_SUPPORT (HA078) ............ 34
      1.1.9.2 Users with critical Developer Privileges in the HANA Catalog (HA136) .......................... 35
        1.1.9.2.1 Users with critical System Privilege CREATE SCHEMA (HA113) ............................ 36
1.1.9.2.2 Users with critical System Privilege CREATE SCENARIO (HA112) .................................................. 36
1.1.9.2.3 Users with critical System Privilege SCENARIO ADMIN (HA119) .................................................. 36
1.1.9.2.4 Users with critical System Privilege CREATE R SCRIPT (HA111) .................................................. 36
1.1.9.2.5 Users with critical System Privilege CREATE STRUCTURED PRIVILEGE (HA114) ......................... 36
1.1.9.2.6 Users with critical System Privilege STRUCTURED PRIVILEGE ADMIN (HA120) ......................... 36
1.1.9.2.7 Users with critical System Privilege EXPORT (HA109) ................................................................. 36
1.1.9.2.8 Users with critical System Privilege IMPORT (HA110) ................................................................. 36
1.1.9.3 Users with critical System Privileges on Users (HA117) .................................................................. 36
  1.1.9.3.1 Users with critical System Privilege USER ADMIN (HA108) ......................................................... 37
  1.1.9.3.2 Users with critical System Privilege ROLE ADMIN (HA107) ......................................................... 38
1.1.9.4 Users with critical system privileges for System Administration (HA049) ........................................... 38
  1.1.9.4.1 Users with critical System Privilege ADAPTER ADMIN (HA140) ................................................. 41
  1.1.9.4.2 Users with critical System Privilege AGENT ADMIN (HA141) .................................................... 41
  1.1.9.4.3 Users with critical System Privilege AUDIT ADMIN (HA099) ..................................................... 41
  1.1.9.4.4 Users with critical System Privilege AUDIT OPERATOR (HA100) ................................................ 41
  1.1.9.4.5 Users with critical System Privilege BACKUP ADMIN (HA142) .................................................. 41
  1.1.9.4.6 Users with critical System Privilege BACKUP OPERATOR (HA143) ............................................ 41
  1.1.9.4.7 Users with critical System Privilege CERTIFICATE ADMIN (HA104) ......................................... 41
  1.1.9.4.8 Users with critical System Privilege CLIENT PARAMETER ADMIN (HA166) ............................. 41
  1.1.9.4.9 Users with critical System Privilege CREATE CLIENTSIDE ENCRYPTION KEYPAIR (HA167) .... 41
  1.1.9.4.10 Users with critical System Privilege CREATE REMOTE SOURCE (HA144) ............................. 41
  1.1.9.4.11 Users with critical System Privilege CREDENTIAL ADMIN (HA103) ........................................... 41
  1.1.9.4.12 Users with critical System Privilege DROP CLIENTSIDE ENCRYPTION KEYPAIR (HA168) .... 41
  1.1.9.4.13 Users with critical System Privilege ENCRYPTION ROOT KEY ADMIN (HA145) ....................... 41
  1.1.9.4.14 Users with critical System Privilege EXTENDED STORAGE ADMIN (HA146) ............................ 41
  1.1.9.4.15 Users with critical System Privilege INFILE ADMIN (HA118) .................................................... 41
  1.1.9.4.16 Users with critical System Privilege LDAP ADMIN (HA121) ...................................................... 41
  1.1.9.4.17 Users with critical System Privilege LICENSE ADMIN (HA147) .................................................. 41
  1.1.9.4.18 Users with critical System Privilege LOG ADMIN (HA148) ....................................................... 41
  1.1.9.4.19 Users with critical System Privilege MONITOR ADMIN (HA149) .............................................. 41
  1.1.9.4.20 Users with critical System Privilege OPTIMIZER ADMIN (HA150) ............................................. 41
  1.1.9.4.21 Users with critical System Privilege RESOURCE ADMIN (HA151) ............................................ 41
  1.1.9.4.22 Users with critical System Privilege SAVEPOINT ADMIN (HA152) ............................................ 41
  1.1.9.4.23 Users with critical System Privilege SERVICE ADMIN (HA153) ............................................... 41
  1.1.9.4.24 Users with critical System Privilege SESSION ADMIN (HA154) ................................................ 41
  1.1.9.4.25 Users with critical System Privilege SSL ADMIN (HA106) ......................................................... 41
  1.1.9.4.26 Users with critical System Privilege TABLE ADMIN (HA155) .................................................... 41
  1.1.9.4.27 Users with critical System Privilege TENANT ADMIN (HA169) ............................................... 41
  1.1.9.4.28 Users with critical System Privilege TRUST ADMIN (HA105) ................................................... 41
  1.1.9.4.29 Users with critical System Privilege VERSION ADMIN (HA156) ................................................. 41
  1.1.9.4.30 Users with critical System Privilege WORKLOAD ADMIN (HA157) ......................................... 41
  1.1.9.4.31 Users with critical System Privilege WORKLOAD ANALYZE ADMIN (HA170) ....................... 42
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.9.4.32</td>
<td>Users with critical System Privilege WORKLOAD CAPTURE ADMIN (HA171)</td>
<td>42</td>
</tr>
<tr>
<td>1.1.9.4.33</td>
<td>Users with critical System Privilege WORKLOAD REPLAY ADMIN (HA172)</td>
<td>42</td>
</tr>
<tr>
<td>1.1.9.5</td>
<td>Users with basic support user privileges (HA137)</td>
<td>42</td>
</tr>
<tr>
<td>1.1.9.5.1</td>
<td>Users with System Privilege CATALOG READ (HA101)</td>
<td>43</td>
</tr>
<tr>
<td>1.1.9.5.2</td>
<td>Users with System Privilege TRACE ADMIN (HA102)</td>
<td>44</td>
</tr>
<tr>
<td>1.1.9.5.3</td>
<td>Users with role PUBLIC (HA138)</td>
<td>45</td>
</tr>
<tr>
<td>1.1.9.6</td>
<td>Users with critical roles (HA062)</td>
<td>46</td>
</tr>
<tr>
<td>1.1.9.6.1</td>
<td>Users with critical role CONTENT_ADMIN (HA115)</td>
<td>46</td>
</tr>
<tr>
<td>1.1.9.6.2</td>
<td>Users with critical role MODELLING (HA116)</td>
<td>48</td>
</tr>
<tr>
<td>1.1.9.7</td>
<td>Users with directly granted privileges (HA050)</td>
<td>49</td>
</tr>
</tbody>
</table>
1 SC_HANA - Security Checks for the SAP HANA Database

1.1 SAP HANA Database

1.1.1 Landscape Overview

Purpose

Provide an overview of customer's SAP HANA system. Some checks are only applicable with specific system usage (for example, system replication), others differ based on the database topology (for example, single node versus distributed system).

Procedure

a) Copy this section from the latest EWA report
b) If an EWA report is not available, check information that is relevant for later checks manually with the following SQL statements:

- HANA Revision

```
SELECT VERSION
FROM SYS.M_DATABASE
```

- Is_Distributed_System Yes/No:

```
SELECT distinct host
FROM SYS.M_Services
```

Distributed System = Yes when number of hosts > 1

- Multi Tenant:

```
SELECT file_name, layer_name, section, key, value
FROM SYS.M_INIFILE_CONTENTS
WHERE file_name = 'global.ini'
  AND section = 'multidb'
  AND key = 'mode'
value = multidb indicates Multi Tenant = Yes (otherwise: value=singledb)
```

- Dynamic Tiering

```
SELECT HOST, PORT, SERVICE_NAME, PROCESS_ID, DETAIL, ACTIVE_STATUS, SQL_PORT, COORDINATOR_TYPE FROM SYS.M_SERVICES
```

Dynamic Tiering = Yes when ACTIVE_STATUS = ‘YES’ and SERVICE_NAME CS ‘ESSERVER’

- Enterprise Information Management (EIM)

```
SELECT HOST, PORT, SERVICE_NAME, PROCESS_ID, DETAIL, ACTIVE_STATUS, SQL_PORT, COORDINATOR_TYPE FROM SYS.M_SERVICES
```

EIM = Yes if ACTIVE_STATUS = ‘YES’ and SERVICE_NAME CS ‘DPSERVER’

- Streaming Server:

```
SELECT HOST, PORT, SERVICE_NAME, PROCESS_ID, DETAIL, ACTIVE_STATUS, SQL_PORT, COORDINATOR_TYPE FROM SYS.M_SERVICES
```

Streaming Server = YES if ACTIVE_STATUS = ‘YES’ and SERVICE_NAME CS ‘STREAMINGSERVER’

- Advanced Function Libraries:

```
SELECT * FROM "SYS"."LCM_SOFTWARE_COMPONENTS"
where component_name = 'HANA_AFL'
```

- System replication = Yes/No

Replication Status = active or error indicates System Replication = Yes
SELECT
    DISTINCT HOST,
    SECONDARY_HOST,
    SECONDARY_ACTIVE_STATUS
FROM SYS.M_SERVICE_REPLICATION
WHERE SECONDARY_ACTIVE_STATUS = 'YES'

- Smart Data Access:

SELECT 'Number of remote sources', count(*) FROM SYS.REMOTE_SOURCES

SDA = YES when count > 0

- XSA

Check manually whether customer is using XSA (XS Advanced) as this is currently not included in EWA, and add the corresponding record to table System Usage (marked red in the template)

Select count(*)
from M_SERVICES
where SERVICE_NAME='xscontroller'
and ACTIVE_STATUS='YES'

XSA = YES when count > 0.

If customer asks specifically for these usages, ask whether expert check is possible. In some cases we may be able to deliver additional checks or provide information in the Wrap-up Call. mailto:hendrik.mueller@sap.com with customer contact details and SO number

**Note:**

1. You can view the history of SP Upgrades (omit TOP 1 to get the complete history):

SELECT TOP 1 VERSION, INSTALL_TIME
FROM SYS.M_DATABASE_HISTORY
ORDER BY INSTALL_TIME DESC

2. Other sources of information. If an Early Watch Alert Report is not available, you compile information manually:

   - Revision Number and System Usage from Overview Screen
     - HANA Studio → Administration Console (double-click on system entry)
     - DBACOCKPIT → Current Status → Overview
   - Host name from
     - HANA Studio → Administration Console → Landscape Tab → Hosts
     - DBACOCKPIT → Configuration Hosts

The tables below provide an overview of your current SAP HANA database configuration.

### 1.1.2 Maintenance of SAP Code

#### 1.1.2.1 Maintenance Status of current SAP HANA Database Revision (SY146)

**Purpose**

To ensure the customer is able to implement fixes to critical security issues in reasonable time.

**Procedure**

Check HANA revision based on the landscape overview section of this report or use the following SQL:

SELECT COMPONENT_NAME, VERSION, VERSION_SP, SP_DESCRIPTION
FROM SYS.LCM_SOFTWARE_COMPONENTS
WHERE COMPONENT_NAME = 'HDB'

Alternatively you can use:

SELECT TOP 1 VERSION, INSTALL_TIME
FROM SYS.M_DATABASE_HISTORY
ORDER BY INSTALL_TIME DESC

- Version is like 1.00.120.0
  - In this case, 120 is the revision number.
  - The Support Package Stack (SPS) is 12
  - The major Release is 1.00
- In some cases the numbers that follow the 3-digit revision number are not 00. In such cases, these figures indicate an SAP HANA maintenance revision, for example, 102.03. In such cases, all 5 figures need to be
included in the report.

- The SPS can be determined from the revision number by taking the first 2 figures of the revision (for revision >= 100). In this case, HANA is SPS 12 (for SPS < 10 only the first figure is to be taken: for example, revision 84 is SPS 8)
- Update the table in the check.

For all Security Notes:
- Filter 'SAP Component' for 'HAN' and select all entries.
- Verify whether some of the newest Security Notes are relevant for the customer system. Inspect the validity information concerning the revision.

**Rating:**

- GREEN: The Support Package Level of your SAP HANA database will not run out of security maintenance within the next 6 months.
- YELLOW: The Support Package Level of the SAP HANA database will run out of security maintenance within the next 6 months.
- RED: The Support Package Level of the SAP HANA database has run out of security maintenance.

**Info:**

- SAP Note 2021789 - SAP HANA 1.0 Revision and Maintenance Strategy
- SAP Note 2378962 - SAP HANA 2.0 Revision and Maintenance Strategy

**RED:**

The Support Package Level of your SAP HANA database has run out of security maintenance. Due to the age of your SAP HANA revision you are likely already missing published and unpublished security fixes. Furthermore, if new vulnerabilities are detected that require a code correction from SAP, SAP does no longer analyze whether your current revision is affected. To ensure the security of your system, you will then need to upgrade to a new Support Package.

**YELLOW:**

The Support Package Level of your SAP HANA database will run out of security maintenance within the next 6 months. Due to the age of your SAP HANA revision your database software is likely already missing published and unpublished security fixes. Furthermore, if critical vulnerabilities are detected that require a code correction from SAP, SAP may soon no longer analyze whether your current revision is affected. To ensure the security of your system, you will then need to upgrade to a new Support Package.

The following table shows your current SAP HANA database revision.

**Recommendation:**

Implement a clear SAP HANA maintenance strategy ensuring that the HANA software is kept up to date. As a general recommendation, an upgrade to the latest HANA revision of an SAP HANA major release should be performed at least once per year.

For more information about the SAP HANA revision and maintenance strategy, see SAP Notes
- SAP Note 2021789 - SAP HANA 1.0 Revision and Maintenance Strategy
- SAP Note 2378962 - SAP HANA 2.0 Revision and Maintenance Strategy
- SAP Note 1948334 - SAP HANA Database Update Paths for Maintenance Revisions for possible update paths.

Note: As of SAP HANA 2.0 SPS 1, Multi Tenancy is mandatory. Systems running as SINGLEDB will be converted. Consequently, several manual security measures will be required in your system to protect the newly created SYSTEMDB.

For additional general information, refer to SAP Note
- SAP Note 2115815 - FAQ: SAP HANA Database Patches and Upgrades

**1.1.2.2 System Recommendations (HANA) (SY133)**

**Purpose**

To check whether the System Recommendations tool is being used. This is a mandatory prerequisite for setting up a strong security patch process.

For more information, refer to https://support.sap.com/sysrec .

**Procedure**

This check is analyzed and rated automatically. No further action is necessary.
Rating
The rating is set automatically.
GREEN: The System Recommendations tool is used and shows results that are up to 31 days old.
YELLOW:
- The System Recommendations tool is used but the results are older than 31 days.
- The System Recommendations tool is not used for this system.
- The System Recommendations tool is not used at all.

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 https://support.sap.com/sysrec.

1.1.3 Communication

1.1.3.1 SAP HANA Network Settings for Internal Services (SY128)

Purpose
Check the settings of the SAP HANA internal network configuration.

Procedure
The check is performed automatically.
Check internal procedure:
Get the parameters from global.ini for section [communication] parameter listeninterface and section [internal_hostname_configuration].
The parameters are rated one by one even if there are dependencies between the parameters for the rating of a parameter.
Sample rules:
- A host-specific setting is not recommended → YELLOW
- Value for key listeninterface = .local → GREEN; = .global or .all → RED; = .internal → GREEN; = <Netmask> → dependent on details; all other values → GREEN
- The key of internal_hostname_resolution is an IP. If it is identical to the net_publicname in the m_host_information, it is rated RED.
- If a RED system or global parameter is overruled on all hosts, it is reset to YELLOW.

