



Data Replication

Setup for Oracle Replications with Remote Log Server Agent

Version 9.7.2

Software Release Date: 1/21/21.



<https://support.hitsw.com>

Document History

Version	Author	Date	Reviewer	Date	Comments
1	JHLorenzin	10/31/17	TLe	11/2/17	
2	JHLorenzin	1/21/21	TLe	1/5/21	
3	JHLorenzin	3/31/21	TLe	3/31/21	

Syniti Data Replication

Table of Contents

The Remote Log Server for Oracle	1
Summary	2
Connection Type	2
Oracle Client with .NET Provider	2
Oracle JDBC Driver & JRE	2
Oracle System Settings.....	2
Oracle Log Retention Time Setting.....	3
Oracle User Permissions	3
Refresh with Oracle as Either Source or Target Database	3
Transactional Replications/Initial Refresh with Oracle as Either Source or Target Database	5
Set Up the Syniti DR Environment.....	9
Add a Source Connection Wizard	9
Select Provider Screen	9
Set Connection String Screen	10
Enable Transactional Replication Wizard	10
Log Type Screen.....	10
Log Settings Screen	10
Change Log Settings Dialog	11
Agent Settings Screen	12
Create Replication Wizard.....	12
Source Log Info.....	13
Run the Remote Log Server	13
Using the Remote Log Server with Oracle ASM Storage.....	13

Syniti Data Replication

This guide describes the setup process for one-way mirroring and synchronization when replicating data from an Oracle database **using the Remote Log Server approach for replicating changed data only.**

For mirroring and synchronization replications using Oracle as a source, Syniti Data Replication offers several alternative approaches. Information on these approaches is available in the [Help Center](#).

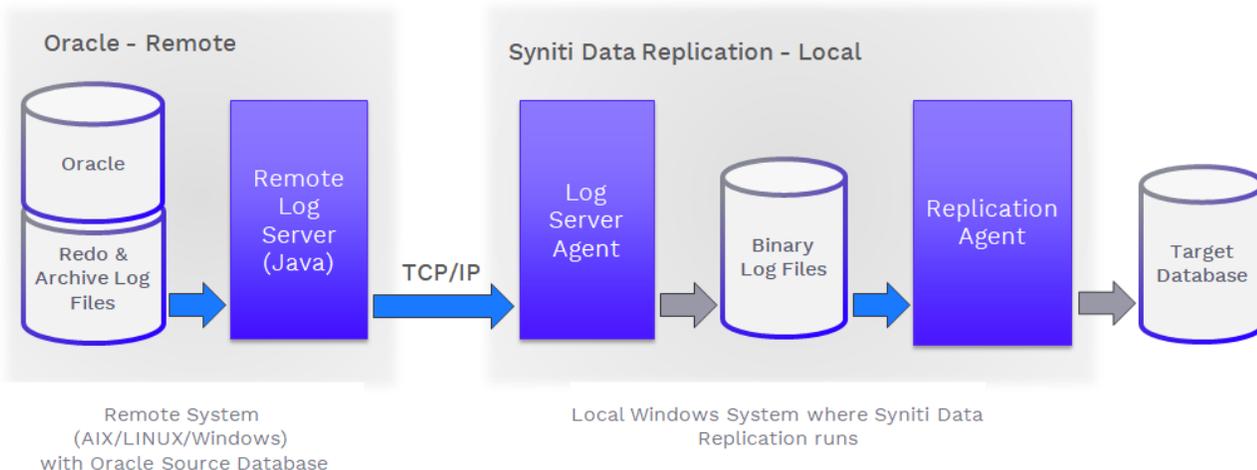
- **Log Reader:** Queries the Oracle Log Miner directly
- **Log Server Agent:** Uses a Windows service and a Log Server component to query the Oracle Log Miner for increased performance when dealing with large amounts of data. This option is supported for Oracle databases version 11 and above.
- **Triggers:** Uses Syniti DR triggers installed on the Oracle database to log changes. Ask the technical support team via the [Help Center](#) to see if this approach would work in your application. Download the separate document [Setup Notes for Oracle Using Triggers](#).

