

sgi[®]



Using the StorHouse/RFS Audit Log

Publication Number
007-6325-001

November 19, 2013

StorHouse[®]



© 2013 Silicon Graphics International Corp. All Rights Reserved; provided portions may be copyright in third parties, as indicated elsewhere herein. No permission is granted to copy, distribute, or create derivative works from the contents of this electronic documentation in any manner, in whole or in part, without the prior written permission of SGI.

Publication Number 007-6325-001

LIMITED RIGHTS LEGEND

The software described in this document is "commercial computer software" provided with restricted rights (except as to included open/free source) as specified in the FAR 52.227-19 and/or the DFAR 227.7202, or successive sections. Use beyond license provisions is a violation of worldwide intellectual property laws, treaties and conventions. This document is provided with limited rights as defined in 52.227-14.

TRADEMARKS AND ATTRIBUTIONS

SGI, SGI InfiniteStorage, the SGI logo, Supportfolio, SGI Trusted Edge, and SGI StorHouse are trademarks or registered trademarks of Silicon Graphics International Corp. or its subsidiaries in the United States and other countries. All other trademarks mentioned herein are the property of their respective owners.



Contents

Welcome	1
Purpose of this Manual.....	1
Audience	1
Contents.....	2
Chapter 1: Configuring StorHouse/RFS to Enable Audit Logging	3
About the StorHouse/RFS Audit Log.....	3
Audit Log Format	4
Audit Log Database and User Table Format	6
RFS Configuration File Parameters that Control Audit Logging and Hashing	8



Chapter 2: Generating Audit Log Reports using SAP Crystal Reports 2011.....	11
Prerequisites.....	11
Creating the Sample Report.....	12
 Chapter 3: Sample Audit Log Reports Created Using SAP Crystal Reports 2011.....	 25
RFS Audit Report - Files Created in the Last 30 Days.....	26
RFS Audit Report - File Hashes for Files Created on the Current Day	27
RFS Audit Report - File Actions by User ID for the Last 30 Days.....	28



Welcome

Welcome to *Using the StorHouse/RFS Audit Log*. The StorHouse/RFS audit log contains records written to a file and/or the RFS audit log database whenever a specific system event occurs. Administrators can use report generation tools such as SAP Crystal Reports 2011 to query the audit log database and build detailed reports that track system usage.

Purpose of this Manual

This manual explains the parameters in the StorHouse/RFS configuration file that control RFS audit logging. It also explains how to query the audit log database to generate customized RFS usage reports. The examples in this manual use SAP Crystal Reports 2011 as the report generation tool of choice. However any similar reporting platform that permits connectivity via ODBC data sources is equally effective.

Audience

The audience of this manual consists of StorHouse/RFS system administrators who are responsible for installing, configuring, and maintaining StorHouse/RFS. It is also comprises database administrators or any persons in charge of using third-party



report generation tools at the customer site. It assumes readers are familiar with StorHouse/RFS operation and setup, including creating and updating StorHouse/RFS profiles in CCI, and the format of the audit log database. It also assumes readers know how to use the third-party report generation tool of choice.

Contents

This manual has three chapters:

- Chapter 1, “Configuring StorHouse/RFS to Enable Audit Logging,” explains the format of the StorHouse/RFS audit log and database and describes how to set up the RFS configuration file parameters that enable audit logging.
- Chapter 2, “Generating Audit Log Reports using SAP Crystal Reports 2011,” explains how to use SAP Crystal Reports 2011 to query the StorHouse/RFS audit log database to produce a report listing all files created in a StorHouse system grouped by RFS server and the user IDs that created the files.
- Chapter 3, “Sample Reports,” contains three sample reports generated from the audit log database using SAP Crystal Reports 2001.



Configuring StorHouse/RFS to Enable Audit Logging

This chapter defines the StorHouse/RFS audit log and database and describes their formats. It also explains the parameters in the StorHouse/RFS configuration file that control audit logging.

About the StorHouse/RFS Audit Log

The StorHouse/RFS audit log contains records written for a given file whenever a specific system event occurs. Administrators can configure the StorHouse/RFS software to generate the audit log as a text file or in database format. For the text file format, StorHouse/RFS writes a local log only and starts a new one every day.

For the database format, StorHouse/RFS initially writes log records to a text file and subsequently bulk loads them into a user table in the audit log database at a user-specified interval. Administrators can submit SQL queries to the audit log table using the SGI ODBC driver directly or by using any third-party report generation platform (for example, SAP Crystal Reports 2011) that permits connectivity via ODBC data sources.

Table 1-1 lists the valid audit log record types and explains the system events that trigger them.

Table 1-1: Audit Log Record Types

Record Type	Information Logged When
Create	StorHouse/RFS creates a file or directory.
Delete	StorHouse/RFS deletes a file or directory.
Rename	StorHouse/RFS renames a file or directory
Modify	A user or application changes file content or metadata for a file or directory.
Access	A user or application opens a file for reading.
Hash	StorHouse/RFS hashes a file on ingest to StorHouse. StorHouse/RFS writes a separate hash record for each specified hash type. For example, hashing a file according to MD5 and SHA1 protocols will create two audit log hash records.

Audit Log Format

Audit log records contain the following tab-separated fields.

- UTC Date in the format YYYY-MM-DD HH:MM:SS.NNNNNN
- Operational event that triggered the logging
- Name of the user who initiated the operation
- Complete path and file name separated by a common delimiter (\)
- Hash value of the path and file name
- Host name of the StorHouse/RFS server
- Complete path and file name of the rename destination (RENAME only)
- Collection name if the file has been collected

- Starting logical block number (LBN) in the collection if the file has been collected
- File size if the file has been collected
- Hash type (for hash entries only)
- Hash value (for hash entries only)

