PUBLIC

SAP HANA Platform 2.0 SPS 00
Document Version: 1.0 – 2016-11-30

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 for your implementation scenario and system environment. Some of these settings are specifically important for the security of your system, and misconfiguration could leave your system vulnerable. This document contains information and recommendations on critical settings.

About this Document

This document contains checklists and recommendations to help you operate and configure SAP HANA securely. However, please note the following:

- The checklists and recommendations contained in this document 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 contained in this document 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.

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.

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.

Related Information

SAP HANA Security Guide

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.
- 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 configured for multitenant database containers, make sure to do this in all tenant databases, including the system database.

  For more information about database users that are created in the SAP HANA database by default, see *SAP HANA User Management* > *Predefined Users* in the SAP HANA Security Guide.
- 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 *Deactivate System User* in the SAP HANA Security Guide.

  > **Remember**
  >
  > If you received a system configured for multitenant database containers, make sure to do this in all tenant databases, including 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, see *Security Administration* > *Managing Data Encryption in SAP HANA* > *Server-Side Encryption Services* > *Change the SSFS Master Keys* in 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 instance secure store in the

file system (SSFS). Alternatively, you can use SAPControl to reset the system PKI with the methods `UpdateSystemPKI[<force>]` and `UpdateInstancePSE[<force>]`.

Related Information

SAP HANA Administration Guide

SAP HANA Security Guide

SAP Control WebService

2 SAP HANA Database

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

> ➜ Tip
>
> SAP Note 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 document.

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 Encryption [page 18]
Recommendations for 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 22]
Recommendations for audit configuration

Recommendations for Trace and Dump Files [page 24]
Recommendations for handling trace and dump files

Recommendations for Multitenant Database Containers [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

Table 1:

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

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	• *SAP HANA User Management* > *Predefined Users* in the SAP HANA Security Guide • *SAP HANA User Management* > *Deactivate the SYSTEM User* in the SAP HANA Security Guide

Password Lifetime of Database Users

Table 2:

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. 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	*SAP HANA Authentication and Single-Sign On* > *Password Policy* in the SAP HANA Security Guide

System Privileges

Table 3:

Default	System privileges authorize system-wide administration commands. The users SYSTEM and _SYS_REPO users have all these privileges by default.

Recommendation	System privileges should only ever be granted to users actually need them. 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 system: - CATALOG READ - TRACE ADMIN In a system 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	• ❯ *SAP HANA Authorization* ❯ *System Privileges* ❯ in the SAP HANA Security Guide • ❯ *SAP HANA Security Administration* ❯ *Managing SAP HANA Users* ❯ *User Authorization* ❯ *System Views for Verifying Users' Authorization* ❯ ❯ in the SAP HANA Administration Guide

System Privileges: Critical Combinations

Table 4:

Default	The users `SYSTEM` and `_SYS_REPO` users 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	• ❯ *SAP HANA Authorization* ❯ *System Privileges* ❯ in the SAP HANA Security Guide • ❯ *SAP HANA Security Administration* ❯ *Managing SAP HANA Users* ❯ *User Authorization* ❯ *System Views for Verifying Users' Authorization* ❯ ❯ in the SAP HANA Administration Guide

System Privilege: DATA ADMIN

Table 5:

Default	The system privilege `DATA ADMIN` is a powerful privilege. It authorizes a user to read all data in system views, as well as to execute all data definition language (DDL) commands in the SAP HANA database. Only the users `SYSTEM` and `_SYS_REPO` users have this privilege by default.
Recommendation	No user or role in a production system 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	• *SAP HANA Authorization* ▸ *System Privileges* in the SAP HANA Security Guide • *SAP HANA Security Administration* ▸ *Managing SAP HANA Users* ▸ *User Authorization* ▸ *System Views for Verifying Users' Authorization* in the SAP HANA Administration Guide

System Privilege: DEVELOPMENT

Table 6:

Default	The system privilege `DEVELOPMENT` authorizes some internal `ALTER SYSTEM` commands. Only the users `SYSTEM` and `_SYS_REPO` users have this privilege by default.
Recommendation	No user or role in a production system 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	• *SAP HANA Authorization* ▸ *System Privileges* in the SAP HANA Security Guide • *SAP HANA Security Administration* ▸ *Managing SAP HANA Users* ▸ *User Authorization* ▸ *System Views for Verifying Users' Authorization* in the SAP HANA Administration Guide

Analytic Privilege: _SYS_BI_CP_ALL

Table 7:

