PUBLIC

SAP HANA Platform 2.0 SPS 05

Document Version: 1.1 – 2021-07-09

**SAP HANA Security Checklists and**

**Recommendations**

©

2021 SAP SE or an SAP

affiliate

company. All rights reserved.

**THE BEST RUN**



**Content**

[1 SAP HANA Security Checklists and Recommendations 3](#_Toc52582)

[1.1 General Recommendations 3](#_Toc52583)

[1.2 Checklist for Secure Handover 4](#_Toc52584)

[2 SAP HANA Database Checklists and Recommendations 6](#_Toc52585)

[2.1 Recommendations for Database Users, Roles, and Privileges 6](#_Toc52586)

[2.2 Recommendations for Network Configuration 14](#_Toc52587)

[2.3 Recommendations for Data Encryption 18](#_Toc52588)

[2.4 Recommendations for File System and Operating System 20](#_Toc52589)

[2.5 Recommendations for Auditing 23](#_Toc52590)

[2.6 Recommendations for Trace and Dump Files 24](#_Toc52591)

[2.7 Recommendations for Tenant Database Management 26](#_Toc52592)

[3 SAP HANA XS, Advanced Model 28](#_Toc52593)

[3.1 Recommendations for XS Advanced Administration User 28](#_Toc52594)

[3.2 Recommendations for Organizations and Spaces 30](#_Toc52595)

[3.3 Recommendations for Network Configuration 31](#_Toc52596)

SAP HANA Security Checklists and Recommendations **Content**

# 1 SAP HANA Security Checklists and Recommendations

SAP HANA has many configuration settings that allow you to customize your system. Some of these settings are important for the security of your system, and misconfiguration could leave your system vulnerable.

The checklists offer recommendations and information about optimizing your security configuration to help you run your SAP HANA securely. However, please note the following:

* The checklists and recommendations offered here are not exhaustive.

In addition, depending on your specific implementation scenario and technical environment, some of the recommendations may not apply or be different.

* Do not use the checks as instructions on how to configure individual settings.

If a particular check result indicates an insecure setting, refer to the indicated documentation and follow the instructions there to change the configuration setting.

* This document does not replace the *SAP HANA Security Guide*, the central document for all information relating to the secure operation and configuration of SAP HANA.

To view the security checklist from SAP HANA cockpit, on the *Database Overview* page, with the *Security and User Management* or *All* view selected, choose the *Security Checklist* link on the *Security Related Links* card.

General Recommendations [page 3]

General recommendations for keeping SAP HANA secure.

Checklist for Secure Handover [page 4]

If you received your SAP HANA system pre-installed from a hardware or hosting partner, there are several things we strongly recommend you do immediately after handover.

**Related Information**

[SAP HANA Security Guide](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US)

## 1.1 General Recommendations

General recommendations for keeping SAP HANA secure.

* Create a security concept for the SAP HANA scenario that you want to implement as early as possible in your implementation project.
* Install SAP HANA revisions that are marked as security-relevant as soon as possible. Do this by checking SAP HANA security notes either directly, or using services provided by SAP Support.

For more information, see *SAP HANA Security Patches* in the *SAP HANA Security Guide*.

SAP HANA Security Checklists and Recommendations

**SAP HANA Security Checklists and Recommendations**

**Related Information**

[SAP HANA Security Patches](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/9abf4ef5267a400781b1b43c32914f3a.html)

## 1.2 Checklist for Secure Handover

If you received your SAP HANA system pre-installed from a hardware or hosting partner, there are several things we strongly recommend you do immediately after handover.

* Change the password of all operating system users, in particular the following:

○ <sid>adm

○ root

○ sapadm

For more information, see your operating system documentation.

* In all databases, review all database users created by the installing party, and delete or deactivate those that are not needed in your scenario.

####  Remember

If you received a system with tenant databases, make sure to do this in all tenant databases and in the system database.

For more information about database users that are created in the SAP HANA database by default, see the *SAP HANA Security Guide*.

● In all databases, change the password of all predefined database users, in particular the password of the database user SYSTEM. In addition, deactivate the SYSTEM user. For more information, see the *SAP HANA Security Guide*.

####  Remember

If you received a system with tenant databases, make sure to do this in all tenant databases and in the system database.

####  Note

Predefined internal technical users (SYS, \_SYS\_\* users) are permanently deactivated and cannot be used to log on. It is not possible to change the password of these users.

* Change the following encryption master keys:

○ Instance secure store in the file system (SSFS)

○ System public key infrastructure (PKI) SSFS

For more information about how to change the encryption master keys, see *SAP Note 2183624 (Potential information leakage using default SSFS master key in HANA)* and the *SAP HANA Administration Guide*.

* Re-create the system public key infrastructure (PKI) used to protect internal communication in order to create new certificates and private keys. You can trigger this by deleting the system PKI SSFS. Alternatively, you can use SAPControl to reset the system PKI with the methods UpdateSystemPKI[<force>] and UpdateInstancePSE[<force>].

SAP HANA Security Checklists and Recommendations **SAP HANA Security Checklists and Recommendations**

####  Note

In a system replication landscape, you must copy the system PKI SSFS data file and key file from the primary system to the same location on the secondary system(s). For more information, see the section on secure internal communication in the *SAP HANA Security Guide*.

#### Related Information

[Deactivate the SYSTEM User](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/c511ddf1767947f0adfc9636148718d9.html)

[Change a Database User](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/626d5b70e24642b58a0a7828689cb375.html) [Change the SSFS Master Keys](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/581593c48739431caaccc3d2ef55c23f.html)

[SAP Control WebService](http://help.sap.com/disclaimer?site=http%3A%2F%2Fscn.sap.com%2Fdocs%2FDOC-14382)Information published on SAP site

[Secure Internal Communication Between Sites in System Replication Scenarios](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/9a2f4243a9ad48ae9fe77c65e51c276f.html) [SAP Note 2183624](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2183624)Information published on SAP site

SAP HANA Security Checklists and Recommendations

**SAP HANA Security Checklists and Recommendations**

# 2 SAP HANA Database Checklists and Recommendations

Checklists and recommendations to help you operate and configure the SAP HANA database securely

|  |
| --- |
|  Tip  SAP Note [1969700](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/1969700) contains collections of useful SQL statements for monitoring and analyzing the SAP  HANA database. The statements contained in the file HANA\_Security\_MiniChecks.txt perform all of the SQL-based checks listed in this documentation. |
|

Recommendations for Database Users, Roles, and Privileges [page 6] Recommendations for securing access to SAP HANA.

Recommendations for Network Configuration [page 14]

Recommendations for integrating SAP HANA securely into your network environment.

Recommendations for Data Encryption [page 18]

Recommendations for data encryption and encryption key management

Recommendations for File System and Operating System [page 20]

Recommendations for secure operating system access and data storage in the file system

Recommendations for Auditing [page 23]

Recommendations for audit configuration

Recommendations for Trace and Dump Files [page 24]

Recommendations for handling trace and dump files

Recommendations for Tenant Database Management [page 26]

Recommendations for securely configuring tenant databases

## 2.1 Recommendations for Database Users, Roles, and Privileges

Recommendations for securing access to SAP HANA.

