Security Guide

Trigger-Based Data Replication Using SAP Landscape Transformation Replication Server

• For SAP HANA Platform 2.0 SPS01

Target Audience
- Consultants
- Administrators
- SAP Hardware Partner
- Others

Customer
2017-11-17
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.

Icons in Body Text

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Caution</td>
</tr>
<tr>
<td>🔴</td>
<td>Example</td>
</tr>
<tr>
<td>📊</td>
<td>Note</td>
</tr>
<tr>
<td>🔍</td>
<td>Recommendation</td>
</tr>
<tr>
<td>⌨️</td>
<td>Syntax</td>
</tr>
</tbody>
</table>

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see Help on Help → General Information Classes and Information Classes for Business Information Warehouse on the first page of any version of SAP Library.

Typographic Conventions

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example text</em></td>
<td>Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.</td>
</tr>
<tr>
<td><strong>Example text</strong></td>
<td>Emphasized words or phrases in body text, graphic titles, and table titles.</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.</td>
</tr>
<tr>
<td><em>Example text</em></td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td><code>&lt;Example text&gt;</code></td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.</td>
</tr>
<tr>
<td><strong>EXAMPLE TEXT</strong></td>
<td>Keys on the keyboard, for example, F2 or ENTER.</td>
</tr>
</tbody>
</table>
# Table of Contents

Copyright .................................................................................................................. 1
Icons in Body Text...................................................................................................... 2
Typographic Conventions ......................................................................................... 2
1. Introduction ........................................................................................................... 4
   Target Audience ..................................................................................................... 4
   Why Is Security Necessary? ................................................................................... 4
   About this Document ................................................................................................. 4
2. Before You Start .................................................................................................... 6
   Related Guides ......................................................................................................... 6
   Important SAP Notes ................................................................................................. 6
   Additional Information .............................................................................................. 7
3. Technical System Landscape .................................................................................. 8
4. User Administration and Authentication .................................................................. 11
5. Authorizations ....................................................................................................... 12
   Authorizations in the SAP HANA System ............................................................... 15
   Restricting Access to the Source System ................................................................. 18
   Network Security ..................................................................................................... 21
   SAP NetWeaver Business Client for WebDynpro Applications ............................ 21
   Communication Destinations ................................................................................... 21
7. Security-Relevant Logging and Tracing .................................................................. 22
8. Data Protection ....................................................................................................... 22
   Read Access Logging ................................................................................................. 23
   Additional Information for INDX-like Tables ........................................................... 24
1. Introduction

This guide does not replace the administration or operation guides that are available for productive operations.

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP Landscape Transformation Replication Server. To assist you in securing SAP Landscape Transformation Replication Server, we provide this Security Guide.

About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Landscape Transformation Replication Server.

Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Before You Start**
  This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- **Technical System Landscape**
  This section provides an overview of the technical components and communication paths that are used by SAP Landscape Transformation Replication Server.

- **User Administration and Authentication**
  This section provides an overview of the user administration and authentication.

- **Authorizations**
  This section provides an overview of the authorization concept that applies to SAP Landscape Transformation Replication Server.
Network and Communication Security

This section provides an overview of the communication paths used by SAP Landscape Transformation Replication Server and the security mechanisms that apply.
2. Before You Start

Related Guides
Pay particular attention to the most relevant sections or specific restrictions as indicated in the table below.

SAP Landscape Transformation Replication Server Guides
For more information about SAP LT Replication Server for SAP HANA, see the resources listed in the table below.

<table>
<thead>
<tr>
<th>Guide</th>
<th>Location</th>
</tr>
</thead>
</table>

SAP HANA Guides
For more information about SAP HANA landscape, security, installation and administration, see the resources listed in the table below.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Quick Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA Landscape, Deployment &amp; Installation</td>
<td><a href="http://help.sap.com/hana">http://help.sap.com/hana</a> → Installation and Upgrade</td>
</tr>
<tr>
<td>SAP HANA Administration</td>
<td><a href="http://help.sap.com/hana">http://help.sap.com/hana</a> → Administration</td>
</tr>
</tbody>
</table>

Important SAP Notes

<table>
<thead>
<tr>
<th>SAP Note</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Note 1514967</td>
<td>Central SAP Note about SAP HANA</td>
</tr>
<tr>
<td>SAP Note 1598623</td>
<td>Current information about SAP HANA</td>
</tr>
</tbody>
</table>
For a list of additional security-relevant SAP Hot News and SAP Notes, see SAP Support Portal at [http://support.sap.com/securitynotes](http://support.sap.com/securitynotes).