The following is a sample text audit log.

```

2012-06-18 20:12:55.155965      C      0      \root\061812
6484964978907623608      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.309951      C      0      \root\061812\file.0
2063546621671238554      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.321187      C      0      \root\061812\file.1
2063546621671238555      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.333209      C      0      \root\061812\file.2
2063546621671238556      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.344526      C      0      \root\061812\file.3
2063546621671238557      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.357120      C      0      \root\061812\file.4
2063546621671238558      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.367932      C      0      \root\061812\file.5
2063546621671238559      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.379244      C      0      \root\061812\file.6
2063546621671238560      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.390375      C      0      \root\061812\file.7
2063546621671238561      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.402254      C      0      \root\061812\file.8
2063546621671238562      LINXSTH.FILETEK.COM
2012-06-18 20:13:19.413201      C      0      \root\061812\file.9
2063546621671238563      LINXSTH.FILETEK.COM
2012-06-18 20:16:00.248189      H
12_13_06\loop_10.all_sizes\all_sizes.105557 -3432954264645978833
LINXSTH.FILETEK.COM
COLL120120618135548(C).LINXSTH.FILETEK.COM 1      105557  MD2
66CE0EE83C420C492098F1EEBB9735D0
2012-06-18 20:16:00.248300      H
12_13_06\loop_10.all_sizes\all_sizes.105557 -3432954264645978833
LINXSTH.FILETEK.COM
COLL120120618135548(C).LINXSTH.FILETEK.COM 1      105557  MD4
952DCCC8B30744E43B43F80C7380D251
2012-06-18 20:16:00.248320      H
12_13_06\loop_10.all_sizes\all_sizes.105557 -3432954264645978833
LINXSTH.FILETEK.COM
COLL120120618135548(C).LINXSTH.FILETEK.COM 1      105557  MD5
3C486C36C625675BC2E894080CDC4433
2012-06-18 20:16:00.248338      H
12_13_06\loop_10.all_sizes\all_sizes.105557 -3432954264645978833

```

```

LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557  SHA
78A6E86AE728BC9BE71D52B5473CD95227D9206F
2012-06-18 20:16:00.248356      H      \rfs0\Jun-18-12-
12_13_06\loop_10.all_sizes\all_sizes.105557      -3432954264645978833
LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557
SHA1B86E09B62F62922EABDFF73C82DB620002F579C2
2012-06-18 20:16:00.248373      H      \rfs0\Jun-18-12-
12_13_06\loop_10.all_sizes\all_sizes.105557      -3432954264645978833
LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557  SHA22
4      8D51687914DBD978F1BD3919C33644B7D98BA68F6604B4C2436FD2D5
2012-06-18 20:16:00.248391      H      \rfs0\Jun-18-12-
12_13_06\loop_10.all_sizes\all_sizes.105557      -3432954264645978833
LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557  SHA25
6
07FC8D1F1DD74BDA83873BBC249677674E0204BDB0D5BEEAEABFA578BB99EA20
2012-06-18 20:16:00.248410      H      \rfs0\Jun-18-12-
12_13_06\loop_10.all_sizes\all_sizes.105557      -3432954264645978833
LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557  SHA38
4
2312237FB13EE7FA88259BAF2D9AAE3CEE9E54FA0C5CF89CF63E140C849CA43114156A
D5F75AEA8D49D8A1D658261B45
2012-06-18 20:16:00.248505      H      \rfs0\Jun-18-12-
12_13_06\loop_10.all_sizes\all_sizes.105557      -3432954264645978833
LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557  SHA51
2
7B20ED72CE21201ED4544E0FAD9D6F6FDA1C63F02F8A8513A8F9E43339ED0AACF51DE5
B4B973ED872F22489D291A84A8F5407FFB1E31986095053D891B32D172
2012-06-18 20:16:00.248525      H      \rfs0\Jun-18-12-
12_13_06\loop_10.all_sizes\all_sizes.105557      -3432954264645978833
LINUXSTH.FILETEK.COM
COLL120120618135548 (C) .LINUXSTH.FILETEK.COM      1      105557  RMD16
0      3741734575AB3BA1422EFBB28F68C672F0BF064C

```

Audit Log Database and User Table Format

Before you can store the audit log in database format, you must create an audit log database and the `_AL` table within that database. You create the audit log database with the `setup_audit_db` utility script. To create the `_AL` table, you must copy the `setup_audit_db` script to your StorHouse SM server system and then run the script as `ftlkoper`. The full path to the `setup_audit_db` script is `/opt/FLTKrfs/bin`.

Table 1-2 defines the fields in the `_AL` table.

Table 1-2: Fields in the _AL Table

Field	Definition	Format
TSTAMP	Date and time the logged event occurred.	TIMESTAMP NOT NULL DEFAULT SYSTIMESTAMP
RECORD_TYPE	Type of event. Valid values are: <ul style="list-style-type: none"> ■ A – access for read ■ C – create ■ D – delete ■ R – rename ■ M – modify ■ H – hash 	CHAR(1) NOT NULL DEFAULT ' '
USERNAME	UNIX user ID of the user who performed the action.	VARCHAR(70) NOT NULL DEFAULT ' '
FILEPATH	Path of the file processed by the event.	VARCHAR(4096) NOT NULL DEFAULT ' '
FILEPATH_HASH	Value used to identify the file in other tables (for example, the locator and security tables).	BIGINT NOT NULL DEFAULT 0
SYSTEMNAME	Name of the StorHouse/RFS server where the event took place.	VARCHAR(64) NOT NULL DEFAULT ' '
OLD_FILEPATH	In move operations, the source path of the file.	VARCHAR(4096) DEFAULT ' '
COLLECTION_NAME	Name of the StorHouse collection file that contains the user file.	VARCHAR(56)
LBN	Logical block number indicating the location of the user file within the collection file.	INTEGER
FILE_SIZE	Size of the user file in bytes.	BIGINT
HASH_TYPE	Type of hashing algorithm (for example, MD5) used for this record.	CHAR(6)
FILEDATA_HASH	Actual hash value of the file (i.e., the MD5 string)	VARBINARY(128)

RES1	Reserved for future use.	VARCHAR (256)
XML	Reserved for future use.	VARCHAR (20000))

The `_AL` table has two indexes:

- A range index on the `TSTAMP` field
- A value index on the `FILEPATH_HASH` field

RFS Configuration File Parameters that Control Audit Logging and Hashing

The parameters that control audit logging and hashing are located in the `AUDITLOG` section and `COLLECTION` definition of a StorHouse/RFS configuration file. Note the following:

- At minimum, you must provide values for the `MaxLoadInterval` and the `Storage` parameters in the `AUDITLOG` section to write data to the audit log database.
- You must configure the `FileAudit` setting for each `Collection` definition that you want to track in the audit log.

Table 1-3 describes the parameters that affect audit logging.

Table 1-3: Parameters That Control Audit Logging and Hashing

Configuration Parameter	Definition
AUDITLOG Section	Globally defines if and where RFS writes audit log data.
FileAuditPath	Fully qualified path where StorHouse/RFS will write the audit/hash records. Note: There is a parameter with the same name in the RFS section of the configuration file. This parameter will be deprecated in the near future. Therefore, always specify FileAuditPath in the AUDITLOG section to enable audit logging.
MaxLoadInterval	Amount of time in minutes between bulk loads of audit log records to the database.
Storage	Name of the StorHouse/RFS storage definition that will contain the audit log database. If blank, StorHouse/RFS will write the audit log in text file format only. You must specify Storage to enable use of the audit log database. You can create a new storage definition to contain the audit log database, or you can set up audit logging to utilize an existing storage definition. Moreover, one or more StorHouse/RFS servers can use the same storage definitions for audit logs, thereby enabling a comprehensive database of all hashes throughout an organization.
Collection Definition	Specifies which events to capture and the type of hashing method for files in this collection.
FileAudit	Types of file and directory actions to be logged for files in this collection. Valid values are: <ul style="list-style-type: none"> ■ A (access) ■ C (create) ■ D (delete) ■ R (rename) ■ M (modify) You may specify one or more values (for example, CDR). Do not separate values with a delimiter. Note that if a value is specified for FileAuditHash, RFS automatically creates a corresponding hash record in the audit log.