#### SYSTEM User

Default The database user SYSTEM is the most powerful database user with irrevocable system privileges. The SYSTEM user is active after database creation.

Recommendation Use SYSTEM to create database users with the minimum privilege set required for their duties (for example, user administration, system administration). Then deactivate SYSTEM. You may however temporarily reactivate the SYSTEM user for emergency or bootstrapping tasks. See *Deactivate the SYSTEM User* in the *SAP HANA Security Guide*.

#####  Note

The SYSTEM user is not required to update the SAP HANA database system; a lesserprivileged user can be created for this purpose. However, to upgrade SAP support package stacks, SAP enhancement packages and SAP systems using the Software Update Manager (SUM) and to install, migrate, and provision SAP systems using the Software Provisioning Manager (SWPM), the SYSTEM user is required and needs to be temporarily reactivated for the duration of the upgrade, installation, migration or provisioning.

|  |  |
| --- | --- |
| How to Verify | In the system view USERS, check the values in columns USER\_DEACTIVATED,  DEACTIVATION\_TIME, and LAST\_SUCCESSFUL\_CONNECT for the user SYSTEM. |
| Related Alert | No |
| More Information | See the sections on predefined users and deactivating the SYSTEM user in the *SAP HANA Security Guide*. |

|  |  |
| --- | --- |
| Default | With the exception of internal technical users (\_SYS\_\* users), the default password policy limits the lifetime of user passwords to 182 days (6 months). |
| Recommendation | Do not disable the password lifetime check for database users that correspond to real people. |

#### Password Lifetime of Database Users

In 3-tier scenarios with an application server, only technical user accounts for the database connection of the application server should have a password with an unlimited lifetime (for

example, SAP<sid> or DBACOCKPIT).

#####  Note

Such technical users should have a clearly identified purpose and the minimum authorization required in SAP HANA.

|  |  |
| --- | --- |
| How to Verify | In the USERS system view, check the value in the column  IS\_PASSWORD\_LIFETIME\_CHECK\_ENABLED. If it is FALSE, the password lifetime check is disabled.  The time of the last password change is indicated in the column LAST\_PASSWORD\_CHANGE\_TIME. |
| Related Alert | No |
| More Information | See the section on the password policy in the *SAP HANA Security Guide*. |

|  |  |
| --- | --- |
| Default | System privileges authorize database-wide administration commands. The users SYSTEM and \_SYS\_REPO have all these privileges by default. |
| Recommendation | System privileges should only ever be granted to users that actually need them. |

#### System Privileges

In addition, several system privileges grant powerful permissions, for example, the ability to delete data and to view data unfiltered and should be granted with extra care as follows:

Only administrative or support users should have the following system privileges in a production database:

* CATALOG READ
* TRACE ADMIN

In a database of any usage type, the following system privileges should be granted only to administrative users who actually need them:

* 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
* WORKLOAD \* ADMIN

How to Verify To check which user has a particular system privilege, query the EFFECTIVE\_PRIVILEGE\_GRANTEES system view, for example:

##### SELECT \* FROM EFFECTIVE\_PRIVILEGE\_GRANTEES WHERE OBJECT\_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'SSL ADMIN' AND GRANTEE

NOT IN ('SYSTEM','\_SYS\_REPO');

|  |  |
| --- | --- |
| Related Alert | No |
| More Information | See the section on system privileges in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. |

#### System Privileges: Critical Combinations

Default The users SYSTEM and \_SYS\_REPO have all system privileges by default.

|  |  |
| --- | --- |
| Recommendation | Critical combinations of system privileges should not be granted together, for example:   * USER ADMIN and ROLE ADMIN * CREATE SCENARIO and SCENARIO ADMIN * AUDIT ADMIN and AUDIT OPERATOR * CREATE STRUCTURED PRIVILEGE and STRUCTUREDPRIVILEGE ADMIN |
| How to Verify | To check a user's privileges, query the EFFECTIVE\_PRIVILEGES system view, for example:  SELECT \* FROM "PUBLIC"."EFFECTIVE\_PRIVILEGES" WHERE USER\_NAME  = '<USER\_NAME>'; |
| Related Alert | No |
| More Information | See the section on system privileges in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. |

#### System Privilege: DATA ADMIN

Default The system privilege DATA ADMIN is a powerful privilege. It authorizes a user to execute all data definition language (DDL) commands in the SAP HANA database. Only the users SYSTEM and \_SYS\_REPO have this privilege by default.

|  |  |
| --- | --- |
| Recommendation | No user or role in a production database should have this privilege. |
| How to Verify | You can verify whether a user or role has the DATA ADMIN privilege by executing the statement:  SELECT \* FROM EFFECTIVE\_PRIVILEGE\_GRANTEES WHERE OBJECT\_TYPE  = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'DATA ADMIN' AND GRANTEE  NOT IN ('SYSTEM','\_SYS\_REPO'); |
| Related Alert | No |

More Information See the section on system privileges in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. See also SAP Note 2950209.

#### System Privilege: DEVELOPMENT

Default The system privilege DEVELOPMENT authorizes some internal ALTER SYSTEM commands.

By default, only the users SYSTEM and \_SYS\_REPO have this privilege.

|  |  |
| --- | --- |
| Recommendation | No user or role in a production database should have this privilege. |
| How to Verify | You can verify whether a user or role has the DEVELOPMENT privilege by executing the statement:  SELECT \* FROM EFFECTIVE\_PRIVILEGE\_GRANTEES WHERE OBJECT\_TYPE = 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'DEVELOPMENT' AND GRANTEE  NOT IN ('SYSTEM','\_SYS\_REPO'); |
| Related Alert | No |
| More Information | If requested by SAP HANA support, this privilege can be granted using SQL. It is not included in the privilege handling overview in the SAP HANA Security Guide.  See the section *System Views for Verifying Users' Authorization* in the *SAP HANA Administration Guide*. |

#### Analytic Privilege: \_SYS\_BI\_CP\_ALL

Default The predefined analytic privilege \_SYS\_BI\_CP\_ALL 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.

Only the predefined roles CONTENT ADMIN and MODELING have the analytic privilege \_SYS\_BI\_CP\_ALL by default. By default, only the user SYSTEM has these roles.

|  |  |
| --- | --- |
| Recommendation | Do not grant this privilege to any user or role in a production database. |
| How to Verify | You can verify whether a user or role has the \_SYS\_BI\_CP\_ALL privilege by executing the statement:  SELECT \* FROM EFFECTIVE\_PRIVILEGE\_GRANTEES WHERE OBJECT\_TYPE  = 'ANALYTICALPRIVILEGE' AND OBJECT\_NAME = '\_SYS\_BI\_CP\_ALL'  AND PRIVILEGE = 'EXECUTE' AND GRANTEE NOT IN  ('SYSTEM','MODELING', 'CONTENT\_ADMIN'); |
| Related Alert | No |

More Information See the sections on privileges and predefined database roles in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*.

|  |  |
| --- | --- |
| **Debug Privileges**  Default | No user has debug privileges |
| Recommendation | The privileges DEBUG and ATTACH DEBUGGER should not be assigned to any user for any object in production systems. |
| How to Verify | You can verify whether a user or role has debug privileges by executing the statements:  SELECT \* FROM GRANTED\_PRIVILEGES WHERE PRIVILEGE='DEBUG' OR  PRIVILEGE='ATTACH DEBUGGER'; |
| Related Alert | No |
| More Information | See the section on privileges in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. |

#### Predefined Catalog Role CONTENT\_ADMIN

Default The role CONTENT\_ADMIN contains all privileges required for working with information models in the repository of the SAP HANA database.

