



## SAP HANA Security Guide - Trigger-Based Data Replication

### Using SAP LT (Landscape Transformation) Replication Server for SAP HANA

- SAP HANA Appliance Software SPS04

#### Target Audience

- Consultants
- Administrators
- SAP Hardware Partner
- Others

Public

Document version 1.0 – 30/04/2012

THE BEST-RUN BUSINESSES RUN SAP



## Copyright

© Copyright 2012 SAP AG. All rights reserved.

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

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group. Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.






Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and

services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

## Icons in Body Text

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

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

Type Style	Description
<i>Example text</i>	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.
<b>Example text</b>	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	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 text	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.
<b>Example text</b>	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE TEXT	Keys on the keyboard, for example, F2 or ENTER.

Introduction .....	4
Before You Start.....	6
Technical System Landscape .....	8
User Administration and Authentication.....	11
Authorizations .....	12
Network and Communication Security.....	16
Network Security .....	16
Communication Destinations.....	16



## 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 the Trigger-Based Data Replication Using SAP LT (Landscape Transformation) Replication Server. To assist you in securing the Trigger-Based Data Replication Using SAP LT Replication Server, we provide this Security Guide.

## About this Document

The Security Guide provides an overview of the security-relevant information that applies to the Trigger-Based Data Replication Using SAP LT 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 the *Trigger-Based Data Replication Using SAP LT 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 the *Trigger-Based Data Replication Using SAP LT Replication Server*.

- **Network and Communication Security**

This section provides an overview of the communication paths used by the *Trigger-Based Data Replication Using SAP LT Replication Server* and the security mechanisms that apply.



## Before You Start

### Related Guides

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

#### SAP LT (Landscape Transformation) Replication Server Guides

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

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace
Trigger-based Replication	<i>Installation Guide</i>	<a href="https://service.sap.com/hana">https://service.sap.com/hana</a> <a href="#">SAP HANA Installation Guide - Trigger Based Replication (SLT)</a>

#### SAP HANA Guides

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

Topic	Guide/Tool	Quick Link
SAP HANA Landscape, Deployment & Installation	<i>SAP HANA Knowledge Center on SAP Service Marketplace</i>	<a href="https://service.sap.com/hana">https://service.sap.com/hana</a> → <a href="#">SAP HANA Master Guide</a> → <a href="#">SAP HANA Installation Guide</a>
SAP HANA Administration & Security	<i>SAP HANA Knowledge Center on SAP Help Portal</i>	<a href="http://help.sap.com/hana">http://help.sap.com/hana</a> <a href="http://help.sap.com/hana_appliance">http://help.sap.com/hana_appliance</a> → <a href="#">SAP HANA Technical Operations Manual</a> → <a href="#">SAP HANA Security Guide</a>

For a complete list of the available SAP Security Guides, see SAP Service Marketplace at <http://service.sap.com/securityguide>.

### Important SAP Notes

SAP Note	Link
<a href="#">SAP Note 1514967 SAP HANA: Central Note</a>	Central SAP Note about SAP HANA appliance software
<a href="#">SAP Note 1598623 SAP HANA appliance software: Central Security Note</a>	Current information about SAP HANA security topics

For a list of additional security-relevant SAP Hot News and SAP Notes, see SAP Service Marketplace at <http://service.sap.com/securitynotes>.

### Additional Information

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

Content	Quick Link on SAP Service Marketplace or SDN
Security	<a href="http://sdn.sap.com/irj/sdn/security">http://sdn.sap.com/irj/sdn/security</a>

Security Guides	<a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a>
Related SAP Notes	<a href="http://service.sap.com/notes">http://service.sap.com/notes</a> <a href="http://service.sap.com/securitynotes">http://service.sap.com/securitynotes</a>
Released platforms	<a href="http://service.sap.com/pam">http://service.sap.com/pam</a>
Network security	<a href="http://service.sap.com/securityguide">http://service.sap.com/securityguide</a>
SAP Solution Manager	<a href="http://service.sap.com/solutionmanager">http://service.sap.com/solutionmanager</a>
SAP NetWeaver	<a href="http://sdn.sap.com/irj/sdn/netweaver">http://sdn.sap.com/irj/sdn/netweaver</a>



## Technical System Landscape

### Use

The SAP LT Replication Server is a replication technology to provide data from SAP 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:

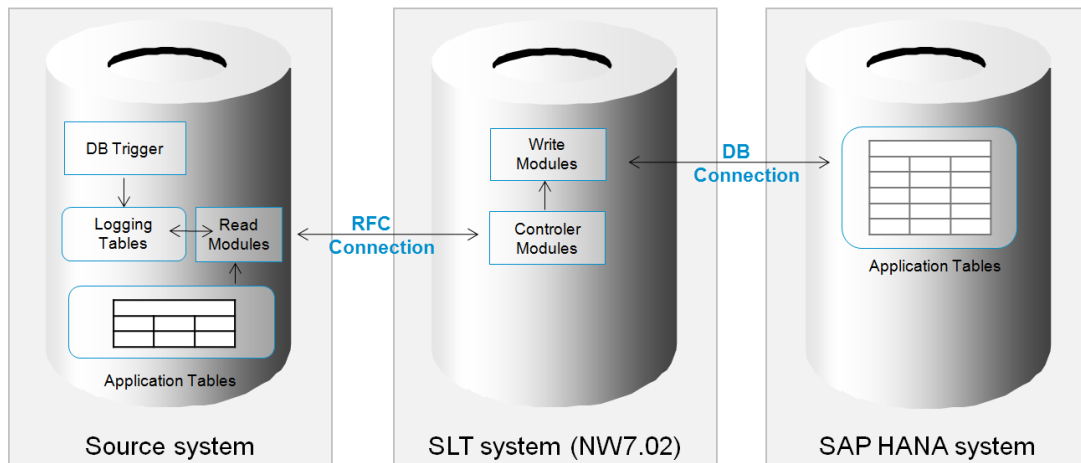
- Source system  
The source system tracks database changes by using database triggers. It records information about changes in the logging tables. The read modules transfer the data from the source system to the SLT system. The relevant data is read from the application tables.
- Non-SAP source system  
The non-SAP 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-SAP source system to the SLT system. The relevant data is read from the application tables.
- SLT system  
If the source is an SAP system, the SLT system polls the logging tables in the source system with a remote function call (RFC) connection. If the source is a non-SAP system, the SLT system polls the logging tables in the non-SAP 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 SLT system and the SAP HANA system communicate by means of a database connection.

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

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

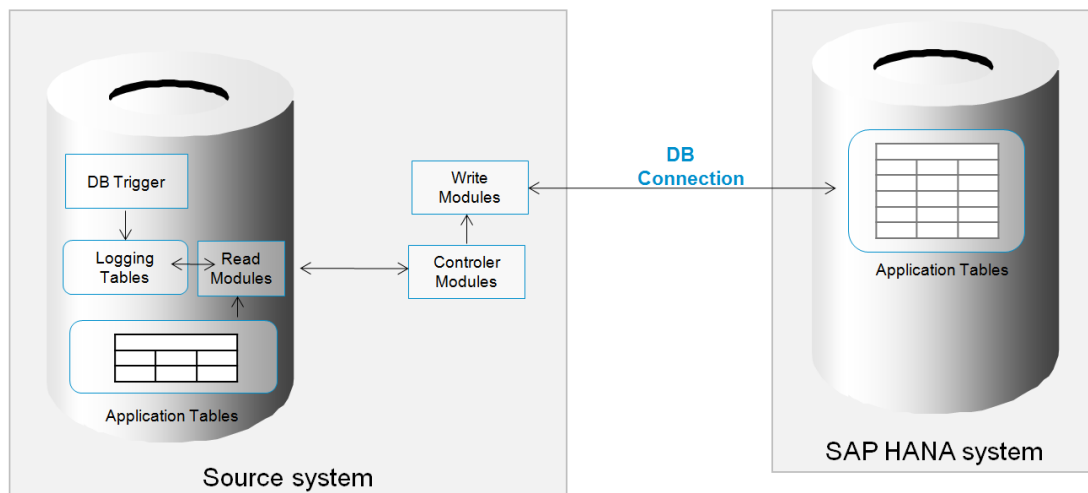
The following figures show the possible technical system landscapes for *Trigger-Based Data Replication Using SAP LT Replication Server*.