FileAuditHash	Types of hashes to perform on files in this collection when they are written to StorHouse. Valid values are: <ul style="list-style-type: none">■ MD5■ SHA■ SHA1■ SHA224■ SHA256■ SHA384■ SHA512■ RMD160 You may specify one or more values (for example, SHA1,SHA224) separated by a comma or space.
---------------	---

You update the RFS configuration file by editing a StorHouse/RFS profile in StorHouse/CCi. A StorHouse/RFS profile is a tool for managing the properties, or operating parameters, of a StorHouse/RFS server. In other words, it is the graphical representation of the sections and definitions in the StorHouse/RFS configuration file. For detailed information about how to update a StorHouse/RFS profile, refer to the *StorHouse/RFS Configuration File Reference Manual*.



Generating Audit Log Reports using SAP Crystal Reports 2011

This chapter explains how to use SAP Crystal Reports 2011 to generate an audit log report that details all StorHouse files sorted by StorHouse/RFS server and user ID that created the file. Although this chapter specifically shows the procedure for creating reports using SAP Crystal Reports 2011, the same concepts can be applied to any reporting tool that can connect to StorHouse via an ODBC data source.

Prerequisites

To use SAP Crystal Reports 2011 to generate audit log reports, you need:

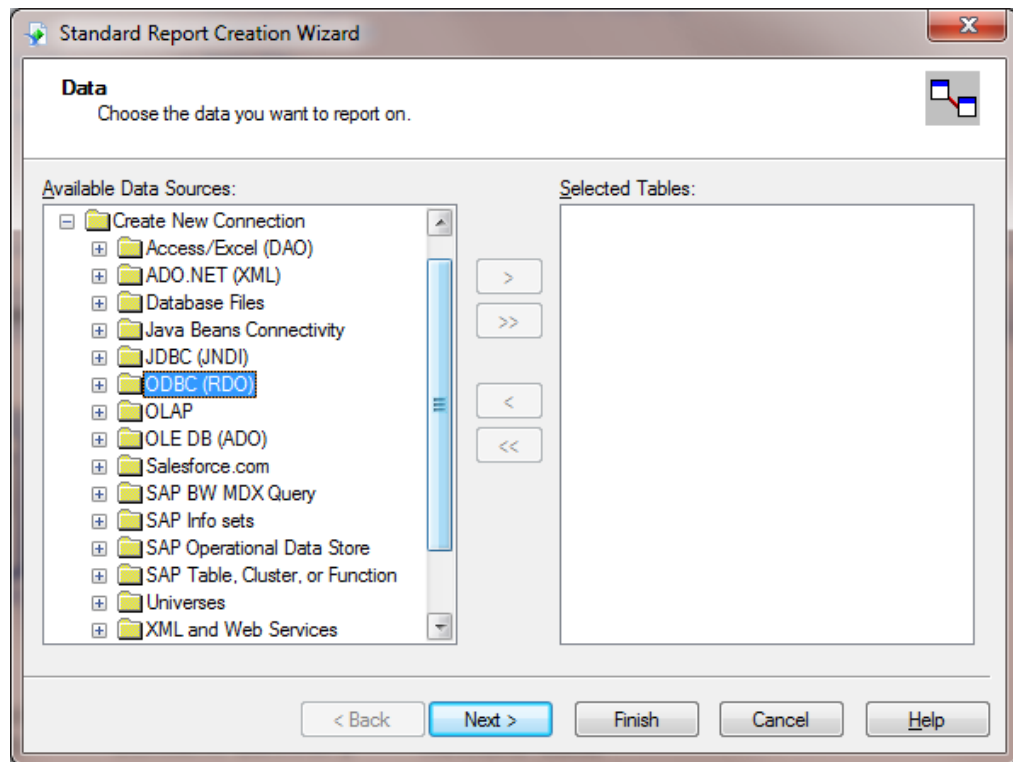
- A StorHouse/RFS server running StorHouse/RFS release v5 or higher
- The SGI ODBC Driver installed and operational on the machine where your reporting application is running
- A version of SAP Crystal Reports 2011

SAP Crystal Reports is available only as a 32-bit application. Therefore, you will need the 32-bit version of the StorHouse/RM ODBC driver.

Creating the Sample Report

Use the following procedure to create the sample audit log report with SAP Crystal Reports 2011.

- ▼ To create a report that details all StorHouse files sorted by RFS server and user ID that created the file
 1. In Crystal Reports, click **Report Wizard**.
 2. In the **Data Source** dialog box, under Create New Connection, select **ODBC (RDO)**.