The user SYSTEM has the role CONTENT\_ADMIN by default.

|  |  |
| --- | --- |
| Recommendation | Only the database user used to perform system updates should have the role  CONTENT\_ADMIN. Otherwise do not grant this role to users, particularly in production databases. It should be used as a role template only. |
| How to Verify | You can verify whether a user or role has the CONTENT\_ADMIN role by executing the statement:  SELECT \* FROM GRANTED\_ROLES WHERE ROLE\_NAME = 'CONTENT\_ADMIN'  AND GRANTEE NOT IN ('SYSTEM'); |
| Related Alert | No |
| More Information | See the section on predefined database roles in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. |

#### Predefined Catalog Role MODELING

Default The role MODELING contains the predefined analytic privilege \_SYS\_BI\_CP\_ALL, which po­

tentially allows a user to access all the data in activated views that are protected by XMLbased analytic privileges, regardless of any other XML-based analytic privileges that apply.

The user SYSTEM has the role MODELING by default.

|  |  |
| --- | --- |
| Recommendation | Do not grant this role to users, particularly in production databases. It should be used as a role template only. |
| How to Verify | You can verify whether a user or role has the MODELING role by executing the statement:  SELECT \* FROM GRANTED\_ROLES WHERE ROLE\_NAME ='MODELING' AND  GRANTEE NOT IN ('SYSTEM'); |
| Related Alert | No |
| More Information | See the section on predefined database roles in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. |

#### Predefined Catalog Role SAP\_INTERNAL\_HANA\_SUPPORT

Default The role SAP\_INTERNAL\_HANA\_SUPPORT contains system privileges and object privileges that allow access to certain low-level internal system views needed by SAP HANA development support in support situations.

No user has the role SAP\_INTERNAL\_HANA\_SUPPORT by default.

|  |  |
| --- | --- |
| Recommendation | This role should only be granted to SAP HANA development support users for their support activities. |
| How to Verify | You can verify whether a user or role has the SAP\_INTERNAL\_HANA\_SUPPORT role by executing the statement:  SELECT \* FROM EFFECTIVE\_ROLE\_GRANTEES WHERE ROLE\_NAME =  'SAP\_INTERNAL\_HANA\_SUPPORT'; |
| Related Alert | ID 63 (Granting of SAP\_INTERNAL\_HANA\_SUPPORT role) |
| More Information | See the section on predefined database roles in the *SAP HANA Security Guide* and the section on system views for verifying user authorization in the *SAP HANA Administration Guide*. |

#### Predefined Repository Roles

Default SAP HANA is delivered with a set of preinstalled software components implemented as SAP

HANA Web applications, libraries, and configuration data. The privileges required to use these components are contained within repository roles delivered with the component itself.

The standard user \_SYS\_REPO automatically has all of these roles. Some may also be granted automatically to the standard user SYSTEM to enable tools such as the SAP HANA cockpit to be used immediately after installation.

|  |  |
| --- | --- |
| Recommendation | As repository roles can change when a new version of the package is deployed, either do not use them directly but instead as a template for creating your own roles, or have a regular review process in place to verify that they still contain only privileges that are in line with your organization's security policy.  Furthermore, if repository package privileges are granted by a role, we recommend that these privileges be restricted to your organization’s packages rather than the complete repository. Therefore, for each package privilege (REPO.\*) that occurs in a role template and is granted on .REPO\_PACKAGE\_ROOT, check whether the privilege can and should be granted to a single package or a small number of specific packages rather than the full repository. |
| How to Verify | To verify whether a user or role has a particular role, execute the following statement, for example:  SELECT \* FROM EFFECTIVE\_ROLE\_GRANTEES WHERE ROLE\_NAME  ='sap.hana.xs.admin.roles::HTTPDestAdministrator'; |
| Related Alert | No |

More Information For a list of all roles delivered with each component, see *SAP HANA Security Reference*

*Information Components Delivered as SAP HANA Content*  in the *SAP HANA Security Guide*.



|  |  |
| --- | --- |
| Default | The CLIENT user parameter can be used to authorize named users in SAP HANA. Only a user with the USER ADMIN system privilege can change the value of the CLIENT parameter already assigned to other users. However, at runtime, any user can assign an arbitrary value to the CLIENT parameter either by setting the corresponding session variable or passing the parameter via placeholder in a query. While this is the desired behavior for technical users that work with multiple clients such as SAP Business Warehouse, S/4 HANA, or SAP Business Suite, it is problematic in named user scenarios if the CLIENT parameter is used to authorize access to data and not only to perform data filtering. |
| Recommendation | Prevent named users from changing the CLIENT user parameter themselves but allow technical users to do so in their sessions and/or queries. |

#### User Parameter CLIENT

How to Verify To verify that users are generally not permitted to change the CLIENT user parameter, en­

sure that the parameter [authorization] secure\_client\_parameter in the global.ini file is set to true:

##### SELECT \* FROM "M\_INIFILE\_CONTENTS" WHERE

KEY='SECURE\_CLIENT\_PARAMETER';

To verify that only permitted roles or users can change the CLIENT user parameter, execute the following statement:

SELECT \* FROM EFFECTIVE\_PRIVILEGE\_GRANTEES WHERE OBJECT\_TYPE

= 'SYSTEMPRIVILEGE' AND PRIVILEGE = 'CLIENT PARAMETER ADMIN';

|  |  |
| --- | --- |
| Related Alert | No |
| More Information | See *SAP Note 2582162 (How to Restrict Use of the CLIENT Parameter)* and the section on authorization in the *SAP HANA Administration Guide*. |

#### Related Information

[Predefined Users](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/de4ee8bbbb5710148a04f023da147c8d.html)

[Deactivate the SYSTEM User](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/c511ddf1767947f0adfc9636148718d9.html)

[Password Policy](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/dce2826dbb571014be628d6279aeeaa3.html)

[System Privileges](https://help.sap.com/viewer/b3d0daf2a98e49ada00bf31b7ca7a42e/LATEST/en-US/cadbcfc38b084808b80b3551b1cd756e.html)

[System Views for Verifying Users' Authorization](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/ddae823e3b27477ea4c949607eebc435.html)

[Predefined Database (Catalog) Roles](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/de421861bb571014846288086be76719.html)

[Predefined Repository Roles](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/1f75daedd55a46068230797ccd0c97f7.html)

[Components Delivered as SAP HANA Content](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/f5929583207c4881ba6f8c924cfaa221.html)

[Restrict Use of the CLIENT User Parameter](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/91af0e7d50a14936a388618974ef8dc1.html)

[SAP Note 2582162](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2582162)Information published on SAP site

[System Views for Verifying Users' Authorization](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/ddae823e3b27477ea4c949607eebc435.html)

[SAP Note 2950209](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2950209)Information published on SAP site

## 2.2 Recommendations for Network Configuration

Recommendations for integrating SAP HANA securely into your network environment.