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, and only the user `SYSTEM` has these roles by default.
Recommendation	Do not grant this privilege to any user or role in a production system.
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	• *SAP HANA Authorization* › *Privileges* in the SAP HANA Security Guide • *SAP HANA Authorization* › *Predefined Database Roles* in the SAP HANA Security Guide • *SAP HANA Security Administration* › *Managing SAP HANA Users* › *User Authorization* › *System Views for Verifying Users' Authorization* › in the SAP HANA Administration Guide

Debug Privileges

Table 8:

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	• *SAP HANA Authorization* › *Privileges* in the SAP HANA Security Guide • *SAP HANA Security Administration* › *Managing SAP HANA Users* › *User Authorization* › *System Views for Verifying Users' Authorization* › in the SAP HANA Administration Guide

Predefined Catalog Role CONTENT_ADMIN

Table 9:

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 systems. 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	• *SAP HANA Authorization* › *Predefined Database Roles* in the SAP HANA Security Guide • *SAP HANA Security Administration* › *Managing SAP HANA Users* › *User Authorization* › *System Views for Verifying Users' Authorization* › in the SAP HANA Administration Guide

Predefined Catalog Role MODELING

Table 10:

Default	The role `MODELING` 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. The user `SYSTEM` has the role `MODELING` by default.
Recommendation	Do not grant this role to users, particularly in production systems. 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	• *SAP HANA Authorization* › *Predefined Database Roles* in the SAP HANA Security Guide • *SAP HANA Security Administration* › *Managing SAP HANA Users* › *User Authorization* › *System Views for Verifying Users' Authorization* › in the SAP HANA Administration Guide

Predefined Catalog Role SAP_INTERNAL_HANA_SUPPORT

Table 11:

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 the 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	• ▶ *SAP HANA Authorization* › *Predefined Database Roles* ◀ in the SAP HANA Security Guide • ▶ *SAP HANA Security Administration* › *Managing SAP HANA Users* › *User Authorization* › *System Views for Verifying Users' Authorization* › ◀ in the SAP HANA Administration Guide

Predefined Roles for Application Function Libraries (AFL)

Table 12:

Default	For each AFL area two roles exists. For PAL and BFL the roles are: • `AFL__SYS_AFL_AFLPAL_EXECUTE` • `AFL__SYS_AFL_AFLPAL_EXECUTE_WITH_GRANT_OPTION` • `AFL__SYS_AFL_AFLBFL_EXECUTE` • `AFL__SYS_AFL_AFLBFL_EXECUTE_WITH_GRANT_OPTION` User `_SYS_AFL` is the creator and owner of these roles. User `SYSTEM` has the privileges to grant these roles to users. User `_SYS_REPO` has the respective role with grant option granted automatically.
Recommendation	Grant these roles only to users who need to execute PAL and BFL procedures.
How to Verify	You can verify whether a user or role has any predefined AFL roles by querying the `EFFECTIVE_ROLE_GRANTEES` system view.
Related Alert	No
More Information	• ▶ *Getting Started with PAL* › *Security* ◀ in the SAP HANA Predictive Analysis Library (PAL) reference • ▶ *Getting Started with BFL* › *Security* ◀ in the SAP HANA Business Function Library (BFL) reference • ▶ *SAP HANA Security Administration* › *Managing SAP HANA Users* › *User Authorization* › *System Views for Verifying Users' Authorization* › ◀ in the SAP HANA Administration Guide

Predefined Repository Roles

Table 13:

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	Application-specific repository roles should only be granted to application users.
How to Verify	You can verify whether a user or role has a particular role by executing the following statement, for example: `SELECT * FROM EFFECTIVE_ROLE_GRANTEES WHERE ROLE_NAME ='sap.hana.security.cockpit.roles::MaintainDataVolumeEncryption';`
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

Related Information

SAP HANA Security Guide
SAP HANA Administration Guide
SAP HANA Business Function Library (BFL)

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 *SAP HANA Network and Communication Security* > *Network Security* in the SAP HANA Security Guide.

Open Ports

Table 14:

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 Master Guide.
How to Verify	Verify opened ports at operating system level using Linux commands such as `netcat` or `netstat`.
Related Alert	No
More Information	• ▶ *SAP HANA Network and Communication Security* > *Communication Channel Security* ◀ in the SAP HANA Security Guide • ▶ *Landscape Management and Network Administration* > *Network Administration* > *Ports and Connections* ◀ in the SAP HANA Administration Guide

Internal Host Name Resolution in Single-Host System

Table 15:

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	Check which ports are listening using the SAP HANA cockpit. This information is available in the *Network Security Information* app available 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	▶ *Landscape Management and Network Administration* > *Network Administration* > *Ports and Connections* ◀ in the SAP HANA Administration Guide

Internal Host Name Resolution in Multiple-Host System

Table 16:

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 addition, 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.