For further details on the setup process, check the *Syniti Data Replication User Guide* available from the Management Center **Help** menu or the *Syniti Data Replication Setup Guide*, available for download in the [Help Center](#).

The Remote Log Server for Oracle

The Remote Log Server (RLS) is a Java application that is installed on the system where the Oracle database resides to read log files directly.

On request from the Syniti DR Log Server Agent, the RLS reads changed records from redo and archive log files then returns them to the Log Server Agent. All retrieved information is returned, and no information is stored by the remote application. The RLS listens for and accepts connections on a TCP/IP port. The Log Server Agent connects to this port to request the RLS to read and return changed records.



Blue arrows represent data to be read/sent from source

Gray arrows represent data to be written from application to target

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

Note that while the user and password for Oracle are encrypted during communication between the RLS and the system running Syniti Data Replication, data is NOT encrypted. Syniti offers a solution called SafeConduct to set up data encryption. All trace and log details for the RLS are sent to the Log Server Agent trace.

NOTE: On an Oracle database that stores all its log files in ASM storage, the RLS will not be able to access or read these log files. Go to [Using the Remote Log Server with Oracle ASM Storage](#) for an approach to handle this situation.

Summary

- Oracle generates redo and archive log files
- Log Server Agent connects to and requests the Remote Log Server to read changed log records
- LSA writes retrieved records to binary log files
- Syniti DR Replication Agent reads records from binary log files and replicates them to target database

Connection Type

Oracle Client with .NET Provider

Before connecting to an Oracle database from Syniti DR Management Center, make sure the Oracle .NET provider is installed and accessible from the system where Syniti DR is running.

On the system where Syniti Data Replication is running, make sure the Oracle .NET provider is installed and accessible.

1. Download the appropriate Oracle client from the Oracle Web site.
2. Run the setup.exe to install the client.

To access the Oracle .NET provider from Syniti DR, you will need to know the Assembly and the path to the Assembly:

Assembly: Oracle.DataAccess (file name: Oracle.DataAccess.dll)

Sample path: C:\oracle10_2\client\odp.net\bin\2.x\Oracle.DataAccess.dll.

Oracle JDBC Driver & JRE

On the system where Oracle is running, a Java Runtime Environment or JRE version 8 or later and an Oracle JDBC Driver version 11 or later are required to run the [Remote Log Server application](#).

1. Download a JRE if you do not have a recommended version installed on your system.
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
2. Download and copy the driver files to a folder, for example: **ojdbc7.jar** and **orai18n.jar**.
<http://www.oracle.com/technetwork/database/enterprise-edition/downloads/112010-win64soft-094461.html>
These jar files need to be included in the Java classpath.

Oracle System Settings

The Remote Log Server application works with Oracle version 11 and above.

On the system where Oracle is running:

- Make sure the database generates readable redo and archive log files. Oracle ASM files are not supported.
- Make sure the user ID that will be used to run the Remote Log Server application has read access to the redo and archived log files.

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

- Create a directory and copy/transfer the files from **ServerFiles/OracleRemoteLogServer folder located in the Syniti DR install directory** to the directory you created.
- The specified port number (default is 45000) must be opened by the firewall.

NOTE: The readme.txt file contained in the directory contains running instructions.

Oracle Log Retention Time Setting

In the Oracle database, log retention time determines how long the transaction information contained in the logs is retained, and not deleted or purged. If the need arises for Syniti Data Replication to read earlier transactions from the database log, the retention time is a crucial parameter in determining the success or failure of this operation. The longer the retention time, the better the chances are of finding the required transactions in the database. If transactions are not found, a replication will fail and subsequently a full refresh is required to resynch the data.

Possible reasons why Syniti DR would need to read earlier transactions are:

- Prolonged stop of the Replication Agent.
- Prolonged disabled time for a replication, or any other condition that puts the replication in recovery mode.
- Prolonged maintenance activity of the servers involved (which may cause downtime of one or more services).
- Long refresh time (during refresh, the backlog of transactions gets larger and the effort to read them will be higher).
- Massive number of transactions executed on the source database for a continued period of time (a condition that impacts performance and, as a consequence, may require the log reader process to fall behind in order to read all transactions).