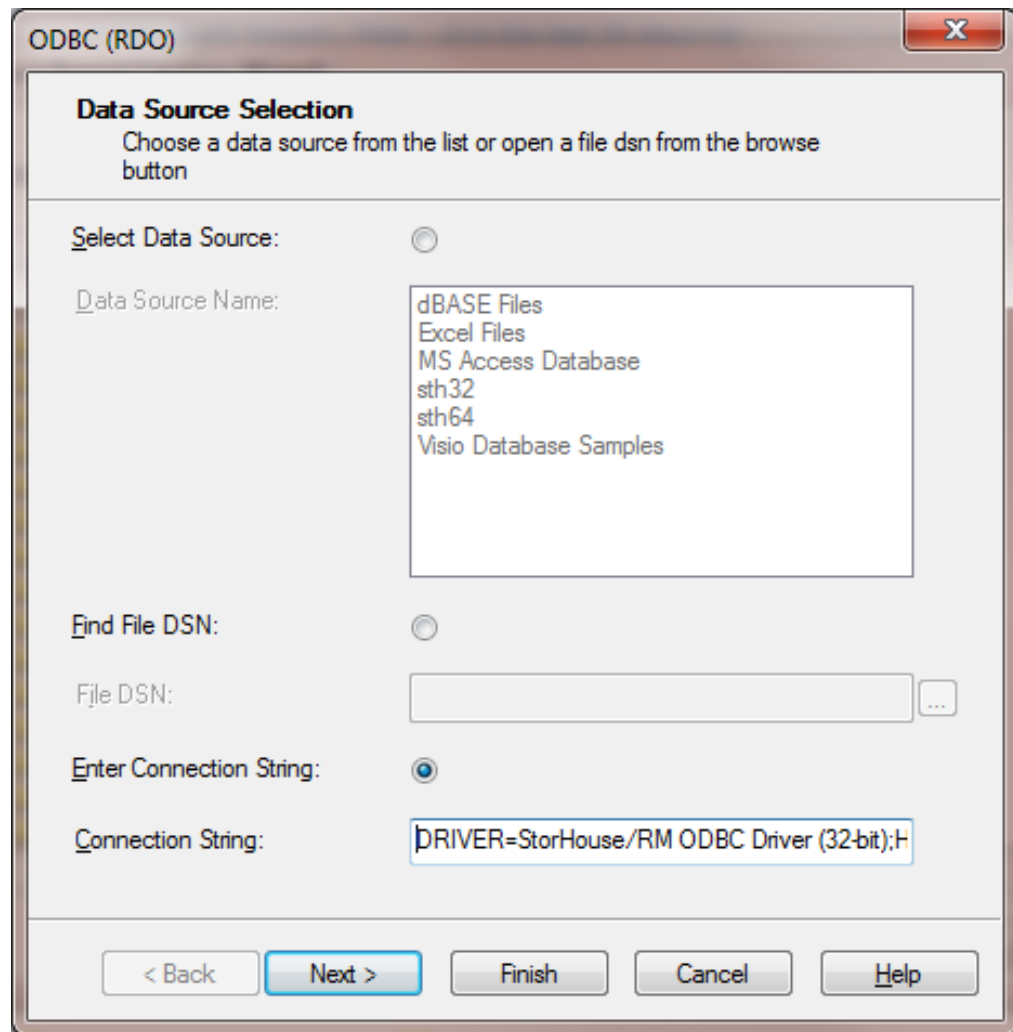
3. When the Data Source Selection dialog opens, SGI provides the connection details. In this example, it is the following connection string:

```
DRIVER=StorHouse/RM ODBC Driver (32-bit);HOST=192.168.10.102[1990];UID=SYSADM;PWD=SYSADM;DATABASE=ARCHIVE;CALLER=
```

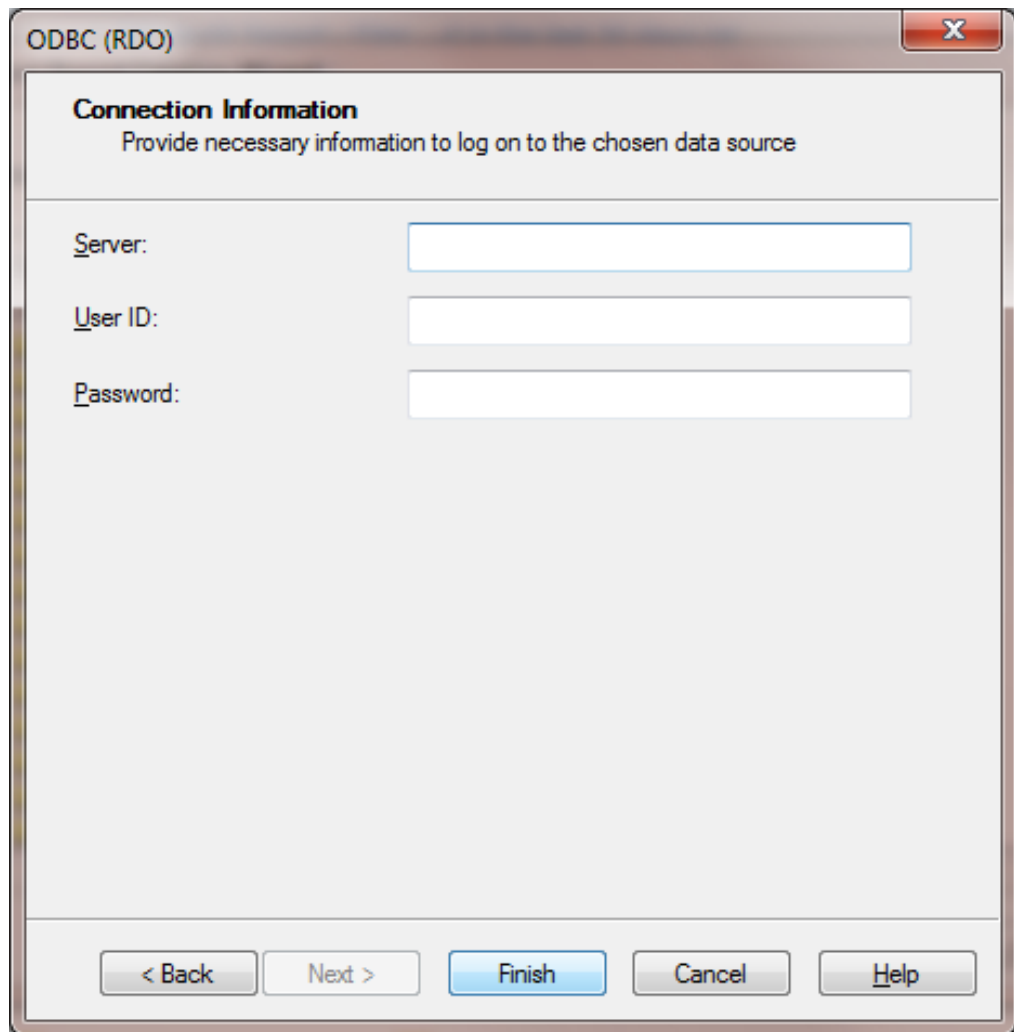
where:

- HOST is the hostname or IP address of your StorHouse server
- UID is the StorHouse account ID used to connect to the database
- PWD is the password for the specified UID
- DATABASE is the name of the database you are connecting to

Note that instead of using a connection string, you could supply a DSN.