How to Verify	Check which ports are listening using the SAP HANA cockpit.
	This information is available in the *Network Security Information* app available 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	▶ *Landscape Management and Network Administration* ▶ *Network Administration* ▶ *Host Name Resolution* ▶ *Internal Host Name Resolution* ▶ in the SAP HANA Administration Guide

Internal Host Name Resolution in System Replication Scenario

Table 17:

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 parameter `[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_communication] internal_hostname_resolution` section. • If a separate network **is not configured** for system replication, the parameter `[system_replication_communication] listeninterface` parameter 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 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.

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	▶ *Landscape Management and Network Administration* ▶ *Network Administration* ▶ *Host Name Resolution* ▶ *Host Name Resolution for System Replication* ▶ in the SAP HANA Administration Guide

Related Information

SAP HANA Security Guide

SAP HANA Master Guide

2.3 Recommendations for Encryption

Recommendations for encryption key management

Instance SSFS Master Key

Table 18:

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	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	• *Data Storage Security in SAP HANA* > *Server-Side Data Encryption* in the SAP HANA Security Guide • *Security Administration* > *Managing Data Encryption in SAP HANA* > *Server-Side Data Encryption Services* > *Change the SSFS Master Keys* in the SAP HANA Administration Guide

System PKI SSFS Master Key

Table 19:

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	• *Data Storage Security in SAP HANA* > *Server-Side Data Encryption* in the SAP HANA Security Guide • *Security Administration* > *Managing Data Encryption in SAP HANA* > *Server-Side Data Encryption Services* > *Change the SSFS Master Keys* in the SAP HANA Administration Guide

Root Encryption Keys

Table 20:

Default	SAP HANA features the following data encryption services: - Data volume encryption - Redo log encryption - An internal encryption service available to applications requiring data encryption Unique root keys are generated for all services in every installation.
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	- *Data Storage Security in SAP HANA* > *Server-Side Data Encryption Services* in the SAP HANA Security Guide - *Security Administration* > *Managing Data Encryption* > *Server-Side Data Encryption Services* in the SAP HANA Administration Guide

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

Table 21:

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	- *Data Storage Security in SAP HANA* > *Secure Storage of Passwords in SAP HANA* > *Secure User Store (hdbuserstore)* in the SAP HANA Security Guide - *Security Administration* > *Managing Data Encryption in SAP HANA* > *Client-Side Encryption (hdbuserstore)* in the SAP HANA Administration Guide - SAP Note 2210637

Data and Log Volume Encryption

Table 22:

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.
How to Verify	Execute the following statement: `SELECT * FROM M_ENCRYPTION_OVERVIEW WHERE SCOPE='LOG' OR SCOPE = 'PERSISTENCE'`
Related Alert	No
More Information	• *Data Storage Security in SAP HANA* > *Server-Side Data Encryption Services* > *Data and Log Volume Encryption* in the SAP HANA Security Guide • *Security Administration* > *Managing Data Encryption in SAP HANA* > *Server-Side Data Encryption Services* > *Enabling and Disabling Encryption of Data and Log Volumes* in the SAP HANA Administration Guide

Related Information

SAP HANA Security Guide
SAP HANA Administration Guide

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

Table 23:

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 in a multiple-container system required for high isolation ℹ 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	*SAP HANA User Management* › *Predefined Database Users* in the SAP HANA Security Guide

OS File System Permissions

Table 24:

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	- SAP Note 2252941 - › *SAP HANA Lifecycle Management* › *SAP HANA Platform Lifecycle Management* › *Check the Installation Using the Command-Line Interface* › in the SAP HANA Administration Guide.