**Additional Information**

For more information about specific topics, see the Quick Links as shown in the table below.

<table>
<thead>
<tr>
<th>Content</th>
<th>Quick Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related SAP Notes</td>
<td><a href="http://support.sap.com/notes">http://support.sap.com/notes</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://support.sap.com/securitynotes">http://support.sap.com/securitynotes</a></td>
</tr>
<tr>
<td>Released platforms</td>
<td><a href="http://support.sap.com/pam">http://support.sap.com/pam</a></td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td><a href="http://support.sap.com/solutionmanager">http://support.sap.com/solutionmanager</a></td>
</tr>
</tbody>
</table>
3. Technical System Landscape

The SAP LT Replication Server is a replication technology to provide data from ABAP systems in a SAP HANA environment. It acts as a key enabler for SAP HANA customers to supply their HANA environment with relevant data.

The following components are used in the technical system landscape:

- **Source system**
  
  The source system tracks database changes by using database triggers. It records information about changes in the logging tables. The read modules transfer the data from the source system to the SAP LT Replication Server system. The relevant data is read from the application tables.

- **Non-ABAP source system**
  
  The non-ABAP source system tracks database changes by using database triggers. It records information about changes in the logging tables. The read modules transfer the data from the non-ABAP source system to the SAP LT Replication Server system. The relevant data is read from the application tables.

- **SAP LT Replication Server system**
  
  If the source is an ABAP system, the SAP LT Replication Server system polls the logging tables in the source system with a remote function call (RFC) connection. If the source system is a non-ABAP system, the SAP LT Replication Server system polls the logging tables in the non-ABAP source system with a database connection.

- **SAP HANA system**
  
  The SAP HANA system contains the SAP HANA database. It is used to store the replicated data. The SAP LT Replication Server system and the SAP HANA system communicate by means of a database connection.

SAP LT Replication Server can be used for replication from ABAP source systems and non-ABAP source systems to the HANA system. For ABAP source systems, SAP LT Replication Server can either be installed within the source system or in a separate ABAP system.

The relevant information required to create the connection between the source system, the SAP LT Replication Server system, and the SAP HANA system is specified within the SAP LT Replication Server system as a *Configuration*. In the *Configuration & Monitoring Dashboard* (transaction LTR), you can define a new configuration.

The following figures show the possible technical system landscapes for SAP LT Replication Server.
Option 1 – ABAP Source System with Separate SAP LT Replication Server System

SAP LT Replication Server is installed in a separate ABAP system. Therefore, two network communication channels are required - the RFC connection to the source system and the connection to the SAP HANA system.

Option 2 – SAP LT Replication Server Installed on ABAP Source System

The SAP LT Replication Server system component is installed in the source system. Therefore, the read modules are located in the source system. Only one external network communication channel is required to connect to the SAP HANA system.
Option 3 - Non-ABAP Source System with Separate SAP LT Replication Server System

For a non-ABAP source system, SAP LT Replication Server needs to be installed in a separate system. In contrast to a setup with an ABAP source system, the read modules are created in the SAP LT Replication Server system. To communicate between the SAP LT Replication Server and the non-ABAP source system, a database connection is used.

Ensure that the database of your non-ABAP source system fulfils all the prerequisites for using SAP LT Replication Server.
4. User Administration and Authentication

SAP LT Replication Server and the ABAP source system use the user management and authentication mechanisms provided by the SAP NetWeaver platform, in particular the SAP NetWeaver Application Server. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP NetWeaver Security Guide [SAP Library] → Application Server ABAP Security Guide also apply to SAP LT Replication Server and a ABAP source systems.

In addition, the following information about user management, administration, and authentication applies to the source systems and the SAP LT Replication Server:

- SAP LT Replication Server
  To access the Configuration and Monitoring Dashboard within the SAP LT Replication Server system, a user with specific authorizations is required. This user can specify a new configuration, which is used to establish the connection between the source system, the SAP LT Replication Server, and the SAP HANA system. For the connection to the SAP HANA system, a user in the SAP HANA system is required that is authorized to create the SAP HANA database schema. You can access the Configuration and Monitoring Dashboard by using transaction LTR.

