Security Guide
SAP Landscape Transformation Replication Server
Document Version: 1.1 – 2019-11-22

CUSTOMER

SAP Landscape Transformation Replication Server

For SAP HANA Platform 2.0 SPS04

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	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.
`Example`	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.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

Version	Date	Change
1.0	2019-01-28	Initial published version for DMIS 2018 SP01.
1.1	2019-09-09	Initial published version for DMIS 2018 SP02.
1.2	2019-11-22	Updated version November 2019.

Table of Contents

1 Introduction

1.1 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.

1.2 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.

1.3 About this Document

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

1.4 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

2.1 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.

Guide	Location
Security Guide - Replicating Data to SAP HANA	http://help.sap.com/sapslt
Installation Guide – Replicating Data to SAP HANA	http://help.sap.com/sapslt
Sizing Guide	https://service.sap.com/sizing → Sizing Guidelines → Database and Technology → SAP In-Memory Computing → SAP Landscape Transformation Replication Server, SAP HANA

2.2 SAP HANA Guides

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

Topic	Quick Link
SAP HANA Landscape, Deployment & Installation	http://help.sap.com/hana → Installation and Upgrade
SAP HANA Administration	http://help.sap.com/hana → Administration
SAP HANA Security	http://help.sap.com/hana → Security

2.3 Important SAP Notes

SAP Note Number	Title	Comment
1514967	SAP HANA: Central Note	Central SAP Note about SAP HANA
1598623	SAP HANA appliance software: Central Security Note	Current information about SAP HANA security topics

3 Technical System Landscape

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

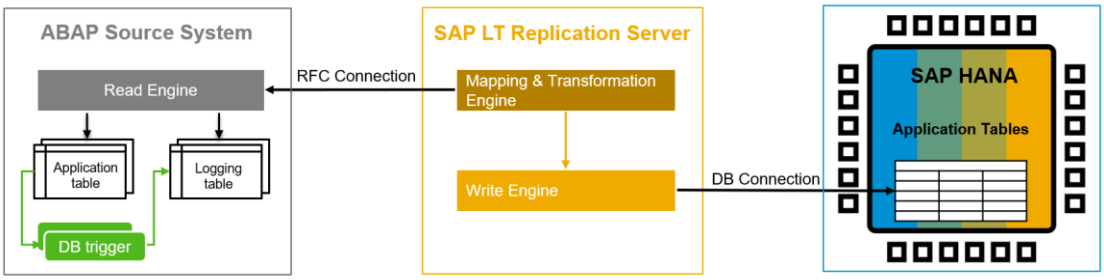
  The SAP HANA system contains the SAP HANA database. It is used to store the replicated data. The SAP LT Replication Server system and the SAP HANA system communicate by means of a database connection.

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 SAP LT Replication Server Cockpit (transaction LTRC), you can define a new configuration.

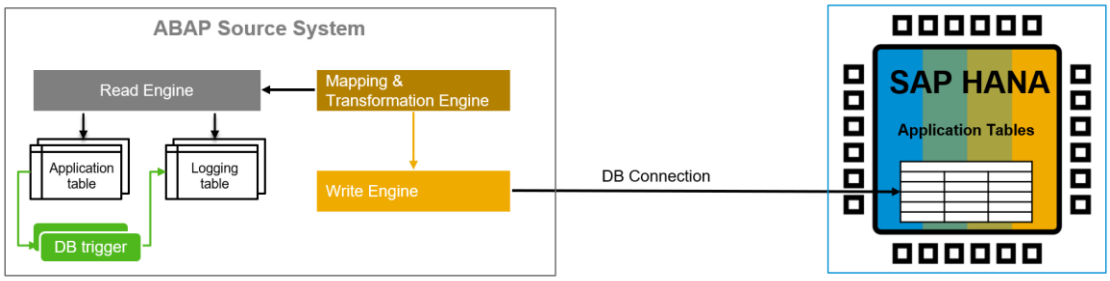
The following figures show the possible technical system landscapes for SAP LT Replication Server.