Rating
If any parameter is rated RED, set a RED rating for the check.
If any parameter is rated YELLOW, but not RED, set a YELLOW rating for the check.
If all parameters are rated GREEN, set a GREEN rating for the check.

Note
IPv6 network masks as values for parameter listeninterface are not evaluated in detail and receive a GREEN rating.

RED: Evaluated Risk - High
With the current parameter settings, the SAP HANA service ports used for internal communication are exposed to a public network and can be used to attack the SAP HANA system.

Command Line: IF "YSAP-SINGLE_HOST" = NO
Recommendation:
Immediate action is required. Configure a separate network for internal communication and set the parameter 'listeninterface' to '.internal'. Ensure that additional parameters are set to reflect the correct mapping of IP address to host name for all hosts of the SAP HANA system.
Select the appropriate name / value pairs based on your documentation of your network topology.
Follow the detailed instructions in SAP Note 2183363 and KBA SAP Note 2222200.

Command Line: ELSEIF "YSAP-SINGLE_HOST" = YES
Recommendation:
Immediate action is required. Set the 'listeninterface' parameter to '.local' to force the SAP HANA internal communication to listen to the SAP HANA internal loopback interface only. Follow the detailed instructions in SAP Note 2183363 and KBA SAP Note 2222200.

**Command Line: ENDIF**

**YELLOW:**

No obvious unsecure settings were detected for the system internal network configuration. However, some settings are not recommended and should be adjusted.

**Recommendation:**

Follow the instructions in SAP Note 2183363.

### 1.1.3.2 SAP HANA Network Settings for System Replication Communication (listeninterface) (SY132)

The check is only applicable if the customer uses system replication.

**Purpose**

To check if SAP HANA internal communication between system replication sites is in a network that is separated from the public network. This helps protect against attacks from public networks.

**Procedure**

The check is performed automatically.

**Manual Procedure:**

1. In the Landscape Overview section, System Usage table, check the System Replication record: System Replication = No  Delete this check from the report
   System Replication = Yes  Perform this check

   Alternatively, you can check:

   a. In the DBA Cockpit or HANA Studio, the Overview Screen – General Information:
      If system replication is configured, there is a replication status entry.
   b. Execute the following SQL:

   ```sql
   SELECT
       host,
       replication_mode,
       replication_status
   FROM SYS.M_SERVICE_REPLICATION
   ```

   **Expected Result:**
   a) Empty table if NO system replication scenario is active.
   b) Table with list of hosts if system replication scenario is active.

2. Check use of dynamic tiering

   Refer to the System Usage table in the Landscape Overview section or run SQL:

   ```sql
   SELECT
       HOST,
       PORT,
       SERVICE_NAME,
       PROCESS_ID,
       DETAIL,
       ACTIVE_STATUS,
       SQL_PORT,
       COORDINATOR_TYPE
   FROM SYS.M_SERVICES
   where ACTIVE_STATUS = 'YES'
   and SERVICE_NAME like '%ESSERVER%'
   ```

   If dynamic tiering is active when this SQL returns a result.

3. Get Host Information:

   ```sql
   SELECT HOST, KEY, VALUE from "SYS"."M_HOST_INFORMATION"
   WHERE Key IN ('net_publicname', 'net_ip_addresses')
   ```

4. Analyze system replication hostname resolution parameters:
SELECT file_name, layer_name, section, key, value
FROM SYS.M_INIFILE_CONTENTS
WHERE file_name = 'global.ini'
    and section = 'system_replication_hostname_resolution'

4.1. Compare parameter in system_replication_hostname_resolution with hosts in M_SERVICE_REPLICATION.
4.1.1. If a host is missing in the listed parameters of section system_replication_hostname_resolution, then add a
line to the Output table and fill the value with the hostname as found in M_SYSTEM_REPLICATION. The Key field
must remain empty since the IP address cannot be determined automatically.
The entry is rated RED.
Add "4" in the "comment" column of the output table.
4.1.2. Entries that are consistent with M_SERVICE_REPLICATION are added to the output table and rated
GREEN.
4.1.3. Parameters that do not correspond to hosts of Site A or Site B of the SR scenario are rated INFO.
For hosts not at all listed in M_SERVICE_REPLICATION, add comment:
"5" [Host is not listed in M_SERVICE_REPLICATION.]
For hosts corresponding to site C, add comment "6" [Parameter not required for this host.]

4.2. Compare field net_publicname for each host mentioned in M_HOST_INFORMATION with the key of
parameters in system_replication_hostname_resolution.
4.2.1. If net_publicname does not include an IP address, then:
YELLOW rating
Add comment "9" [Entry requires manual analysis (net_publicname <> IP address).]
4.2.2 If values are equal:
RED rating
Add comment "7" [IP address = net_publicname [M_HOST_INFORMATION]]
4.2.3. GREEN rating if values are unequal

4.3. If net_publicname is not an IP address, then check net_ip_addresses for each host
(M_HOST_INFORMATION):
RED rating for each host that contains only one entry. Add comment "8" [Only 1 IP address found in
net_ip_addresses
(This indicates use of a public network for SR communication)]

5. Analyze system replication communication parameters:
SELECT file_name, layer_name, section, key, value
FROM SYS.M_INIFILE_CONTENTS
WHERE file_name = 'global.ini'
    and section = 'system_replication_communication'

5.1. Parameter 'listeninterface'
5.1.1. Value = .internal → GREEN rating
no further check is required here. Parameters allowed_sender and enable_ssl are rated GREEN.
5.1.2. value = .global
GREEN rating if 3-tier SR scenario or dynamic tiering, else RED.
If RED, then add comment "1" [Expected Value: .internal]
Parameter 'allowed_sender' is rated
GREEN if value is a comma-separated list of hostnames;
else: RED.
If RED, then add comment "2" [Comma-separated list of hostnames expected.]
Parameter 'enable_ssl' is rated
GREEN if value = 'on'
RED if value = empty (DEFAULT) or 'off'
YELLOW if other value detected
If RED or YELLOW, then enter comment "3". [TLS encrypted communication with value = 'on' expected when
listeninterface = .global]

6. Complete the update of the Output table, including rating and comments.
   - For each correct entry in the parameter table, provide a GREEN rating
   - For each missing or incorrect entry in the parameter table, provide a YELLOW or RED rating
   - For each surplus entry, provide an INFO rating
   - For each entry with an unclear result, provide a YELLOW rating

7. Remove comments that are not referenced in the Output table.
Result for various scenarios that are not GREEN:
7.1. In a two-tier scenario listeninterface = .global results in YELLOW rating and comment: Expected
Value: .internal
7.2. Both parameters, allowed_sender and enable_ssl are not OK:
both parameters are listed with **RED** rating
Comment allowed_sender: comma-separated list of hostnames expected.
Comment enable_ssl: TLS encrypted communication expected when listeninterface = .global

7.3. If a) or b) are OK, then both parameters are rated **GREEN** in the output table. Both parameters are in section system_replication_communication.

8. If host-specific parameter settings are identified, then add comment "10". If parameter is rated **GREEN** so far, then re-rate to **YELLOW**. If parameter is already rated **YELLOW** or **RED**, then no action is required.

**Rating:**

Rate the overall check according to the following rules:

**GREEN** RATING:
1. listeninterface = .internal + maintained_hostname_resolution + use of a dedicated SR network
2. listeninterface = .global + allowed_sender = [hostname list] or .global + enable_ssl = on (3-tier or DT)

**YELLOW** RATING:
1. listeninterface = .internal and use of a dedicated SR network could not be validated (e.g. net_publicname <> IP address)
2. listeninterface = .global + allowed_sender = [hostname list] or .global + enable_ssl = on in a 2-tier environment without DT
3. host-specific settings detected

**RED** RATING
All other cases.

**Note:** See HANA_Security_MinCheck ID 412S

**RED:** Evaluated Risk – High

With current parameter settings, the default (public) network route is used for system replication communication or the system replication communication is not strictly restricted to the hosts of your scenario. This can be used to attack your SAP HANA system.

**Recommendation:**

Immediate action is recommended. Implement one of the best practices outlined below:
Enable TLS encryption for system replication communication to ensure that all communication is limited to hosts having the same system PKI. As of SAP HANA 1.0 SPS 10, a system PKI is automatically set up as part of the installation. It is ready for use without further configuration:

1. Set parameter enable_ssl to value 'on'. The parameter is in file global.ini, section system_replication_communication.
2. Encrypt the Internal Communication of SAP HANA by changing parameter ssl to value 'system_pki'. This parameter is in file global.ini, section [communication].

Both parameters are not case sensitive and must be set on all sites of your replication scenario. After making the change, you must restart your SAP HANA system.

This is the simplest approach to secure system replication communication. It is recommended for all current SAP HANA revisions: SAP HANA 1.0 revision 122.15 (January 2018) or later and SAP HANA 2.0 revision 12.4 (February 2018) or 24 (March 2018) or 30 (April 2018) or any later revision of the respective Support Package).

If your system is already configured with separate networks for public, internal, and system replication communication, you can also choose an alternative approach. With such a network topology, you can ensure that hosts listen to system replication communication only on the dedicated ports of the separate network and reject incoming requests on other interfaces:
1. Set parameter listeninterface in section system_replication_communication to '.internal'.
2. In section system_replication_hostname_resolution of the global.ini file, add new parameters that define a correct mapping of IP address to hostname for each host of your SR scenario. Select the appropriate name / value pairs based on your documentation of your network topology. Entries for hosts of neighboring sites must be included as a minimum.

Note that some SAP HANA scenarios do not support the parameter setting listeninterface = .internal. If you choose this option, refer to the SAP HANA Security Guide on SAP Help Portal.

**YELLOW:** Evaluated Risk – Medium

Some settings were detected in your configuration of system replication communication that are not according to SAP Best Practices, for example:
1. Parameter listeninterface in file global.ini, section system_replication_communication is set to '.internal', but the use of a dedicated non-public network for system replication communication could not be validated automatically.

Please review the value for net_public name in SAP HANA system view M_HOST_INFORMATION.
2. Host-specific settings have been detected for some parameters. Best practice is to configure parameters in the SAP HANA SystemDB in layer SYSTEM (appears as layer DEFAULT when checked from an SAP HANA tenant).

**Recommendation:**

Review and adjust the YELLOW-rated parameter settings based on the comments provided above. For details, refer to the SAP HANA Security Guide.

### 1.1.3.3 TLS protection of JDBC / ODBC Client Connections is not configured (HA023)

**Purpose**

Check for TLS protection of JDBC / ODBC Connections. TLS encrypted communication ensures that sensitive information such as user name / password is not transmitted in plain text between client and server.

**Procedure**

1. Execute the following SQL statement:

   ```sql
   SELECT file_name, layer_name, section, key, value
   FROM SYS.M_INIFILE_CONTENTS
   WHERE file_name = 'global.ini'
   AND KEY = 'sslenforce'
   AND VALUE = 'true'
   ```

   **Rating**

   - GREEN rating if Value = 'true'.
   - YELLOW rating if no record is returned, or if VALUE ≠ 'true'.

   **YELLOW:**

   Integrity and privacy of communication from JDBC / ODBC clients to SAP HANA is not protected against man-in-the-middle attacks and fake servers gaining information from clients. An eavesdropper may be able to access or manipulate the data.

   Current parameter setting allows unencrypted communication from JDBC / ODBC clients to the SAP HANA System.

   **Recommendation:**

   Implement Transport Layer Security (TLS) protected client-to-server communication according to the SAP HANA Security Guide and enforce the use of secure communication by setting parameter sslenforce = true. For additional information, see the Secure Communication Between SAP HANA and JDBC/ODBC Clients chapter of the SAP HANA Security Guide.

### 1.1.4 Data Persistence

#### 1.1.4.1 Change of SSFS Master Keys (HA026)

**Purpose**

To check whether encryption keys used for protecting the integrity of persisted data have been changed so that they are not known outside the customer’s organization.

**Procedure**

1. Use the following SQL to check the change date of SSFS Encryption Keys.

   ```sql
   SELECT * FROM SYS.M_HOST_INFORMATION
   WHERE KEY IN ('ssfs_masterkey_changed', 'ssfs_masterkey_systempki_changed')
   ```

2. Check whether the keys have actually been changed and whether the change date is after the handover date communicated in the questionnaire.
3. If the system was installed by the customer, mark the “Date of system handover” as “not applicable”.

**Rating**

- YELLOW rating if at least one of the following criteria is met:
  1. At least one master key has not been changed at all.
  2. Last change of at least one master key was before the communicated handover date.
GREEN rating in all other cases.

Note
See HANA_Security_MiniCheck ID 410 S, 512S

YELLOW:
At least one master key has not been changed from its default or the change date of a master key is older than the communicated handover date of the system from your partner to your organization.

Evaluated Risk - Medium
SSFS master keys may be known outside your organization. Knowledge of the instance SSFS master key allows decryption of the generated encryption root keys and increases the risk of unauthorized individuals being able to read encrypted data.

Knowledge of the system PKI SSFS master key allows data that has been encrypted in the course of TLS protected internal communication to be read.

The change dates of SSFS master keys have been checked based on information from system view M_HOST_INFORMATION.

Recommendation:
Change the SSFS master keys of your system. Make sure that all prerequisites are met and that you follow strictly the detailed instructions documented in the SAP HANA Administration Guide, section: Managing Data Encryption in SAP HANA.

1.1.4.2 Change of Encryption Root Keys (HA058)

Purpose
To check whether measures have been performed to mitigate the risk that encryption root keys are known outside the customer organization.

Procedure
1. The check is only applicable to SAP HANA SPS 12 and higher. Otherwise delete the check from the report.
2. Use the following SQL to get information on Encryption Root Keys:

   SELECT * FROM SYS.ENCRYPTION_ROOT_KEYS

3. Update the table in the report with the obtained data (including handover date from questionnaire if available)

Rating
YELLOW rating if there is at least 1 encryption root key with create_timestamp older than the communicated handover date

GREEN rating in all other cases.

YELLOW:
At least one encryption root key does not comply with SAP recommendations.

Evaluated Risk - Medium
Encryption root keys are used to encrypt data at rest (that is data files, log files, backup files) as well as sensitive data such as passwords or other application-specific data. If encryption keys are known outside your organization, there is an increased risk of unauthorized people being able to read sensitive data.

Availability and creation date of unique encryption root keys have been checked based on information in system view ENCRYPTION_ROOT_KEYS. The check for each root key is rated YELLOW if at least one of the following criteria is met:

1. Version = 0 (No change of encryption root key after installation).
2. Create Date is older than communicated handover date.