**General Recommendations**

For general recommendations, please read the section on network security in the *SAP HANA Security Guide*.

#### Open Ports

Default During installation, ports such as SQL 3<instance\_no>15 and HTTP 80<instance\_no> are opened by default.

|  |  |
| --- | --- |
| Recommendation | Only ports that are needed for running your SAP HANA scenario should be open. For a list of required ports, see the *SAP HANA Administration Guide*. |
| How to Verify | Verify opened ports at operating system level using Linux commands such as netcat or netstat. |
| Related Alert | No |
| More Information | See the section on communication channel security in the *SAP HANA Security Guide* and the section on ports and connections in the *SAP HANA Administration Guide*. |

#### Internal Host Name Resolution in Single-Host System

Default SAP HANA services use IP addresses to communicate with each other. Host names are mapped to these IP addresses through internal host name resolution, a technique by which the use of specific and/or fast networks can be enforced and communication restricted to a specific network. In single-host systems, SAP HANA services listen on the loopback interface only (IP address 127.0.0.1).

In global.ini files, the [communication] listeninterface is set to **.local**.

|  |  |
| --- | --- |
| Recommendation | Do not change the default setting. |
| How to Verify | Using SAP HANA cockpit, check which ports are listening.  This information is available in the *Network Security Information* app in the *SAP HANA Security Overview* catalog. The value of the *Listening On* field should be *Local Network*.  Alternatively, execute the following SQL statement:  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE SECTION =  'communication' AND KEY = 'listeninterface'; |
| Related Alert | No |
| More Information | See the section about ports and connections in the *SAP HANA Administration Guide*. |

#### Internal Host Name Resolution in Multiple-Host System

Default In a distributed scenario with multiple hosts, the network needs to be configured so that inter-service communication is operational throughout the entire landscape. The default configuration depends on how you installed your system.

Recommendation Multiple-host systems can run with or without a separate network definition for inter-service communication. The recommended setting depends accordingly:

* If a separate network is configured for internal communication, the parameter [communication] listeninterface should be set to **.internal**. In addi­

tion, you should add key-value pairs for the IP addresses of the network adapters used for SAP HANA internal communication in the [communication] internal\_hostname\_resolution section.

* If a separate network is not configured for internal communication, the parameter [communication] listeninterface should be set to **.global**. This setting exposes internal SAP HANA service ports, so it is strongly recommended that you secure internal SAP HANA ports with an additional firewall.

#####  Note

Communication properties are in the default configuration change blocklist (multidb.ini). This means that they cannot initially be changed in tenant databases. They must be changed from the system database. If appropriate for your scenario, you can remove these properties from the change blocklist. SAP HANA deployment scenarios are described in the *SAP HANA Master Guide*. For more information about how to edit the change blocklist, see the *SAP HANA Administration Guide*.

|  |  |
| --- | --- |
| How to Verify | Check which ports are listening using the SAP HANA cockpit.  This information is available in the *Network Security Information* app in the *SAP HANA Security Overview* catalog. The value of the *Listening On* field should be *Global Network* or *Internal Network*.  Alternatively, execute the following SQL statements:  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE SECTION =  'communication' AND KEY = 'listeninterface';  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE SECTION =  'internal\_hostname\_resolution'; |
| Related Alert | 86 (Internal communication is configured too openly) |
| More Information | See the section on internal hostname resolution in the *SAP HANA Administration Guide*. |

#### Host Name Resolution in System Replication

Default The parameter [system\_replication\_communication] listeninterface

parameter is set to **.global**.

Recommendation The recommended setting depends on whether or not a separate network is defined for internal communication:

* If a separate internal network channel is configured for system replication, the param­

eter [system\_replication\_communication] listeninterface parameter should be **.internal**. You also need to add key-value pairs for the IP addresses of the network adapters for the system replication in the

[system\_replication\_hostname\_resolution] section.

* If a separate network is not configured for system replication, the parameter

[system\_replication\_communication] listeninterface should be

set to **.global**. However, in this case, it is important to secure communication using TSL/SSL and/or to protect the SAP HANA landscape with a firewall. In the

[system\_replication\_hostname\_resolution] section, add entries for all

hosts of neighboring sites (at a minimum) or all hosts of own site as well as for all hosts of neighboring sites. In addition, set the parameter

[system\_replication\_communication] allowed\_sender to restrict

possible communication to specific hosts. The parameter value must contain a list of the foreign hosts that are part of the SAP HANA system replication landscape.

#####  Note

Communication properties are in the default configuration change blocklist (multidb.ini). This means that they cannot initially be changed in tenant databases. They must be changed from the system database. If appropriate for your scenario, you can remove these properties from the change blocklist. SAP HANA deployment scenarios are described in the *SAP HANA Master Guide*. For more information about how to edit the change blocklist, see the *SAP HANA Administration Guide*.

|  |  |
| --- | --- |
| How to Verify | To check the value of the above parameters, execute the following statements:  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE SECTION =  'system\_replication\_communication' AND KEY =  'listeninterface';  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE SECTION =  'system\_replication\_communication' AND KEY =  'internal\_hostname\_resolution';  SELECT \* FROM "PUBLIC". "M\_INIFILE\_CONTENTS"WHERE SECTION = 'system\_replication\_communication' AND KEY =  'allowed\_sender'; |
| Related Alert | No |
| More Information | See the section on hostname resolution for system replication in the *SAP HANA Administration Guide*. |

#### Related Information

[Communication Channels](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/dbbe3e28bb571014ad62c73d8bac100b.html)

[Network Security](https://help.sap.com/viewer/4e9b18c116aa42fc84c7dbfd02111aba/LATEST/en-US/335deb08092e4c60b5c159e7983aec7c.html)

[Ports and Connections](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/a9326f20b39342a7bc3d08acb8ffc68a.html)

[Internal Host Name Resolution](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/3fd4912896284029931997903c75d956.html)

[Host Name Resolution for System Replication](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/c0cba1cb2ba34ec89f45b48b2157ec7b.html)

## 2.3 Recommendations for Data Encryption

Recommendations for data encryption and encryption key management

#### Instance SSFS Master Key

Default The instance secure store in the file system (SSFS) protects internal root keys in the file system. A unique master key is generated for the instance SSFS in every installation.