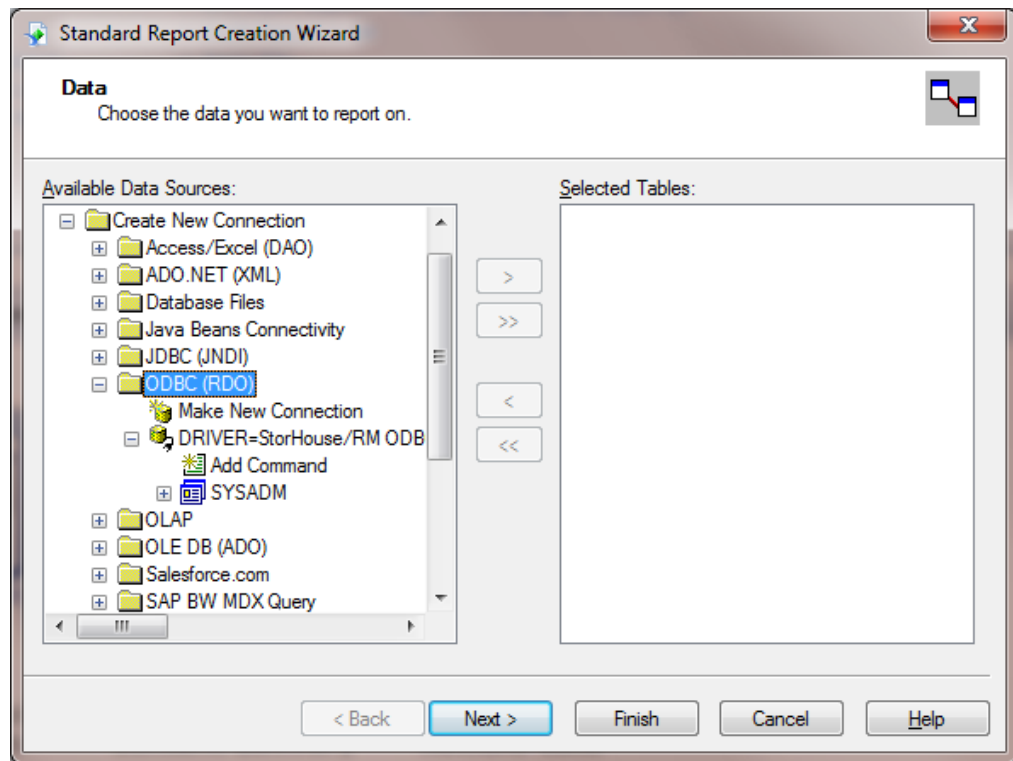
4. Click **Next**.
5. Leave the Connection Information dialog box text boxes blank as the supplied connection string already contains server, user ID, and password information.



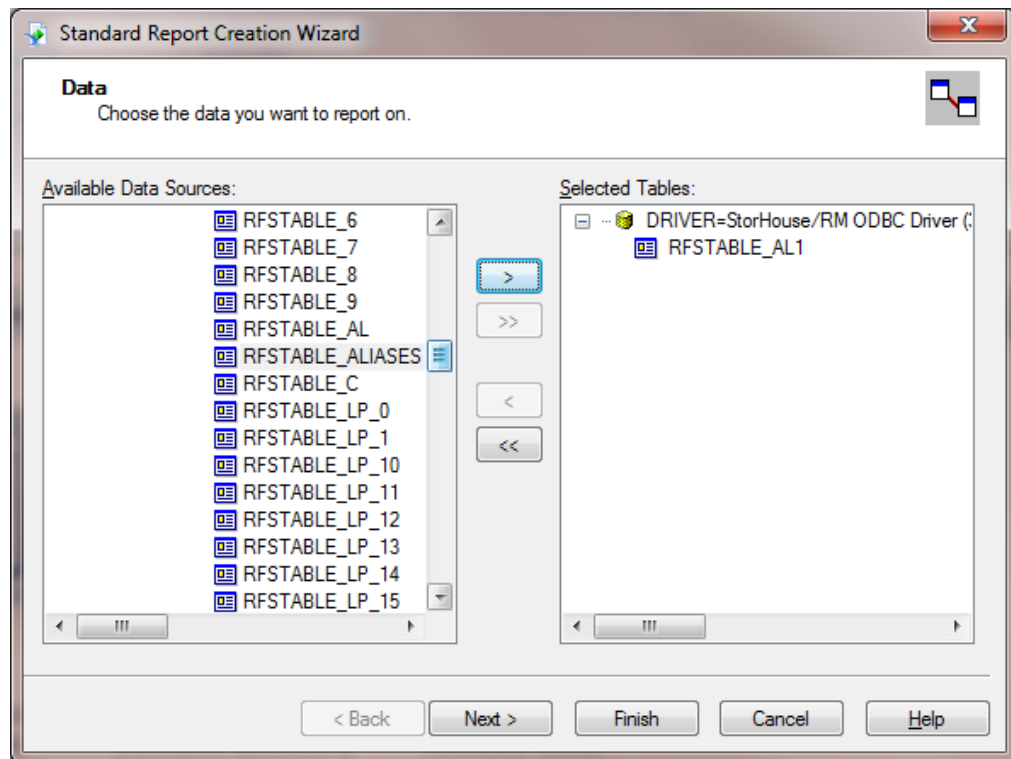
The image shows a Windows-style dialog box titled "ODBC (RDO)". The window has a standard title bar with a close button (X) in the top right corner. The main content area is titled "Connection Information" and contains the instruction "Provide necessary information to log on to the chosen data source". Below this, there are three input fields: "Server:", "User ID:", and "Password:", each followed by a text box. At the bottom of the dialog, there are five buttons: "< Back", "Next >", "Finish" (which is highlighted in blue), "Cancel", and "Help".