Recommendation:
Create a new encryption root key in your system. Ensure that all prerequisites are met and that you follow strictly the detailed instructions documented in the section ‘Change the Root Encryption Key for Data Volume Encryption’ in the SAP HANA Administration Guide https://help.sap.com/hana/SAP_HANA_Administration_Guide_en.pdf. Note that for some root keys it is mandatory to back up the new root key to a root key backup file (*.rkb) in a
secure location. Otherwise, or when losing the backup file, the database cannot be recovered successfully. It is recommended that you test the procedures in a suitable environment prior to productive use.

1.1.5 Auditing

1.1.5.1 SAP HANA Auditing Status (HA028)

Purpose
To ensure that auditing is enabled to allow customers to detect and analyze security incidents.

Procedure
Execute SQL statement:

```sql
SELECT file_name, layer_name, section, key, value
FROM SYS.M_INIFILE_CONTENTS
WHERE layer_name != 'DEFAULT'
AND KEY = 'global_auditing_state'
```

Rating

**GREEN**: VALUE = true

**RED**: VALUE = parameter does not exist or VALUE is not 'true'

Note

The parameter is not included in SAP HANA ini files by default. To activate auditing, the customer has to add the parameter.

See HANA_Security_MiniCheck ID 710

**RED**: Auditing is disabled in the security settings of your SAP HANA database.

Evaluating Risk - High

If auditing is disabled, the execution of critical activities including unauthorized access or changes may remain undetected. Information that is required for the analysis of security incidents may be missing.

The following critical parameter has been checked:

Recommendation:

Activate SAP HANA auditing from the security console of the SAP HANA studio and define appropriate audit policies.

Useful sources of information for the SAP HANA audit trail are:

- SAP HANA Security Guide
- SAP HANA Administration Guide
- SAP HANA Audit Trail Best Practice in the SCN

1.1.5.2 No valid SAP HANA Audit Policies exist (HA057)

Purpose

Make sure that at least one audit policy is configured when auditing is active.

Procedure

Check for valid audit policies in the system:

```sql
SELECT COUNT (*)
FROM SYS.AUDIT_POLICIES
WHERE IS_VALID = 'TRUE'
AND IS_AUDIT_POLICY_ACTIVE = 'TRUE'
```

Rating

**GREEN** rating if at least one policy is valid

**RED** rating if no policy is valid

Note

The audit policy table is initially empty. The customer has to add audit policies.

**RED**: Evaluated Risk - High
If no valid audit policies are configured, only changes to the actual audit configuration will be tracked. The execution of critical activities including unauthorized access or changes will not be audited and may remain undetected. Information that is required for the analysis of security incidents may be missing.

The number of actually configured audit policies has been checked based on table SYS.AUDIT_POLICIES:

**Recommendation:**

Define appropriate audit policies. As a minimum set of audit policies, we recommend that you apply rules for the following:

- Unsuccessful connection attempts of all users
- All actions performed by standard super users, such as the SYSTEM user

You may also consider implementing audit policies, for example:

- As a type of change document in cases where the usual trace files are not enough
- On actions performed by users that are provided to a third party (for example, support users or users for external auditors)

Useful sources of information for the SAP HANA audit trail are:

- SAP HANA Security Guide
- SAP HANA Administration Guide
- SAP HANA Audit Trail Best Practice in the SCN

### 1.1.5.3 Inappropriate Default Audit Trail Type (HA029)

**Procedure**

1. Check the defined system default for the HANA audit trail type:

   ```sql
   SELECT file_name, layer_name, section, key, value
   FROM SYS.M_INIFILE_CONTENTS
   WHERE file_name = 'global.ini'
   AND KEY = 'default_audit_trail_type'
   ```

2. **Expected result (correct value):** CSTABLE or SYSLOGPROTOCOL

**Note**

See HANA_Security_MiniCheck ID 720S

**YELLOW:**

The default audit trail type of your system is CSVFILE.

**Evaluated Risk - Medium**

With the use of audit trail type CSVFILE, the audit trail is not protected against unauthorized access and manipulations cannot be traced back to the user. A user who performed unauthorized activities may be able to cover this up easily afterwards.

The following critical parameter has been checked:

**Recommendation:**

Do not use CSV text file as the audit trail for a production system, because it has severe restrictions.

1) It is not sufficiently secure.
   - By default, this file is written to the same directory as trace files, so database users with the system privilege CATALOG READ, TRACE ADMIN, or INIFILE ADMIN can access it. At operating system level, any user in the SAPSYS group can access it.
2) Audit trails are created for each server in a distributed system. This makes it more difficult to trace audit events that were executed across multiple servers (distributed execution).

Use either SYSLOGPROTOCOL or CSTABLE as audit trail target. Delete existing CSVFILES or move them to a secure directory.

### 1.1.5.4 Policies with inappropriate Audit trail type (HA030)

**Procedure**

1. Check defined audit trail type for the implemented Audit Policies:

   ```sql
   SELECT AUDIT_POLICY_NAME, IS_AUDIT_POLICY_ACTIVE, IS_VALID, TRAIL_TYPE
   FROM SYS.AUDIT_POLICIES
   WHERE trail_type = 'CSVFILE'
   ```

2. **Expected Result:** Empty list or no

3. Update the table in the report with a list of audit policies of trail type CSVFILE
Rating

4. **YELLOW** rating when at least 1 policy with audit trail type CSVFILE is defined
5. **GREEN**: Other

**Note:** See HANA_Security_MiniCheck ID 723S

**YELLOW** Evaluated Risk - 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.

At least one audit policy with audit trail type CSVFILE is defined in your system. The table below lists the identified audit policies.

**Recommendation:**

Review all audit policies with audit trail type CSVFILE and either change the audit trail to CSTABLE or SYLOGPROTOCOL, or delete the audit policy.

Delete existing CSVFILES or move them to a secure directory. By default, CSVFILES are written to the same directory as Diagnosis Files.

Useful sources of information for the SAP HANA audit trail are:
- [http://scn.sap.com/docs/DOC-51098](http://scn.sap.com/docs/DOC-51098) for SAP HANA Audit Trail Best Practice in the SCN

### 1.1.6 Diagnosis Files

#### 1.1.6.1 Database Trace set to debug level (HA032)

**Purpose**

To ensure that information that might be sensitive is not written to trace files.

**Procedure**

1. Check whether Database Trace is enabled:

   ```sql
   SELECT 'Database trace', FILE_NAME, SECTION, KEY, VALUE
   FROM M_INIFILE_CONTENTS
   WHERE SECTION = 'trace'
   AND LAYER_NAME != 'DEFAULT'
   AND LAYER_NAME != 'DATABASE'
   AND KEY = 'trace'
   ```

   If trace is inactive, the statement will return an empty list.

   If trace is active, the statement will return the VALUE = on

2. Check for components of database trace that are set to debug level:

   ```sql
   SELECT 'Traces debug level', FILE_NAME, SECTION, KEY, VALUE
   FROM DUMMY D
   LEFT OUTER JOIN M_INIFILE_CONTENTS P
   ON P.SECTION = 'trace'
   AND P.LAYER_NAME != 'DEFAULT'
   AND LOWER(P.VALUE) = 'debug'
   ```

   3. If the results list is empty, acceptable trace levels are configured.

   If records are displayed in the results list, trace level ‘debug’ is configured for some components of the database trace.

   Copy records in the table of this check.

   We do not distinguish between critical and uncritical trace components.

**Rating**

**YELLOW** rating if database trace is active and on trace level ‘debug’ for at least one component

**GREEN** rating for all other cases

**Note:**
YELLOW: Evaluated Risk - Medium

With trace level 'debug', the database trace files may contain sensitive data. As part of a trace file, such data is accessible to all users who are granted the system privilege CATALOG_READ or TRACE ADMIN or INIFILE ADMIN.

Settings for the database trace have been checked based on information in M_INIFILE_CONTENTS:

Recommendation:

Restore the default trace settings and move trace files to a secure location to ensure the confidentiality of sensitive data. Investigate the specific reason and context for this trace setting.

You have two options to analyze recent use of the database trace:

1. Review the SAP HANA audit trail. Prerequisite: Audit Policy “System Configuration Change” had been enabled for all users.
2. Review recent parameter changes in trace files (HANA SPS10 and higher).

Use SQL statement HANA_Configuration_Parameters_Changes_Rev100+ from SAP Note 1969700 - SQL Statement Collection for SAP HANA to get a list of parameter changes logged in the current trace files.

1.1.6.2 SQL trace including results configured (HA033)

Purpose

To ensure that information that might be sensitive is not written to trace files as common practice or by accident.

Procedure

1. Check whether the SQL trace is enabled (indexserver.ini only).

   SELECT 'SQL trace', * 
   FROM M_INIFILE_CONTENTS 
   WHERE FILE_NAME = 'indexserver.ini' 
   AND SECTION = 'sqltrace' 
   AND LAYER_NAME != 'DEFAULT' 
   AND KEY = 'trace'

   If trace is inactive, the statement will return an empty list.
   If trace is active, the statement will return the VALUE = on

2. Check for traces with the setting all_with_results

   SELECT 'SQL trace', * 
   FROM M_INIFILE_CONTENTS 
   WHERE FILE_NAME = 'indexserver.ini' 
   AND SECTION = 'sqltrace' 
   AND LAYER_NAME != 'DEFAULT' 
   AND KEY = 'level'

   If the trace level is according to the default value, the statement will return an empty list.
   If the trace level is modified, the statement will return the VALUE.
   The critical setting is VALUE = 'all_with_results'.
   This setting is never the default setting

Rating

RED rating if the SQL trace is active and the trace level is 'all_with_results'
YELLOW rating if the SQL trace is not active and the trace level is 'all_with_results'
GREEN rating for all other cases

Note:

See HANA_Security_MiniCheck ID 815

RED: Evaluated Risk - High

Result sets of SQL statements may contain sensitive data. As part of a trace file, such data is accessible to all users with authorization to access diagnosis files (system privilege CATALOG_READ, TRACE ADMIN, and INIFILE ADMIN). This allows the user to bypass the application’s authority checks and to compromise the confidentiality of business data.

YELLOW: Evaluated Risk - Medium
Result sets of SQL statements may contain sensitive data. As part of a trace file, such data is accessible to all users with authorization to access diagnosis files (system privilege CATALOG_READ, TRACE ADMIN, and INIFILE ADMIN). This allows the user to bypass the application's authority checks and to compromise the confidentiality of business data.

With the current trace setting, result sets are included in the next SQL trace unless the user actively changes the trace level.

Settings for the database trace have been checked based on information in M_INIFILE_CONTENTS:

**Recommendation:** Immediately restore the default trace settings and remove index server trace files from their default location to ensure confidentiality of productive data. Investigate the specific reason and context for this trace setting.

You have two options to analyze recent use of the SQL trace:

1. Review the SAP HANA audit trail. Prerequisite: Audit policy "System Configuration Change" has been enabled for all users.
2. Review recent parameter changes in trace files (HANA SPS10 and higher).

Use SQL statement HANA_Configuration_Parameters_Changes_Rev100+ from [SAP Note 1969700](https://support.sap.com) to get a list of parameter changes logged in current trace files.

Note: Never include result sets in the SQL trace on productive systems. Always try to reproduce issues in another system with non-productive data.

### 1.1.6.3 Dump files older than 42 days (HA034)

**Purpose**
Traces and dump files may contain sensitive data. Therefore, it should be ensured that dump files that are no longer needed are removed.

**Procedure**

1. Check for old RTE Dump files:

   ```sql
   SELECT 'RTE Dump older than 42 days', COUNT(*)
   FROM M_TRACEFILES
   WHERE UPPER(FILE_NAME) LIKE '%RTEDUMP%'
     AND DAYS_BETWEEN(FILE_MTIME, CURRENT_TIMESTAMP) > 42
   ```

2. Check for old Crash Dump files

   ```sql
   SELECT 'Crash Dump older than 42 days', COUNT(*)
   FROM M_TRACEFILES
   WHERE UPPER(FILE_NAME) LIKE '%CRASHDUMP%'
     AND DAYS_BETWEEN(FILE_MTIME, CURRENT_TIMESTAMP) > 42
   ```

   If no old trace files exist, both statements will display '?' or ' ' in column COUNT. Otherwise a number of trace files is shown.

3. Update the table in the report with data collected

**Rating**

- **YELLOW** when old files are found.
- **GREEN** rating for all other cases

**Note:**

See HANA_Security_MinCheck ID 820S

**YELLOW: Evaluated Risk – Medium**

RTF dump files and crash dump files may contain sensitive data that should only be used in the context of analyzing a specific problem. As part of a runtime dump or crash dump files, such data is accessible to all users who are granted the system privilege CATALOG_READ or TRACE ADMIN or INIFILE ADMIN. This may allow these users to bypass the authority checks of the application and compromise confidentiality of business data.

The number of dump files older than 42 days has been checked based on system view M_TRACEFILES. At least one dump file older than 42 days has been identified.

The table below lists the file count for different types of dumps:

**Recommendation:**
1.1.7 Authentication

1.1.7.1 SAP HANA Password Policy (SY115)

**Purpose**
To evaluate the SAP HANA password policy parameters.

**Procedure**
Read the M_PASSWORD_POLICY view and compare all data with the recommended values. If the current parameter is set weaker than the recommended one, rate the parameter **YELLOW**. If it is set stronger or equal to the recommendation, rate the parameter **GREEN**.

**Manual Procedure**
Obtain password policy setting. The following setting will show password policy settings that deviate from the SAP default:

```sql
SELECT *
FROM SYS.M_INIFILE_CONTENTS
WHERE file_name = 'indexserver.ini'
  AND section = 'password policy'
  AND layer_name != 'DEFAULT'
```

Using this statement will provide you with required values only (omit the condition regarding the layer_name to also view default values):

```sql
(SELECT file_name, layer_name, key, value
FROM SYS.M_INIFILE_CONTENTS
WHERE file_name = 'indexserver.ini'
  AND section = 'password policy'
  AND layer_name != 'DEFAULT'
  AND key IN (
    'force_first_password_change',
    'maximum_unused_inital_password_lifetime',
    'minimal_password_length'
  )
ORDER BY key
)
UNION ALL
(SELECT '', '', '', '' FROM dummy) -- empty line
UNION ALL
(SELECT file_name, layer_name, key, value
FROM SYS.M_INIFILE_CONTENTS
WHERE file_name = 'indexserver.ini'
  AND section = 'password policy'
  AND layer_name != 'DEFAULT'
  AND key IN (
    'detail_error_on_connect',
    'last_used_passwords',
    'maximum_invalid_connect_attempts',
    'maximum_password_lifetime',
    'maximum_unused_productive_password_lifetime',
    'minimum_password_lifetime',
    'password_expire_warning_time',
    'password_layout',
    'password_lock_for_system_user',
    'password_lock_time'
  )
ORDER BY key
)
```

**Rating**
If one of the parameters `force_first_password_change`, `maximum_unused_inital_password_lifetime`, or `minimal_password_length` is rated **YELLOW**, rate the check **YELLOW**.
If the check is not rated **YELLOW**, rate it **GREEN**.
Note

Disregard the ratings of the other parameters. They are shown for information purposes only. You can highlight deviations from the SAP standard with the rating INFO.

YELLOW:

Recommendation:
Adapt all values to the recommended or stronger settings.

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.

