



## SAP HANA Security Guide – Log Based Replication

### ■ SAP HANA Appliance Software SPS 04

#### Target Audience

- Consultants
- Administrators
- SAP Hardware Partner
- Others

Public  
Document version 1.0 – 04/30/2012

## 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
Technical System Landscape .....	4
User Administration and Authentication .....	6
Integration into Single Sign-On Environments .....	7
Authorizations .....	7
Credentials summary .....	9
Network Security .....	10
Data Storage Security .....	11
Operating system security .....	12
Security Logging and Tracing .....	12
Other Security-Relevant Information.....	13

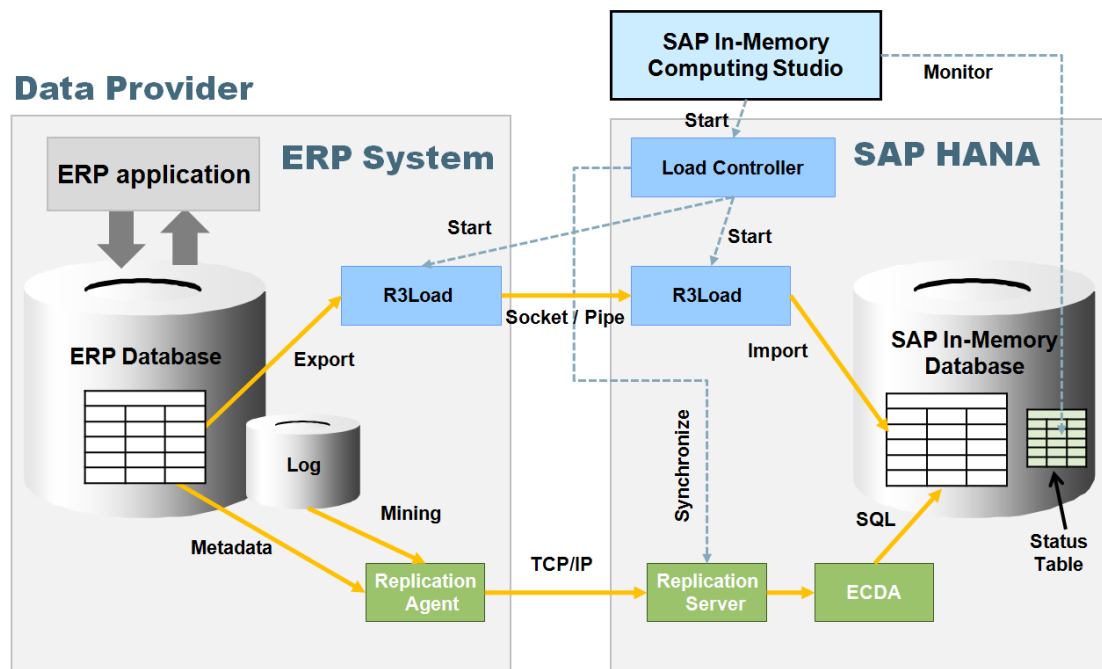
## Introduction

This document covers security considerations for the Log-Based Replication scenario of the SAP HANA system. It forms part of the overall SAP HANA security documentation.

For more information about SAP HANA administration and security, see the SAP HANA Knowledge Center on SAP Help Portal <http://help.sap.com/hana> → System Administration and Security

## Technical System Landscape

The figure below shows an overview of the technical system landscape for the Transaction Log Based Data Replication Using Sybase Replication.



The Sybase replication utilities transfer activity from primary databases to replicate databases. The primary database is typically an SAP ERP or CRM system, and the replicate database is the SAP HANA database.

On the Primary CRM or ERP system, a Replication Agent is installed to capture the changes that occur on the underlying CRM or ERP system and transmit this activity to a Replication Server. The Replication Server receives that information and distributes it to the SAP HANA database.

An overview of the replication components is provided below

### Replication Agent

The Replication Agent communicates with the Primary ERP or CRM database using JDBC client connection over TCP/IP.

The Replication Agent initiates communication to the Replication Server and Replication Server System Database using JDBC client connections over TCP/IP.

## Replication Server

The Replication Server accepts communication requests from the Replication Agent. The Replication Agent user and password are preconfigured. User and password information is stored in the Replication Server System Database (RSSD). Passwords are stored as encrypted values. For details on password administration please see section the User Administration section in this document.

The Replication Server initiates communication to the SAP HANA database using ODBC client connections over TCP/IP. The ODBC client is implemented by a gateway process server – Enterprise Connect Data Access (ECDA). At the lowest level, the Replication Server connects to the ECDA gateway over TCP/IP. The ECDA gateway opens a corresponding connection to the SAP HANA database via ODBC. The user and password credentials supplied by the Replication Server to the ECDA gateway are passed through to the SAP HANA database for validation and authorization.