Option 1 – ABAP Source System with Separate SAP LT Replication Server System



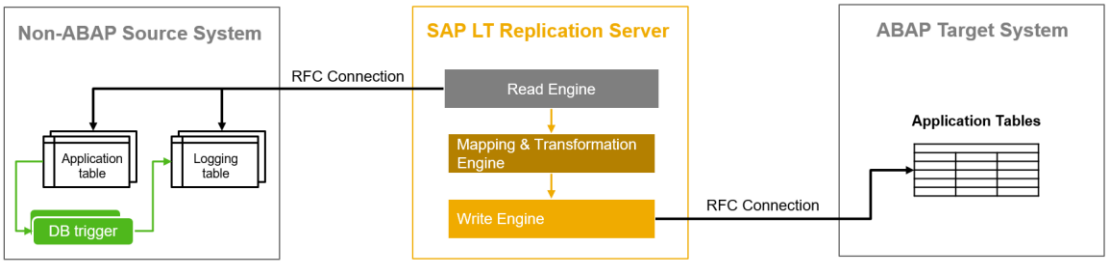
SAP LT Replication Server is installed in a separate ABAP system. Therefore, two network communication channels are required - the RFC connection to the source system and the connection to the SAP HANA system.

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 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 system:

- SAP LT Replication Server

  To access the SAP LT Replication Server Cockpit in the SAP LT Replication Server system, a user with specific authorizations is required. This user can create a new configuration, which is used to establish the connection between the source system, the SAP LT Replication Server, and the SAP HANA system.

  There are two possibilities for replicating data to SAP HANA using SAP Landscape Transformation Replication Server. The database connection to the target system is either managed by SAP LT Replication Server or not (for more information, see the SAP LT Replication Server application help at http://help.sap.com/sapslt).

  If the database connection to the target system is managed by SAP LT Replication Server, a user in the SAP HANA system is required that is authorized to create the SAP HANA database schema. You can access the SAP LT Replication Server Cockpit by using transaction `LTRC`.

  If the database connection to the target system is not managed by SAP LT Replication Server, you need to ensure that the database schema (replication schema) that will contain the target tables already exists. You then create a secondary database connection to the SAP HANA system. We recommend creating one replication user for each replication schema. We also recommend that 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. This means that only the SAP LT Replication Server can connect as replication user to the SAP HANA system. The replication user needs full access to the target database schema (EXECUTE, SELECT, INSERT, UPDATE, and DELETE privileges), and has read access to schema SYS.

- ABAP Source System

  In order to access the ABAP source system by RFC, a communication user is required. To create an 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.

Note

The user role SAP_IUUC_REPL_ADMIN is required to use SAP Landscape Transformation Replication Server. By default, this role does not allow 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.

> Note
>
> 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.

5.1 Authorization Objects

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

5.1.1 S_DMIS

Description: Authority object for SAP SLO Data migration

Authorization fields:

Field name	Heading
MBT_PR_ARE	MBT PCL: Scenario
MBT_PR_LEV	MBT PCL: Processing Role Level
ACTVT	Activity

5.1.2 S_DMC_S_R

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

Authorization fields

Field name	Heading
ACTVT	Activity

5.1.3 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.

5.1.4 S_DMIS_MOM

Description: Authorizations for MWB/ Migration Object Modeler

Authorization fields:

Field name	Heading
ACTVT	Activity

If you need to check, create, edit, or delete migration objects by using MWB or transaction `LTMOM`, these authorizations will be checked.

5.2 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`).

5.2.1 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

> **Note**
>
> With SAP Landscape Transformation Replication Server SP13, new versions of the roles SAP_IUUC_REPL_ADMIN and SAP_IUUC_REPL_DISPLAY were delivered. If you are upgrading to SP15 from a lower release (not SP13), you must ensure that you have the new versions of these roles in the relevant clients.

5.2.2 User Roles for ABAP Source System

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

SAP_IUUC_REPL_REMOTE

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

> **Note**
>
> 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.

5.2.3 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.

Note

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_REPL_REMOTE 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

5.3 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.

Depending on the scenario you have chosen for your replication to SAP HANA, different requirements for authorizations apply:

5.3.1 Option 1: Replicating to SAP HANA System (database connection managed by SAP)

5.3.1.1 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:

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.
- CATALOG READ

  This privilege is required to read the existing schemas in the SAP HANA database. This prevents a schema being created that has the same name as an existing schema.