|  |  |
| --- | --- |
| Recommendation | If you received your system pre-installed from a hardware or hosting partner, we recommend that you change the master key of the instance SSFS immediately after handover to ensure that it is not known outside of your organization. |
| How to Verify | Using SAP HANA cockpit, check the change date of the master key.  This information is available in SAP HANA cockpit on the resource overview page. |
| Related Alert | 84 (Insecure instance SSF encryption configuration) |
| More Information | See the section on server-side data encryption in the *SAP HANA Security Guide* and the section on changing the SSFS master keys in the *SAP HANA Administration Guide*. |

#### System PKI SSFS Master Key

Default The system public key infrastructure (PKI) SSFS protects the X.509 certificate infrastructure that is used to secure internal TLS/SSL-based communication. A unique master key is generated for the system PKI SSFS in every installation.

|  |  |
| --- | --- |
| Recommendation | If you received your system pre-installed from a hardware or hosting partner, we recommend that you change the master key of the instance SSFS immediately after handover to ensure that it is not known outside of your organization. |
| How to Verify | Check the change date of the master key in the SAP HANA cockpit.  This information is available in the SAP HANA cockpit on the resource overview page. |
| Related Alert | 84 (Insecure instance SSF encryption configuration) |
| More Information | See the section on server-side data encryption in the *SAP HANA Security Guide* and the section on changing the SSFS master keys in the *SAP HANA Administration Guide*. |

#### Root Encryption Keys

Default SAP HANA features the following data encryption services:

* Data volume encryption
* Redo log encryption
* Data and log backup encryption
* An internal encryption service available to applications requiring data encryption Unique root keys are generated for all services in every database.

|  |  |
| --- | --- |
| Recommendation | If you received your system pre-installed from a hardware or hosting partner, we recommend that you change all root keys immediately after handover to ensure that they are not known outside of your organization. |
| How to Verify | Query system view ENCRYPTION\_ROOT\_KEYS. |
| Related Alert | No |
| More Information | See the sections on server-side data encryption in the *SAP HANA Security Guide* and the *SAP HANA Administration Guide*. |

#### Encryption Key of the SAP HANA Secure User Store (hdbuserstore)

Default The secure user store (hdbuserstore) is a tool installed with the SAP HANA client. It is used to store SAP HANA connection information, including user passwords, securely on clients.

Information contained in the SAP HANA secure user store is encrypted using a unique encryption key.

|  |  |
| --- | --- |
| Recommendation | If you are using the current version of the SAP HANA client, there is no need to change the encryption key of the secure user store. However, if you are using an older version of the SAP HANA client, we recommend changing the encryption key after installation of the SAP HANA client. |
| How to Verify | You know the encryption has been changed if the file SSFS\_HDB.KEY exists in the directory where the SAP HANA client is installed. |
| Related Alert | No |
| More Information | See the sections on hdbuserstore in the *SAP HANA Security Guide* and *SAP HANA Administration Guide*, as well as SAP Note 2210637. |

|  |  |
| --- | --- |
| Default | Data and log volume encryption are not enabled |
| Recommendation | We recommend that you enable data and log volume encryption immediately after installation or handover from your hardware or hosting partner, and after you have changed the root encryption keys for both services. |

#### Data and Log Volume Encryption

How to Verify Execute the following statement:

##### SELECT \* FROM M\_ENCRYPTION\_OVERVIEW WHERE SCOPE='LOG' OR

SCOPE = 'PERSISTENCE'

|  |  |
| --- | --- |
| Related Alert | No |
| More Information | See the section on data and log volume encryption in the *SAP HANA Security Guide* and the section on enabling encryption of data and log volumes in the *SAP HANA Administration Guide*. |

#### Related Information

[Server-Side Data Encryption Services](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/b30fda1483b34628802a8d62bd5d39df.html)

[Change the SSFS Master Keys](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/581593c48739431caaccc3d2ef55c23f.html)

[Change the Secure User Store Encryption Key](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/3a6e4636bb7e49b69178efe2eae365f6.html)

[Changing Encryption Root Keys](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/acbd74a41ea344f29e4aa5ebc57303a1.html)

[Secure User Store (hdbuserstore)](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/dd95ac9dbb571014a7d7f0234d762fdb.html)

[SAP Note 2210637](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2210637)Information published on SAP site

[Data and Log Volume Encryption](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/dc01f36fbb5710148b668201a6e95cf2.html)

[Enabling Encryption of Data and Log Volumes](https://help.sap.com/viewer/afa922439b204e9caf22c78b6b69e4f2/2.12.0.0/en-US/2ca763d3bd7d4cc187a6737ecc3cb396.html)

## 2.4 Recommendations for File System and Operating System

Recommendations for secure operating system access and data storage in the file system

#### General Recommendation

Stay up to date on security recommendations available for your operating system and consider them in the context of your implementation scenario and security policy.

See also the following SAP Notes:

* SAP Note 1944799 (SUSE Linux Enterprise Server 11.x for SAP Applications)
* SAP Note 2009879 (Red Hat Enterprise Linux (RHEL) 6.x)

#### Operating System Users

Default Only operating system (OS) users that are needed for operating SAP HANA exist on the SAP HANA system, that is:

* sapadm (required to authenticate to SAP Host Agent)
* <sid>adm (required by the SAP HANA database)
* Dedicated OS users for every tenant database if the system is configured for high isolation

#####  Note

There may be additional OS users that were installed by the hardware vendor. Check with your vendor.

|  |  |
| --- | --- |
| Recommendation | Ensure that no additional unnecessary users exist. |
| How to Verify | Refer to your operating system documentation |
| Related Alert | No |
| More Information | See the section on predefned users in the *SAP HANA Security Guide*. |

#### OS File System Permissions

Default The access permission of files exported to the SAP HANA server can be configured using

the [import\_export] file\_security parameter in the indexserver.ini configuration file. The default permission set is 640 ([import\_export] file\_security=medium).

|  |  |  |
| --- | --- | --- |
| Recommendation | Do not change default access permission of exported files. In addition, ensure that only a limited number of database users have the system privilege IMPORT and EXPORT. | |
| How to Verify | ● | You can verify the parameter setting by executing the command:  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE  SECTION = 'import\_export' AND KEY = 'file\_security'; |
|  | ● | You can verify which users or roles have the IMPORT or EXPORT privilege by executing the statement:  SELECT \* FROM EFFECTIVE\_PRIVILEGE\_GRANTEES WHERE (OBJECT\_TYPE = 'SYSTEMPRIVILEGE') AND (PRIVILEGE =  'EXPORT' OR PRIVILEGE='IMPORT'); |
|  | ● | You can verify the permissions of directories in the file system using the SAP HANA database lifecycle manager (HDBLCM) resident program with installation parameter check\_installation. |
| Related Alert | No |  |
| More Information | See the section on checking the installation of an SAP HANA system using the SAP HANA database lifecycle manager (HDBLCM) in the SAP HANA Administration Guide, as well as SAP Note 2252941. | |