- ABAP Source System
  In order to access the ABAP source system by RFC, a communication user is required. To create a RFC connection, a user with specific authorizations has to be created in the source system. The communication user can access the source system exclusively by RFC and cannot execute steps in dialog mode directly in a system. For more information about this user type, see the section User Types in the SAP Web AS ABAP Security Guide.

  The user role SAP_IUUC_REPL_ADMIN is required to use SAP Landscape Transformation Replication Server. By default, this role does not allows users to view the data that is replicated from the source system to the target system. However, the authorization object S_DMIS (with activity 29) allows users to view the data that is being replicated (by means of the replication logging function).

For the replication target, the authorization and authentication mechanisms provided by the SAP HANA database are used.

- Non-ABAP source system
  To access the non-ABAP source systems by a database connection, the relevant user must be created with all necessary authorizations in the non-ABAP source system. Contact your system administrator to get a user with the relevant authorizations as described under Authorizations in chapter 5.
5. Authorizations

The SAP LT Replication Server and the ABAP source system use the authorization concept provided by the SAP NetWeaver AS ABAP. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply to the SAP LT Replication Server.

In SAP NetWeaver, authorizations are assigned to users based on roles.

For more information about how to create roles, see Role Administration (SAP Library)

Specific authorizations apply for each system. To control the actions that a user is authorized to perform, authorizations for the source system(s) and the SAP LT Replication Server system are available in the user profiles.

The following SAP NetWeaver based authorization objects are especially important for using the SAP LT Replication Server:

- **S_DMIS**
  
  Description: Authority object for SAP SLO Data migration

  **Authorization fields**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Heading</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBT_PR_ARE</td>
<td>MBT PCL: Scenario</td>
</tr>
<tr>
<td>MBT_PR_LEV</td>
<td>MBT PCL: Processing Role Level</td>
</tr>
<tr>
<td>ACTVT</td>
<td>Activity</td>
</tr>
</tbody>
</table>

- **S_DMC_S_R**

  Description: MWB: Reading / writing authorization in sender / receiver

  **Authorization fields**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Heading</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT</td>
<td>Activity</td>
</tr>
</tbody>
</table>

- **S_DMIS_SLT**

  Description: Control Authority on Configuration Level in SAP LT Replication Server system.

  You can use this authorization object to restrict access to specific configurations. To do this, you specify an authorization group (either when creating a configuration, or after you have created a configuration on the Administration tab in transaction LTRC). Note if you want to use authorization object S_DMIS_SLT, you have to add it to the roles for the relevant users manually.
User Roles

Depending on the system and the support patch level, different roles and authorizations are required for the user.

You can generate roles using the profile generator (transaction PFCG).

User Roles for SAP Landscape Transformation Replication Server

You can generate and use the following role to display, change, create, or delete configurations:

- SAP_IUUC_REPL_ADMIN

You can generate and use the following role to display configurations only; this role does not permit the creation of a new configuration, or changes to any settings:

- SAP_IUUC_REPL_DISPLAY

With SAP Landscape Transformation Replication Server SP13, there are new versions of the roles SAP_IUUC_REPL_ADMIN and SAP_IUUC_REPL_DISPLAY. If you are upgrading to SP13 from a lower release, you must ensure that you have the new versions of these roles in the relevant clients.

User Roles for ABAP Source System

For an ABAP source system, generate and use the following role:

- SAP_IUUC_REPL_REMOTE

Do not use the DDIC user. Roles are not generated by default. Grant and generate all roles.

With SAP Landscape Transformation Replication Server SP13, there is a new version of the role SAP_IUUC_REPL_REMOTE. If you are upgrading to SP13 from a lower release, you must ensure that you have the new version of this role in the relevant clients.

User Roles for Non-ABAP Source System

To establish a secondary database connection from an ABAP system to an external database, the connection data and the user data of a user are required. This user must be authorized to establish a connection to the external database. The ABAP system connects to a specific schema from the database. To perform the replication and initially load a specific table from a given schema, the database user must have privileges for the following actions:

- Selecting from the table
- Creating a table in the given schema (for creating the logging table)
- Selecting from the logging table
- Deleting the logging table
• Creating database triggers for the table
• Deleting the triggers
• Creating synonyms for the specific table
• Deleting the synonyms

Depending on the specific external database system, the process of granting privileges to a user can vary.

