Reference Guide
D301533X412
April 2012

OpenEnterprise Security Replication Reference Guide (V2.83)

Remote Automation Solutions

EMERSON

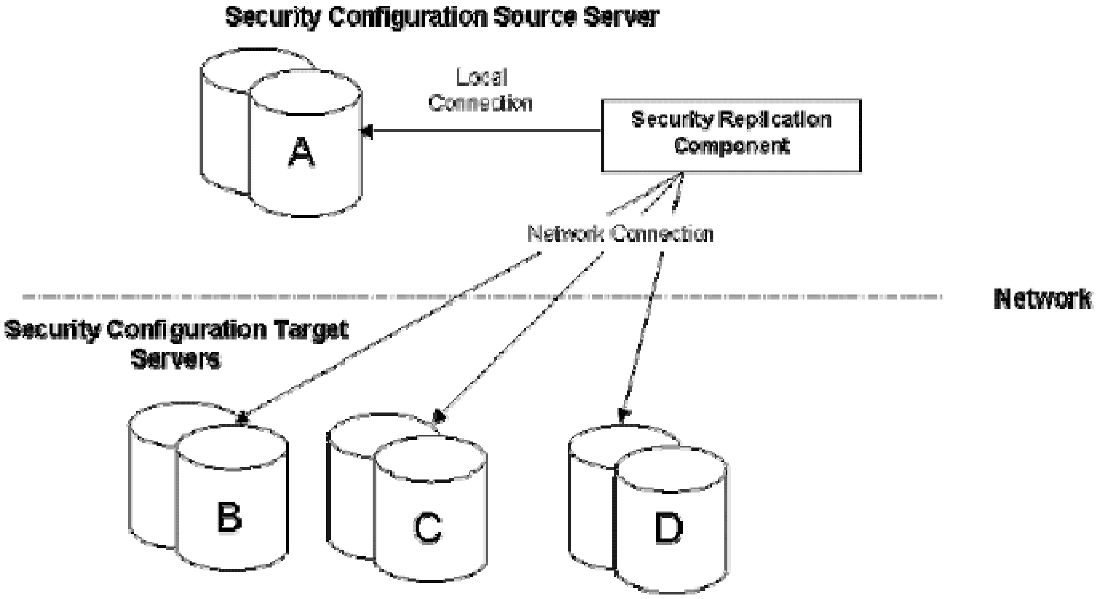
Website: www.EmersonProcess.com/Remote

Contents

1 Security Replication

OpenEnterprise Security Replication enables database security configuration to be maintained across a number of OpenEnterprise databases distributed over a wide area network. In the diagram below, four separate OpenEnterprise databases are configured so that their security configuration remains the same at all times.

Security Replication is implemented by the Security Replication Component. This runs on the designated Security Configuration Source Server (A in the example below). After connecting to the local database, it obtains the dataservice address for the Target Security Configuration Servers (B, C and D in the example below), from the *SecurityReplication* table. It then makes a connection to the Target Servers, and ensures that security configuration is replicated across the whole system according to the directives contained in the *SecurityReplication* table.


Security Configuration Source Server
Local Connection
Security Replication Component
A
Network Connection
Network
Security Configuration Target Servers
B
C
D

1.1 Security Replication Table

In order to replicate all security configuration data, the Security Replication component copies and maintains data from the following tables/views.

- UserConfig – Contains all user and security group configuration.
- AccessAreaConfig – Contains the list of access areas configured for the system.
- AccessArea – Contains the access area to user and security group associations.
- Token_table – Contains all tokens configured on the system
- TokenGroup_table – Contains all token groups configured for the system.
- TokenAccess_table – Contains the token to user and security group associations.
- TokenGroupAccess_table – Contains the token group to user and security group associations.

- Table_Privileges – Reflects all access privileges defined on the tables and views within the OpenEnterprise schema.
- Column_Privileges – Reflects all access privileges defined on individual columns within the OpenEnterprise schema.