To manage conditions like those above, a log retention time of 72 hours is recommended. If 72 hours is not possible, a reasonable heuristic to use is: take the longest refresh time among all replications, and multiply that by two, with a minimum log retention time of 4 hours. However, note that if an extended period of downtime occurs on the system running Syniti Data Replication or Oracle, these suggestions will not be sufficient and a full refresh will be needed when the system restarts.

Oracle User Permissions

When setting up replications that use Oracle as either a source or target database, you need to be sure that the user ID used for making connections to the database has sufficient privileges to complete all the operations required for Syniti DR to perform a replication.

This section is organized by the type of replication you want to perform. It describes in detail all the user authorities that will be required during the setup and execution of replications.

Refresh with Oracle as Either Source or Target Database

1. AUTHORITY TO CONNECT TO DATABASE

To open a connection to an Oracle database, you need specific authority for a user ID using either of the following two syntaxes:

```
grant create session to <uid>;
```

OR

```
grant connect to <uid>;
```

Example where sdruser is the user ID:

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

```
grant create session to sdruser;  
OR  
grant connect to sdruser;
```

2. AUTHORITY TO SELECT CATALOG

To display a list of tables and show fields in the table in the Management Center (for selecting a source or target table and for setting which fields to replicate), Syniti DR runs a SELECT_CATALOG command. If the user ID has insufficient privileges, an error is generated on the Oracle server.

```
grant select on SYS.ALL_USERS to <uid>;  
grant select on SYS.ALL_TABLES to <uid>;  
grant select on SYS.ALL_TAB_COMMENTS to <uid>;  
grant select on SYS.ALL_OBJECTS to <uid>;  
grant select on SYS.ALL_VIEWS to <uid>;  
grant select on SYS.ALL_TAB_COLUMNS to <uid>;  
grant select on SYS.ALL_COL_COMMENTS to <uid>;  
grant select on SYS.ALL_CONSTRAINTS to <uid>;  
grant select on SYS.ALL_CONS_COLUMNS to <uid>;  
grant select on SYS.USER_CONSTRAINTS to <uid>;  
grant select on SYS.USER_CONS_COLUMNS to <uid>;  
grant select on SYS.ALL_IND_COLUMNS to <uid>;
```

Example where sdruser is the user ID:

```
grant select on SYS.ALL_USERS to sdruser;  
etc.
```

3. AUTHORITY TO SELECT TABLES

Syniti DR runs a SELECT statement to identify records to replicate. Therefore, the user ID used to make a connection must have adequate authority to run a SELECT statement for tables involved in replication.

```
grant select on <table> to <UID>;
```

Example where sdruser is the user ID:

```
grant select on SAMPLE.EMPLOYEES to sdruser;
```

4. AUTHORITY TO UPDATE TABLES, CREATE TABLES (Optional)

(Note: Needed only when Oracle is a target)

To create a target table in the Management Center (as part of the Create Table Wizard), Syniti DR requires the permissions below. You first need to grant a quota on the tablespace in which you want to create a table or index. You can either grant unlimited tablespace to the user:

```
grant unlimited tablespace to <uid>;
```

Or, just define a quota limit on a specific tablespace:

```
alter user <uid> QUOTA 100M on <tablespace name>;
```

Then you can grant create permissions and update permissions (insert, update and delete.)

```
grant create on <table> to <uid>;  
grant insert, update, delete on <table> to <uid>;
```

Example where sdruser is the user ID:

Syniti Data Replication

```
grant unlimited tablespace to sdruser;  
grant create on SAMPLE.EMPLOYEES to sdruser;  
grant insert, update, delete on SAMPLE.EMPLOYEES to sdruser;
```

The insert, update and delete commands can be as broad as needed. They can also be granted to entire schemas or to all database tables.