6. Click **Finish**.
7. On the **Data** dialog box, expand **SYSADM**.

■ ■ ■ ■ Using the StorHouse/RFS Audit Log

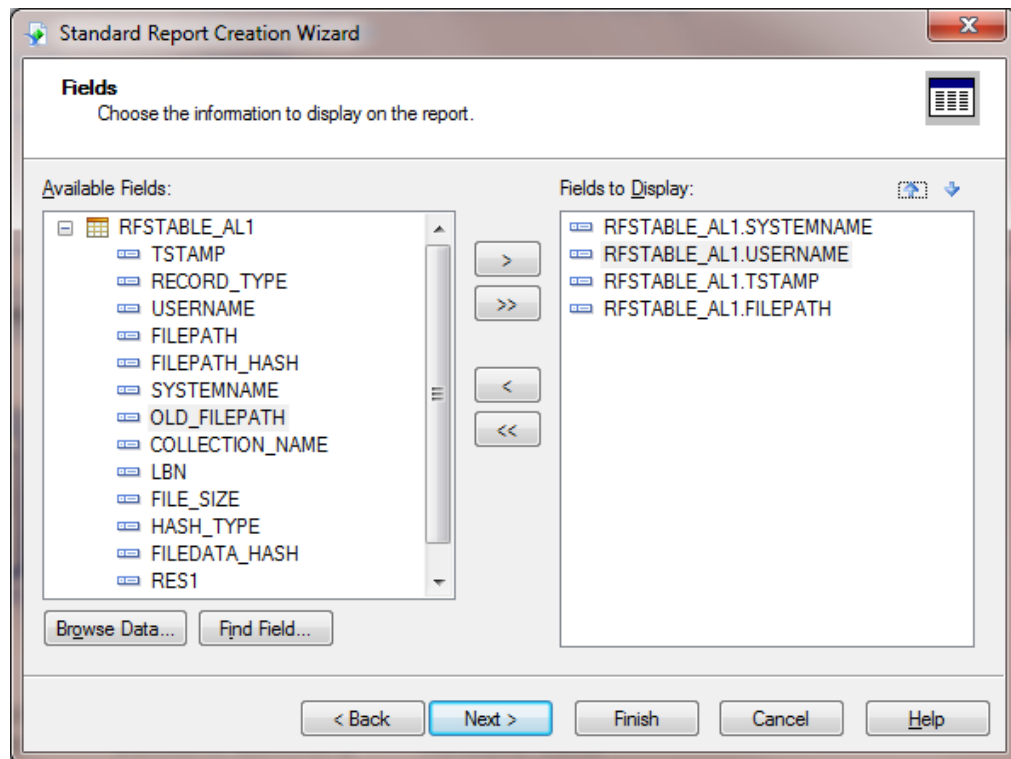


8. Under **Available Data Sources**, Select **TABLENAME_AL**, and then click the arrow to move it to the **Selected Tables** column on the right.



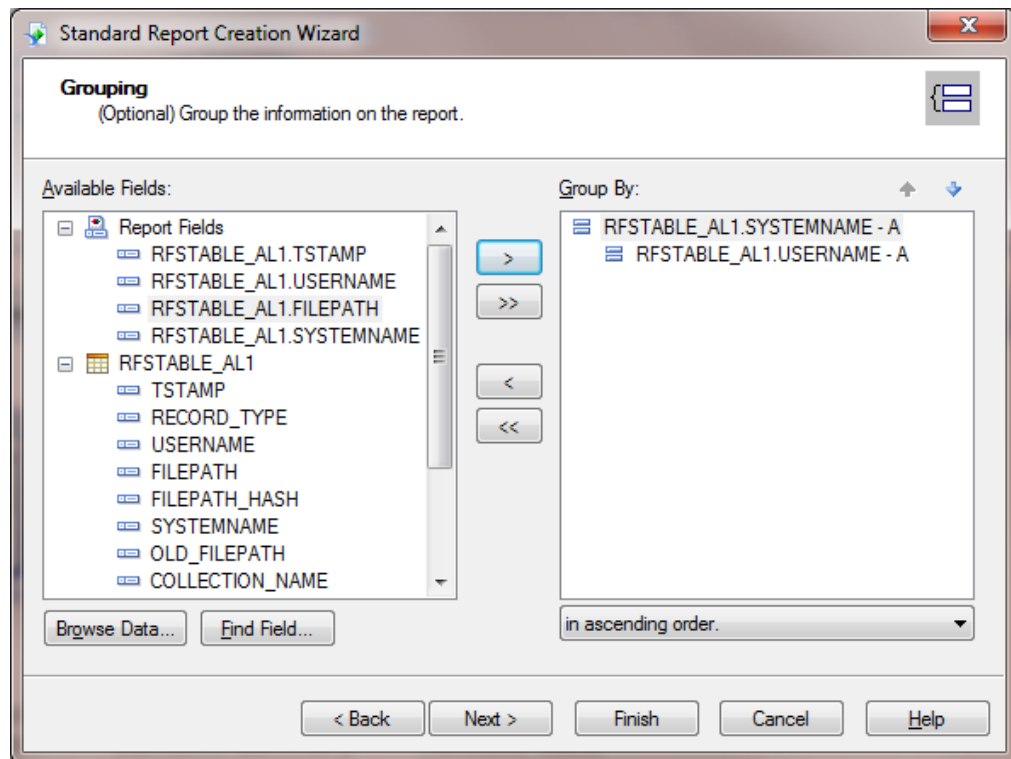
9. Click **Next**.

10. Under **Available Fields**, select **SYSTEMNAME**, **USERNAME**, **TSTAMP**, and **FILEPATH**, and then click the arrow to move each selected field to the **Fields to Display** column on the right.



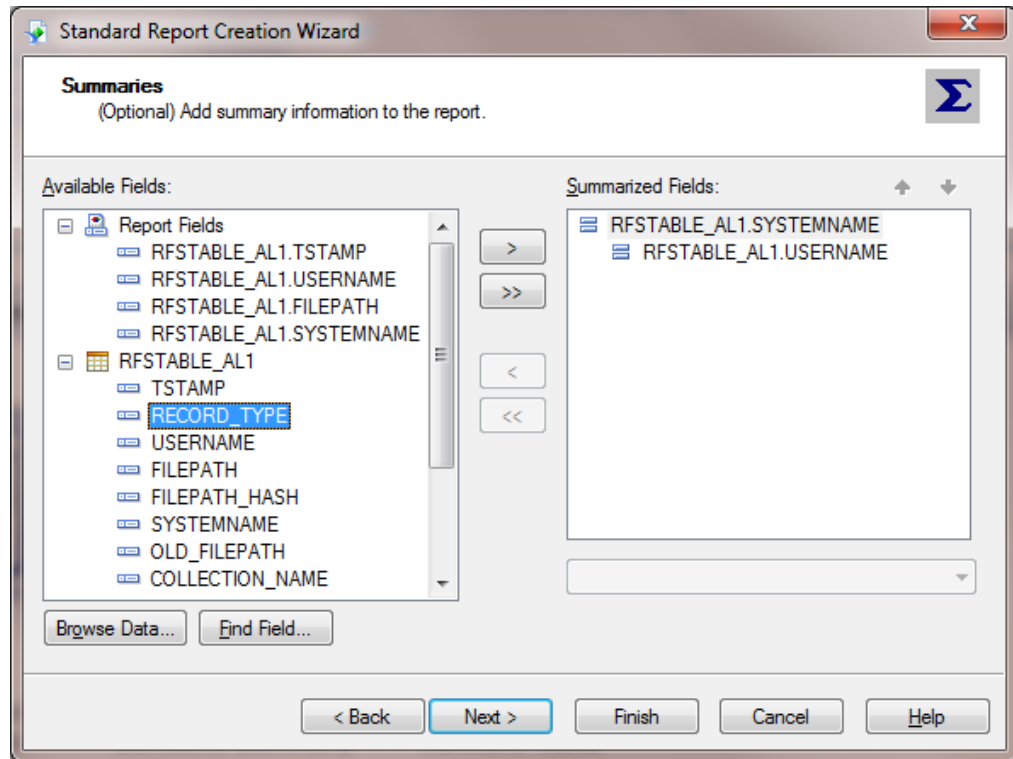
11. Click **Next**.

12. On the **Grouping** dialog box, under **Available Fields**, select **SYSTEMNAME** and **USERNAME**. Then click the arrow to move these fields to the **Group By** column on the right.