#### OS Security Patches

Default OS security patches are not installed by default

|  |  |
| --- | --- |
| Recommendation | Install OS security patches for your operating system as soon as they become available. If a security patch impacts SAP HANA operation, SAP will publish an SAP Note where this fact is stated. It is up to you to decide whether to install such patches. |
| How to Verify | Refer to your operating system documentation |
| Related Alert | No |
| More Information | * SAP Note 1944799 (SUSE Linux Enterprise Server 11.x for SAP Applications) * SAP Note 2009879 (Red Hat Enterprise Linux (RHEL) 6.x) |

#### OS sudo Configuration

Default Users have to either specify the root password or be part of a dedicated user group to be able to run arbitrary commands as root.

|  |  |
| --- | --- |
| Recommendation | Do not change your sudo configuration to allow users such as <sid>adm to use sudo to run arbitrary commands as root without specifying the root password. |
| How to Verify | Check the /etc/sudoers file. The specific configuration may vary with your Linux distribution, but configuration options to look for are:   * Defaults targetpw   This setting requires the root password to be provided when running sudo in general.   * ALL ALL=(ALL) ALL   This should only be used if Defaults targetpw is also set.  If you use the storage connector option to mount SAP HANA volumes, during SAP HANA installation your sudo configuration is modified to allow <sid>adm to run a dedicated set of commands as root, such as:  <sid>adm ALL=NOPASSWD: /sbin/multipath,/sbin/multipathd,/etc/ init.d/multipathd,/usr/bin/sg\_persist,/bin/mount [...]  This is intentional and does not pose a security risk. However, <sid>adm should not be able to run arbitrary commands as root without proper authentication. |
| Related Alert | No |
| More Information | See the sudo and sudoers documentation (man 8 sudo, man 5 sudoers) |

#### Related Information

[Predefined Users](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/de4ee8bbbb5710148a04f023da147c8d.html)

[Check the Installation Using the Command-Line Interface](https://help.sap.com/viewer/2c1988d620e04368aa4103bf26f17727/LATEST/en-US/3d1b1608d7334ff08ace1fafd42f3a03.html)

[Secure User Store (hdbuserstore)](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/dd95ac9dbb571014a7d7f0234d762fdb.html)

[SAP Note 2252941](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2252941) Information published on SAP site[SAP Note 1944799](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/1944799)Information published on SAP site

[SAP Note 2009879](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2009879)Information published on SAP site

## 2.5 Recommendations for Auditing

Recommendations for audit configuration

#### Auditing

Default Auditing is disabled by default.

|  |  |
| --- | --- |
| Recommendation | Verify whether auditing is required by your security concept, for example to fulfill specific compliance and regulatory requirements. |
| How to Verify | Check the status of auditing in the SAP HANA cockpit  This information is available on the *Auditing* card of the *SAP HANA Security Overview* catalog.  Alternatively, you can execute the following statement:  SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE SECTION =  'auditing configuration' AND KEY = 'global\_auditing\_state'; |
| Related Alert | No |
| More Information | See the sections on auditing in the *SAP HANA Security Guide* and the *SAP HANA Administration Guide*. |

#### Audit Trail Target: syslog

Default The default audit trail target is syslog (SYSLOGPROTOCOL) for the system database

|  |  |
| --- | --- |
| Recommendation | If you are using syslog, ensure that it is installed and configured according to your requirements (for example, for writing the audit trail to a remote server). |
| How to Verify | Refer to your operating system documentation |
| Related Alert | No |
| More Information | See the section on audit trails in the *SAP HANA Security Guide* and your operating system documentation. |

#### Audit Trail Target: CSV Text File

Default The audit trail target CSV text file (CSVTEXTFILE) is not configured by default

|  |  |
| --- | --- |
| Recommendation | Do not configure CSV text file (CSVTEXTFILE) as an audit trail target in a production system as it has severe restrictions. |
| How to Verify | Check the configured audit trail targets in the *Auditing* of the SAP HANA cockpit Alternatively, execute the following statements:   * SELECT \* FROM "PUBLIC" . "M\_INIFILE\_CONTENTS" WHERE   SECTION = 'auditing configuration' AND VALUE =  'CSVTEXTFILE';   * SELECT \* FROM "PUBLIC"."AUDIT\_POLICIES" WHERE   TRAIL\_TYPE='CSV'; |
| Related Alert | No |
| More Information | See the section on audit trails in the *SAP HANA Security Guide*. |

#### Related Information

[Auditing Activity in SAP HANA](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/ddcb6ed2bb5710148183db80e4aca49b.html)

[Audit Trails](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/db560e7bbb57101490d4a1364440077f.html)

[Auditing Activity in the SAP HANA Database](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/48fd6586304c4f859bf92d64d0cd8b08.html)

[CREATE AUDIT POLICY Statement (Access Control)](https://help.sap.com/viewer/4fe29514fd584807ac9f2a04f6754767/LATEST/en-US/20d3d56075191014af43d6487fcaa603.html)

## 2.6 Recommendations for Trace and Dump Files

Recommendations for handling trace and dump files

#### Trace Files

Default Basic tracing of activity in database components is enabled by default, with each database service writing to its own trace file. Other traces (for example, SQL trace, expensive statements trace, performance trace) must be explicitly enabled.

Users with the system privilege CATALOG READ can read the contents of trace files in the SAP HANA database explorer. At operating system level, any user in the SAPSYS group can access the trace directory: /usr/sap/<SID>/HDB<instance>/<host>/trace/

<db\_name>

Recommendation ● Enable tracing to troubleshoot specific problems only and then disable.

* Exercise caution when setting or changing the trace level. A high trace level may expose certain security-relevant data (for example, database trace level DEBUG or SQL trace level ALL\_WITH\_RESULTS).
* Delete trace files that are no longer needed.

|  |  |
| --- | --- |
| How to Verify | You can check which traces are enabled and how they are configured, as well as view trace files in the SAP HANA database explorer. |
| Related Alert | No |
| More Information | See the section on security risks of trace and dump files in the *SAP HANA Security Guide* and the section on traces in the *SAP HANA Administration Guide*. |

#### Dump Files

Default The system generates core dump files (for example, crash dump files) automatically. Runtime (RTE) dump files can be triggered explicitly, for example by using the SAP HANA database management console (hdbcons) or as part of a full system information dump (fullSystemInfoDump.py) using the SAP HANA cockpit.

RTE dump files must be generated by the <sid>adm user.

#####  Caution

Technical expertise is required to use hdbcons. To avoid incorrect usage, use hdbcons only with the guidance of SAP HANA development support.

To create RTE dump files in a running system as part of a full system information dump in the SAP HANA cockpit, a user requires the EXECUTE privilege on procedure SYS.FULL\_SYSTEM\_INFO\_DUMP\_CREATE.

Dump files are stored in the trace directory and have the same access permissions as other trace files (see above).