Note that we directly query the tables, rather than the views for token configuration. This is because we must ensure that all configuration within those tables is copied, rather than the limited subset that might be available from the associated Views, due to access area allocations.

1.1.1 Users and Groups

Probably the most obvious security configuration information is that for the Users and Security Groups that are configured for the system.

The Security Replication component will use the UserConfig view in order to access and replicate this information around a distributed OpenEnterprise system.

The UserConfig view provides a subset of the information contained within the Users table and is what the Security Configuration Tool uses when managing security configuration. It therefore contains all attributes that define a User, or a Security Groups profile.

1.1.2 Access Area Configuration

Access Areas are used to provide object-based security within OpenEnterprise. In order for a user to see objects they must first be given access to the Access Area to which those objects are assigned.

Access Area configuration is defined by two tables. The first, AccessAreaConfig, provides a list of the access areas configured within the system. The second, AccessArea, is used to assign Users and Security Groups to those Access Areas.

There is a fair amount of CL (the database Command Language) associated with the AccessArea table. Most of it is to handle the allocation of Access Areas to Security Groups. If an Access Area is given to a group, then the CL ensures that that Access Area is also given to all members of the group.

Similarly if you delete an AccessAeaConfig table entry then any AccessArea entries relating to that record are automatically deleted.

Finally if a new AccessAreaConfig table entry is created the SYSTEM user is automatically given access to it, by the creation of the AccessArea table entry for it.

These can cause problems to the Security Replication component, especially given that the order in which records are returned from a query are arbitrary, meaning that contentions between records being added by the Security Replication component and those being added by the CL can occur.

The Security Replication component will ensure that the source and target databases are consistent, but it is possible that transaction failures may occur, and be reported through the Security Replication component's User Interface.

1.1.3 Token Configuration

There are four tables used to provide configuration information relating to Security Tokens. The Replication component accesses the tables rather than the Views to ensure that ALL configuration is obtained and copied, rather than relying on the correct Access Area allocations being available to the configured security user of the Replication component.

The replication of Token configuration is fairly straightforward with no contentions with the CL associated with the token tables.

1.1.4 Table Access Configuration

The replication of access privilege information is potentially the most complex part of the Security Replication component. Not only do we have to imply any GRANT/REVOKE statements based on the contents of the table_privilege and column_privilege tables, but we also have the added complexity that we need to maintain the Grantor of those access privileges across the target databases as well.

To do this we make use of a dedicated socket connection, which is used purely for performing the necessary GRANT/REVOKE statements. Based on the Grantor of those privileges we log on to that socket and perform the access privilege replication.

Additional complications are that each individual access privilege statements must be applied to the database separately, and we also have the added issue that the order that records are returned from these tables is not in the order in which any GRANT statements where applied.

We will therefore have to perform a sort of the records obtained from the source database to ensure that any cascaded GRANT statements are applied in the correct order.

1.2 Configuration

Configuration of the Security Replication component is as follows: -

1. Setting up Security Replication policy in the SecurityReplication table. See the Example Configuration for more information on this aspect.
2. If the Security Replication component is being managed by the Session Manager, it will need to be configured as part of the OpenEnterprise session.
3. If the Security Replication component is running on a different computer to the Security Configuration Source server, or the data service is not set to the default 'rtrdb1', it must be provided with the correct Command Line switch.
4. The OE Security Manager on any connected workstations should be configured so that the target servers are listed as Fallback Databases. See the Settings Editor and Security Manager documentation for details.

1.2.1 The Security Replication Table

The *SecurityReplication* table provides the Replication Component with the information it needs to implement the Security Replication strategy. An entry must be created in this table for each target database for which security replication is required.

The Replication Component maintains an active query on the SecurityReplication table, and will apply changes in configuration WITHOUT having to be restarted.The table below explains the attributes of this table.