5. AUTHORITY TO DROP TABLES, ALTER TABLES (**Optional**) (**Note: Needed only when Oracle is a target**)

The use of these commands from within Syniti DR is entirely optional (i.e. not necessary for running a refresh replication.) They are used if you choose to remove a table from Oracle or change the table via the Management Center SQL Query tab. The following commands can be as broad as needed. They can also be granted to entire schemas or to all database tables.

```
grant alter on <table> to <uid>;  
grant drop on <table> to <uid>;
```

Transactional Replications/Initial Refresh with Oracle as Either Source or Target Database

This section includes information for mirroring where Oracle is the data source, and synchronization where Oracle can be either the “source” or “target” data source.

1. AUTHORITY TO CONNECT TO DATABASE

To open a connection to an Oracle database, you need specific authority for a user ID using either of the following two syntaxes:

```
grant create session to <uid>;  
OR  
grant connect to <uid>;
```

Example where sdruser is the user ID:

```
grant create session to sdruser;  
OR  
grant connect to sdruser;
```

2. AUTHORITY TO SELECT A CATALOG

To display a list of tables and show fields in the table in the Management Center (for selecting a source or target table and for setting which fields to replicate), Syniti DR runs a SELECT_CATALOG command. If the user ID has insufficient privileges, an error is generated on the Oracle server.

```
grant select on SYS.ALL_USERS to <uid>;  
grant select on SYS.ALL_TABLES to <uid>;  
grant select on SYS.ALL_TAB_COMMENTS to <uid>;  
grant select on SYS.ALL_OBJECTS to <uid>;  
grant select on SYS.ALL_VIEWS to <uid>;  
grant select on SYS.ALL_TAB_COLUMNS to <uid>;  
grant select on SYS.ALL_COL_COMMENTS to <uid>;  
grant select on SYS.ALL_CONSTRAINTS to <uid>;  
grant select on SYS.ALL_CONS_COLUMNS to <uid>;
```

Syniti Data Replication

```
grant select on SYS.USER_CONSTRAINTS to <uid>;
grant select on SYS.USER_CONS_COLUMNS to <uid>;
grant select on SYS.ALL_IND_COLUMNS to <uid>;
```

Example where sdruser is the user ID:

```
grant select on SYS.ALL_USERS to sdruser;
```

etc.

3. AUTHORITY TO SELECT TABLES

Syniti DR runs a SELECT statement to identify records to replicate. Therefore, the user ID used to make a connection must have adequate authority to run a SELECT statement for tables involved in replication.

```
grant select on <table> to <UID>;
```

Example where sdruser is the user ID:

```
grant select on SAMPLE.EMPLOYEES to sdruser;
```

4. AUTHORITY TO UPDATE TABLES, CREATE TABLES (Optional)

(Note: Needed only when Oracle is a target)

To create a target table in the Management Center (as part of the Create Table Wizard), Syniti DR requires the permissions below.

You first need to grant a quota on the tablespace in which you want to create a table or index. You can either grant unlimited tablespace to the user:

```
grant unlimited tablespace to <uid>;
```

Alternatively, just define a quota limit on a specific tablespace:

```
alter user <uid> QUOTA 100M on <tablespace name>;
```

Then you can grant create permissions and update permissions (insert, update and delete.)

```
grant create on <table> to <uid>;
```

```
grant insert, update, delete on <table> to <uid>;
```

Example where sdruser is the user ID:

```
grant unlimited tablespace to sdruser;
```

```
grant create on SAMPLE.EMPLOYEES to sdruser;
```

```
grant insert, update, delete on SAMPLE.EMPLOYEES to sdruser;
```

The insert, update and delete commands can be as broad as needed. They can also be granted to entire schemas or to all database tables.

5. AUTHORITY TO DROP TABLES, ALTER TABLES (Optional)

(Note: Needed only when Oracle is a target)

The use of these commands from within Syniti DR is entirely optional (i.e. not necessary for running a refresh replication.) They are used if you choose to remove a table from Oracle or change the table via the Management Center SQL Query tab. The following commands can be as broad as needed. They can also be granted to entire schemas or to all database tables.

```
grant alter on <table> to <uid>;
```

```
grant drop on <table> to <uid>;
```

Syniti Data Replication

6. AUTHORITY TO SET UP A CONNECTION FOR TRANSACTIONAL REPLICATIONS (logminer)

(Note: Needed only when Oracle is a source in mirroring replications)

When setting up the connection for transactional replications (where Oracle is serving as the source of data, either for mirroring or for synchronization), you may need additional privileges that are not required for replication operations. You need to alter the database to enable SUPPLEMENTAL LOG.