⚠️ If you want to transfer data from non-ABAP source systems, the relevant user in the SAP Landscape Transformation Replication Server system needs the role SAP_IUUC_REPLREMOTE in addition to the role SAP_IUUC_REPL_ADMIN. Alternatively, you can adjust the role SAP_IUUC_REPL_ADMIN. Ensure that the following activities for the authorization object S_DMC_S_R are selected:

01 - Create or Generate
33 - Read
34 - Write
40 - Create in DB
41 - Delete in DB
**Authorizations in the SAP HANA System**

The replicated data is stored in the SAP HANA system. The authorization concept of the SAP HANA database is used.

**Initial User**

The SAP LT Replication Server requires an initial user, which is used to create a database connection from the SAP LT Replication Server to the SAP HANA system. The database connection is automatically created when you set up a new configuration.

Create a new user with the following authorizations in the SAP HANA system as described below:

**System Privileges**

On the tab *System Privileges*, add the following system privileges:

- CREATE SCHEMA
- ROLE ADMIN
  - This privilege is required for creating roles for data provisioning and for accessing the schema. This privilege can be revoked once the configuration has been created.
- USER ADMIN
  - If you want SAP Landscape Transformation Server to create a new target schema, the system creates the schema on the HANA database together with the corresponding user. In order to do this, both privileges CREATE SCHEMA and USER ADMIN are required. The privilege USER ADMIN can be revoked once the schema has been created.

**SQL Privileges**

In the SAP HANA system, the table `RS_REPLICATION_COMPONENTS` contains information about the source systems connected the SAP HANA system via SAP Landscape Transformation Server. In order to register a new configuration when one is created, and to deregister a configuration when one is deleted, certain SQL privileges are required.

When you create the first SAP LT Replication Server configuration for an SAP HANA database, the SQL schema `SYS_REPL` is created in the SAP HANA database. If another database user requires access to this configuration (or configurations created after this one), then you need to assign the system privileges mentioned above to this user, as well as the following SQL privileges:

- On the tab *SQL Privileges*, add the SQL object `SYS_REPL`, and select the following privileges:
  - EXECUTE
  - SELECT
  - INSERT
  - UPDATE
  - DELETE
Replication User

The SAP LT Replication Server creates the replication user by using the initial user for this operation. One replication user is created for each replication schema. The replication user has the same name as the corresponding schema.

The replication user is used to connect from the SAP LT Replication Server to the SAP HANA system for replication. The authentication information for the replication user is generated by the SAP LT Replication Server and stored as a secondary database connection in the SAP LT Replication Server. This means that only the SAP LT Replication Server can connect as replication user to the SAP HANA system.

The replication user has the following authorizations:

- SELECT authorization on table SYS_REPL_RS_REPLICATION_COMPONENTS to read SAP LT Replication Server configuration information

Replication Roles

The following roles are defined and have authorization on the target schema on the SAP HANA system:

- `<REPLICATION_SCHEMA>_DATA_PROV`
  Assign this role to users who configure and monitor the data provisioning process. This role has the right to select data in the replication schema and to insert values into the RS_ORDER table within the replication schema.

- `<REPLICATION_SCHEMA>_POWER_USER`
  This role provides full control over the contents of the replication schema.

  Assign this role only for urgent operations, such as maintenance operations. The rights granted by this role allow the user to perform operations that can destroy the consistency of the replicated data.

- `<REPLICATION_SCHEMA>_USER_ADMIN`
  This role provides access to the database stored procedures RS_GRANT_ACCESS and RS_REVOKE_ACCESS. They are used for fine-grained access control on the replication schema content.

- `<REPLICATION_SCHEMA>_SELECT_USER`
  This role contains select privilege of the entire replication target schema.

Note that the access rights assigned to each of these roles do not include a grant option. This means that users who have been granted these roles cannot grant the individual privileges to other users and roles. This is due to the fact that granted privileges depend on the privilege of the granting user: If the granting user is revoked the privilege, or is entirely dropped, the granted privileges are also revoked.