Attribute Name	Data Type	Description
DataService	Char primary key	The data service to which the security configuration information is to be replicated.
CopyUsers	Bool default TRUE	Indicates whether User and security group information should be replicated to the target database. If the CopyUsers attribute is set to FALSE then this also automatically prevents replication of access area, tokens and access

		privileges. This is because all of these are dependent in some way upon the list of users and groups being consistent in the source and target databases.
CopyToken	Bool default TRUE	Indicates whether information in the Token, TokenAccess, TokenGroup and TokenGroupAccess tables should be replicated to the target database.
CopyAccessArea	Bool default TRUE	Indicates whether the contents of the AccessAreaConfig, and AccessArea tables should be replicated to the target database.
CopyAccessPrivileges	Bool default TRUE	Indicates whether any changes in access privileges will be applied to the target database.
DeleteTargetUsers	Bool default FALSE	If extra users, (or groups) exist in the target database, then this attribute can be used to dictate whether those additional users are deleted by the Replication Component
DeleteTargetTokens	Bool default FALSE	If additional token configuration exists in the target database, then this attribute can be used to indicate that the additional configuration should be deleted. This applies to records in the token, tokengroup, tokenaccess and tokengroupaccess tables.
DeleteTargetAccessAreas	Bool default FALSE	If additional access area configuration exists in the target database then this attribute is used to indicate if that additional configuration should be deleted. This will apply to records in the AccessAreaConfig and the AccessArea tables.

1.2.2 Session Configuration

To modify the settings for the Security Replication task, select the task from the task list of the Session Manager, select the Stop option on the context menu. Then select the Properties option from the same context menu. This will bring up the Task Properties dialog. For more details, refer to the Session Manager help file.

1.2.2.1 The Task Page

On the Task page of the dialog, fill in the following fields.

1.2.2.1.1 Program

This is the Security Replication Component's path and file name. It defaults to the *C:\Program Files\Bristol\OpenEnterprise\bin* directory.

1.2.2.1.2 Run program in the following folder

This will be the Data directory of the OpenEnterprise project.

1.2.2.1.3 Program Arguments

This will be:-

–s <dataservice>. For example: *–s Server1:rtrdb1,Server2:rtrdb1* for a Redundant session or *–s eastregion* for a Standalone session..

If no –s command line argument is defined the Security Replication Component will automatically attempt to connect to the rtrdb1 data service.

1.2.3 Example Configuration

On a distributed system of three databases, the security configuration database is identified by the data service controlroom1:rtrdb1,controlroom2:rtrdb1. The two target databases are identified by the data services, remote1:rtrdb1 and remote2:rtrdb1.

For remote1:rtrdb1 we wish to replicate ALL security replication configuration, and at the same time delete any additional security configuration found. For remote2:rtrdb1 we are only concerned in maintaining consistency of users and security groups, and access privileges.

The Security Replication component would be invoked as follows:

OEReplication –s controlroom1:rtrdb1,controlroom2:rtrdb1

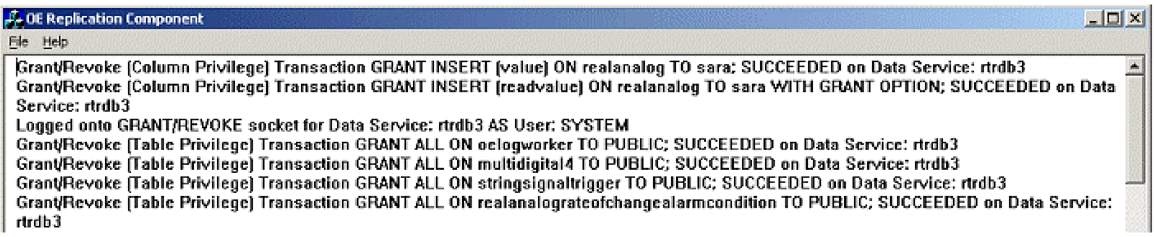
The SecurityReplication table within the redundant *controlroom1:rtrdb1,controlroom2:rtrdb1* database would need to be configured thus:

Attribute Name	For remote1:rtrdb1	For remote2:rtrdb1
DataService	Remote1:rtrdb1	Remote2:rtrdb1
CopyUsers	TRUE	TRUE
CopyToken	TRUE	FALSE
CopyAccessArea	TRUE	FALSE
CopyAccessPrivilege	TRUE	TRUE
DeleteTargetUsers	TRUE	FALSE
DeleteTargetTokens	TRUE	FALSE
DeleteTargetAccessAreas	TRUE	FALSE

1.3 The Security Replication User Interface

The Security Replication Component's User Interface provides diagnostic information that can be used to determine if any problems in the replication of security configuration has occurred. This is in the form of a list, with the newest entries at the top of the window, and a scroll bar to allow previous diagnostic information to be reviewed.

Note: The fact that transactions fail does not necessarily indicate that the target databases are out of step with the source database.



```
Grant/Revoke [Column Privilege] Transaction GRANT INSERT [value] ON realanalog TO sara; SUCCEEDED on Data Service: rtrdb3
Grant/Revoke [Column Privilege] Transaction GRANT INSERT [readvalue] ON realanalog TO sara WITH GRANT OPTION; SUCCEEDED on Data Service: rtrdb3
Logged onto GRANT/REVOKE socket for Data Service: rtrdb3 AS User: SYSTEM
Grant/Revoke [Table Privilege] Transaction GRANT ALL ON oelogworker TO PUBLIC; SUCCEEDED on Data Service: rtrdb3
Grant/Revoke [Table Privilege] Transaction GRANT ALL ON multidigital4 TO PUBLIC; SUCCEEDED on Data Service: rtrdb3
Grant/Revoke [Table Privilege] Transaction GRANT ALL ON stringsignaltrigger TO PUBLIC; SUCCEEDED on Data Service: rtrdb3
Grant/Revoke [Table Privilege] Transaction GRANT ALL ON realanalograteofchangealarmcondition TO PUBLIC; SUCCEEDED on Data Service: rtrdb3
```

2 Index

DISCLAIMER

Bristol, Inc., Bristol Babcock Ltd, Bristol Canada, BBI SA de CV and the Flow Computer Division , are wholly owned subsidiaries of Emerson Electric Co. doing business as Remote Automation Solutions ("RAS"), a division of Emerson Process Management. ROC, FloBoss, ROCLINK, Bristol, Bristol Babcock, ControlWave, TeleFlow and Helicoid are trademarks of RAS. AMS, PlantWeb and the PlantWeb logo are marks of Emerson Electric Co. The Emerson logo is a trademark and service mark of the Emerson Electric Co. All other marks are property of their respective owners.

The contents of this publication are presented for informational purposes only. While every effort has been made to ensure informational accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. RAS reserves the right to modify or improve the designs or specifications of such products at any time without notice. All sales are governed by RAS' terms and conditions which are available upon request. RAS does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any RAS product remains solely with the purchaser and end-user.

Engineered and supported by:

Remote Automation Solutions,

Blackpole Road, Worcester, WR3 8YB, UK

Registered office: Meridian East, Leicester, LE19 1UX

Registered in England and Wales, Registration No. 00671801

VAT Reg No. GB 705 353 652

Emerson Process Management
Remote Automation Solutions
1100 Buckingham St
Watertown, CT 06795
T 1 (860) 945 2200
F 1 (860) 945 2278
www.EmersonProcess.com/Remote
binfo@EmersonProcess.com

Emerson Process Management
Remote Automation Solutions
Blackpole Road
Worcester, WR3 8YB
T 44 (0) 1905 856848
F 44 (0) 1905 856930
www.EmersonProcess.com/Remote
oedsupport@EmersonProcess.com