In Syniti Data Replication (DBMoto) versions 7.0.4 and above, the supplemental log is enabled at the table level by default rather than for the entire database. In the default case, you need an ALTER DATABASE privilege to set up supplemental logging and an ALTER TABLE privilege on each table to be replicated when setting up a replication. If the table already has a supplemental log set, then Syniti Data Replication does not need this privilege. You can control whether supplemental logging is enabled at the table or database level using the Oracle Setup Info dialog available from the Connection Properties dialog (under Transaction Log Type.)

To set up supplemental logging independent of Syniti DR (i.e. not through the Oracle Setup Info dialog), use the following commands:

For database-level supplemental logging:

```
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY, UNIQUE INDEX) COLUMNS
```

For minimal/table-level supplemental logging:

```
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA
```

In this last case, also an ALTER TABLE statement will be used on each replicated table:

```
ALTER TABLE MYSCHEMA.MYTABLE ADD SUPPLEMENTAL LOG GROUP <groupname> (<pkList>) ALWAYS
```

Where *pkList* is a comma-separated list of the primary keys of the table, while *groupname* is an internally generated name of the supplemental log group.

If using a dictionary file (required for Oracle 8.1, optional for later versions) you need execute permission to build the dictionary file.

```
grant alter table to <uid>;
grant alter database to <uid>;
grant execute on sys.dbms_logmnr_d to <uid>;
```

Example:

```
grant alter table to sdruser
grant alter database to sdruser
grant execute on sys.dbms_logmnr_d to sdruser;
```

7. AUTHORITY TO SET UP TRANSACTIONAL REPLICATIONS and ACCESS REDO/ARCHIVED LOGS (logminer)

(Note: Needed only when Oracle is a source in mirroring replications)

When setting up the connection for transactional replications (where Oracle is serving as the source of data, either for mirroring or for synchronization), the following permissions are also required: SELECT_TABLE

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

permissions on the source table (see above); execute permission to run the logminer; and access all system tables to retrieve log information and the last transaction ID.

```
grant execute on sys.dbms_logmnr to <uid>;
grant select on sys.v_$parameter to <uid>;
grant select on sys.v_$log to <uid>;
grant select on sys.v_$logfile to <uid>;
grant select on sys.V_$logmnr_contents to <uid>;
grant select on sys.V_$thread to <uid>;
grant select on sys.V_$archive_dest to <uid>;
grant select on SYS.AUD$ to <uid>;
```

To use archived logs to identify database changes for mirroring, you must execute the following:

```
grant select on sys.v_$archived_log to <uid>;
```

For Oracle versions 10g and above, execute the following:

```
grant select any transaction to <uid>;
```

For Oracle versions 12c and above, execute the following:

```
grant select on cdb_pdb$ to <uid>;
grant logmining to <uid>;
grant select on sys.v_$database to <uid>;
grant select on sys.v_$containers to <uid>;
grant select on DBA_LOG_GROUPS to <uid>;
grant select on DBA_LOG_GROUP_COLUMNS to <uid>;
grant EXECUTE_CATALOG_ROLE to <uid>;
```

Example:

```
grant select any transaction to sdruser;
grant logmining to sdruser;
grant select on sys.v_$archived_log to sdruser;
grant execute on sys.dbms_logmnr to sdruser;
grant select on sys.v_$parameter to sdruser;
grant select on sys.v_$log to sdruser;
grant select on sys.v_$logfile to sdruser;
grant select on sys.V_$logmnr_contents to sdruser;
grant select on sys.V_$thread to sdruser;
grant select on sys.V_$archive_dest to sdruser;
grant select on SYS.AUD$ to sdruser;

grant select on sys.v_$database to sdruser;
grant select on sys.v_$containers to sdruser;
grant select on DBA_LOG_GROUPS to sdruser;
grant select on DBA_LOG_GROUP_COLUMNS to sdruser;
```