OS Security Patches

Table 25:

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)

Related Information

SAP HANA Security Guide

SAP HANA Administration Guide

2.5 Recommendations for Auditing

Recommendations for audit configuration

Auditing

Table 26:

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* tile 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	• ▶ *Auditing Activity in SAP HANA Systems* › in the SAP HANA Security Guide • ▶ *Security Administration* › *Auditing Activity in SAP HANA Systems* › in the SAP HANA Administration Guide

Audit Trail Target: syslog

Table 27:

Default	The default global audit trail target is syslog (`SYSLOGPROTOCOL`)
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	• ▶ *Auditing Activity in SAP HANA Systems* › *Audit Trails* › in the SAP HANA Security Guide • Your operating system documentation

Audit Trail Target: CSV Text File

Table 28:

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 SAP HANA cockpit This information is available in the *Auditing* app, which is available with the *SAP HANA Security Overview* catalog. 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	*Auditing Activity in SAP HANA Systems* ▸ *Audit Trails* in the SAP HANA Security Guide

Related Information

SAP HANA Security Guide

SAP HANA Administration Guide

2.6 Recommendations for Trace and Dump Files

Recommendations for handling trace and dump files

Trace Files

Table 29:

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 studio. 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 in the Administration editor of the SAP HANA studio on the *Trace Configuration* tab. - You can view trace files in the Administration editor of the SAP HANA studio on the *Diagnosis Files* tab and using the SAP HANA Database Explorer, which is integrated into the SAP HANA cockpit and SAP Web IDE for SAP HANA.
Related Alert	No
More Information	- *Security Risks of Trace and Dump Files* in the SAP HANA Security Guide - *System Administration* ▶ *Getting Support* ▶ *Configure Traces* in the SAP HANA Administration Guide

Dump Files

Table 30:

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`). 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 studio, 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 studio. At operating system level, any user in the `SAPSYS` group can access their storage location: `/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 Administration editor of the SAP HANA studio on the *Diagnosis Files* tab. - You can download the file collections generated by a full system information dump in the Administration editor of the SAP HANA studio on the *Diagnosis Files* tab.
Related Alert	No

More Information	• *Security Risks of Trace and Dump Files* in the SAP HANA Security Guide • *System Administration* › *Getting Support* › *Collecting Diagnosis Information for SAP Support* in the SAP HANA Administration Guide

2.7 Recommendations for Multitenant Database Containers

Recommendations for securely configuring tenant databases

SAML-Based User Authentication

Table 31:

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	• *SAP HANA Network and Communication Security* › *Secure Communication Between SAP HANA and JDBC/ODBC Clients* › *SSL Configuration on the SAP HANA Server* in the SAP HANA Security Guide • *Certificate Management in SAP HANA* › *Certificate Collections* in the SAP HANA Security Guide

Configuration Blacklist

Table 32:

Default	A configuration change blacklist (`multidb.ini`) is delivered with a default configuration. The parameters contained in the blacklist 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 blacklisted, execute the statement: `SELECT * FROM "PUBLIC". "M_INIFILE_CONTENTS" WHERE FILE_NAME = 'multidb.ini';`
Related Alert	No
More Information	• *SAP HANA Security Reference Information* › *Default Blacklisted System Properties in Multitenant Database Containers* in the SAP HANA Security Guide • *System Administration* › *Managing Multitenant Database Containers* › *Creating and Configuring Tenant Databases* › *Prevent Changes to System Properties in Tenant Databases* in the SAP HANA Administration Guide

Restricted Features

Table 33:

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	• *SAP HANA Security Reference Information* › *Restricted Features in Multitenant Database Containers* in the SAP HANA Security Guide • *System Administration* › *Managing Multitenant Database Containers* › *Creating and Configuring Tenant Databases* › *Disable Features on a Tenant Database* in the SAP HANA Administration Guide

Related Information

SAP HANA Security Guide

3 SAP HANA XS, Advanced Model

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

3.1 Recommendations for XSA Administration User

Recommendations for XSA administration user

XSA_ADMIN User

Table 34:

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 XSA 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 PARAMETER = 'XS_RC_XS_CONTROLLER_ADMIN'` i Note This statement can only be executed by a user administrator.
Related Alert	No
More Information	*Security for SAP HANA Extended Application Services, Advanced Model* > *User Administration and Authentication in SAP HANA XS Advanced* > *Predefined XSA Users* in the SAP HANA Security Guide

Initial Setup with XSA_ADMIN

Table 35:

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: 1. Perform the basic settings that require the administrative access rights of `XSA_ADMIN` as required: ○ Install custom SSL certificates (`xs trust-certificate` and `xs set-certificate` commands) ○ Appoint at least one XSA 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) 2. Grant one or more XSA users the following role collections: ○ `XS_AUTHORIZATION_ADMIN` (managing roles, role-collections, and so on) ○ `XS_USER_ADMIN` (assigning role-collections to XSA users) 3. Deactivate the `XSA_ADMIN` with the following SQL statement: `ALTER USER XSA_ADMIN DEACTIVATE USER NOW` i 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	*Security for SAP HANA Extended Application Services, Advanced Model* › *Authorization in SAP HANA XS Advanced* › *Scopes, Attributes, and Role Collections* in the SAP HANA Security Guide