The following select user role that can be granted to others is automatically created in the schema in the SAP HANA system:

- `<schema>_SELECT_USER_GRANTABLE`
Note that for configurations created using SP11 or lower, this role must be created manually in the SAP HANA system. For more information, see SAP Note 2307329.

Managing Access to Replicated Tables
Access to replicated tables is managed by a user of the role <REPLICATION_SCHEMA>_USER_ADMIN by calling either the procedure RS_GRANT_ACCESS or RS_REVOKE_ACCESS.

Access to the configuration and monitoring tables that start with prefix ‘RS_’ cannot be granted or revoked by this procedure.

Granting Access
Access to a table is granted by calling the procedure RS_GRANT_ACCESS, which has the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLENAME</td>
<td>Table name to grant privileges</td>
</tr>
<tr>
<td>GRANTEE</td>
<td>User/Role that is granted privileges</td>
</tr>
<tr>
<td>SELECT_PRIVILEGE</td>
<td>‘X’ to grant SELECT privilege, ‘ ’ for no operation</td>
</tr>
<tr>
<td>INSERT_PRIVILEGE</td>
<td>‘X’ to grant INSERT privilege, ‘ ’ for no operation</td>
</tr>
<tr>
<td>UPDATE_PRIVILEGE</td>
<td>‘X’ to grant UPDATE privilege, ‘ ’ for no operation</td>
</tr>
<tr>
<td>DELETE_PRIVILEGE</td>
<td>‘X’ to grant DELETE privilege, ‘ ’ for no operation</td>
</tr>
</tbody>
</table>

Revoking Access
Access to a table is revoked by calling the procedure RS_REVOKE_ACCESS, which has the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLENAME</td>
<td>Table name to revoke privilege</td>
</tr>
<tr>
<td>GRANTEE</td>
<td>User/Role that is revoked a privilege</td>
</tr>
<tr>
<td>SELECT_PRIVILEGE</td>
<td>‘X’ to revoke SELECT privilege, ‘ ’ for no operation</td>
</tr>
<tr>
<td>INSERT_PRIVILEGE</td>
<td>‘X’ to revoke INSERT privilege, ‘ ’ for no operation</td>
</tr>
<tr>
<td>UPDATE_PRIVILEGE</td>
<td>‘X’ to revoke UPDATE privilege, ‘ ’ for no operation</td>
</tr>
<tr>
<td>DELETE_PRIVILEGE</td>
<td>‘X’ to revoke DELETE privilege, ‘ ’ for no operation</td>
</tr>
</tbody>
</table>
Monitoring Access Management

Calling RS_GRANT_ACCESS and RS_REVOKE_ACCESS writes log entries into the table RS_MESSAGES. The Component field of the RS_MESSAGES table is populated with RS_GRANT_ACCESS or RS_REVOKE_ACCESS respectively. The following information is logged:

- Affected table (column TABLENAME)
- Time stamp of operation (column MESSAGETIME)
- Errors in granting / revoking privileges (column LINE)
  - Try to grant to / revoke from reserved table
  - Try to grant on non-existent table
  - Try to grant to / revoke from non-existent user or role
- Privileges granted / revoked by user in the form of a line (column LINE)
  <PRIVILEGE> TO <USER> BY <CURRENT_USER> or
  <PRIVILEGE> FROM <USER> BY <CURRENT_USER> or
  Where <CURRENT_USER> is the calling user of the procedure.

Restricting Access to the Source System

There may be situations where you want to control the access of the SAP LT Replication Server to data in source systems. To do this, you can use the control table IUUC_TAB_ALLOWED in the SAP ABAP-based source system. In this table, you can specify which configuration can access which table in the source system, and you can also limit the data access to a particular client.

Note about Unrestricted Access

If table IUUC_TAB_ALLOWED is empty then every configuration in every SAP LT Replication Server system has unrestricted access to all tables in the source system.

If table IUUC_TAB_ALLOWED contains at least one entry, then the system restricts the access to data in the source system to only those entries. If you want additional access to data, you need to create additional entries in the table.