Syniti Data Replication

```
grant EXECUTE_CATALOG_ROLE to sdruser;
```

For Oracle versions 12c and above using Pluggable Database (PDB) all the GRANT statements should be run on the container:

```
grant execute on sys.dbms_logmnr_d to <uid> container=ALL;
grant select on sys.v_$parameter to <uid> container=ALL;
grant select on sys.v_$log to <uid> container=ALL;
grant select on sys.v_$logfile to <uid> container=ALL;
grant select on sys.V_$logmnr_contents to <uid> container=ALL;
grant select on sys.V_$thread to <uid> container=ALL;
grant select on sys.V_$archive_dest to <uid> container=ALL;
grant select on sys.v_$archived_log to <uid> container=ALL;
grant select any transaction to <uid> container=ALL;
grant select on cdb_pdbs to <uid> container=ALL;
grant logmining to <uid> container=ALL;
grant select on sys.v_$database to <uid> container=ALL;
grant select on sys.v_$containers to <uid> container=ALL;
grant select on DBA_LOG_GROUPS to <uid> container=ALL;
grant select on DBA_LOG_GROUP_COLUMNS to <uid> container=ALL;
grant EXECUTE_CATALOG_ROLE to <uid> container=ALL;
```

NOTE: If you are using Oracle versions 12c and above Pluggable Database (PDB) architecture, contact the support team via [the Help Center](#) for additional instructions.

Set Up the Syniti DR Environment

This section describes the settings for a source connection that uses Oracle with the Remote Log Server Agent.

Add a Source Connection Wizard

Select Provider Screen

Assembly

The value for Oracle should be the pathname to the .NET Assembly Oracle.DataAccess (file name: Oracle.DataAccess.dll.) For later versions of Oracle, you can leave the Assembly field blank because the dll path should be available to Syniti DR. (The dll is registered during installation of the Oracle .NET Data Provider.) If the value is not available, Syniti DR displays a message when you continue in the Source Connection wizard, allowing you to go back and type in the path. Find out the location of the assembly in your environment by searching for the file name Oracle.DataAccess.dll, then enter the path and the assembly file name as in the example below.

Example:

```
C:\oracle10_2\client\odp.net\bin\2.x\Oracle.DataAccess.dll.
```

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

Set Connection String Screen

Data Source

Type the IP address of the server, then a colon and the port number, followed by / and the Oracle service name (for Oracle versions 11 and later) as in the example below.

```
122.333.4.555:1521/ORADB1
```

User ID

Enter a user ID which will be exclusively used by Syniti DR and has the authority to read the database transaction log (redo log.) See a detailed list of authorities needed.

For Synchronization Replications:

The login/user ID that you provide must be unique to Syniti DR. It should not be used for any transactions occurring in either database involved in the synchronization. Syniti DR does not replicate transactions by the user you specify in this connection. This user ID is used by Syniti DR during synchronization to read the database logs and perform the synchronization operations. Therefore, any transactions found in the logs with this user ID are not replicated as part of the synchronization data.

Enable Transactional Replication Wizard

For transactional replications (mirroring and synchronization), use the Enable Transactional Replication wizard after setting up a source connection. The following field(s) require specific information for Oracle.

Log Type Screen

Select Log Server Agent.

Log Settings Screen

Log Settings

The Log Settings field displays the Oracle data source where the log is stored. This field is read-only and by default matches the data source specified in the source connection. If you are using the multitenant database architecture introduced in Oracle 12, and connecting to a pluggable database, you may need to modify the log location to match the Oracle root, or container, database. To modify the log location, click the [...] button.