5.3.1.2 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 Replication 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

> Note:
>
> You can use the following SQL script to create this user in the SAP HANA system:

```
create user SLT_USR password <pwd>;
grant user admin to SLT_USR;
grant CREATE SCHEMA to SLT_USR;
grant ROLE ADMIN to SLT_USR;
grant CATALOG READ to SLT_USR;

grant insert on schema _SYS_REPO to SLT_USR;
grant delete on schema _SYS_REPO to SLT_USR;
grant update on schema _SYS_REPO to SLT_USR;
grant select on schema _SYS_REPO to SLT_USR;

grant insert on schema SYS_REPL to SLT_USR with grant option;
grant delete on schema SYS_REPL to SLT_USR with grant option;
grant update on schema SYS_REPL to SLT_USR with grant option;
grant select on schema SYS_REPL to SLT_USR with grant option;
grant execute on schema SYS_REPL to SLT_USR with grant option;
```

5.3.1.3 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.

5.3.1.4 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.

  > **Note**
  >
  > 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 privileges 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.

5.3.1.5 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.

> **Note**
>
> Access to the configuration and monitoring tables that start with prefix 'RS_' cannot be granted or revoked by this procedure.

5.3.1.6 Granting Access

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

Parameter	Description
TABLENAME	Table name to grant privileges
GRANTEE	User/Role that is granted privileges
SELECT_PRIVILEGE	'X' to grant SELECT privilege, ' ' for no operation
INSERT_PRIVILEGE	'X' to grant INSERT privilege, ' ' for no operation
UPDATE_PRIVILEGE	'X' to grant UPDATE privilege, ' ' for no operation
DELETE_PRIVILEGE	'X' to grant DELETE privilege, ' ' for no operation

5.3.1.6.1 Revoking Access

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

Parameter	Description
TABLENAME	Table name to revoke privilege
GRANTEE	User/Role that is revoked a privilege
SELECT_PRIVILEGE	‘X’ to revoke SELECT privilege, ‘ ‘ for no operation
INSERT_PRIVILEGE	‘X’ to revoke INSERT privilege, ‘ ‘ for no operation
UPDATE_PRIVILEGE	‘X’ to revoke UPDATE privilege, ‘ ‘ for no operation
DELETE_PRIVILEGE	‘X’ to revoke DELETE privilege, ‘ ‘ for no operation

5.3.1.7 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.

5.3.2 Option 2: Replicating to SAP HANA System (database connection not managed by SAP)

5.3.2.1 Schemas in Target Database

Whereas the schema in the target database is created by SAP LT Replication Server for option 1, for this option you need to ensure that the database schema (replication schema) that will contain the target tables already exists.

5.3.2.2 Replication User

We recommend creating one replication user for each replication schema. We also recommend that 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. This means that only the SAP LT Replication Server can connect as replication user to the SAP HANA system.

The replication user needs full access to the target database schema (EXECUTE, SELECT, INSERT, UPDATE, and DELETE privileges), and has read access to schema SYS.

> Note
>
> Your system administrator needs to provide the required authorizations for any users that require access to replicated tables. SAP LT Replication Server does not create any roles for accessing the replicated tables.

5.3.3 Restricting Access to the Source System

Important Information

By default, the SAP LT Replication Server system has unrestricted access to all tables in the ABAP-based SAP source system.

However, there may be situations where you want to restrict the access to data. To do this, you can use table DMC_C_WL_TABL_OP in the ABAP-based SAP source system. This table is delivered empty, which means that the SAP LT Replication Server system has unrestricted access to all tables.

In this table, you can specify which remote RFC user can access which tables in the source system. In addition, you can specify the type of the action that can be performed on the table. The following actions are possible:

- Read table metadata
- Load data from the table
- Replicate data from the table
- Create a freeze trigger for the table

  A standard database trigger records changes to a table (INSERT, UPDATE, and DELETE statements) in a logging table. If a freeze trigger exists for a table, then the system returns an error message if a standard database trigger records a change for the table. Instead of creating an entry in the logging table for the

trigger, the system creates an error message. In this way, you can use freeze triggers to prevent changes to the source system table, and to be informed if any attempt is made to change data in the table.

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

If the action READ_METADATA is permitted for a table, and the table has include structures, you must also permit the action READ_METADATA for the include structures. Note that it is not necessary to permit other actions such as LOAD_DATA or REPLICATE_DATA for the include structures.