The Replication Server initiates communication to its Replication Server System Database (RSSD) using Sybase Open Client/Server protocol over TCP/IP. User / port and database values of the RSSD are preconfigured. The RSSD passwords are stored as encrypted values in a configuration file.

The host name where the Replication Server is installed (HANA Appliance) is provided to the Replication Server during initial configuration. User ID and Password for SAP HANA database access are prompted for during the same initial configuration. User and password for SAP HANA database access are stored in the RSSD with password values encrypted.

For details on user and password administration please see section the User Administration section in this document.

## Enterprise Connect Data Access

The Enterprise Connect Data Access (ECDA) component implements the ODBC interface to the SAP HANA database. The replicate database (SAP HANA database) is passed all credentials. Access to ECDA is only allowed if access to the replicate database is also allowed.

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> <ul style="list-style-type: none"> <li>• <a href="#">SAP HANA Master Guide</a></li> <li>• <a href="#">SAP HANA Installation Guide</a> → see chapter <i>Installing Log-Based Replication</i></li> </ul>
SAP HANA Administration & Security	<i>SAP HANA Knowledge Center on SAP Help Portal</i>	<a href="http://help.sap.com/hana_appliance">http://help.sap.com/hana_appliance</a> <ul style="list-style-type: none"> <li>• <a href="#">SAP HANA Technical Operations Manual</a></li> <li>• <a href="#">SAP HANA Security Guide</a></li> </ul>

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



## User Administration

The Log-Based replication server components do not provide access to personal or customer data. The sole purpose of the users within the system is to provide administrative access.

### Replication Agent

The Replication Agent allows a single administrative user to log into the Replication Agent server. The administrative user may perform any configuration or administrative task of the Replication Agent server.

The value of the Replication Agent administrative user is stored in a configuration property named `ltm_admin_user`.

- The value of the `ltm_admin_user` parameter is the user name authorized to log in to the Replication Agent.
- To change the value of the `ltm_admin_user` parameter, use the Replication Agent `ra_set_login` command.
- If you change the value of the `ltm_admin_user` parameter with the `ra_set_login` command, the new value is recorded in the configuration file immediately. However, you must shut down and restart the Replication Agent instance to make the new administrator name take effect.

By default, the Replication Agent is preconfigured with an administrative user name of 'sa' and a null (empty) password.

The value of the Replication Agent administrative user password is stored in a configuration property named `ltm_admin_pw`

- The value of the `ltm_admin_pw` parameter is encrypted in the Replication Agent configuration file.
- To change the value of the `ltm_admin_pw` parameter, use command `ra_set_login`.
- When you change the value of the `ltm_admin_pw` parameter with `ra_set_login`, the new value is recorded in the configuration file immediately. However, you must shut down and restart the Replication Agent instance to make the new password take effect.

**Syntax:** `ra_set_login username, password`

**Parameters:**

`username`

The login name of the Replication Agent administrator

`password`

The password of the Replication Agent administrator

### Replication Server

**Note:** The Replication Server maintains credentials for access by the Replication Agent, and access to the Replication Server System Database (RSSD). As these are preconfigured, the processes for their modification are not documented.

The Replication Server allows for multiple administrative users to be defined and to log into the Replication Agent server. A user with an administrative role may perform any configuration or administrative task of the Replication Server.

By default, the Replication Server is preconfigured with an administrative user name of 'sa' and a null (empty) password.

The value of the Replication Server administrative user password is stored in the Replication Server System Database (RSSD). The password may be changed using the "alter user" command.

Syntax:

```
alter user username
    set password {new_passwd | null}
    [verify password old_passwd]
```

The Replication Server maintains credentials to access the SAP HANA Database through ECDA. The user name and password is stored in the Replication Server System Database (RSSD). The password may be changed using the "alter connection" command.

Syntax:

```
alter connection to HANADC2SVC.UDB2NEWDB
    set password to new_passwd
```

## Enterprise Connect Data Access

No credentials are stored or used by this component.



## Integration into Single Sign-On Environments

Not supported by Sybase Replication components.



## Authorizations

The authorizations used by the Sybase Replication components are used to provide connectivity of the Replication components themselves, as well as for data capture and data transfer purposes. As a result, the authentication criteria are less restrictive than a comparable database product that stores end user data.

Specifically, Replication component credentials:

- do not have an expiration
- do not have minimum lengths or minimum content (number of numbers, capital letters, etc).
- passwords do not change
- no history of past credentials is maintained (passwords may be reused)

## Replication Agent

The Replication Agent communicates with the Primary ERP or CRM database using JDBC. The database user / password / host / port and database values are provided to the Replication Agent during initial configuration.

The host and port values where the Replication Server is installed are provided to the Replication Agent during initial configuration.

The Replication Agent has user information for accessing the primary ERP or CRM system (DB user). It also holds the user information required to communicate with the Replication Server. It also holds a user to query the Replication Server RSSD and its own embedded RASD (Replication Agent System Database).