Click [...] to open the [Change Log Settings dialog](#) to:

- Change the Oracle server where the log is stored (for Oracle 12 multitenant database installations).
- Set a path to an Oracle dictionary file (primarily for Oracle versions up to 9)
- Change the archived log settings

Supplemental Log Minimal Level/Supplemental Log Database Level

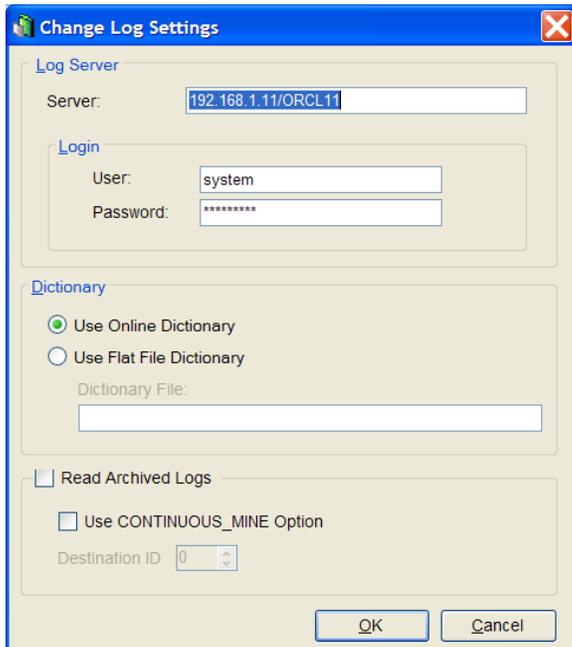
These fields are set automatically depending on what type of supplemental logging is currently set for your Oracle source connection. For transactional replications where Oracle is a source database, Syniti DR requires supplemental logging to be enabled at least at the minimal level (and later at the table level) to record sufficient information about changes to the data in the table.

Minimal Level establishes minimal supplemental logging at the database level, then, during replication setup, you can add logging for the specific table(s) involved in the replication.

Database Level establishes supplemental logging for the entire database, including primary key and index information for all tables. If you have a large number of tables in your database, and they are not involved in Syniti DR replications, you should be aware that supplemental logging can add unnecessary processing time/log information.

Syniti Data Replication

Change Log Settings Dialog



Server

Specifies the Oracle data source where the log is stored. If you are using the multitenant database architecture introduced in Oracle 12, and connecting to a pluggable database, you need to modify the log location to match the Oracle root, or container, database.

User

User ID for the Oracle data source where the log is stored.

Password

Password for the Oracle data source where the log is stored.

Dictionary File

If the log miner dictionary is defined as a flat file (typically only for Oracle versions up to 9), type the path and file name for an Oracle dictionary file. The Oracle dictionary file should already be defined in your Oracle environment. See [Setup for Different Oracle Versions](#) for more information.

Read Archived Logs

When checked, Syniti DR accesses Oracle archived redo logs for transactions in addition to the online redo logs. Check with your Oracle system administrator to see if your database is configured to use ARCHIVELOG mode. If it is, you can check the **Read Archived Logs** option to ensure that all transactions between mirroring intervals are identified by Syniti DR. For example, if your mirroring interval is set for 90 seconds, but within that time the online logs fill with transactions, the online logs are archived as needed to accommodate additional transactions. If you check the **Read Archived Logs** option, Syniti DR will be able to locate the last transaction ID from the archived log. Note that the **Read Archived Logs** option is not useful when using the default setting on Oracle databases, NOARCHIVELOG mode.

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

Use CONTINUOUS_MINE Option

When **ReadArchivedLogs** is checked, the **Use CONTINUOUS_MINE Option** is checked by default. The CONTINUOUS_MINE option instructs the Oracle log reader to load archived log files continuously as they get created, instead of loading a batch of files statically when the log reader is initially instantiated. Syniti DR can therefore replicate transactions as they are backed up. However, Oracle recommends that the CONTINUOUS_MINE option should not be used in a RAC (Real Application Cluster) environment where RAC nodes are continuously enabled/disabled.