**Option 1 – SAP Source System with Separate SLT System**



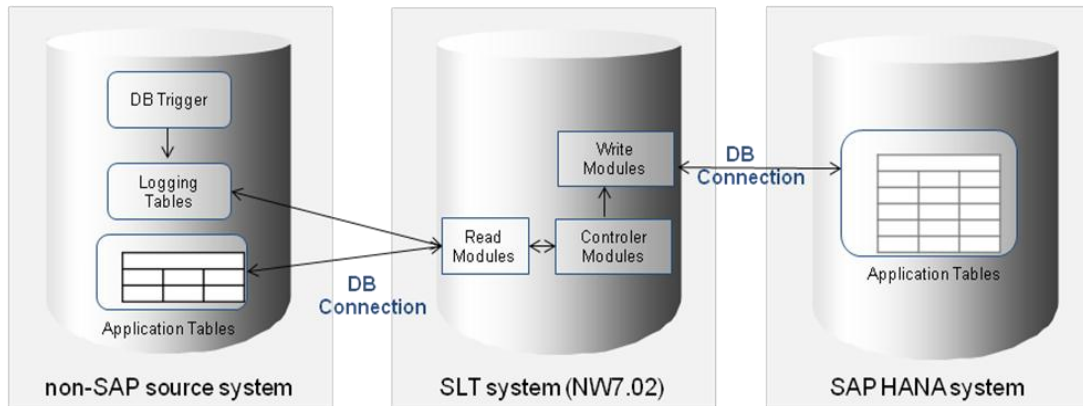
The SAP LT Replication Server is installed in a separate SAP system. Therefore, two network communication channels are required - the RFC connection to the source system and the connection to the SAP HANA system.

**Option 2 – SAP Source System with SLT Installation**



The SLT 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-SAP Source System with Separate SLT System**



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



Ensure that the database of your non-SAP source fulfils all prerequisites for using the SAP LT Replication Server.



## User Administration and Authentication

### Use

The SAP LT Replication Server and the SAP 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 the SAP LT Replication Server and a SAP source system.

Additionally, 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, 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 is required with specific SAP HANA authorizations. You can access the *Configuration and Monitoring Dashboard* by using transaction *LTR*.

- SAP source system

In order to access the SAP 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*.



Users who have access to the SLT system, also have indirect access to the production data in the source system and can see the stored information. Therefore, we recommend limiting the number of users in the SLT system to a minimum amount to prevent unauthorized access to production data.

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

- Non-SAP source system

To access the non-SAP source systems by a database connection, the relevant user must be created with all necessary authorizations in the non-SAP source system. Contact your system administrator to get a user with the relevant authorizations as described under [Authorizations](#).

## Authorizations

### Use

The SAP LT Replication Server and the SAP 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 role maintenance, use the profile generator (transaction PFCG) on the AS ABAP.



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 SLT 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*

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

- S\_DMC\_S\_R

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

*Authorization fields*

Field name	Heading
ACTVT	Activity

## User Roles

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

### User Roles for SAP LT Replication Server

Depending on your source system, use the specific roles to run your operations within the SAP LT Replication Server.

### User Roles for SAP Source System Based on DMIS SP06/SP07

For an SAP source system which is based on DMIS SP06, generate and use the following role to create a user:

- SAP\_IUUC\_REPL\_REMOTE



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

### User Roles for Non-SAP Source System

To establish a secondary database connection from an SAP 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 SAP 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.

## Authorization 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.

We recommend creating a new user (name as preferred) with the same authorizations as the SYSTEM user in the SAP HANA system.

### 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

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.

### 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:

Parameter	Description
TABLERNAME	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

### Revoking Access

Access to a table is revoked by calling the procedure RS\_REVOKE\_ACCESS, which has the following parameters:

Parameter	Description
TABLERNAME	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

### 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 TABLERNAME)
- 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.



## Network and Communication Security



### Network Security

Access to SAP 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-SAP 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.



### Communication Destinations

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

#### SAP Source System

1. Create a user (type *Dialog*) in your source system with the relevant roles. Depending on the SAP system that you use, the following information about user roles apply:
  - [User Roles for SAP Source System Based on DMIS SP06](#)
2. Create an RFC connection (type 3 – ABAP) from the SLT system to the source system with the created user. If both systems are Unicode, specify this RFC as Unicode.



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 NONE.

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

#### Non-SAP Source System

To establish a secondary database connection, the user must have the required privileges as described under [User Roles for Non-SAP Source System](#).

Use the created database connection to define the connection between the SAP 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 automatically created.