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

1.1.8 Users

1.1.8.1 Activation Status and Validity of User SYSTEM (SY134)

Purpose
To check that user SYSTEM is deactivated after installation.

Procedure
1. If customer provided you system access with user SYSTEM, then rate the check red. No further action is required.
2. Check if user SYSTEM is active. Use the following SQL statement:
   ```sql
   SELECT USER_NAME, VALID_FROM, VALID_UNTIL, USER_DEACTIVATED, DEACTIVATION_TIME
   FROM SYS.USERS
   WHERE USER_NAME = 'SYSTEM'
   ```

Rating
GREEN if: user_deactivated = TRUE or user_deactivated = FALSE and VALID_TO is in the past
RED if: user_deactivated = FALSE and VALID_TO is in the future or initial

Note
See HANA_Security_MiniCheck ID 120S

RED:
Active standard users are an easy and widely used target for hacking attacks since they are available in every system. Furthermore, the user SYSTEM is like a super user with very powerful user authorizations that cannot be revoked.

The activation status and validity dates (VALID FROM and VALID TO) of user SYSTEM have been checked in system table USERS.

Recommendation:
Review the current usage of user SYSTEM and set up and test a user and role concept, so that the use of user SYSTEM becomes obsolete.
Deactivate the user account with the SQL statement:
```
ALTER USER SYSTEM DEACTIVATE USER NOW.
```

To prevent misuse of user SYSTEM, activate related audit policies in your SAP HANA system as described in the SAP HANA Administration Guide.

1.1.8.2 User SYSTEM has recently been used (HA040)

Purpose
Check for recent use of User SYSTEM.

Procedure
1. If customer provided you system access with user SYSTEM, then rate the check red. No further action is required.
2. In all other cases: Execute the following SQL
SELECT USER_NAME, VALID_FROM, VALID_UNTIL, USER_DEACTIVATED, DEACTIVATION_TIME 
LAST_SUCCESSFUL_CONNECT, LAST_INVALID_CONNECT_ATTEMPT 
FROM SYS.USERS 
WHERE USER_NAME = 'SYSTEM'

Rating

Red: If user System has been used within the last 7 days
YELLOW: If user System has been used in the last 8 to 30 days
GREEN: In all other cases

RED: Evaluated Risk - High

If the user SYSTEM is used, then user activity in the system cannot be traced back to a unique identity.

YELLOW: Evaluated Risk - Medium

If the user SYSTEM is used, then user activity in the system cannot be traced back to a unique identity.

The last successful logon date of user SYSTEM has been checked in table USERS.

Recommendation:
Identify for what purpose and by whom the user SYSTEM is currently being used in your organization, for example, use by administrators, service and support delivery, or technical interfaces. If necessary, the analysis of HANA audit trail, HANA system views, and trace files can provide further insight and help verification.

Set up a role and authorization concept and create new personalized users and assign them the required minimal authorizations.

1.1.8.3 Confidentiality of SYSTEM user password (HA065)

Purpose
Check whether the password of user SYSTEM might be known outside the customer’s organization.

Procedure
Execute the following SQL

SELECT USER_NAME, ADMIN_GIVEN_PASSWORD, LAST_PASSWORD_CHANGE_TIME, 
PASSWORD_CHANGE_NEEDED 
FROM SYS.USERS 
WHERE USER_NAME = 'SYSTEM'

Rating

RED: When LAST_PASSWORD_CHANGE_TIME < Handover Date as communicated in questionnaire or LAST_PASSWORD_CHANGE_TIME = ?
GREEN: other cases

RED: Evaluated Risk - High

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

The date of the last password change has been determined based on system table USERS.

Recommendation:
Change password of user SYSTEM immediately.

1.1.8.4 Several users with multiple invalid connect attempts (HA042)

Purpose
Multiple invalid connection attempts by several users may indicate hacking attempt.

Procedure
1. Check for users with multiple invalid connection attempts.

SELECT USER_NAME, USER_DEACTIVATED, DEACTIVATION_TIME, LAST_SUCCESSFUL_CONNECT, 
LAST_INVALID_CONNECT_ATTEMPT 
FROM SYS.USERS 
WHERE USER_NAME = 'SYSTEM'
LAST_INVALID_CONNECT_ATTEMPT, INVALID_CONNECT_ATTEMPTS
FROM PUBLIC.USERS
WHERE (not user_name = 'SYS' and not user_name like '_SYS_%')
    and INVALID_CONNECT_ATTEMPTS > '5'

Extended version which omits inactive users:
SELECT p.USER_NAME, p.USER_DEACTIVATED, p.DEACTIVATION_TIME, p.LAST_SUCCESSFUL_CONNECT,
p.LAST_INVALID_CONNECT_ATTEMPT, p.INVALID_CONNECT_ATTEMPTS
FROM PUBLIC.USERS AS p
join sys.users as u on p.user_name = u.user_name
where not (p.user_name like '_SYS%' or p.user_name = 'SYS' or p.user_name = 'SYSTEM')
    and u.user_deactivated = 'FALSE'
    and u.valid_from <= now()
    and (u.valid_until >= now() or u.valid_until is null)
    and p.INVALID_CONNECT_ATTEMPTS > '5'

2. Determine total number of users in system
SELECT count(*) FROM PUBLIC.USERS
WHERE (not user_name = 'SYS' and not user_name like '_SYS_%')

Extended version that shows various counts:
SELECT 'All users' as USER_GROUP, count(*) FROM PUBLIC.USERS AS p
UNION ALL
SELECT 'Active users' as USER_GROUP, count(*) FROM PUBLIC.USERS AS p
join sys.users as u on p.user_name = u.user_name
where not (p.user_name like '_SYS%' or p.user_name = 'SYS' or p.user_name = 'SYSTEM')
    and u.user_deactivated = 'FALSE'
    and u.valid_from <= now()
    and (u.valid_until >= now() or u.valid_until is null)
UNION ALL
SELECT 'System users' as USER_GROUP, count(*) FROM PUBLIC.USERS AS p
where     (p.user_name like '_SYS%' or p.user_name = 'SYS' or p.user_name = 'SYSTEM')

Rating
A) Systems with fewer than 100 users:
RED if there are at least 5 users with INVALID_CONNECT_ATTEMPTS > 10
YELLOW if 4 ≥ () ≥ 1
GREEN if there are no users with INVALID_CONNECT_ATTEMPTS > 10

B) Systems with more than 100 users:
RED if there are at least 5% of users with INVALID_CONNECT_ATTEMPTS > 10
YELLOW if there are up to 4% of users with INVALID_CONNECT_ATTEMPTS > 10
GREEN if there are no users with INVALID_CONNECT_ATTEMPTS > 10

**RED: Evaluated Risk - High**
Invalid connection attempts recorded for multiple users may indicate an attack aiming for unauthorized access.

**YELLOW: Evaluated Risk - Medium**
Invalid connection attempts recorded for multiple users may indicate an attack aiming for unauthorized access.

The system view USERS has been checked for users with multiple invalid connection attempts:

Recommendation:
Analyze the audit trail to understand details of these connection attempts. Check with users about potential issues they have experienced.
You may get additional information from analyzing system views such as M_CONNECTIONS and by searching the index server trace files.
Note that these files are not stored in a secure place and therefore may have been manipulated during an attack.
If no audit trail for this use case is available, then activate an audit policy for invalid connection attempts of all users.
1.1.8.5 Users with disabled password lifetime (HA043)

Purpose
Identify users with disabled password lifetime and make sure that these are accepted exceptions from the password policy.

Procedure
1. Get list of users with disabled password lifetime:

```sql
SELECT USER_NAME, LAST_SUCCESSFUL_CONNECT, PASSWORD_CHANGE_TIME, IS_PASSWORD_ENABLED,
       IS_SAP_LOGON_TICKET_ENABLED
FROM public.users
WHERE not (user_name like '_SYS%' or user_name = 'SYS' or user_name = 'SYSTEM')
   and password_change_time IS NULL
```

Here is a variant showing all interesting fields of the table:

```sql
SELECT USER_NAME, IS_PASSWORD_ENABLED, PASSWORD_CHANGE_TIME, LAST_PASSWORD_CHANGE_TIME,
       ADMIN_GIVEN_PASSWORD, PASSWORD_CHANGE_NEEDED, IS_PASSWORD_LIFETIME_CHECK_ENABLED,
       LAST_SUCCESSFUL_CONNECT, LAST_INVALID_CONNECT_ATTEMPT, INVALID_CONNECT_ATTEMPTS,
       VALID_FROM, VALID_UNTIL, USER_DEACTIVATED, DEACTIVATION_TIME,
       IS_KERBEROS_ENABLED, IS_SAML_ENABLED, IS_X509_ENABLED, IS_SAP_LOGON_TICKET_ENABLED,
       IS_SAP_ASSERTION_TICKET_ENABLED
FROM public.users
WHERE not (user_name like '_SYS%' or user_name = 'SYS' or user_name = 'SYSTEM')
   and password_change_time IS NULL
```

On older HANA installations, such as on HANA 1.00 SP 10, you cannot read all these fields. Simply omit them or comment them out:

```sql
SELECT USER_NAME, IS_PASSWORD_ENABLED, PASSWORD_CHANGE_TIME,
       /* LAST_PASSWORD_CHANGE_TIME, */
       ADMIN_GIVEN_PASSWORD, PASSWORD_CHANGE_NEEDED,
       /* IS_PASSWORD_LIFETIME_CHECK_ENABLED, */
       LAST_SUCCESSFUL_CONNECT, LAST_INVALID_CONNECT_ATTEMPT, INVALID_CONNECT_ATTEMPTS,
       VALID_FROM, VALID_UNTIL, USER_DEACTIVATED, DEACTIVATION_TIME,
       IS_KERBEROS_ENABLED, IS_SAML_ENABLED, IS_X509_ENABLED
FROM public.users
WHERE not (user_name like '_SYS%' or user_name = 'SYS' or user_name = 'SYSTEM')
   and password_change_time IS NULL
```

2. Compare with list of Technical Users provided in the Service Questionnaire.

3. Copy the list of identified users to the table below.

4. Create a rating for each user based on the following criteria:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>YELLOW</td>
<td>The user has not been communicated as a known Technical User in the Service Questionnaire.</td>
</tr>
<tr>
<td>GREEN</td>
<td>The user has been communicated as a known Technical User in the Service Questionnaire.</td>
</tr>
</tbody>
</table>

Rating
Check is rated **YELLOW** when number of users not listed as technical users in questionnaire ≥ 1

Note:
See HANA_Security_MiniCheck ID 130S

**YELLOW** Evaluated Risk - Medium
When a password has been compromised, unauthorized access through this user is possible until the password is changed.

The following table lists all active, valid users with disabled password lifetime that are able to authenticate with user name and password.

Note: The table may contain users created by SAP HANA in the context of deploying, for example, XS classic or XS Advanced Scenarios.

Recommendation:
For Technical Users, often the password lifetime check is disabled in order to ensure that productive use of the system is not stopped simply because the password lifetime has exceeded the defined thresholds. However, the risk associated with long maximum password lifetimes applies to all users.

Review the listed users and perform the following actions:
1. Deactivate or delete users that are no longer in use.
2. Enable password lifetime for all users that are not Technical Users.
3. For all Technical Users, check whether alternative authentication methods such as certificate-based authentication are available, and replace password-based login when feasible.
4. Consider enabling password lifetime for less critical technical users and trigger a password change based on alerts (Alert "Expiration of database user passwords", Alert ID 62).
5. For those technical users that need to keep a password-based logon and disabled password lifetime, make sure that a procedure is implemented in your organization to ensure regular password change and compliance with the password policy at all times.

1.1.8.6 Age of last password change of users with disabled password lifetime (HA044)

Purpose
Ensure that passwords are changed at adequate intervals, even when the password lifetime check is disabled.

Procedure
1. Execute SQL statement to identify the users.

```sql
SELECT user_name, last_password_change_time
FROM users
WHERE is_password_enabled = 'TRUE'
AND is_password_lifetime_check_enabled = 'FALSE'
AND DAYS_BETWEEN(last_password_change_time, CURRENT_TIMESTAMP) >
(SELECT value
FROM M_Password_Policy
WHERE property = 'maximum_password_lifetime')
AND user_deactivated = 'FALSE'
AND valid_from <= now()
AND (valid_until >= now()
OR valid_until is null)
```

Rating
YELLOW: if at least one user is identified.
GREEN: Otherwise

YELLOW: Evaluated Risk - Medium

When a password has been compromised, unauthorized access through this user is possible until the password is changed.

The following table lists all active, valid users with disabled password lifetime whose age of last password change exceeds the number of days defined in your password policy parameter 'maximum_password_lifetime' of the view M_PASSWORD_POLICY. See also check SAP HANA Password Policy (HA036):

Recommendation:
Review the listed users. Password complexity of these users must be greatly increased compared with other users. If this is in doubt, change their password immediately.

Implement a procedure to ensure sufficient complexity of passwords upon user creation. We also recommend implementing a procedure to trigger a password change for Technical Users at regular intervals, or implementing other authentication methods.

1.1.8.7 No use of Restricted Users (HA045)

Purpose
End users who directly access SAP HANA with personal users should have minimal database authorizations, for example, unable to access public system views, unable to create database objects such as tables, and so on.

**Procedure**

1. Determine total number of users in system

   ```sql
   SELECT count(*)
   FROM PUBLIC.USERS
   WHERE (not user_name = 'SYS' and not user_name like '_SYS_%')
   and USER_DEACTIVATED = 'FALSE'
   ```

2. Determine total number of restricted users

   ```sql
   SELECT count(*)
   FROM PUBLIC.USERS
   WHERE (not user_name = 'SYS' and not user_name like '_SYS_%')
   and USER_DEACTIVATED = 'FALSE'
   and IS_RESTRICTED = 'TRUE'
   ```

3. Optional: User names of restricted users:

   ```sql
   SELECT USER_NAME, USER_DEACTIVATED, DEACTIVATION_TIME, IS_RESTRICTED
   FROM public.users
   WHERE (not user_name = 'SYS' and not user_name like '_SYS_%')
   and IS_RESTRICTED = 'TRUE'
   and USER_DEACTIVATED = 'FALSE'
   ```

**Rating**

1. YELLOW rating if number of end users > 100 and number of restricted users < 10%
2. GREEN rating in all other cases.

**YELLOW:** Evaluated Risk - Medium

A large number of end users are able to access system views and create objects in their own database schema. This may allow users to access information that is not intended for their use, or to perform activities on own database objects that affect the overall stability and information security of the system.

More than 100 active users have been found in your system, but the number of restricted users is lower than 10%.

**Recommendation:**

Create users as a restricted user to ensure that users are initially created without any privileges in SAP HANA, and assign them only those roles that are required for performing expected application tasks.

As of SAP HANA 2.0, existing users can be converted into restricted users. See the SAP HANA Administration Guide for details.

### 1.1.8.8 Potentially obsolete users (HA046)

**Purpose**

Identify users who do not work in the system so they can be deactivated.