Runtime dump files created as part of a full system information dump can be retrieved by users with the EXECUTE privilege on the procedure

SYS.FULL\_SYSTEM\_INFO\_DUMP\_RETRIEVE using the SAP HANA cockpit. At operating system level, any user in the SAPSYS group can access their storage loca­

tion: /usr/sap/SID/SYS/global/sapcontrol/snapshots

|  |  |  |
| --- | --- | --- |
| Recommendation | ● | Generate runtime dump files to analyze specific error situations only, typically at the request of SAP support. |
|  | ● | Delete dump files that are no longer needed. |
| How to Verify | ● | You can view core dump files in the SAP HANA database explorer |
|  | ● | You can download the file collections generated by a full system information dump in the SAP HANA cockpit. |
| Related Alert | No |  |

More Information See the section on security risks of trace and dump files in the *SAP HANA Security Guide* and the section on collecting diagnosis information for SAP Support in the *SAP HANA Administration Guide*.

#### Related Information

[Security Risks of Trace, Dump, and Captured Workload Files](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/0bf41211c7a940cbbf1b4bb9876ddd8f.html)

[Collecting Diagnosis Information for SAP Support](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/65744703d3a64ad89517cdd307d550d6.html)

## 2.7 Recommendations for Tenant Database Management

Recommendations for securely configuring tenant databases

#### SAML-Based User Authentication

Default All tenant databases use the same trust store as the system database for SAML-based user authentication

|  |  |
| --- | --- |
| Recommendation | To prevent users of one tenant database being able to log on to other databases in the system (including the system database) using SAML, create individual certificate collections with the purpose **SAML** and **SSL** in every tenant database.  In addition, specify a non-existent trust store for every tenant database using the [communication] sslTrustStore property in the global.ini file. |
| How to Verify | Execute the following statements:   * In the tenant database: SELECT \* FROM PSES WHERE PURPOSE ='SAML' OR PURPOSE ='SSL'; * In the system database: SELECT \* FROM   SYS\_DATABASES.M\_INIFILE\_CONTENTS WHERE  DATABASE\_NAME='<TENANT\_DB\_NAME>' AND  SECTION='communication' AND KEY = 'ssltruststore'; |
| Related Alert | No |
| More Information | See the sections on SSL configuration on the SAP HANA server and certficate collections in the *SAP HANA Security Guide*. |

#### Configuration Blocklist

Default A configuration change blocklist (multidb.ini) is delivered with a default configuration.

The parameters contained in the blocklist can only be changed by a system administrator in the system database, not by the administrators of individual tenant databases.

|  |  |
| --- | --- |
| Recommendation | Verify that the parameters included in the multidb.ini file meet your requirements and customize if necessary. |
| How to Verify | To see which parameters are blocklisted, execute the statement:  SELECT \* FROM "PUBLIC". "M\_INIFILE\_CONTENTS" WHERE FILE\_NAME  = 'multidb.ini'; |
| Related Alert | No |
| More Information | See the section on default blocklisted system properties in tenant databases in the *SAP HANA Security Guide* and the section on how to prevent changes to system properties in tenant databases in the *SAP HANA Administration Guide*. |

#### Restricted Features

Default To safeguard and/or customize your system, it is possible to disable certain database features that provide direct access to the file system, the network, or other resources, for example import and export operations and backup functions.

No features are disabled by default.

|  |  |
| --- | --- |
| Recommendation | Review the list of features that can be disabled and disable those that are not required in your implementation scenario. |
| How to Verify | To see the status of features, query the system view  M\_CUSTOMIZABLE\_FUNCTIONALITIES:  SELECT \* FROM "PUBLIC". "M\_CUSTOMIZABLE\_FUNCTIONALITIES"; |
| Related Alert | No |
| More Information | See the section on restricted features in tenant databases in the *SAP HANA Security Guide* and the section on how to disable features on tenant databases in the *SAP HANA Administration Guide*. |

#### Related Information

[TLS/SSL Configuration on the SAP HANA Server](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/de15ffb1bb5710148386ffdfd857482a.html)

[Certificate Collections](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/75d0cfec8e4f44c3a649d26e9cefa314.html)

[Default Blocklisted System Properties in Tenant Databases](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/fcdfe0bdac344c2897efe3aa4719c381.html)

[Prevent Changes to System Properties in Tenant Databases](https://help.sap.com/viewer/78209c1d3a9b41cd8624338e42a12bf6/LATEST/en-US/cd34680fe57242ef8a5e7199739e972c.html)

[Restricted Features in Tenant Databases](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/LATEST/en-US/9d580c6463804799b9781c97ab6ebe19.html)

[Disable Features on a Tenant Database](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/LATEST/en-US/e44815d6a1b244b4991bad3a46be3673.html)

# 3 SAP HANA XS, Advanced Model

Checklists and recommendations to help you operate and configure the SAP HANA XS Advanced Model runtime securely

Recommendations for XS Advanced Administration User [page 28]

Recommendations for XS advanced administration user

Recommendations for Organizations and Spaces [page 30]

Recommendations for setting up organizations and spaces

Recommendations for Network Configuration [page 31]

Recommendations for integrating SAP HANA XS advanced securely into your network environment.

## 3.1 Recommendations for XS Advanced Administration User

Recommendations for XS advanced administration user

|  |  |
| --- | --- |
| Default | XSA\_ADMIN is a first-level administrator user with irrevocable privileges. This user has unlimited access to the Controller and therefore needs to be handled carefully. |
| Recommendations | * Change the XSA\_ADMIN password at regular intervals. * Avoid creating other powerful users with privileges similar to XSA\_ADMIN. * Keep the number of people with XSA\_ADMIN credentials as small as possible. Delegate specific tasks like space management to lesser-privileged users instead.   Alternatively, set up lesser-privileged XS advanced users to run the server without the administrative user. Then deactivate the XSA\_ADMIN user. See the next section. |
| How to Verify | SELECT DISTINCT USER\_NAME FROM USER\_PARAMETERS WHERE |

#### XSA\_ADMIN User

PARAMETER = 'XS\_RC\_XS\_CONTROLLER\_ADMIN'

#####  Note

This statement can only be executed by a user administrator.

|  |  |
| --- | --- |
| Related Alert | No |
| More Information | See the section on predefined XS advanced users in the *SAP HANA Security Guide*. |

|  |  |
| --- | --- |
| Default | The XSA\_ADMIN user can use the Controller without any restrictions and is the only user in a position to do the initial setup of the model. This includes appointing at least one Org Manager who is able to set up spaces, and managing global resources such as buildpacks and external brokers. |
| Recommendations | Set up your system so that XSA\_ADMIN is not needed for normal system operation. You can do this as follows: |

#### Initial Setup with XSA\_ADMIN

1. Perform the basic settings that require the administrative access rights of XSA\_ADMIN as required:
   1. Install custom SSL certificates (xs trust-certificate and xs setcertificate commands)

○ Appoint at least one XS advanced user to be OrgManager of each organization (strongly recommended)

○ Register all required service brokers (optional)

○ Create all required shared domains (optional)

○ Create all required custom buildpacks (optional)

○ Create all required runtimes (optional)

○ Configure logical databases (optional)

○ Set up global environment variables (xs set\_running| staging\_environment\_variable\_groups command) (optional)

1. Grant one or more XS advanced users the following role collections:
   1. XS\_AUTHORIZATION\_ADMIN (managing roles, role-collections, and so on)

○ XS\_USER\_ADMIN (assigning role-collections to XS advanced users)