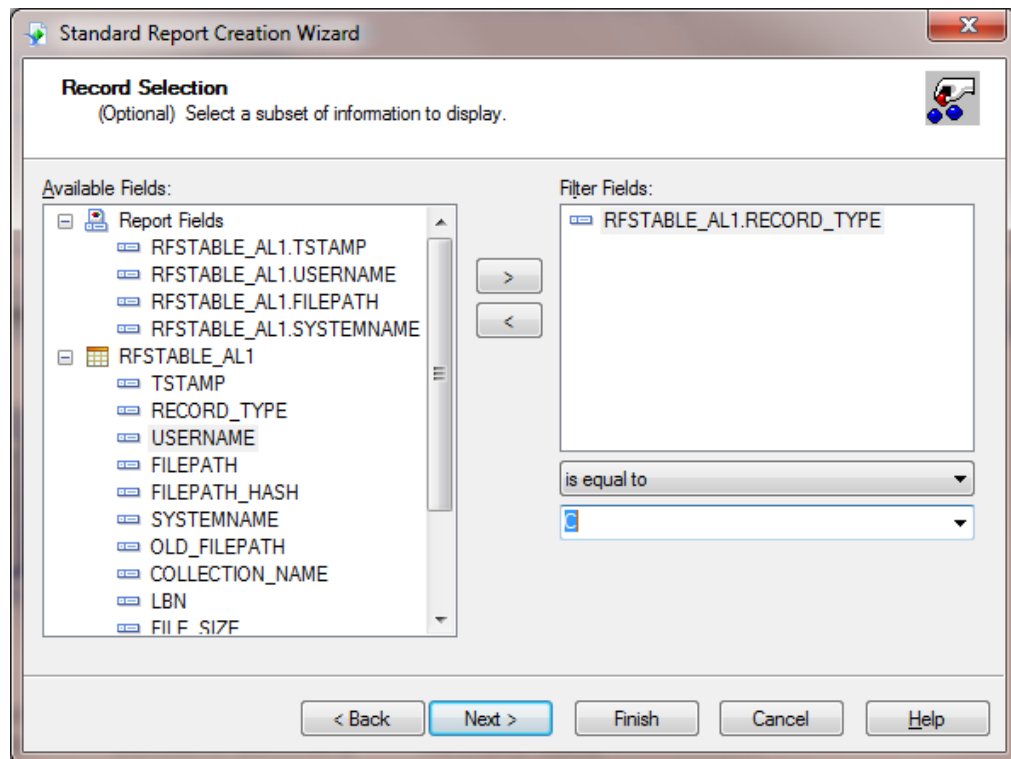


13. Click **Next**.

14. Review the Summaries dialog box, and leave it as is.



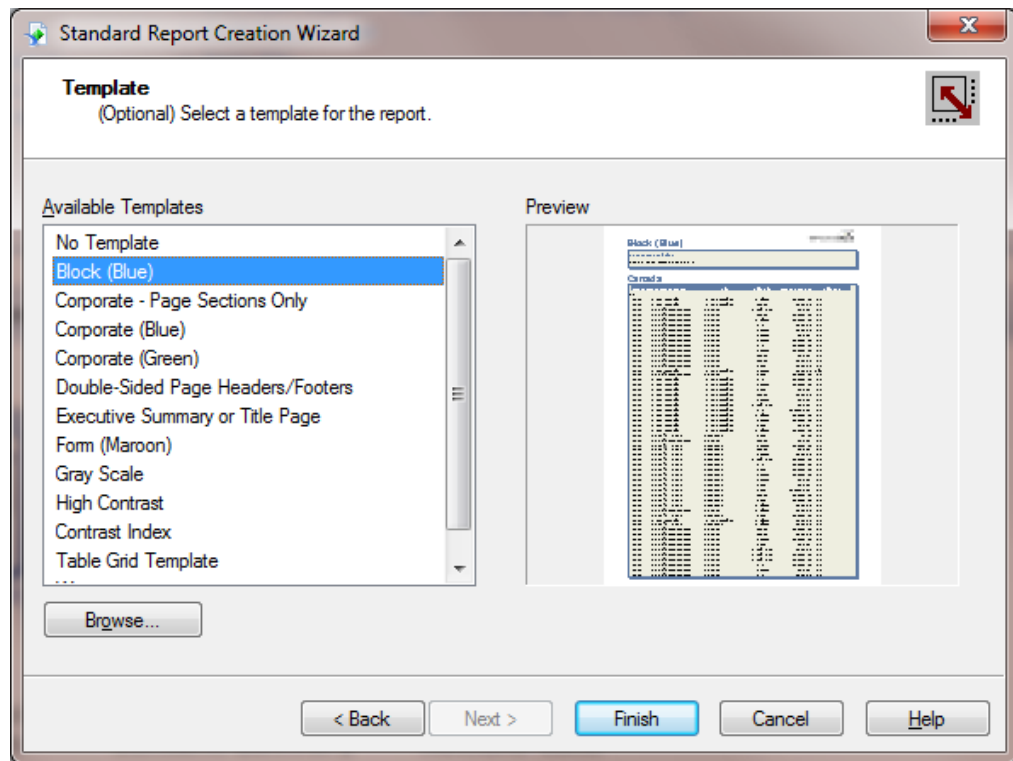
15. Click **Next**.
16. On the **Record Selection** dialog box, select **RECORD_TYPE**. Then click the arrow to move it to the **Filter Fields** column on the right.
17. In the **Filter Fields** column, click the arrow next to the **is equal to** drop-down list, and select **C** to display records only for a “Create” event.