## Replication Server

The Replication Server communication requests from the Replication Agent are authenticated using a user and password. The Replication Agent user and password is preconfigured. The user and password information is stored in the Replication Server System Database.

The Replication Server has user information for accessing the replicate database (SAP HANA database user). It also holds a user to query its own Replication Server RSSD.

## Enterprise Connect Data Access

Access to the Enterprise Connect Data Access (ECDA) component is only permitted if access to the replicate database is also permitted. It does not maintain or require authorization credentials.



## Credentials summary

The table below contains a summary of all credentials used by the Log-Based Replication system.

<b>Credential owner</b>	<b>Purpose</b>	<b>Storage Mechanism</b>	<b>Change mechanism</b>	<b>Document Section</b>
Replication Agent	Administration of Replication Agent	Configuration file	“ra_set_login” command	User Administration
Replication Agent	Access to replication server	Configuration file	None – preconfigured at install time	User Administration
Replication Agent	Access to ERP system via JDBC	Configuration file	None – preconfigured at install time	Authorizations
Replication Server	Administration of Replication Server	RSSD	“alter user” command	User Administration
Replication Server	Access from Replication Agent	RSSD	None – preconfigured at install time	User Administration
Replication Server	Access to SAP HANA database via ECDA	RSSD	“alter connection” command	User Administration

## Network Security

All Sybase replication utilities use TCP/IP connections to communicate with the Primary and Replicate databases, as well as communication between the Replication Agent and Replication Server

### Communication ports

The following table shows the communication ports in use by the Sybase Replication components.

Component	System location	Ports
Replication Agent	ERP / CRM System	2141 and 2142.
Replication Server	SAP Hana System	2121 and 2122
ECDA gateway	SAP Hana System	2131

### Communication channels

The table below shows the communication channels used by Log-Base replication, the protocol used for the connection and the type of data transferred.

Communication Path	Protocol Used	Type of Data Transferred	Data Requiring Special Protection
R3Load (ERP System) to R3Load (SAP HANA System)	JDBC	Initial Replication data	Replication Data
Replication Agent to Replication Server	JDBC	Delta replication data	Replication Data

TCP/IP communications are expected to occur within the same LAN, domain or firewall. No encryption is provided.

Encryption of communication between the Sybase components is not supported. SAP recommends customers use network-level security or the separation of different network zones to protect communications.

## **Data Storage Security**

The system components of the Log-Based replication system do not store or provide access to user data. The only information stored by the replication components is for system configuration and authorization information (usernames, passwords).

### **Replication Agent**

Usernames and passwords are stored in a configuration file. Passwords are stored as encrypted values.

### **Replication Server**

Usernames and password information is stored in the Replication Server System Database. Passwords are stored as encrypted values.

## **Configuration**

Both Replication Agent and Replication Server maintain configuration information. This information is stored by each server in the configuration file and in an embedded database.

The configuration file information contains information necessary to start the server, while the embedded database contains advanced configuration related to the processing of replication.

The interface to change configuration file information is provided by the administrative interface of the server. The administrative access is obtained by logging into the server (Replication Agent, Replication Server) and issue administrative commands, the results of which may be stored in the configuration file or embedded database as appropriate. As the configuration file contains critical data required to successfully start the server, its accidental corruption or removal should be prevented by limiting update access to those OS users responsible for starting the server.

## **Operating system security**

### **File permissions**

Access to all files under `/usr/sap/sybase` should be protected by the operating system file level permissions.

### **System processes**

The Log-based Replication components run as operating systems processes. The operating system user that starts the Sybase Replication component processes must have particular operating system permissions in order to successfully start the servers:

#### **Replication Agent**

The operating system user that starts the Replication Agent process should be the owner of all files installed for the Replication Agent on the Primary host machine (ERP or CRM system). This recommendation applies to all the files stored under `/usr/sap/sybase`.

The Replication Agent may be configured to access archived transaction logs of the primary database. This access is required so that the Replication Agent can remove the archive logs when their content is no longer required. If the archive log removal feature is enabled, the operating system user that starts the Replication Agent process will need to have Update file authority to the directory and archive files.

#### **Replication Server**

The OS user that starts the Replication Server process should be the owner of all files installed for the Replication Server on the SAP HANA system. This is all files stored under `/usr/sap/sybase`.

## **Security Logging and Tracing**

The Sybase Replication components do not provide exclusive logging or tracing of security related access activity and/or failures. Most connection failures are recorded in the general system log files of the Replication Agent and Replication Server. Limited information is provided, and failures are reported.



## Other Security-Relevant Information

### Encryption

Sybase Replication components use the following encryption tools (for compliance verification)

#### Replication Server

FIPS Certification:

[Common Criteria conformance for Replication Server 15.2](#)

Description of Replication Server using "Sybase Common Security Infrastructure (CSI)"

#### Replication Agent

Written in Java, uses the Java Cryptography Extensions and Certicom as the cryptology provider; for more information, see [Security Builder® Crypto™ Features](#)