**Procedure**

1. Check for users who have never logged on to the system

   ```sql
   SELECT USER_NAME, CREATE_TIME, LAST_SUCCESSFUL_CONNECT, LAST_INVALID_CONNECT_ATTEMPT
   FROM SYS.USERS
   WHERE not user_name in ( 'SYSTEM', '_SYS_REPO')
   and user_deactivated = 'FALSE'
   and valid_from <= now()
   and ( valid_until >= now() or valid_until is null )
   and (DAYS_BETWEEN(CREATE_TIME, CURRENT_TIMESTAMP) > 180)
   and (LAST_SUCCESSFULCONNECT is NULL
   or DAYS_BETWEEN(LAST_SUCCESSFUL_CONNECT, CURRENT_TIMESTAMP) > 180)
   ```

2 Count the number of remaining users.

3. Copy the listed users to the table below

**Rating**

**YELLOW:** If users are found
**GREEN:** All other cases.
Note:
For convenience, you can download the result of the SQL to Microsoft Excel and apply filters there. Make sure that your results set is not cut off due to limited number of records that are configured in HANA Studio or DBACockpit.

**YELLOW: Evaluated Risk - Medium**

Obsolete users are a promising target for attacks since these users will not recognize strange behavior in the system.

Users have been detected that are active and valid, but have never logged on to the system.
Note: Users created in the last six months are excluded from the check.

**Recommendation:**
The number of database users should be kept to a minimum. The table below provides a list of potentially obsolete users. Check whether the listed users are actually required. Deactivate obsolete users or set an expiration date.

### 1.1.9 Authorizations

#### 1.1.9.1 Users with highly critical privileges or with roles that must not be assigned in productive systems (HA048)

**Purpose**
To identify system privileges and roles assigned in the SAP HANA system that must not be granted to users in production systems.

**Procedure**
1. Perform the checks for each privilege and role.
2. Update this check with the results.

**Rating**
Automatic rating according to worst case rule.

**Note:**

**RED: Evaluated Risk - High**

These authorizations allow users to access or change any data without a further authority check, or they authorize users to execute activities that are only allowed to be used by SAP Development.

The system has been checked for users with highly critical privileges and roles that must not be assigned to users in production systems.
The rating is **RED** if the checked authorization is granted to at least one user. User SYSTEM and _SYS_REPO are excluded from the analysis.

**Recommendation:**
Review the detailed description for each critical privilege and role, and follow the specific recommendation. Make sure that the authorizations listed above are not granted to users in a production environment.

Review the users listed in the table below and revoke authorizations unless they are required for a documented, approved reason.

#### 1.1.9.1.1 Users with critical System Privilege DATA ADMIN (HA073)

**Purpose**
Identify users with system-wide Superuser authorization for creating, changing, and deleting objects such as tables, views, or procedures.

**Manual Procedure**
1. Identify all users and roles with System Privilege DATA ADMIN.

Use SQL statements from SAP Note 1969700. In their Modification section, replace '%' with 'DATA ADMIN'. Use HANA_Security_GrantedRolesAndPrivileges for HANA 1.0 and Revision < 120 and
2. Download the result as a Microsoft Excel file and copy the users and roles into the tables of this report.

3. Update this check and its parent check HA048 with the count of users with the privilege DATA ADMIN.

Note:
- Count all users, direct grants, as well as users with grants through roles.
- Count each user once only.

**Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)**

1. Identify count of users with DATA ADMIN privilege:

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User'
   FROM SYS.EFFECTIVE_PRIVILEGE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
     AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
     AND p.PRIVILEGE = 'DATA ADMIN'
     and not (p.grantee = 'SYSTEM'
               or p.grantee = '_SYS_REPO')
     and u.user_deactivated = 'FALSE'
     and u.valid_from <= now()
     and (u.valid_until >= now() or u.valid_until is null)
   GROUP BY OBJECT_TYPE, PRIVILEGE
   ORDER BY OBJECT_TYPE, PRIVILEGE
   ```

2. Identify user names with privilege DATA ADMIN (if customer has rejected the listing of user names in the report, then omit this step)

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE
   FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
     AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
     AND p.PRIVILEGE = 'DATA ADMIN'
     and not (p.grantee = 'SYSTEM'
               or p.grantee = '_SYS_REPO')
     and u.user_deactivated = 'FALSE'
     and u.valid_from <= now()
     and (u.valid_until >= now() or u.valid_until is null)
   ```

3. Identify roles with privilege DATA ADMIN. The statement lists all roles including those roles that inherit the DATA ADMIN privilege from other roles.

   ```sql
   SELECT GRANTEE_SCHEMA_NAME, GRANTEE
   from SYS.EFFECTIVE_PRIVILEGE_GRANTEES
   where GRANTEE_TYPE = 'ROLE'
     and OBJECT_TYPE = 'SYSTEMPRIVILEGE'
     and PRIVILEGE = 'DATA ADMIN'
   ```

4. Update the tables with the data from the SQL statements.

**Rating**

**RED** Rating when at least 1 user with DATA ADMIN privilege is identified.

**RED: Evaluated Risk - High**

System privilege DATA ADMIN provides the authorization to execute any Data Definition Language (DDL) command in the SAP HANA database, for example, to drop tables or to modify table definitions of any object in any schema.

Users and roles 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.

**Recommendation:**
Remove the DATA ADMIN privilege from all user accounts except the SYSTEM and _SYS_REPO users. Also, technical users such as the SAP<SID> user of an ABAP system do not require the DATA ADMIN privilege, because all change operations of the SAP<SID> user are limited to the SAP<SID> schema.

By default, every user has all privileges in the objects in their own schema. Any authorization in additional schemas shall be evaluated and granted based on a specific use case. Such authorizations typically include privileges in schemas that are used by SAP HANA internally, for example: SELECT privilege in tables and system views in schema SYS and _SYS_STATISTICS, EXECUTE privilege in specific procedures in the SAP HANA platform (for example, for granting or revoking user privileges, or for handling objects included in transports) and DELETE privilege for executing housekeeping tasks (for example, cleaning up SQL execution plans). Authorizations in schemas of other applications should be replaced by setting up dedicated database connections or other interfaces.

Consider also removing the DATA ADMIN privilege from all roles in your system, or deleting such roles to prevent misuse.

The effective grantees of privileges and roles can be validated manually using the SQL query:

HANA_Security_GrantedRolesAndPrivileges from SAP Note 1969700. In its Modification section, replace %' with 'DATA ADMIN' as input for the Privilege.

As of HANA 1.0 SPS 12, you can also use the views Effective_privilege_grantees and Effective_role_grantees, for example:

```sql
SELECT * FROM SYS.EFFECTIVE_PRIVILEGE_GRANTEES WHERE PRIVILEGE = 'DATA ADMIN' AND OBJECT_TYPE = 'SYSTEMPRIVILEGE';
```

1.1.9.1.2 Users with critical System Privilege DEVELOPMENT (HA079)

**Purpose**

Identify users with Superuser Authorization for internal ALTER SYSTEM commands.

**Manual Procedure**

1. Identify all users and roles with System Privilege DATA ADMIN.

Use SQL statements from SAP Note 1969700. In their Modification section, replace '%' with 'DEVELOPMENT'. Use

HANA_Security_GrantedRolesAndPrivileges for HANA 1.0 and Revision < 120 and

HANA_Security_GrantedRolesAndPrivileges_1.0.120+ for HANA 1.0 Revision > 120 or HANA 2.0.

2. Download the result as a Microsoft Excel file and copy the users and roles into the tables of this report.

3. Update this check and its parent check HA048 with the count of users with the privilege DEVELOPMENT.

**Note:**

- Count all users, direct grants, as well as users with grants through roles.
- Count each user once only.

**Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)**

1. Identify count of users with DEVELOPMENT privilege:

```sql
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE ), 'User'
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
WHERE p.GRANTEE_TYPE='USER'
AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
AND p.PRIVILEGE = 'DEVELOPMENT'
and not (p.grantee = 'SYSTEM'
    or p.grantee = '_SYS_REPO')
and u.user_deactivated = 'FALSE'
and u.valid_from <= now() and (u.valid_until >= now() or u.valid_until is null)
GROUP BY OBJECT_TYPE, PRIVILEGE
ORDER BY OBJECT_TYPE, PRIVILEGE
```
2. Identify user names with privilege DEVELOPMENT (if customer has rejected the listing of user names in the report, then omit this step)

```
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
  AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
  AND p.PRIVILEGE = 'DEVELOPMENT'
  and not (p.grantee = 'SYSTEM'
          or p.grantee = '_SYS_REPO')
  and u.user_deactivated = 'FALSE'
  and u.valid_from <= now()
  and (u.valid_until >= now() or u.valid_until is null)
```

3. Identify roles with privilege DATA ADMIN. The statement lists all roles including those roles that inherit the DEVELOPMENT privilege from other roles)

```
SELECT GRANTEE_SCHEMA_NAME, GRANTEE
from EFFECTIVE_PRIVILEGE_GRANTEES
where GRANTEE_TYPE = 'ROLE'
  and OBJECT_TYPE = 'SYSTEMPRIVILEGE'
  and PRIVILEGE = 'DEVELOPMENT'
```

4. Update the tables with the data from the SQL statements.

**Rating**

**RED** Rating when at least 1 user with DEVELOPMENT privilege is identified.

Users in your SAP HANA system have the DEVELOPMENT 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 since these users have the DEVELOPMENT privilege by design and the privilege cannot be revoked from these users.

**1.1.9.1.3 Users with critical Analytical Privilege _SYS_BI_CP_ALL (HA077)**

**Purpose**

To identify users with superuser authorization for activated content.

**Manual Procedure**

1. Identify all users and roles with Analytical Privilege _SYS_BI_CP_ALL'.

Use SQL statements from SAP Note 1969700. In the Modification section, replace the following:

- PRIVILEGE: Replace '%’ with 'EXECUTE'
- OBJECT_NAME: Replace '%’ with '_SYS_BI_CP_ALL'
- OBJECT_TYPE: Replace '%’ with 'ANALYTICALPRIVILEGE'

Use `HANA_Security_GrantedRolesAndPrivileges` for HANA 1.0 and Revision < 120 and `HANA_Security_GrantedRolesAndPrivileges_1.0.0.120+` for HANA 1.0 Revision > 120 or HANA 2.0.

2. Download the result as a Microsoft Excel file and copy the users and roles into the tables of this report.

3. Update this check and its parent check HA048 with the count of users with the privilege _SYS_BI_CP_ALL.

**Note:**

- Count all users, direct grants, as well as users with grants through roles.
- Count each user once only.

**Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)**

1. Identify count of users with _SYS_BI_CP_ALL privilege:

```
SELECT DISTINCT OBJECT_NAME, OBJECT_TYPE, COUNT ( DISTINCT p.GRANTEE), 'User'
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
  on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
  AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
  AND p.PRIVILEGE = 'DEVELOPMENT'
  and not (p.grantee = 'SYSTEM'
          or p.grantee = '_SYS_REPO')
  and u.user_deactivated = 'FALSE'
  and u.valid_from <= now()
  and (u.valid_until >= now() or u.valid_until is null)
```
ON p.GRANTEE = u.user_name  
WHERE p.GRANTEE_TYPE='USER'  
  AND p.OBJECT_TYPE = 'ANALYTICALPRIVILEGE'  
  AND p.OBJECT_NAME = '_SYS_BI_CP_ALL'  
  AND p.PRIVILEGE = 'EXECUTE'  
  and not p.grantee = 'SYSTEM'  
  and u.user_deactivated = 'FALSE'  
  and u.valid_from  <= now()  
  and (u.valid_until >= now() or u.valid_until is null)  
GROUP BY OBJECT_TYPE, OBJECT_NAME

2. Identify user names with privilege _SYS_BI_CP_ALL (if customer has rejected the listing of user names in the report, then omit this step)

SELECT OBJECT_NAME, OBJECT_TYPE, GRANTEE  
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p  
JOIN SYS.USERS as u  
on p.GRANTEE = u.user_name  
WHERE p.GRANTEE_TYPE='USER'  
  AND p.OBJECT_TYPE = 'ANALYTICALPRIVILEGE'  
  AND p.OBJECT_NAME = '_SYS_BI_CP_ALL'  
  AND p.PRIVILEGE = 'EXECUTE'  
  and not p.grantee = 'SYSTEM'  
  and u.user_deactivated = 'FALSE'  
  and u.valid_from  <= now()  
  and (u.valid_until >= now() or u.valid_until is null)  
GROUP BY p.OBJECT_TYPE, p.OBJECT_NAME, p.GRANTEE

3. Identify roles with privilege _SYS_BI_CP_ALL. The statement lists all roles including those roles that inherit the _SYS_BI_CP_ALL privilege from other roles)

SELECT GRANTEE_SCHEMA_NAME, GRANTEE  
from EFFECTIVE_PRIVILEGE_GRANTEES  
where GRANTEE_TYPE = 'ROLE'  
  and OBJECT_TYPE = 'ANALYTICALPRIVILEGE'  
  and OBJECT_NAME = '_SYS_BI_CP_ALL'  
  and PRIVILEGE = 'EXECUTE'  

4. Update the tables with the data from the SQL statements.

5. Remove the ABAP Schema User from the tables as this user requires the _SYS_BI_CP_ALL privilege.

Rating

RED Rating when at least 1 user with _SYS_BI_CP_ALL privilege is identified.

Users in your SAP HANA system have the _SYS_BI_CP_ALL analytic 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 user is not considered, because it has the _SYS_BI_CP_ALL privilege by design and the privilege cannot be revoked from these users.

1.1.9.1.4 List of users with critical Object Privilege DEBUG (HA074)

Purpose

Identify users with DEBUG Privileges in your production system.

Manual Procedure

1. Identify all users and roles with Object Privilege DEBUG.

Use SQL statements from SAP Note 1969700. In their Modification section, replace '%' with 'DEBUG' as input for Privilege.

Use HANA_Security_GrantedRolesAndPrivileges for HANA 1.0 and Revision < 120 and  
HANA_Security_GrantedRolesAndPrivileges_1.00.120+ for HANA 1.0 Revision > 120 or HANA 2.0.

2. Download the result as a Microsoft Excel file and copy the users and roles  
into the tables of this report.
3. Update this check and its parent check HA048 with the count of users with the privilege DEBUG.

**Note:**
- Count all users, direct grants, as well as users with grants through roles.
- Count each user once only.

**Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)**

1. Identify roles with DEBUG privilege and update the table with the result:

   ```sql
   SELECT DISTINCT GRANTEE_SCHEMA_NAME, GRANTEE
   FROM GRANTED_PRIVILEGES
   WHERE PRIVILEGE = 'DEBUG'
   AND GRANTEE_TYPE = 'ROLE'
   ```

2. Identify users with indirect grants of DEBUG privilege through roles by checking the effective role grantees for all roles obtained above. Note that roles with the same role_name may exist in different role_schema_names.

   You can simplify this step by combining all roles of the same schema into an in-List:

   ```sql
   You replace WHERE role_name = '<ROLE_NAME>'
   with WHERE role_name IN ('<ROLE_NAME1>', '<ROLE_NAME2>')
   ```

   You also need to specify the role_schema_name. When role_schema_name is empty, you remove this part of the where clause or you specify AND role_schema_name = "".

   Update the table with the result.