The fields in table DMC_C_WL_TABL_OP are described below:

Field	Description
RFC_USER	The user specified in the RFC connection used to connect to the ABAP-based source system.
TABLENAME	The name of the table in the source system.
READ_METADATA	If set to 'X', then the SAP LT Replication Server system is permitted to read metadata for the table.
LOAD_DATA	If set to 'X', then the SAP LT Replication Server system is permitted to load data from the specified table.
REPLICATE_DATA	If set to 'X', then the SAP LT Replication Server system is permitted to replicate data from the specified table.
FREEZE_TRIGGER	If set to 'X', then the SAP LT Replication Server system is permitted to create a freeze trigger for the specified table.

Note: If you permit the actions LOAD_DATA or REPLICATE_DATA for a table, then you must also permit the action READ_METADATA for the table. This is because SAP LT Replication Server needs to read the metadata of a table before performing the initial load or starting the replication process.

5.3.3.1 Examples

Example 1

In the example outlined in the table below, the SAP LT Replication Server system (specifically user SJOHN) is not permitted to perform any actions for the source system table SBOOK.

Note that as long as table DMC_C_WL_TABL_OP contains at least one entry, the SAP LT Replication Server system is not permitted to perform any action for any source system tables. If you want additional access to data, you need to create additional entries in the table.

Note the SAP LT Replication Server system is connected to the ABAP-based SAP source system by means of an RFC connection created with the user SJOHN.

RFC_USER	TABLENAME	READ_METADATA	LOAD_DATA	REPLICATE_DATA	FREEZE_TRIGGER
SJOHN	SBOOK				

Example 2

In the example outlined in the table below, the SAP LT Replication Server system (specifically user SJOHN) is permitted to load data from the source system table SBOOK.

Note the SAP LT Replication Server system is connected to the ABAP-based SAP source system by means of an RFC connection created with the user SJOHN.

RFC_USER	TABLENAME	READ_METADATA	LOAD_DATA	REPLICATE_DATA	FREEZE_TRIGGER
SJOHN	SBOOK	X	X		

Example 3

In the example outlined in the table below, the SAP LT Replication Server system (specifically user SJOHN) is permitted to read metadata from the source system table SBOOK, and also to replicate data from the table.

Note the SAP LT Replication Server system is connected to the ABAP-based SAP source system by means of an RFC connection created with the user SJOHN.

RFC_USER	TABLENAME	READ_METADATA	LOAD_DATA	REPLICATE_DATA	FREEZE_TRIGGER
SJOHN	SBOOK	X		X	

Note:

For SAP Landscape Transformation Replication Server versions SP13 and lower, table IUUC_TAB_ALLOWED was used to restrict access to the ABAP-based SAP source system. For SP14 and higher, table DMC_C_WL_TABL_OP is used to restrict access. If you are installing SAP LT Replication Server for the first time (using SP15), both tables will be delivered empty, and you can use table DMC_C_WL_TABL_OP as described in this section.

If you are upgrading to SP15 from a lower SP, the system checks whether there are any entries in table DMC_C_WL_TABL_OP. If the table is empty, the system checks whether there are any entries in table IUUC_TAB_ALLOWED. If there are entries in table IUUC_TAB_ALLOWED, then these entries will be considered by the system. If you subsequently make an entry in table DMC_C_WL_TABL_OP, then only table DMC_C_WL_TABL_OP will be considered by the system; table IUUC_TAB_ALLOWED will be disregarded completely. So, while it is possible to continue using table IUUC_TAB_ALLOWED, we strongly recommend using table DMC_C_WL_TABL_OP instead.

Note that if you permit actions for a table using table IUUC_TAB_ALLOWED, and the table has include structures, you must also permit actions for the include structures.

6 Network and Communication Security

6.1 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.

If any of the participating systems are located in a public network or are connected to a public network, then you need to establish suitable protection mechanisms such as introducing a firewall.

6.2 Communication Destinations

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

6.3 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.

   Note:

   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.

6.4 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.

6.5 SAP HANA System

If the database connection from the SAP LT Replication Server system to the SAP HANA system is managed by SAP LT Replication Server, then the database connection is created automatically.

If the database connection from the SAP LT Replication Server system to the SAP HANA system is not managed by SAP LT Replication Server, then you need to establish a secondary database connection as described in the SAP LT Replication Server operations guide and in the application help (https://help.sap.com/sapslt). Note that the user must have the required privileges as described in section "Authorizations in the SAP HANA System" of chapter "Authorizations".

The created database connection is then used to define the connection between the SAP LT Replication Server and the target database within your new configuration.