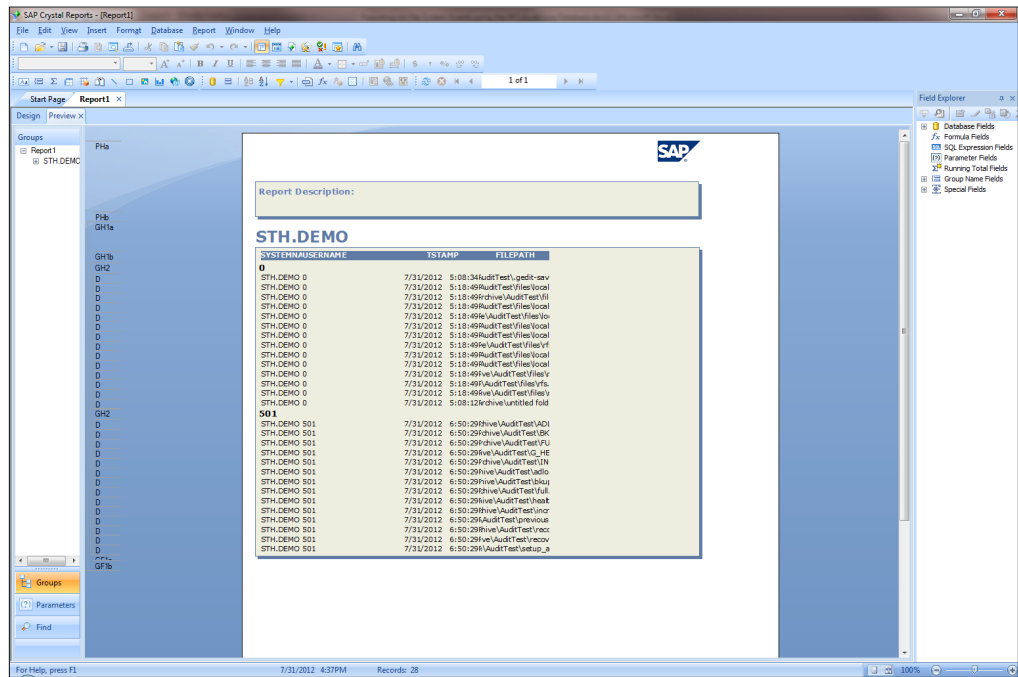
18. Click **Next**.

19. On the **Template** dialog box, under **Available Templates**, select a template (in this example, **Block (Blue)**).

■ ■ ■ ■ Using the StorHouse/RFS Audit Log



You have now created a basic report that shows all files created in your system. The report groups files by RFS server and the user ID that created them.



■ ■ ■ ■ Using the StorHouse/RFS Audit Log

C H A P T E R 3

Sample Audit Log Reports Created Using SAP Crystal Reports 2011

This chapter contains the following sample audit log reports generated with SAP Crystal Reports 2011:

- Files created in the last 30 days
- File hashes for files created on the current day
- File actions by user ID for the last 30 days

SGL distributes these reports in PDF and .rpt formats in a file called Sample Reports.zip.

RFS Audit Report - Files Created in the Last 30 Days

This report shows all files created on the system for the last 30 days grouped by server and user.

RFS Audit Report - Files created in the last 30 days

Report Description: This report shows all files created within RFS over the last 30 days grouped by Server and then userID.

STH.DEMO

System Name	UserID	Time Stamp	File Path
0			
STH.DEMO	0	07/31/2012 17:08:12	\\archive\untitled folder
STH.DEMO	0	07/31/2012 17:08:34	\\archive\AuditTest\gedit-save-FQMLIW
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\rfs_profile.cfg
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\rfs.cfg
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\rfstab
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath\RFSSTATS.HTML
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath\RFSCONFIG.HTML
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath\RFSSTATS.TXT
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath\TEMPLATE.RFSALIAS.HTML
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath\RFSSTATS.XML
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\localpath\RFSINFO.TXT
STH.DEMO	0	07/31/2012 17:18:49	\\archive\AuditTest\files\rfsas.cfg
STH.DEMO	0	08/01/2012 17:17:56	\\archive\AuditTest\untitled folder
STH.DEMO	0	08/01/2012 17:18:06	\\archive\AuditTest\newrfs.cfg
501			
STH.DEMO	501	07/31/2012 18:50:29	\\archive\AuditTest\ADLOG
STH.DEMO	501	07/31/2012 18:50:29	\\archive\AuditTest\adlog.log
STH.DEMO	501	07/31/2012 18:50:29	\\archive\AuditTest\BKUP
STH.DEMO	501	07/31/2012 18:50:29	\\archive\AuditTest\bkup.log
STH.DEMO	501	07/31/2012 18:50:29	\\archive\AuditTest\FULL

RFS Audit Report - File Hashes for Files Created on the Current Day

This report shows the MD5 hashes (assuming this feature has been enabled in the configuration) for all files created on the current day.

RFS Audit Report - File Hash's for files created today

Report Description: Shows the MD5 HASH value for files created today

STH.DEMO

System Name	FILEDATA_HASH	FILEPATH
STH.DEMO	55B62870D7AD9463C322637074FAAF4C	\\archive\AuditTest\also\files\localpath\RFSCONFIG.HTML
STH.DEMO	51F6E7C5C1C211AAACEAB961C8DDFD72C	\\archive\AuditTest\Audit\Reports\RFS Audit Report - File Hash's for files c
STH.DEMO	C70D79E0F77D5748F85330D9FD78C8F89	\\archive\AuditTest\also\files\localpath\RFSINFO.TXT
STH.DEMO	76DE38FF2FFC32C7BDBB3AB1CE69A000	\\archive\AuditTest\Audit\Reports\RFS Audit Report - File Hash's for files c
STH.DEMO	086A7E3500EEB92213408B5A6708802	\\archive\AuditTest\also\files\localpath\RFSSTATS.HTML
STH.DEMO	68341774CC168A11B975A052A24B1045	\\archive\AuditTest\Audit\Reports\RFS Audit Report - Files created in the t
STH.DEMO	807BAFC94B2487063732607A237A4496	\\archive\AuditTest\also\files\localpath\RFSSTATS.TXT
STH.DEMO	ACA6DD4C78FD3A66DFE9470395431C3	\\archive\AuditTest\Audit\Reports\RFS Audit Report - Files created in the t
STH.DEMO	AFE81CB68E62445500304F2E9051D61	\\archive\AuditTest\also\files\localpath\RFSSTATS.XML
STH.DEMO	FD29F44A54FDDA829E1BDD305E0C8D35	\\archive\AuditTest\Audit\Reports\RFS Audit Report - RFS Events.rpt
STH.DEMO	3216B09F50C63DB9009284877BE3F584	\\archive\AuditTest\also\files\localpath\TEMPLATE_RFSALIAS.HTML
STH.DEMO	4BDFAB9F860DD4FD14B120109D589988	\\archive\AuditTest\Audit\Reports\Reporting on File System Events using t
STH.DEMO	DC28FAE514684DDCC3549094DC35389B	\\archive\AuditTest\also\files\vrfs.cfg
STH.DEMO	8361575799D891CC7C39F903E50927F	\\archive\AuditTest\Audit\Reports\Reporting on File System Events using t
STH.DEMO	F99C99E1A23AE78D4B83C03E88DC4152	\\archive\AuditTest\also\files\vrfs.profile.cfg
STH.DEMO	389AFAD9E28092E75BC0819D64E9DBF	\\archive\AuditTest\also\files\vrfsas.cfg
STH.DEMO	5F384107607E69E4EB214E03F7B08558	\\archive\AuditTest\also\files\vrfstab

RFS Audit Report - File Actions by User ID for the Last 30 Days

This report shows file actions by user ID for the last 30 days in a graphical rather than a list format.