Destination ID

This option allows you to set the location from which Syniti DR will pick up Oracle archived logs for replication. When the value is set to the default, 0, Syniti DR searches for Oracle archived logs in the standard destination, ('FLASH RECOVERY AREA (FRA)'). A value between 1 and 31 specifies an alternative location to retrieve archived logs. Oracle users can retrieve a list of all archive locations by running the query: `SELECT * FROM V$ARCHIVE_DEST`. This feature is useful when your environment includes a customized archive setup and you want to instruct Syniti DR use a specific location for archived logs.

Agent Settings Screen

1. Check the **Use Remote LSA** option.
2. Specify the IP Address and port number where the Syniti Remote Log Server runs and listens (this should be the Address of the server on which the Oracle database resides.)

The screenshot shows the 'Enable Transactional Replication Wizard' window for Syniti Data Replication. The 'Agent Settings' tab is selected in the left-hand navigation pane. The main area contains the following fields and options:

- Log Server Agent Settings:**
 - Log Server Folder:
 - Log Files Folder:
 - Prefix:
 - Log File Size: (with a dropdown arrow)
 - Keep Max Files: (with a dropdown arrow)
 - Extra Options:
 - Trace:
- Use Log Container
 - Server:
 - User - Password: (with a masked password field)
- Use Remote Server. Address / Port: /
- Windows Service:
 - Prefix:
 - Name:
 - Service Name: **Syniti_LSA_oracle_alphaserver**
 - Start Service after completing the wizard

At the bottom of the window are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Create Replication Wizard

After creating source and target connections, and setting up for transactional replications, create the replication. The following fields require specific information for Oracle Remote Log Server Agent.

Copyright © 2021 BackOffice Associates, LLC d/b/a Syniti. All rights reserved. This document contains confidential and proprietary information and reproduction is prohibited unless authorized by Syniti. Names appearing within the product manuals may be trademarks of their respective owners.

Syniti Data Replication

Source Log Info

Service Name

This is a unique identifier for your Oracle Server. The value is obtained automatically from your Oracle database server and cannot be modified.

Dictionary File

If using Oracle 9 or later, you can leave this field blank to use the online dictionary. If you prefer to supply a dictionary file, provide a path and dictionary file name on your Oracle database server. The online dictionary/dictionary file contains table information that is used in replication.

Run the Remote Log Server

Before starting the Syniti Replication Agent, start the Remote Log Server application that you installed on the Oracle system as follows.

The main class of the SRLS is **com.syniti.remotelogserver.StartServer**

Run the application from a command line:

```
java -cp remotelogserver.jar:ojdbc7.jar:orail8n.jar com.syniti.remotelogserver.StartServer
```

By default, the server will listen and accept connections on port number 45000. A different port number can be explicitly specified with the parameter **-port**. For example:

```
java -cp remotelogserver.jar:ojdbc7.jar:orail8n.jar com.syniti.remotelogserver.StartServer -port:45001
```

Note that if the system running the Remote Log Server application is restarted at any time, you will also need to restart the application. To avoid this extra step, it is highly recommended that you set up an automatic restart. The ServerFiles/OracleRemoteLogServer folder includes files with an example of how to do this for Linux. On a Microsoft Windows server, you need to create a task to set up an automatic restart. Check Windows help for more information on how to do this.

Using the Remote Log Server with Oracle ASM Storage

On an Oracle database that stores all its log files in ASM storage, the RLS is unable to access or read these log files. It is possible to duplicate the redo and archived log files on native disk storage outside of ASM so that the RLS can access them. These operations should be well planned by a database administrator to ensure that there is enough disk space and the archived log files are properly purged as part of the archive log management workflow.

For redo log files, a new file member must be added to EACH redo log group.

For example:

```
ALTER DATABASE ADD LOGFILE MEMBER '/usr/db1store/redo/myredo01.log' TO GROUP 1;  
ALTER DATABASE ADD LOGFILE MEMBER '/usr/db1store/redo/myredo02.log' TO GROUP 2;
```

Syniti Data Replication

For archived log files, specify a new archive destination.

For example:

```
ALTER SYSTEM SET LOG_ARCHIVE_DEST_2='LOCATION=/usr/db1store/redo ' SCOPE = BOTH;
```

Last Updated on 3/31/21