The fields in table IUUC_TAB_ALLOWED are described below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLT_SID</td>
<td>The SAP LT Replication Server system ID.</td>
</tr>
<tr>
<td>CONFIG_GUID</td>
<td>The SAP LT Replication Server system configuration</td>
</tr>
<tr>
<td>TABNAME</td>
<td>The source system table name</td>
</tr>
</tbody>
</table>
### Field: **ALL_CLIENTS**

In this field, you can specify whether the configuration can only access the client specified in the RFC connection associated with the configuration (a blank entry) or whether the configuration can access data in all clients (an X). Note that read access to a single client is only possible if the option Read from Single Client must be set to active when you created the configuration. If this flag is not active, and the field ALL_CLIENT contains a blank entry, then read access will be completely blocked.

#### Examples

<table>
<thead>
<tr>
<th>SLT_SID</th>
<th>CONFIG_GUID</th>
<th>TABNAME</th>
<th>ALL_CLIENTS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLT</td>
<td>4713</td>
<td>SFLIGHT</td>
<td>x</td>
<td>Configuration 4713 from the SAP LT Replication Server system <code>SLT</code> can access data in table SFLIGHT in all clients. Read access to all other tables in the source system is blocked.</td>
</tr>
<tr>
<td>PLT</td>
<td>1234</td>
<td>C1ES_GO</td>
<td></td>
<td>Configuration 1234 from SAP LT</td>
</tr>
<tr>
<td>SLT_SID</td>
<td>CONFIG_GUID</td>
<td>TABNAME</td>
<td>ALL_CLIENTS</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SLT</td>
<td>4711</td>
<td>SFLIGHT</td>
<td>x</td>
<td>Every configuration in every connected SAP LT Replication Server system can access data in table SFLIGHT in all clients. Read access to all other tables in the source system is blocked.</td>
</tr>
<tr>
<td>SLT</td>
<td>4711</td>
<td>SPLANE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. Network and Communication Security

Network Security
Access to ABAP source systems using SAP LT Replication Server takes place exclusively through RFC connections. For more information about security-relevant information concerning RFC, see the SAP Library on SAP Help Portal.

For non-ABAP source systems a database connection has to be established to transfer the data from the source to the SAP LT Replication Server. For more information, refer to the relevant database vendor documentation.

SAP NetWeaver Business Client for WebDynpro Applications

In order to ensure compliance with security standards, the Configuration and Monitoring Dashboard (transaction LTR) requires the use of the SAP NetWeaver Business Client 3.5 or 4.0.

The reason for this is that the SAP NetWeaver Business Client supports a logout for all Web Dynpro windows. Web browsers do not support this logout feature. For example if you use a web browser to access the work center, there is no option to logout. Simply closing the web browser window does not log the user out of the system. The session runs on the server until it times out, and this is a potential security risk.

For more information about how to configure the SAP NetWeaver Business Client, see the SAP Landscape Transformation Replication Server installation guide and the SAP Landscape Transformation Replication Server Application operations guide.

Communication Destinations
The SAP LT Replication Server does not come with fixed destinations or user names. The following communication destinations need to be created:

ABAP Source System
1. Create a user (type Dialog) in your source system with the role SAP_IUUC_REPL_REMOTE.
2. Create an RFC connection (type 3 – ABAP) from the SAP LT Replication Server system to the source system with the created user. If both systems are Unicode, specify this RFC as Unicode.
   
   ![Warning icon]

   Do not use the DDIC user for RFC connection. If the source system and the SAP LT Replication Server are the same system, also create an RFC connection. Do not use the option NONE.

3. Use the created RFC to define the connection between the ABAP source system and the SAP LT Replication Server within your new configuration.
Non-ABAP Source System

To establish a secondary database connection, the user must have the required privileges as described under User Roles for Non-ABAP Source System.

Use the created database connection to define the connection between the ABAP source system and the SAP LT Replication Server within your new configuration.

SAP HANA System

If you set up a new configuration, the database connection from the SAP LT Replication Server system to the SAP HANA system is created automatically.

7. Security-Relevant Logging and Tracing

SAP Landscape Transformation Replication Server uses the logging and tracing capabilities provided by the SAP NetWeaver AS ABAP platform. For example, the logging of security-related events is handled by the security audit log (transaction SM19, transaction SM20).

For more information see: SAP NetWeaver Security Guide -> Logging and Tracing.