Related Information

SAP HANA Security Guide

3.2 Recommendations for Organizations and Spaces

Recommendations for setting up organizations and spaces

Operating System User

Table 36:

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	• 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. • Each space should use an own dedicated OS user only for this space.
How to Verify	Current space user settings 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	▶ *Security for SAP HANA Extended Application Services, Advanced Model* › *Authorization in SAP HANA XS Advanced* › *Organizations and Spaces* ◀ in the SAP HANA Security Guide

SAP Space

Table 37:

Default	System applications are deployed to the SAP space by default.
Recommendations	Use the PROD space to deploy your applications or create new spaces accordingly. Don't deploy your applications to the SAP space to ensure isolation.
How to Verify	Applications (`xs apps`) with target space SAP should list only system applications (deployer, product-installer and so on).
Related Alert	No
More Information	▶ *Security for SAP HANA Extended Application Services, Advanced Model* › *Authorization in SAP HANA XS Advanced* › *Organizations and Spaces* ◀ in the SAP HANA Security Guide

Logon with xs CLI

Table 38:

Default	XSA session is stored in the file system of the current OS user

Recommendations	We recommend log on to XSA (`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

SAP HANA Security Guide

3.3 Recommendations for Network Configuration

Recommendations for integrating SAP HANA XSA securely into your network environment.

Network and Communication Security

Table 39:

Default	The Platform Router, which is realized by an SAP Web Dispatcher instance, exposes the public endpoint for the entire system. The router is configured in a way that all application and public server endpoints 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 endpoints are accessible from outside the system. This can be accomplished by means of network zones and firewalls.
How to Verify	Get in contact with your network administrators to verify this fact.
Related Alert	No
More Information	• *Security for SAP HANA Extended Application Services, Advanced Model* > *Technical System Landscape of SAP HANA XS Advanced* > *Application Server Components* in the SAP HANA Security Guide • *Security for SAP HANA Extended Application Services, Advanced Model* > *Network and Communication Security with SAP HANA XS Advanced* > *Public Endpoints* in the SAP HANA Security Guide

Security Areas

Table 40:

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 contact with your network administrators to verify this fact.
Related Alert	No
More Information	▶ *Security for SAP HANA Extended Application Services, Advanced Model* ▶ *Network and Communication Security with SAP HANA XS Advanced* ▶ *Certificate Management* ▶ in the SAP HANA Security Guide

Certificate Management

Table 41:

Default	By default, the XSA server runs with self-signed certificate for all domains.
Recommendations	Configure the XSA 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 browser when loading from a specific domain.
Related Alert	No
More Information	• ▶ *Security for SAP HANA Extended Application Services, Advanced Model* ▶ *Network and Communication Security with SAP HANA XS Advanced* ▶ *Certificate Management* ▶ in the SAP HANA Security Guide • SAP note 2243019

Related Information

SAP HANA Security Guide

Important Disclaimer for Features in SAP HANA Platform, Options and Capabilities

SAP HANA server software and tools can be used for several SAP HANA platform and options scenarios as well as the respective capabilities used in these scenarios. The availability of these is based on the available SAP HANA licenses and the SAP HANA landscape, including the type and version of the back-end systems the SAP HANA administration and development tools are connected to. There are several types of licenses available for SAP HANA. Depending on your SAP HANA installation license type, some of the features and tools described in the SAP HANA platform documentation may only be available in the SAP HANA options and capabilities, which may be released independently of an SAP HANA Platform Support Package Stack (SPS). Although various features included in SAP HANA options and capabilities are cited in the SAP HANA platform documentation, each SAP HANA edition governs the options and capabilities available. Based on this, customers do not necessarily have the right to use features included in SAP HANA options and capabilities. For customers to whom these license restrictions apply, the use of features included in SAP HANA options and capabilities in a production system requires purchasing the corresponding software license(s) from SAP. The documentation for the SAP HANA optional components is available in SAP Help Portal at http://help.sap.com/hana_options. If you have additional questions about what your particular license provides, or wish to discuss licensing features available in SAP HANA options, please contact your SAP account team representative.

Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).

go.sap.com/registration/ contact.html