For more information about the two options for replicating data to SAP HANA, see the application help at http://help.sap.com

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 Privacy and Protection

8.1 Overview

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.

> Note
>
> 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

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business purpose	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.
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Deletion	Deletion of personal data so that the data is no longer usable.
Retention period	The time period during which data must be available.

Term	Definition
End of purpose (EoP)	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.

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

> ### Caution
>
> 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.

8.2 Deletion of Personal Data

SAP LT Replication Server might transfer data (personal data) that is subject to the data protection laws applicable in specific countries. Usually, this data is not persisted nor accessible within the SAP LT Replication Server system. The data is only present in-memory during the replication process.

The only exception to this is the replication logging feature (refer to chapter 8 of the SAP LT Replication Server Operations Guide). With this feature, the content of replicated tables may be stored in the SAP LT Replication Server system for a certain amount of time, customizable by the SAP LT Replication Server user. The data is persisted in a cluster table which means that it cannot be accessed by using database tools such as transaction `SE16`.

Nevertheless, it is possible to access this data by using an SLT expert function in transaction `LTRC` (if the user is authorized to use the expert function). As part of the data privacy and protection mechanisms, access to the data may be logged via Read Access Logging (described in the next chapter).

The data stored by the replication logging feature is permanently deleted once the defined threshold for temporary storage is reached and the SAP LT Replication Server cleanup report `(IUUC_HOUSEKEEPING)` is executed. The cleanup report is executed at three different points in time:

1. When the SAP LT Replication Server system is restarted.
2. At midnight.
3. Whenever the configuration that uses the replication logging feature is deactivated and activated again.

The customization of the retention period (threshold for deletion) can be configured by using transaction `LTRS`.

8.3 Read Access Logging

Read access to personal data is partially based on legislation, and it is subject to logging functionality. 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, fields related to bank account data), and when they did so.

In RAL, you can configure which read-access information to log and under which conditions.

Within SAP LT Replication Server, Read Access Logging has been configured for the Replication Logging feature, where data replicated from a source system to a target system is temporarily stored in the SAP LT Replication Server system (refer to chapter 8 of the SAP LT Replication Server Operations Guide). As SAP LT Replication Server does not know about the content of the tables which are replicated and whether these tables contain personal data, any access to the temporary storage will be logged if Read Access Logging is activated. The log will provide information that a certain user accessed data for a certain table.

Prerequisites

Before you can use the delivered RAL configurations, the following prerequisites are met:

- Ensure that your SAP Basis release supports RAL. For more information, see SAP Note 1969086.
- You have enabled RAL in each system client.

Activating the RAL Configuration

1. In transaction `SRALMANAGER`, on the *Administration* tab page, choose *Configuration*.
2. Choose the desired channel, which is “Dynpro”.
3. Choose *Search*.

   The system displays the available configurations for the selected channel.

   An example configuration for SAP LT Replication Server replication logging feature is SAP_CA_LT_LTRC_DYNPRO.
4. Choose *Display Configuration* for detailed information on the configuration. For specific channels, related recordings can also be displayed.
5. Select the configuration and choose *Activate*.

More Information

For general information on Read Access Logging, see the product assistance for SAP NetWeaver on SAP Help Portal at http://help.sap.com/netweaver → *SAP NetWeaver Library: Function-Oriented View* → *System Security for SAP NetWeaver AS for ABAP Only*.

For up-to-date information on the delivered RAL configurations, see SAP Note 1514967.

8.4 Keeping Data in the Target System Secure

Once data is extracted from a source table and is moved to a table in the target system, the SAP LT Replication Server authorization concept no longer applies. That is, data in target tables can be read using functions that are not part of SAP LT Replication Server, and that lack the authorizations that are in place when SAP LT Replication Sever reads data from the source system. You must therefore ensure that access to data in the target system is managed in a secure way.

8.5 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:

Authority Object	Field 1	Field 2	Field 3
S_TCODE	TCD		
Field Values	CNV_INDX_OVERVIEW		
S_DMIS	MBT_PR_ARE	MBT_PR_LEV	ACTVT
Field Values	SLOP	PACKAGE	02
S_TABU_DIS	DICBERLCS	ACTVT	
Field Values	DM06	03	
S_TABU_NAM	ACTVT	TABLE	
Field Values	03	INDX-like table to which access is required (for example PCL2)	

www.sap.com/contactsap

Material Number