8. Data Protection

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This section describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

In the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the simplified blocking and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>

SAP HANA Platform
Security Guide – Trigger-Based Data Replication Using SAP LT Replication Server

<table>
<thead>
<tr>
<th>Personal data</th>
<th>Information about an identified or identifiable natural person.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business purpose</td>
<td>A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.</td>
</tr>
<tr>
<td>Blocking</td>
<td>A method of restricting access to data for which the primary business purpose has ended.</td>
</tr>
<tr>
<td>Deletion</td>
<td>Deletion of personal data so that the data is no longer usable.</td>
</tr>
<tr>
<td>Retention period</td>
<td>The time period during which data must be available.</td>
</tr>
<tr>
<td>End of purpose (EoP)</td>
<td>A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorization.</td>
</tr>
</tbody>
</table>

Some basic requirements that support data protection are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and require appropriate TOMs:

- **Access control**: Authentication features as described in section User Administration and Authentication.
- **Authorizations**: Authorization concept as described in section Authorizations.
- **Read access logging**: As described in section Read Access Logging.
- **Transmission control / Communication security**: as described in section Network and Communication Security [Page 17]

**Separation by purpose**: Is subject to the organizational model implemented and must be applied as part of the authorization concept.

⚠️

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

**Read Access Logging**

If no trace or log is stored that records which business users have accessed data, it is difficult to track the person(s) responsible for any data leaks to the outside world. The Read Access Logging (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data, for example, of a business partner, and in which time frame.

In RAL, you can configure which read-access information to log and under which conditions.
For more information about RAL, Read Access Logging in the documentation for SAP NetWeaver

**Additional Information for INDX-like Tables**

Data in INDX-like tables is stored in a compressed and raw data format. Data from an INDX-like table cannot be read in a usual way. Only applications that have specific authorizations can read data from these tables, and write its data to standard tables in a readable format.

SAP Landscape Transformation Replication Server is such an application. It can transfer data from INDX-like tables to a standard table in the target system in a readable format.

Data from INDX-like tables may need to be made transparent for audit or analysis purposes. However, once data is extracted from an INDX-like table, and is moved to a standard table in a readable format, the original authorization concept no longer applies. That is, data in standard tables can be read using functions that are not application-dependent, and which typically lack the authorizations that applied to the source INDX-like table. For example, standard tables can be accessed by using transaction SE16.

INDX-like tables can contain data of a personal or sensitive personal nature. This type of table is used extensively by SAP ERP HCM. Examples of HCM data that is stored in INDX-like tables include payroll and absence data, though any conceivable type of sensitive data could be stored in these tables. The customer must ensure that the transparent data extracted from INDX-like tables is protected in a manner that conforms to local data protection regulations.

An additional consideration for INDX-like tables concerns transaction CNV_INDX_OVERVIEW. If a user has the authorizations required to use this transaction, they can view the data from INDX-like tables directly. This data can be highly sensitive, and the environment could be productive. With sufficient authorizations, a user can simply select an INDX-like table, then an application area such as Payroll Results, and then view individual records containing, for example, wage type and money amounts for specific personnel numbers.

Since transaction CNV_INDX_OVERVIEW is so critical, there is no standard role that enables a user to use it. In addition, the authorizations required are very strict and should only be granted to a user that has a specific requirement to test or analyze an SAP Landscape Transformation Replication Server function. It must be understood that a user with the required authorizations can then see all the data in the specifically selected INDX-like table.

The following table outlines the required authorizations:

<table>
<thead>
<tr>
<th>Authority Object</th>
<th>Field 1</th>
<th>Field 2</th>
<th>Field 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_TCODE</td>
<td>TCD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field Values</td>
<td>CNV_INDX_OVERVIEW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S_DMIS</td>
<td>MBT_PR_ARE</td>
<td>MBT_PR_LEV</td>
<td>ACTVT</td>
</tr>
<tr>
<td>Field Values</td>
<td>SLOP</td>
<td>PACKAGE</td>
<td>02</td>
</tr>
<tr>
<td>S_TABU_DIS</td>
<td>DICBERLCS</td>
<td></td>
<td>ACTVT</td>
</tr>
<tr>
<td>Field Values</td>
<td>DM06</td>
<td>03</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td><strong>S_TABU_NAME</strong></td>
<td>ACTVT</td>
<td>TABLE</td>
<td></td>
</tr>
<tr>
<td>Field Values</td>
<td>03</td>
<td>INDX-like table to which access is required (for example PCL2)</td>
<td></td>
</tr>
</tbody>
</table>