   ```sql
   SELECT DISTINCT GRANTEE
   from EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   where p.role_name = '<ROLE_NAME>'
   and p.role_schema_name = '<ROLE_SCHEMA_NAME>'
   and p.GRANTEE_TYPE = 'USER'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   ```

3. Identify users with direct grant of DEBUG privileges and update the table with the result:

   ```sql
   SELECT DISTINCT GRANTEE_TYPE, GRANTEE
   FROM GRANTED_PRIVILEGES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.PRIVILEGE = 'DEBUG'
   AND p.GRANTEE_TYPE = 'USER'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   ```

**Rating**

**RED** Rating when at least 1 user with DEBUG privilege is identified.

**Note**

Even user SYSTEM must not have DEBUG Privilege. You can verify this by verifying the grantor of this privilege in the view effective_privileges:

```sql
SELECT *
FROM effective_privileges
WHERE PRIVILEGE = 'DEBUG'
AND USER_NAME = 'SYSTEM'
```

Users in your SAP HANA system have the DEBUG 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.

### 1.1.9.1.5 List of users with critical Object Privilege ATTACH DEBUGGER (HA075)

**Purpose**
Identify users with ATTACH DEBUGGER Privileges in your productive system. This authorization allows users to attach themselves to another user’s session in debug mode.

**Manual Procedure**

1. Identify all users and roles with Object Privilege ATTACH DEBUGGER.

Use SQL statements from SAP Note 1969700. In their Modification section, replace ‘%’ with ‘ATTACH DEBUGGER’ as input for Privilege.

Use $HANA\_Security\_GrantedRolesAndPrivileges$ for HANA 1.0 and Revision < 120 and $HANA\_Security\_GrantedRolesAndPrivileges\_1.00.120+$ for HANA 1.0 Revision > 120 or HANA 2.0.

2. Download the result as a Microsoft Excel file and copy the users and roles into the tables of this report.

3. Update this check and its parent check HA048 with the count of users with the privilege ATTACH DEBUGGER.

**Note:**
- Count all users, direct grants, as well as users with grants through roles.
- Count each user once only.

**Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)**

1. Identify roles with ATTACH DEBUGGER privilege and update the table with the result:

   ```sql
   SELECT DISTINCT GRANTEE_SCHEMA_NAME, GRANTEE
   FROM GRANTED_PRIVILEGES
   WHERE PRIVILEGE = 'ATTACH DEBUGGER'
   AND GRANTEE_TYPE = 'ROLE'
   ```

2. Identify users with indirect grants of ATTACH DEBUGGER privilege through roles by checking the effective role grantees for all roles obtained above. Note that roles with the same role_name may exist in different role_schema_names.

   You can simplify this step by combining all roles of the same schema into an in-List:

   You replace WHERE role_name = '<ROLE_NAME>'
   with WHERE role_name IN ('<ROLE_NAME1>', '<ROLE_NAME2>')

   You also need to specify the role_schema_name.

   When role_schema_name is empty, you remove this part of the where clause or you specify AND role_schema_name = ''.

   Update the table with the result.

   ```sql
   SELECT DISTINCT GRANTEE
   from EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   where role_name = '<role_name>'
   and role_schema_name = '<role_schema_name>'
   and p.GRANTEE_TYPE = 'USER'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   ```

3. Identify users with direct grant of ATTACH DEBUGGER privileges and update the table with the result:

   ```sql
   SELECT DISTINCT GRANTEE_TYPE, GRANTEE
   FROM GRANTED_PRIVILEGES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.PRIVILEGE = 'ATTACH DEBUGGER'
   AND p.GRANTEE_TYPE = 'USER'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   ```

**Rating**
**RED** Rating when at least 1 user with ATTACH DEBUGGER privilege is identified.

Users in your SAP HANA system have the ATTACH DEBUGGER 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.

### 1.1.9.1.6 Users with critical Application Privilege sap.hana.xs.debugger::Debugger (HA076)

**Purpose**

Identify users with sap.hana.xs.debugger::Debugger Application Privilege in your productive system.

**Manual Procedure**

1. Identify all users and roles with Application Privilege `sap.hana.xs.debugger::Debugger`

   Use SQL statements from SAP Note 1969700. In their Modification section, replace '%' with 'sap.hana.xs.debugger::Debugger' as input for Privilege.

   Use `HANA_Security_GrantedRolesAndPrivileges` for HANA 1.0 and Revision < 120 and `HANA_Security_GrantedRolesAndPrivileges_1.00.120+` for HANA 1.0 Revision > 120 or HANA 2.0.

2. Download the result as a Microsoft Excel file and copy the users and roles into the tables of this report.

3. Update this check and its parent check HA048 with the count of users with the privilege `sap.hana.xs.debugger::Debugger`.

**Note:**

- Count all users, direct grants, as well as users with grants through roles.
- Count each user once only.

**Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)**

1. Identify roles with `sap.hana.xs.debugger::Debugger` privilege and update the table with the result:

   ```sql
   SELECT DISTINCT GRANTEE_SCHEMA_NAME, GRANTEE
   FROM GRANTED_PRIVILEGES
   WHERE PRIVILEGE = 'sap.hana.xs.debugger::Debugger'
   AND GRANTEE_TYPE = 'ROLE'
   ```

2. Identify users with indirect grants of `sap.hana.xs.debugger::Debugger` privilege through roles by checking the effective role grantees for all roles obtained above. Note that roles with the same role_name may exist in different role_schema_names.

   You can simplify this step by combining all roles of the same schema into an in-List:

   You replace `WHERE role_name = '<ROLE_NAME>'` with `WHERE role_name IN ('<ROLE_NAME1>', '<ROLE_NAME2>')`

   You also need to specify the role_schema_name.

   When role_schema_name is empty, you remove this part of the where clause or you specify AND role_schema_name = "".

   Update the table with the result.

   ```sql
   SELECT DISTINCT GRANTEE
   from EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   where role_name = '<role_name>'
   and role_schema_name = '<role_schema_name>'
   and p.GRANTEE_TYPE = 'USER'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   ```

3. Identify users with direct grant of `sap.hana.xs.debugger::Debugger` privileges and update the table with the result:
SELECT DISTINCT GRANTEE_TYPE, GRANTEE
FROM GRANTED_PRIVILEGES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.PRIVILEGE = 'sap.hana.xs.debugger::Debugger'
AND p.GRANTEE_TYPE = 'USER'
and u.user_deactivated = 'FALSE'
and u.valid_from  <= now()
and (u.valid_until >= now() or u.valid_until is null)

4. Note:

As of SAP HANA 2.0 SPS 1, the procedure can be simplified using the following SQL:

SELECT GRANTEE_TYPE, GRANTEE, GRANTOR
FROM EFFECTIVE_PRIVILEGE_GRANTEE
WHERE privilege = 'sap.hana.xs.debugger::Debugger'
AND object_type = 'APPLICATIONPRIVILEGE';

Indirect assignments of the privilege via roles can be identified by checking whether the name of a grantor corresponds to a grantee of grantee_type = 'ROLE'.

Rating

RED rating if at least 1 user with sap.hana.xs.debugger::Debugger privilege is identified.

Users in your SAP HANA system have the Application Privilege sap.hana.xs.debugger::Debugger.

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.

1.1.9.1.7 List of users with critical Role SAP_INTERNAL_HANA_SUPPORT (HA078)

Purpose

To identify users with role SAP_INTERNAL_HANA_SUPPORT. This standard role is restricted to use by SAP Development Support.

Procedure

1. As of SPS 12: Execute preconfigured SQL statements embedded into this report to identify the number of users assigned to an authorization:

Identify the number of users with role SAP_INTERNAL_HANA_SUPPORT and update the table in the report:

SELECT p.ROLE_NAME, COUNT( DISTINCT p.GRANTEE )
FROM SYS.EFFECTIVE_ROLE_GRANTEE as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
/* AND  p.ROLE_NAME = 'SAP_INTERNAL_HANA_SUPPORT'  */
and u.user_deactivated = 'FALSE'
and u.valid_from  <= now()
and (u.valid_until >= now() or u.valid_until is null)
group by role_name

Get the list of users and roles with role SAP_INTERNAL_HANA_SUPPORT:

SELECT DISTINCT p.ROLE_NAME, p.GRANTEE, p.GRANTEE_TYPE
FROM SYS.EFFECTIVE_ROLE_GRANTEE as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.ROLE_NAME = 'SAP_INTERNAL_HANA_SUPPORT'
/* AND  p.ROLE_SCHEMA_NAME = '' */
and u.user_deactivated = 'FALSE'
and u.valid_from  <= now()
and (u.valid_until >= now() or u.valid_until is null)
order by p.GRANTEE_TYPE

IMPORTANT: The above statements are valid as of SAP HANA 2.0 SPS 1. For HANA 2.0 SPS 0 and HANA 1.0 SPS 12, remove the clause

AND p.ROLE_SCHEMA_NAME = "

SC_HANA - Security Checks for the SAP HANA Database 34/49
Confidential
EFFECTIVE_ROLE_GRANTEES is not available for earlier releases. Use SQL statement HANA_Security_GrantedRolesAndPrivileges from SAP Note 1969700 to obtain the information. In the modification section of this SQL, replace '%' with the role name 'SAP_INTERNAL_HANA_SUPPORT'.

2. Update the table with the number of users per privilege and role.

3. Update the tables below with the identified user names and role names. If the customer has not requested the list of user names, update only the table with role names and delete the table for the user names.

4. Check whether identified user names correspond to users listed in the questionnaire.

Rating

YELLOW when at least 1 user is identified that is not listed in the questionnaire.

GREEN in all other cases.

Note:

See HANA_Security_MiniCheck ID 310S

Users that have not been mentioned in the questionnaire as preconfigured users for SAP Development Support have the role SAP_INTERNAL_HANA_SUPPORT in your SAP HANA system.

1.1.9.2 Users with critical Developer Privileges in the HANA Catalog (HA136)

Purpose

Identify users with system privileges related to development of catalog objects.

Procedure

1. Execute the following SQL statement to identify the number of users assigned to critical system privileges:

```sql
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User'
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER' and p.OBJECT_TYPE = 'SYSTEMPRIVILEGE' and p.PRIVILEGE IN ('EXPORT', 'IMPORT', 'CREATE R SCRIPT', 'CREATE SCENARIO', 'SCENARIO ADMIN', 'CREATE SCHEMA', 'CREATE STRUCTURED PRIVILEGE', 'STRUCTURED PRIVILEGE ADMIN') and not p.grantee in ('SYSTEM', '_SYS_REPO') and u.user_deactivated = 'FALSE' and u.valid_from <= now() and (u.valid_until >= now() or u.valid_until is null)
GROUP BY OBJECT_TYPE, PRIVILEGE
ORDER BY OBJECT_TYPE, PRIVILEGE
```

2. Use the following statement to get the list of users for all critical privileges instead of the count of users:

```sql
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER' and p.OBJECT_TYPE = 'SYSTEMPRIVILEGE' and p.PRIVILEGE IN ('EXPORT', 'IMPORT', 'CREATE R SCRIPT', 'CREATE SCENARIO', 'SCENARIO ADMIN')
```

Confidential
'CREATE SCHEMA',
'CREATE STRUCTURED PRIVILEGE',
'STRUCTURED PRIVILEGE ADMIN'
)
and not (p.grantee = 'SYSTEM'
    or p.grantee like '_SYS_REPO')
and u.user_deactivated = 'FALSE'
and u.valid_from <= now()
and (u.valid_until >= now() or u.valid_until is null)
ORDER BY OBJECT_TYPE, PRIVILEGE, GRANTEE

2. Exclude Firefighter users specified in the Service Questionnaire.
3. Update the table with number of users per privilege.
4. Update the tables of the privilege-specific checks with the identified user names.

Rating
YELLOW when at least 1 authorization is granted to a user.

Note:
See HANA_Security_MiniCheck ID 215S

YELLOW: Evaluated Risk - Medium

Manual actions on catalog objects directly in the production system may lead to the system malfunctioning due to human error or untested changes. In addition, users may gain unauthorized access to data more easily since typical change control procedures are not enforced.

Users other than SYSTEM and _SYS_REPO have been granted critical system privileges for catalog objects in your system.

Recommendation:
All development should be performed in a development environment outside the production system and then transported using SAP standard tools for software logistics. In such a scenario, all changes and activation of objects are handled by the _SYS_REPO user.

Review the privileges listed in this check and consider revoking them from all users to prevent any development activity in the production system at SAP HANA user level. Consider storing these privileges in a repository role, so that a user with USER ADMIN privilege can grant them to a firefighter user in exceptional circumstances.

If you decide that technical users of an application may keep these privileges, ensure that appropriate change control settings and authorization concepts are in place at application level.

1.1.9.2.1 Users with critical System Privilege CREATE SCHEMA (HA113)

1.1.9.2.2 Users with critical System Privilege CREATE SCENARIO (HA112)

1.1.9.2.3 Users with critical System Privilege SCENARIO ADMIN (HA119)

1.1.9.2.4 Users with critical System Privilege CREATE R SCRIPT (HA111)

1.1.9.2.5 Users with critical System Privilege CREATE STRUCTURED PRIVILEGE (HA114)

1.1.9.2.6 Users with critical System Privilege STRUCTURED PRIVILEGE ADMIN (HA120)

1.1.9.2.7 Users with critical System Privilege EXPORT (HA109)

1.1.9.2.8 Users with critical System Privilege IMPORT (HA110)

1.1.9.3 Users with critical System Privileges on Users (HA117)

Purpose
Identify users with System Privileges for User Access Management.

Automatic Procedure (for HANA 1.0 SPS 12 and HANA 2.0)
1. Identify count of users with USER ADMINISTRATION privileges:
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User' FROM SYS.EFFECTIVE_PRIVILEGE_GRANTEES as p JOIN SYS.USERS as u on p.GRANTEE = u.user_name WHERE p.GRANTEE_TYPE='USER' AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND p.PRIVILEGE IN ('USER ADMIN', 'ROLE ADMIN') and not (p.grantee = 'SYSTEM' or p.grantee = '_SYS_REPO') and u.user_deactivated = 'FALSE' and u.valid_from <= now() and (u.valid_until >= now() or u.valid_until is null) GROUP BY OBJECT_TYPE, PRIVILEGE ORDER BY OBJECT_TYPE, PRIVILEGE

2. Identify user names with privilege DATA ADMIN (if customer has rejected the listing of user names in the report, then omit this step)

SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE FROM EFFECTIVE_PRIVILEGE_GRANTEES as p JOIN SYS.USERS as u on p.GRANTEE = u.user_name WHERE p.GRANTEE_TYPE='USER' AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE' AND p.PRIVILEGE IN ('USER ADMIN', 'ROLE ADMIN') and not (p.grantee = 'SYSTEM' or p.grantee = '_SYS_REPO') and u.user_deactivated = 'FALSE' and u.valid_from <= now() and (u.valid_until >= now() or u.valid_until is null)

3. Identify roles with privilege DATA ADMIN. The statement lists all roles including those roles that inherit the DATA ADMIN privilege from other roles)

SELECT GRANTEE_SCHEMA_NAME, GRANTEE, PRIVILEGE from SYS.EFFECTIVE_PRIVILEGE_GRANTEES where GRANTEE_TYPE = 'ROLE' and OBJECT_TYPE = 'SYSTEMPRIVILEGE' and PRIVILEGE IN ('USER ADMIN', 'ROLE ADMIN')

4. Update the tables with the data from the SQL statements.

Rating

RED rating when at least 1 user other than User Administrator is granted a privilege.

RED rating when a user is granted ROLE ADMIN privilege.

RED: Evaluated Risk - High

If users other than user administrators are authorized to create and change users, or if user administrators are able to create and change roles, then existing user management processes may be violated and users may gain unauthorized access to data or other critical privileges (or combinations of privileges).

Users other than the user administrators specified in the Service Questionnaire are granted system privileges for users.

Standard users SYSTEM and _SYS_REPO are also excluded from this check.

Recommendation:

Revoke the listed privileges from all users other than user administrators.

Grant privileges only through repository roles and revoke the privilege ROLE ADMIN from all users (Firefighter user is OK).

1.1.9.3.1 Users with critical System Privilege USER ADMIN (HA108)

RED: Evaluated Risk - High

If users other than user administrators are able to create or change users, users may gain unauthorized access to data or users may be able to change the system configuration so that the overall security is compromised.

Recommendation:
Review the listed users and revoke the USER ADMIN privilege from all users other than user administrators.

If a large number of user administrators are required in your environment, then consider implementing an identity management system to help assure compliance with user and authorization management.

1.1.9.3.2 Users with critical System Privilege ROLE ADMIN (HA107)

**RED: Evaluated Risk - High**

System privilege ROLE ADMIN provides the authorization to create or maintain catalog roles in the SAP HANA database and to grant or revoke catalog roles for users.

A user with the system privilege ROLE ADMIN can grant all of its own roles and privileges to other users. If the authorization concept is based on catalog roles, then the user administrator is typically able to take full control of the system.

**Recommendation:**

It is recommended to limit the use of catalog roles in production systems to exceptional cases only.

As standard, it is strongly recommended that you create roles in a development environment and then transport the tested roles along predefined transport routes to the production system.

This can be achieved by implementing roles as repository roles using the XS classic development environment, which is available for SAP HANA 1.0 and SAP HANA 2.0. As of SAP HANA 2.0 SPS 1, it is recommended that you consider implementing a role concept in an XSA environment (due to planned deprecation of XS classic).

Remove the ROLE ADMIN privilege from all user accounts except the SYSTEM and _SYS_REPO users.

In some SAP scenarios, a technical user such as the SAP<SID> user of an ABAP system may use the ROLE ADMIN privilege to create application-specific authorizations from the application layer. If this is the case in your environment, then make sure that an authorization concept for managing users and authorizations is in place at application level and that the SAP<SID> user is sufficiently protected against misuse.

In addition, you should verify whether the ROLE ADMIN privilege is actually required in day-to-day operations, or if its use is limited to the initial setup and dedicated maintenance activities.

The general recommendation is to remove the ROLE ADMIN privilege completely, or to grant it on a temporary basis only.

Also, it is recommended that you replace generated catalog roles with manually created repository roles that are then transported to production.

1.1.9.4 Users with critical system privileges for System Administration (HA049)

**Purpose**

To identify system privileges assigned to users other than the administrator.

**Procedure**

1. Execute the following SQL statement to identify the number of users assigned to critical system privileges:

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User'
   FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
   AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
   AND p.PRIVILEGE IN ( 'ADAPTER ADMIN', 'AGENT ADMIN', 'AUDIT ADMIN', 'AUDIT OPERATOR', 'BACKUP ADMIN', 'BACKUP OPERATOR', 'CERTIFICATE ADMIN', 'CREATE REMOTE SOURCE', 'CREDENTIAL ADMIN', 'ENCRYPTION ROOT KEY ADMIN', 'EXTENDED STORAGE ADMIN', 'INIFILE ADMIN', 'LDAP ADMIN', 'LICENSE ADMIN',
   ```
'LOG ADMIN',
'MONITOR ADMIN',
'OPTIMIZER ADMIN',
'RESOURCE ADMIN',
'SAVEPOINT ADMIN',
'SERVICE ADMIN',
'SESSION ADMIN',
'SSL ADMIN',
'TABLE ADMIN',
'TRUST ADMIN',
'VeRSION ADMIN',
'WORKLOAD ADMIN'
)
and not p.grantee in ('SYSTEM', '_SYS_REPO')
and u.user_deactivated = 'FALSE'
and u.valid_from <= now()
and (u.valid_until >= now() or u.valid_until is null)
GROUP BY OBJECT_TYPE, PRIVILEGE
ORDER BY OBJECT_TYPE, PRIVILEGE

2. Use the following statement to get the list of users for all critical privileges instead of the count of users:

```
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
AND p.PRIVILEGE IN ({
  'ADAPTER ADMIN',
  'AGENT ADMIN',
  'AUDIT ADMIN',
  'AUDIT OPERATOR',
  'BACKUP ADMIN',
  'BACKUP OPERATOR',
  'CERTIFICATE ADMIN',
  'CREATE REMOTE SOURCE',
  'CREDENTIAL ADMIN',
  'ENCRYPTION ROOT KEY ADMIN',
  'EXTENDED STORAGE ADMIN',
  'INIFILE ADMIN',
  'LDAP ADMIN',
  'LICENSE ADMIN',
  'LOG ADMIN',
  'MONITOR ADMIN',
  'OPTIMIZER ADMIN',
  'RESOURCE ADMIN',
  'SAVEPOINT ADMIN',
  'SERVICE ADMIN',
  'SESSION ADMIN',
  'SSL ADMIN',
  'TABLE ADMIN',
  'TRUST ADMIN',
  'VERSION ADMIN',
  'WORKLOAD ADMIN'
})
and not (p.grantee = 'SYSTEM' 
  or p.grantee like '_SYS_REPO')
and u.user_deactivated = 'FALSE'
and u.valid_from <= now()
and (u.valid_until >= now() or u.valid_until is null)
ORDER BY OBJECT_TYPE, PRIVILEGE, GRANTEE
```

2. If you received a Service Questionnaire, remove all communicated system administration users and firefighter users.

3. Update the table with number of users per privilege and role.
4. Update the tables of the privilege-specific checks with the identified user names.

**Rating**

**YELLOW** if at least one authorization is granted to more than one user that has not been excluded.

**YELLOW**: Evaluated Risk - Medium

Critical system privileges can be used to perform actions that may compromise the security of the system or its data. The more users that are assigned to these privileges, the higher the risk. Usually, these privileges must only be granted to users for system or database administration.

For a description of the checked authorizations, see *SAP HANA Security Guide, Chapter System Privileges* (Reference). With HANA 2.0 SPS 2, the documentation of critical privileges has been greatly enhanced and provides comprehensive information relevant also for earlier releases.

The system has been checked for users assigned to system privileges that are used for typical Basis Administration tasks in your system.

The users SYSTEM and _SYS_REPO and all Administration Users specified in the Service Questionnaire are excluded from the check.

The check is rated **YELLOW** because at least one system privilege is granted to more than 5 users.

The table lists critical administration privileges and the number of users that are assigned to them. Refer to the subchecks for the list of identified user names.

**Recommendation:**

Review the assignment of the listed system privileges and minimize user authorizations where appropriate.

Based on a strict need-to-know principle, only system administrators and dedicated firefighter users are expected to require these privileges for their actual roles and responsibilities.

If the response time to incidents needs to be optimized, it is best practice to improve the ability of administration users to get involved more quickly rather than to add additional support users to the grantees of critical authorizations.

The security of your system can be improved further if privileges for rare activities (such as the management of encryption root keys or licenses) are granted only on a temporary basis in the context of a documented service request or scheduled activity.
1.1.9.4.1 Users with critical System Privilege ADAPTER ADMIN (HA140)
1.1.9.4.2 Users with critical System Privilege AGENT ADMIN (HA141)
1.1.9.4.3 Users with critical System Privilege AUDIT ADMIN (HA099)
1.1.9.4.4 Users with critical System Privilege AUDIT OPERATOR (HA100)
1.1.9.4.5 Users with critical System Privilege BACKUP ADMIN (HA142)
1.1.9.4.6 Users with critical System Privilege BACKUP OPERATOR (HA143)
1.1.9.4.7 Users with critical System Privilege CERTIFICATE ADM (HA104)
1.1.9.4.8 Users with critical System Privilege CLIENT PARAMETER ADMIN (HA166)
1.1.9.4.9 Users with critical System Privilege CREATE CLIENTSIDE ENCRYPTION KEYPAIR (HA167)
1.1.9.4.10 Users with critical System Privilege CREATE REMOTE SOURCE (HA144)
1.1.9.4.11 Users with critical System Privilege CREDENTIAL ADM (HA103)
1.1.9.4.12 Users with critical System Privilege DROP CLIENTSIDE ENCRYPTION KEYPAIR (HA168)
1.1.9.4.13 Users with critical System Privilege ENCRYPTION ROOT KEY ADMIN (HA145)
1.1.9.4.14 Users with critical System Privilege EXTENDED STORAGE ADMIN (HA146)
1.1.9.4.15 Users with critical System Privilege INIFILE ADMIN (HA118)
1.1.9.4.16 Users with critical System Privilege LDAP ADMIN (HA121)
1.1.9.4.17 Users with critical System Privilege LICENSE ADMIN (HA147)
1.1.9.4.18 Users with critical System Privilege LOG ADMIN (HA148)
1.1.9.4.19 Users with critical System Privilege MONITOR ADMIN (HA149)
1.1.9.4.20 Users with critical System Privilege OPTIMIZER ADMIN (HA150)
1.1.9.4.21 Users with critical System Privilege RESOURCE ADMIN (HA151)
1.1.9.4.22 Users with critical System Privilege SAVEPOINT ADMIN (HA152)
1.1.9.4.23 Users with critical System Privilege SERVICE ADMIN (HA153)
1.1.9.4.24 Users with critical System Privilege SESSION ADMIN (HA154)
1.1.9.4.25 Users with critical System Privilege SSL ADMIN (HA106)
1.1.9.4.26 Users with critical System Privilege TABLE ADMIN (HA155)
1.1.9.4.27 Users with critical System Privilege TENANT ADMIN (HA169)
1.1.9.4.28 Users with critical System Privilege TRUST ADMIN (HA105)
1.1.9.4.29 Users with critical System Privilege VERSION ADMIN (HA156)
1.1.9.4.30 Users with critical System Privilege WORKLOAD ADMIN (HA157)
1.1.9.4.31 Users with critical System Privilege WORKLOAD ANALYZE ADMIN (HA170)

1.1.9.4.32 Users with critical System Privilege WORKLOAD CAPTURE ADMIN (HA171)

1.1.9.4.33 Users with critical System Privilege WORKLOAD REPLAY ADMIN (HA172)

1.1.9.5 Users with basic support user privileges (HA137)

**Purpose**

Identify users that do not require common authorizations in the SAP HANA system.

**Validity**

The check is available as of SAP HANA 1.0 SPS 12

**Manual Procedure**

Execute the following SQL statement to identify the number of users assigned to critical system privileges:

```sql
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User'
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
  AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
  AND p.PRIVILEGE IN ('CATALOG READ', 'TRACE_ADMIN')
  and not (p.grantee = 'SYSTEM' or p.grantee like '_SYS_REPO')
  and u.user_deactivated = 'FALSE'
  and u.valid_from <= now()
  and (u.valid_until >= now() or u.valid_until is null)
GROUP BY OBJECT_TYPE, PRIVILEGE
ORDER BY OBJECT_TYPE, PRIVILEGE
```

2. Use the following statement to get the list of users for all critical privileges instead of the count of users:

```sql
SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE
FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
  AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
  AND p.PRIVILEGE IN ('CATALOG READ', 'TRACE_ADMIN')
  and not (p.grantee = 'SYSTEM' or p.grantee like '_SYS_REPO')
  and u.user_deactivated = 'FALSE'
  and u.valid_from <= now()
  and (u.valid_until >= now() or u.valid_until is null)
ORDER BY OBJECT_TYPE, PRIVILEGE, GRANTEE
```

2. If you received a Service Questionnaire, remove all communicated system administration users.

3. Update the table with number of users per privilege and role.

4. Update the tables of the privilege-specific checks with the identified user names.

4. Perform the equivalent steps for role 'PUBLIC' as described for HA138.

**Automated Procedure**

1. Identify users with System Privileges 'CATALOG READ' and 'TRACE ADMIN' based on information from System View EFFECTIVE_PRIVILEGE_GRANTEES.

2. Identify users with role 'PUBLIC' based on information in SYSTEM VIEW EFFECTIVE_ROLE_GRANTEES.

3. Filter the results by excluding all users specified in the Service Questionnaire and all internal HANA users listed in Check HA052.

4. Update the table of this check and its subchecks.
Rating

The check is rated **YELLOW** when a subcheck returns more than 5 users that have not been excluded upfront.

**YELLOW** Evaluated Risk - Medium

Users with the commonly granted roles and privileges of this check may gain access to sensitive data that can be used for attacks.

Users have been identified in your system with privileges that should only be granted to users with SAP Basis tasks.

The following users are excluded from this check and all its subchecks:
1. All users specified in the Service Questionnaire
2. All users that have been created automatically as part of the SAP HANA deployment.

A list of automatically created users is included in the overview of HANA users (HA052) in the Users chapter of this report.

Note that for the role ‘PUBLIC’, those users that are created automatically with the deployment of SAP HANA are also excluded, since these internal users are created as Standard Users automatically, which have the role ‘PUBLIC’ by default.

**Recommendation:**

Review the assignment of the analyzed privileges and roles and consider minimizing user authorizations where appropriate, based on the need-to-know principle. Revoke the listed privileges and roles from all users who do not require them for their current roles and responsibilities in your organization. Refer to the additional details provided in the subchecks.

### 1.1.9.5.1 Users with System Privilege CATALOG READ (HA101)

**Purpose**

Identify system privileges assigned to users other than administrator.

**Procedure**

1. Execute the following SQL statement to identify the number of users assigned to critical system privileges:

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User'
   FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
   AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
   AND p.PRIVILEGE = 'CATALOG READ'
   and not p.grantee in ('SYSTEM', '_SYS_REPO')
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   GROUP BY OBJECT_TYPE, PRIVILEGE
   ORDER BY OBJECT_TYPE
   , PRIVILEGE
   ```

2. Use the following statement to get the list of users for all critical privileges instead of the count of users:

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE
   FROM EFFECTIVE_PRIVILEGE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
   AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'
   AND p.PRIVILEGE = 'CATALOG READ'
   and not (p.grantee = 'SYSTEM'
   or p.grantee like '_SYS_REPO')
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   ORDER BY OBJECT_TYPE, PRIVILEGE, GRANTEE
   ```

2. If you received a Service Questionnaire, remove all communicated users.

3. Update the tables with the identified user names.

4. Update the table in parent check HA137 with the number of users with this privilege.
Rating

**YELLOW** when privilege is granted to at least one user that has not been excluded.

**Note:**

See HANA_Security_MiniCheck ID 215S

### 1.1.9.5.2 Users with System Privilege TRACE ADMIN (HA102)

**Purpose**

Identify system privileges assigned to users other than administrator.