1. Deactivate the XSA\_ADMIN with the following SQL statement:

ALTER USER XSA\_ADMIN DEACTIVATE USER NOW

#####  Note

In an emergency, a user with system privilege USER ADMIN can reactivate this

user with the SQL statement:ALTER USER XSA\_ADMIN ACTIVATE USER NOW

|  |  |
| --- | --- |
| How to Verify | In the system view USERS, check the values in columns USER\_DEACTIVATED, DEACTIVATION\_TIME, and LAST\_SUCCESSFUL\_CONNECT for the user XSA\_ADMIN. |
| Related Alert | No |
| More Information | See the section on scopes, attributes, and role collections in the *SAP HANA Security Guide*. |

#### Related Information

[Predefined XS Advanced Users](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/04ede29ac92841c58c1749b070a66c4b.html)

[Scopes, Attributes, and Role Collections](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/26c4f75496fd4de0a1c8bc8f2d30a5f2.html)

## 3.2 Recommendations for Organizations and Spaces

Recommendations for setting up organizations and spaces

#### Space Isolation

Default The instances of applications in the same space run with the same operating system (OS) user. Each space can have a different OS user.

|  |  |
| --- | --- |
| Recommendations | For space isolation, each space should use an own dedicated OS user only for this space. |
| How to Verify | Current space user mapping can be viewed with the xs spaces command. The user column shows the used OS user for each listed space. |
| Related Alert | No |
| More Information | See the section on organizations and spaces in the *SAP HANA Security Guide*. |

#### Privileges of Space Operating System (OS) User

Default Spaces are mapped to operating system (OS) users that are used to stage and run applica­

tions.

|  |  |
| --- | --- |
| Recommendations | * Don’t use <sid>adm or any other high privileged OS user as a space OS user. * Restrict the privileges of the space OS user as much as possible. |
| How to Verify | Current space user mapping can be viewed with the xs spaces command. Verify the OS privileges of each OS users listed. |
| Related Alert | No |
| More Information | See the section on organizations and spaces in the *SAP HANA Security Guide*. |
| **SAP Space**  Default | System applications are deployed to the SAP space by default. |
| Recommendations | Use the PROD space to deploy your applications, or create new spaces for the applications as required. To ensure isolation, do not deploy your applications to the SAP space. In addition, do not assign the SpaceDeveloper role to platform users in the SAP space, unless it is absolutely necessary. |
| How to Verify | Log on to the SAP space and use the xs apps command to confirm that the list of applications running in the target space (SAP) includes only system applications, for example, the deployer, the product-installer, etc. |

Related Alert No

|  |  |
| --- | --- |
| More Information | See the section on organizations and spaces in the *SAP HANA Security Guide*. |
| **Logon with xs CLI**  Default | XS advanced session is stored in the file system of the current OS user |
| Recommendations | We recommend logging on to XS advanced (xs login command) only with a personal OS user with a home directory that is not readable to other OS users. |
| How to Verify | - |
| Related Alert | No |

**Related Information**

[Organizations and Spaces](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/0cb80d7bc5b54ddda700b3f797039203.html)

## 3.3 Recommendations for Network Configuration

Recommendations for integrating SAP HANA XS advanced securely into your network environment.

#### Network and Communication Security

Default The XS advanced platform router, which is realized by an SAP Web Dispatcher instance, ex­

poses the public end point for the whole system. The router is configured in a way that all application and public server end points are represented by an external URL. External requests are routed to the appropriate back-end instance according to the internal routing table.

|  |  |
| --- | --- |
| Recommendations | Limit network access to your system in a way that only the platform router's end points are accessible from outside the system. This can be accomplished by means of network zones and firewalls. |
| How to Verify | Get in touch with your network administrators. |
| Related Alert | No |
| More Information | See the sections on XS advanced application server components and public end points in the *SAP HANA Security Guide*. |

Default The XS advanced platform router, which is realized by an SAP Web Dispatcher instance, accepts cipher suites TLS 1.0, TLS 1.1 and TLS 1.2 for external requests, by default. The weaker suite TLS 1.0 is allowed due to the fact that a lot of clients do not support higher protocol versions.

|  |  |
| --- | --- |
| Recommendations | If the limitation for some non-compatible clients is accepted, it is recommended to disable all TLS versions below TLS 1.2 as described in the *SAP HANA Administration Guide*. |
| Related Alert | No |

More Information See the following section of the *SAP HANA Administration Guide*: Start of the navigation path *Application Run-Time*

*Services* Next navigation step *Maintaining the SAP HANA XS Advanced Model Run Time* Next navigation step *Configuring the XS Advanced Platform Router* Next navigation step *Configuring the Platform Router with INI Parameters* End of the navigation path

|  |  |
| --- | --- |
| **Security Areas**  Default | The JDBC connection to the SAP HANA database is not encrypted by default. |
| Recommendations | Activate JDBC TLS/SSL between application server and the SAP HANA database in all scenarios. Configure custom SSL certificates as described in the SAP HANA Security Guide. |
| How to Verify | Get in touch with your network administrators. |
| Related Alert | No |
| More Information | See the section on XS advanced certificate management in the *SAP HANA Security Guide*. |

#### Certificate Management

Default By default, the XS advanced server runs with self-signed certificate for all domains.

|  |  |
| --- | --- |
| Recommendations | Configure the XS advanced server to accept a custom certificate for all your domains, especially the shared domain (used for XS CLI communication). Custom certificates can be upload by using the xs set-certificate command for each domain. |
| How to Verify | Check the certificate in your Web browser when loading from a specific domain. |
| Related Alert | No |
| More Information | See the section on XS advanced certificate management in the *SAP HANA Security Guide*, as well as SAP Note 2243019 in *Related Information* below. |

#### Related Information

[Application Server Components](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/fadfbccfeb694fc4a12e7266aa45233f.html)

[Public Endpoints](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/df6fea46d3d54cd38aee006ae7b240bf.html)

[XS Advanced Certificate Management](https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.05/en-US/854144c2d4dc429f840fcee45595917c.html)

[Configuring the XS Advanced Platform Router](https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/74b9cf2638a54c0aa67131ad52482054.html)

[SAP Note 2243019](http://help.sap.com/disclaimer?site=https://launchpad.support.sap.com/#/notes/2243019)Information published on SAP site

**Important Disclaimer for Features in SAP HANA**

For information about the capabilities available for your license and installation scenario, refer to the [Feature Scope Description for SAP HANA](https://help.sap.com/viewer/de855a01ee2248dfb139088793f8802a/latest/en-US).

SAP HANA Security Checklists and Recommendations **Important Disclaimer for Features in SAP HANA**

**Important Disclaimers and Legal Information**

### Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information. About the icons:

* Links with the icon Information published on non-SAP site: You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
* The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
* SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
* Links with the icon Information published on SAP site: You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

### Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

### Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

### Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

### Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

SAP HANA Security Checklists and Recommendations

**Important Disclaimers and Legal Information**

#### www.sap.com/contactsap

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.

### THE BEST RUN