**Procedure**

1. Execute the following SQL statement to identify the number of users assigned to critical system privileges:

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, COUNT ( DISTINCT p.GRANTEE), 'User'  
   FROM EFFECTIVE_PRIVILEGE_GRANTEES as p  
   JOIN SYS.USERS as u  
   on p.GRANTEE = u.user_name  
   WHERE p.GRANTEE_TYPE='USER'  
   AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'  
   AND p.PRIVILEGE = 'TRACE ADMIN'  
   and not p.grantee in ('SYSTEM', '_SYS_REPO')  
   and u.user_deactivated = 'FALSE'  
   and u.valid_from <= now()  
   AND (u.valid_until >= now() or u.valid_until is null)  
   GROUP BY OBJECT_TYPE, PRIVILEGE  
   ORDER BY OBJECT_TYPE, PRIVILEGE
   ```

2. Use the following statement to get the list of users for all critical privileges instead of the count of users:

   ```sql
   SELECT DISTINCT p.OBJECT_TYPE, p.PRIVILEGE, p.GRANTEE  
   FROM EFFECTIVE_PRIVILEGE_GRANTEES as p  
   JOIN SYS.USERS as u  
   on p.GRANTEE = u.user_name  
   WHERE p.GRANTEE_TYPE='USER'  
   AND p.OBJECT_TYPE = 'SYSTEMPRIVILEGE'  
   AND p.PRIVILEGE = 'TRACE ADMIN'  
   and not (p.grantee = 'SYSTEM'  
   or p.grantee like '_SYS_REPO')  
   and u.user_deactivated = 'FALSE'  
   and u.valid_from <= now()  
   AND (u.valid_until >= now() or u.valid_until is null)  
   ORDER BY OBJECT_TYPE, PRIVILEGE, GRANTEE
   ```

3. If you received a Service Questionnaire, remove all communicated users.

4. Update the tables with the identified user names.

5. Update the table in parent check HA137 with the number of users with this privilege.

**Rating**

**YELLOW** when privilege is granted to at least one user that has not been excluded.

**Note:**

See HANA_Security_MiniCheck ID 215S

**YELLOW** Estimated Risk - Medium

The system privilege TRACE ADMIN authorizes the configuration of traces such as the database trace and the SQL trace. Trace files may contain sensitive runtime information related to the system or business data that is otherwise protected by more specific authority checks. Tracing can also heavily impact the overall performance of a system.

At least one user with system privilege TRACE ADMIN has been identified in your system, which may not require this privilege for its expected tasks.

**Recommendation:**

Grant the TRACE ADMIN privilege only to a limited number of security-aware users that require this privilege as part of Root Cause Analysis tasks.
In many organizations, only system administrators and 2nd-level support have the TRACE ADMIN privilege, while ordinary support users are required to contact system administrators when they require specific trace information.

1.1.9.5.3 Users with role PUBLIC (HA138)

Purpose

Identify users with role PUBLIC. Users with this role have read access to sensitive information in SAP HANA System Views.

Procedure

1. As of SPS 12: Execute preconfigured SQL statements embedded into this report to identify the number of users assigned to an authorization:

   Identify the number of users with role PUBLIC and update the table in the report:

   ```
   SELECT p.ROLE_NAME, COUNT(DISTINCT p.GRANTEE)
   FROM SYS.EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
   AND p.ROLE_NAME = 'PUBLIC'
   /* AND p.ROLE_SCHEMA_NAME = '' */
   and not p.grantee = 'SYSTEM'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   group by role_name
   ```

   Get the list of users and roles with role PUBLIC:

   ```
   SELECT DISTINCT p.ROLE_NAME, p.GRANTEE, p.GRANTEE_TYPE
   FROM SYS.EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.ROLE_NAME = 'PUBLIC'
   /* AND p.ROLE_SCHEMA_NAME = '' */
   and not p.grantee = 'SYSTEM'
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   order by p.GRANTEE_TYPE
   ```

   IMPORTANT: The above statements are valid as of SAP HANA 2.0 SPS 1. For HANA 2.0 SPS 0 and HANA 1.0 SPS 12, remove the clause
   
   ```
   AND p.ROLE_SCHEMA_NAME = ''
   ```

   EFFECTIVE_ROLE_GRANTEES is not available for earlier releases. Use SQL statement HANA_Security_GrantedRolesAndPrivileges from SAP Note 1969700 to obtain the information. In the modification section of this SQL, replace '%' with the role name 'PUBLIC'.

   2. Update the table with the number of users.

   3. Update the tables with the identified user names.

   If the customer has not requested the list of user names, update only the table with role names and delete the table for the user names.

   4. Check whether identified user names correspond to users listed in the questionnaire.

Rating

YELLOW when at least 1 user is identified that is not listed in the questionnaire at all.
GREEN in all other cases.

Note:

See HANA_Security_MiniCheck ID 310S

YELLOW:

Estimated Risk: Users with role PUBLIC have read access to system views that contain sensitive information that might allow successful attacks to be performed on the system.
The system has been checked for users with role PUBLIC.
The following users are excluded from this check and all its subchecks:
1. All users specified in the Service Questionnaire
2. All users that have been created automatically as part of the SAP HANA deployment.

A list of automatically created users is included in the overview of HANA users (HA052) in the Users chapter of this report.

Note that for the role 'PUBLIC', those users that are created automatically with the deployment of SAP HANA are also excluded, since these internal users are created as Standard Users automatically, which have the role 'PUBLIC' by default.

**Recommendation:**
Review the listed users and revoke the privilege from all users who are not required to perform analysis or administration tasks in the system as part of their job.

For all users, consider replacing the standard role with authorizations that are tailored to those tables and views that are actually required for the user to perform the expected tasks. For example, it may not be appropriate to provide a Support User full read access for user and authorization data, configured authentication methods, or connect information stored in the SAP HANA database.

Documentation of all system views is available on SAP Help Portal, in the SAP HANA SQL and System View Reference Guide.

Note that the role is granted automatically when a user is created as a Standard User. As of SAP HANA 2.0, it is possible to reconfigure Standard Users as Restricted Users. The procedure is described in the SAP HANA Administration Guide.

### 1.1.9.6 Users with critical roles (HA062)

**Purpose**
To identify system privileges and roles assigned in the SAP HANA system that must not be granted to users in production systems.

**Procedure**
1. Perform the checks for each privilege and role.
2. Update this check with the results.

**Rating**
Automatic rating according to worst case rule.

**Note:**

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

The system has been checked for the number of users assigned to critical roles and authorizations. At least one critical role is granted to at least one user.

The table lists critical roles that are recommended to be assigned restrictively and the number of users that are assigned to them. The SYSTEM and _SYS_REPO users are excluded from the analysis.

**Recommendation:**
Review the users assigned to the listed critical roles carefully and minimize user authorizations where appropriate.

### 1.1.9.6.1 Users with critical role CONTENT_ADMIN (HA115)

**Purpose**
To identify users with role CONTENT_ADMIN. Users with this role have superuser authorization for working with information models in the repository of the SAP HANA database.

**Procedure**
1. As of SPS 12: Execute preconfigured SQL statements embedded into this report to identify the number of users assigned to an authorization:
Identify the number of users with role CONTENT_ADMIN and update the table in the report:

```sql
SELECT p.ROLE_NAME, COUNT(DISTINCT p.GRANTEE )
FROM SYS.EFFECTIVE_ROLE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE p.GRANTEE_TYPE='USER'
  AND p.ROLE_NAME = 'CONTENT_ADMIN'
/* AND p.ROLE_SCHEMA_NAME = '' */
  and not p.grantee = 'SYSTEM'
  and u.user_deactivated = 'FALSE'
  and u.valid_from <= now()
  and (u.valid_until >= now() or u.valid_until is null)
group by role_name
```

Get the list of users and roles with role CONTENT ADMIN:

```sql
SELECT DISTINCT p.ROLE_NAME, p.GRANTEE, p.GRANTEE_TYPE
FROM SYS.EFFECTIVE_ROLE_GRANTEES as p
JOIN SYS.USERS as u
on p.GRANTEE = u.user_name
WHERE  p.ROLE_NAME = 'CONTENT_ADMIN'
/* AND  p.ROLE_SCHEMA_NAME = '' */
  and not p.grantee = 'SYSTEM'
  and u.user_deactivated = 'FALSE'
  and u.valid_from <= now()
  and (u.valid_until >= now() or u.valid_until is null)
order by p.GRANTEE_TYPE
```

IMPORTANT: The above statements are valid as of SAP HANA 2.0 SPS 1. For HANA 2.0 SPS 0 and HANA 1.0 SPS 12, remove the clause
  AND  p.ROLE_SCHEMA_NAME = ''
EFFECTIVE_ROLE_GRANTEES is not available for earlier releases.
Use SQL statement HANA_Security_GrantedRolesAndPrivileges from SAP Note 1969700 to obtain the information. In the modification section of this SQL, replace '%' with the role name 'CONTENT_ADMIN'.

2. Update the table with number of users per privilege and role
3. Update the tables below with the identified user names and role names.
If the customer has not requested the list of user names, update only the table with role names and delete the table for the user names.
4. Check whether identified user names correspond to users listed in the questionnaire.

**Rating**

**YELLOW** when at least 1 user is identified that is not listed in the questionnaire.  
**GREEN** in all other cases.

**Note:**

See HANA_Security_MinCheck ID 310S

**YELLOW: Evaluated Risk - Medium**

The role CONTENT_ADMIN contains all privileges required for working with information models in the repository of the SAP HANA database.

Users that have not been mentioned as users who perform system updates have the CONTENT_ADMIN role in your SAP HANA system.

The user SYSTEM is not considered, because this user has the CONTENT_ADMIN role by design and the role cannot be revoked from this user.

**Recommendation:**

In productive systems, the role CONTENT_ADMIN must only be granted to the database user that performs system updates. This may include the schema user of your SAP system.

Do not grant this role to other users. Use it only as a template for creating a set of custom roles with appropriate segregation of duty.

Review the listed users and roles and remove the role CONTENT_ADMIN as far as possible.
1.1.9.6.2 Users with critical role MODELLING (HA116)

Purpose

Identify users with role MODELLING. The role MODELLING contains the predefined analytic privilege _SYS_BI_CP_ALL, which potentially allows a user to access all the data in activated views that are protected by XML-based analytic privileges, regardless of any other XML-based analytic privileges that apply.

Procedure

1. As of SPS 12: Execute preconfigured SQL statements embedded into this report to identify the number of users assigned to an authorization:

   ```sql
   SELECT p.ROLE_NAME, COUNT( DISTINCT p.GRANTEE )
   FROM SYS.EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.GRANTEE_TYPE='USER'
       AND p.ROLE_NAME = 'MODELING'
       /* AND p.ROLE_SCHEMA_NAME = '' */
       and not p.grantee = 'SYSTEM'
       and u.user_deactivated = 'FALSE'
       and u.valid_from <= now()
       and (u.valid_until >= now() or u.valid_until is null)
   group by role_name
   
   Get the list of users and roles with the role MODELLING:
   
   ```sql
   SELECT DISTINCT p.ROLE_NAME, p.GRANTEE, p.GRANTEE_TYPE
   FROM SYS.EFFECTIVE_ROLE_GRANTEES as p
   JOIN SYS.USERS as u
   on p.GRANTEE = u.user_name
   WHERE p.ROLE_NAME = 'MODELING'
       /* AND p.ROLE_SCHEMA_NAME = '' */
       and not p.grantee = 'SYSTEM'
       and u.user_deactivated = 'FALSE'
       and u.valid_from <= now()
       and (u.valid_until >= now() or u.valid_until is null)
   order by p.GRANTEE_TYPE
   
   IMPORTANT: The above statements are valid as of SAP HANA 2.0 SPS 1. For HANA 2.0 SPS 0 and HANA 1.0 SPS 12, remove the clause
       AND p.ROLE_SCHEMA_NAME = ''
   
   EFFECTIVE_ROLE_GRANTEES is not available for earlier releases.
   Use SQL statement HANA_Security_GrantedRolesAndPrivileges from SAP Note 1969700 to obtain the information. In the modification section of this SQL, replace '%' with the role name 'MODELING'.

2. Update the table with number of users per privilege and role

3. Update the tables below with the identified user names and role names.
   If the customer has not requested the list of user names, update only the table with role names and delete the table for the user names.

Rating

YELLOW when at least 1 user is identified.
GREEN in all other cases.

Note:

See HANA_Security_MiniCheck ID 311S

YELLOW Evaluated Risk - Medium

The role MODELLING contains the predefined analytic privilege _SYS_BI_CP_ALL, which potentially allows a user to access all the data in activated views that are protected by XML-based analytic privileges, regardless of any other XML-based analytic privileges that apply.

Users that have not been mentioned as users who perform system updates have the MODELLING role in your SAP HANA system.
The user SYSTEM is not considered, because this user has the MODELING role by design and the role cannot be revoked from this user.

**Recommendation:**

In productive systems, the role MODELING must not be granted to any database user. Use it only as a template for creating a set of custom roles with appropriate segregation of duty.

In some scenarios, the role MODELING is required for the Schema User of an SAP system. Review the listed users and roles and remove the role MODELING as much as possible.

**1.1.9.7 Users with directly granted privileges (HA050)**

**Purpose**

Privileges should only be granted via roles to enable an authorization management based on a need-to-know principle.

**Procedure**

1. Execute the following SQL:

   ```sql
   select p.grantee, count( * )
   from sys.granted_privileges as P
   join sys.users as u
   on p.GRANTEE = u.user_name
   where p.grantee_type = 'USER'
   and not (p.grantee like '_SYS%' or p.grantee = 'SYS' or p.grantee = 'SYSTEM')
   and u.user_deactivated = 'FALSE'
   and u.valid_from <= now()
   and (u.valid_until >= now() or u.valid_until is null)
   group by grantee
   order by count( * ) desc;
   ```

2. Count the number of users with COUNT > 1 (otherwise all standard users will be counted due to object authorization on own schema)

3. Copy a list of users with directly granted privileges into the table below.

**Rating**

- **YELLOW**: users with directly granted privileges exist
- **GREEN**: other cases

**YELLOW:**

At least one user is identified with directly assigned privileges.

Note: Normal database users are automatically granted an object privilege for their own database schema. This privilege is not taken into account in this check.

**Evaluated Risk - Medium**

Privileges, that are granted directly to a user, cannot easily be related to a specific role in the organization and the respective set of tasks. As a result, it is difficult to limit a user’s authorizations according to the need-to-know principle.

**Recommendation:**

Review the need for directly granted privileges and create a set of repository roles that reflects the affected tasks of your users.

Granting privileges by means of repository roles helps to keep control of the required privileges: If a user has diverse responsibilities, some privileges may be required in a different context. Without initially granting privileges multiple times via different roles it may be difficult to identify which privileges can be revoked if a user discontinues some of their responsibilities.

Check the table below for the identified user names.

**List of users with directly granted privileges**

The following table provides an overview of users with directly granted privileges: