Oracle® Fusion Middleware

Administering the Oracle WebCenter Content Storage Connector for Microsoft SharePoint

11*g* Release 1 (11.1.1)

E38670-01

July 2013

Documentation for administrators that describes how to administer the Oracle WebCenter Content Storage Connector with Microsoft SharePoint 2010.

ORACLE

Oracle Fusion Middleware Administering the Oracle WebCenter Content Storage Connector for Microsoft SharePoint, 11*g* Release 1 (11.1.1)

E38670-01

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Victor Owuor

Contributing Author: Jean Rao

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface vii

Audience vii
Documentation Accessibility vii
Related Documents vii
Conventions viii

1 Introduction

1.1 Connector Overview 1-1
1.2 Architectural Overview 1-1
1.3 Connector Setup 1-3

2 Installation

2.1 Software Requirements 2-1
2.1.1 Software Requirements on the SharePoint Environment 2-1
2.1.2 Software Requirements on the WebCenter Content Environment 2-1
2.2 Prerequisites 2-2
2.2.1 Remote Blob Storage 2-2
2.2.2 SQL User and Active Directory Accounts 2-2
2.2.2.1 Database User on the SQL Server 2-2
2.2.2.2 Active Directory Account with Farm Administrative Privileges 2-2
2.3 Installing the Connector on SharePoint 2-3
2.3.1 Extracting the Contents of the Connector Package for SharePoint 2-3
2.3.2 Deploying and Installing the Connector 2-3
2.3.3 Registering the WebCenter Content RBS Provider 2-6
2.4 Installing the Connector on the WebCenter Content Server 2-7
2.4.1 Installing the SharePointConnector Component 2-8
2.4.2 Enabling the SharePointConnector 2-10
2.4.3 Creating a WebCenter Content User 2-12
2.4.4 Creating the SPConnectorServices Wsdl 2-12
2.4.5 WebCenter Content cluster environment settings 2-13
2.4.5.1 Accessing SharePoint services from WebCenter Content with Connector Component 2-13
2.4.5.2 Accessing WebCenter Content services from SharePoint with Connector Component 2-13
2.4.6 Stubs Deployment 2-14

3 Configuration

3.1 Configuring Farm-level Settings 3-1
3.1.1 Configuring Connection Settings 3-1
3.1.2 Configuring Security Settings at the Farm Level 3-3
3.1.3 Mapping WebCenter Content Fields with SharePoint Metadata at the Farm Level 3-3
3.2 Activating and Configuring the Connector 3-5
3.2.1 Activating the Connector for a SharePoint Content Database 3-6
3.2.2 Configuring Scope Rules and Conditions 3-6
3.2.2.1 Adding a Scope Configuration Rule 3-9
3.2.2.2 Updating a Scope Configuration Rule 3-11
3.2.2.3 Deleting a Scope Configuration Rule 3-13
3.2.3 Configuring Security Settings for Locations (Optional) 3-13
3.2.3.1 Configuring Security Settings for a Site Collection, Site, or Document Library 3-14
3.2.3.2 Deleting Security Settings for a Site Collection, Site, or Document Library 3-15
3.2.4 Mapping WebCenter Content Fields with SharePoint Metadata at the Document Library Level (Optional) 3-16

4 Migration

4.1 Externalization Migration 4-1
4.2 Scope-based Migration 4-3

5 Document Storage and Operations

5.1 Document Storage in WebCenter Content When Creating or Updating Documents in SharePoint 5-1
5.2 Document Retrieval from WebCenter Content When Reading or Downloading Documents in SharePoint 5-2
5.3 Document Deletion from WebCenter Content 5-2
5.4 Document Operations in WebCenter Content 5-2

6 Log Information

6.1 Modifying Log Settings in SharePoint 6-1
6.2 Viewing Logs in SharePoint 6-3
6.3 Modifying Log Settings in WebCenter Content 6-3
6.4 Viewing Event Logs in WebCenter Content 6-4

7 Connector Deactivation and Uninstallation

7.1 Deactivating and Cleaning Up the Connector for a SharePoint Content Database 7-1
7.1.1 Deactivating the Connector on a SharePoint Content Database 7-1
7.1.2 Performing Reverse Migration 7-2
7.1.3 Running the RBS Maintainer Utility 7-3
7.1.4 Cleaning Up the Connector for a SharePoint Content Database 7-3
7.2 Deleting the Connection between SharePoint and WebCenter Content 7-4
7.3 Uninstallation 7-4
7.3.1 Uninstalling the Connector from the SharePoint Environment 7-4

7.3.1.1 Uninstalling and Retracting the Connector 7-4
7.3.1.2 Unregistering the WebCenter Content RBS Provider 7-5
7.3.2 Disabling the Connector from WebCenter Content 7-5

A Troubleshooting

A.1 Introduction to Troubleshooting A-1
A.2 Resolving Common Problems A-2
A.2.1 No Execution Notifications while Installing RBS A-2
A.2.2 RBS Installation Failed A-3
A.2.3 The Error "WCCConnector solution is already added/deployed" Appears when Deploying the WebCenter Content Connector Web Solution Package on SharePoint A-4
A.2.4 The Error "Login failed for user 'username'" Appears while Installing the WebCenter Content Connector on SharePoint A-4
A.2.5 SQL Authentication Issues A-4
A.2.6 On WebCenter Content, the Connection Configuration Page Displays an Error A-5
A.2.7 On WebCenter Content, the Metadata, Security, or Add Scope Rule Page Displays an Error A-5
A.2.8 SQL Authentication Issues A-6
A.3 Frequently Asked Questions A-6
A.4 Using My Oracle Support for Additional Troubleshooting Information A-7

Preface

The WebCenter Content Storage Connector for Microsoft SharePoint 2010 enables organizations to use the structured storage of SharePoint 2010 with the document maintenance capabilities of WebCenter Content. The connector facilitates building a robust document management system.

Note:

- This administration guide introduces the WebCenter Content Storage Connector exclusively for Microsoft SharePoint 2010 components and explains how to install, configure, and administer the Connector on SharePoint and Oracle platforms.
- Where ever ' SharePoint' occurs in this guide, it implies that Microsoft SharePoint 2010 is being used.

Audience

This administration guide is intended for system administrators who need to install and configure the WebCenter Content Storage Connector for Microsoft SharePoint 2010. System administrators can also use this guide to manage the WebCenter Content Storage Connector for Microsoft SharePoint 2010 configuration requirements and activity log files.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11g Release 1 documentation set:

- *Oracle Fusion Middleware Administering Oracle WebCenter Content*
- *Oracle Fusion Middleware Managing Oracle WebCenter Content*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

This chapter provides an overview about the Oracle WebCenter Content Storage Connector for Microsoft SharePoint 2010.

This chapter covers the following topics:

- Section 1.1, "Connector Overview"
- Section 1.2, "Architectural Overview"
- Section 1.3, "Connector Setup"

1.1 Connector Overview

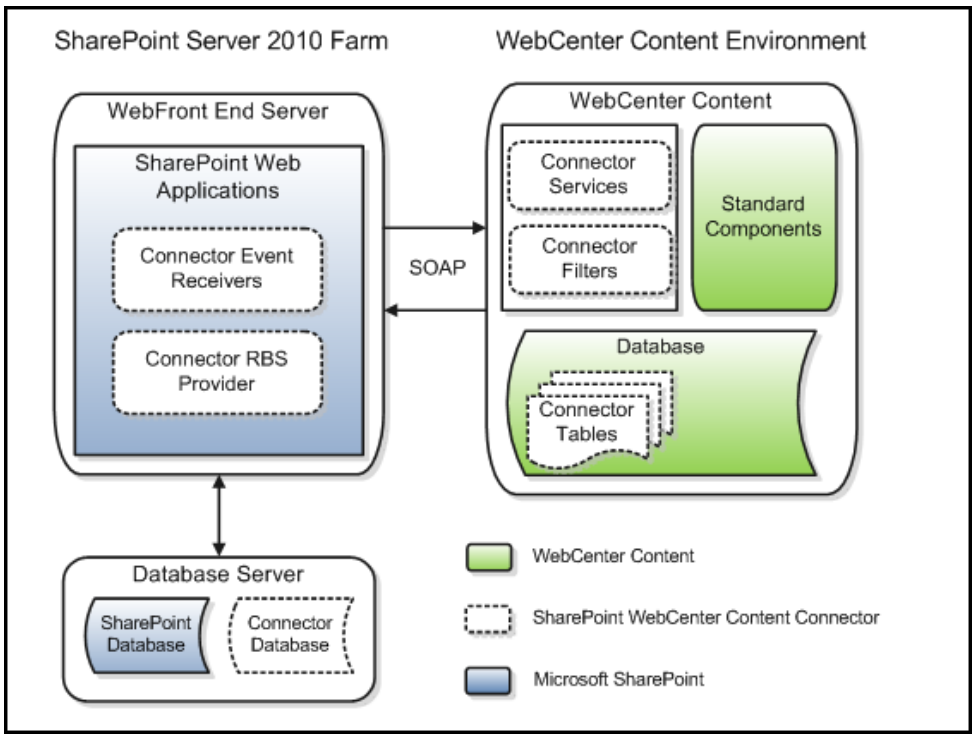
The primary responsibility of the connector is to transfer and store documents, with their metadata, from the SharePoint library to WebCenter Content Server repository. The connector replicates upload, update, check in, check out, discard check out, and delete operations from SharePoint to WebCenter Content Server repository. Using the connector, you can perform the following tasks:

- Configure connection settings.
- Configure security settings.
- Map SharePoint metadata.
- Activate the connector.
- Configure scope rules and conditions.
- Perform data migration.

1.2 Architectural Overview

The following diagram illustrates the connector architecture on both SharePoint and WebCenter Content.

Figure 1–1 Connector Architecture



Connector architecture on SharePoint environment:

- **Connector databases**: The connector consists of two different types of databases: the connector configuration database and the connector custom database. These databases are stored on the same SQL Server instance where the SharePoint databases are stored.

  The connector configuration database stores configuration information, such as connection settings, activation settings, scope rule configuration, and migration job details.

  The connector custom database stores documents and stubs for the document stored on WebCenter Content. Each SharePoint Content Database has a different connector configuration database.

- **Connector RBS Provider:** The connector leverages the Remote Blob Storage (RBS) to externalize documents from SharePoint. All the documents uploaded on SharePoint are initially stored in the connector custom database. The RBS Provider also reads and deletes the documents from the connector custom database or from WebCenter Content, depending on the location of the document.

- **Connector Event Receiver**: The connector leverages the event receiver framework of SharePoint to replicate operations, such as add, update, check out, check in, and discard check out, on WebCenter Content. The event receiver also evaluates the scope rule to decide whether the document must be moved from the connector custom database to WebCenter Content.

Connector architecture on WebCenter Content environment:

- **Connector tables**: The connector stores connection, metadata, and security settings on the database of WebCenter Content.

- **Connector Filter**: The connector leverages the filter framework of WebCenter Content to perform connector-specific operations on documents that are transferred from SharePoint. The connector has two types of filters, action filters and restrict filters. The action filter assigns metadata and security to documents before storing them in WebCenter Content. The restrict filter restricts any user from modifying any action, such as check in, check out, or update metadata on SharePoint content that is stored in WebCenter Content.
- **Connector services**: The connector provides different services on WebCenter Content to perform configurations for the connector. The connector provides services for connection, activation, metadata, security, scope rule, and migration configuration.

1.3 Connector Setup

The following procedure lists the tasks that you must perform to set up and use the connector:

1. Install the connector on SharePoint. For more information, see Section 2.3.
2. Install the connector on the WebCenter Content Server. For more information, see Section 2.4.
3. Configure connection settings. For more information, see Section 3.1.1.
4. Configure security settings at the farm level. For more information, see Section 3.1.2.
5. Map WebCenter Content fields with SharePoint metadata at farm level. For more information, see Section 3.1.3.
6. Activate the connector for a SharePoint content database. For more information, see Section 3.2.1.
7. Configure scope rules and conditions. For more information, see Section 3.2.2.
8. Configure security settings for locations (optional). For more information, see Section 3.2.3.
9. Map WebCenter Content Fields with SharePoint metadata at document library level (optional). For more information, see Section 3.2.4.
10. Perform externalization or scope-based migration (optional). For more information, see Section 4.
11. Set up the cluster environment. To install the SharePoint connector on WebCenter Content cluster environment, see the following sections:
    - Section 2.4.5.1, "Accessing SharePoint services from WebCenter Content with Connector Component"
    - Section 2.4.5.2, "Accessing WebCenter Content services from SharePoint with Connector Component"

2 Installation

This chapter provides information about how you can install the WebCenter Content Storage Connector for Microsoft SharePoint 2010 on the WebCenter Content environment and the SharePoint environment.

This chapter covers the following topics:

- Section 2.1, "Software Requirements"
- Section 2.2, "Prerequisites"
- Section 2.3, "Installing the Connector on SharePoint"
- Section 2.4, "Installing the Connector on the WebCenter Content Server"

2.1 Software Requirements

This section lists the software requirements for the connector on the SharePoint environment and the WebCenter Content environment.

2.1.1 Software Requirements on the SharePoint Environment

This section lists the SharePoint version and database that the connector supports on the SharePoint environment.

- Microsoft SharePoint 2010 Enterprise Edition with Service Pack 1
- SQL Server 2008 R2 Enterprise Edition

2.1.2 Software Requirements on the WebCenter Content Environment

This section lists the WebCenter Content version, JDK version, and browsers that the connector supports on the WebCenter Content environment.

- Oracle WebCenter Content 11.1.1.8.0 and later
- JDK 1.6
- The connector supports the following browsers:
  - Internet Explorer version 8 or later
  - Mozilla Firefox version 17.0.0 or later
  - Chrome version 23.0.1271.95 or later
  - Safari version 3.1.2. or later

2.2 Prerequisites

Before installing the connector, you must ensure that:

- You install and enable Remote Blob Storage (RBS) on at least one SharePoint content database.
- You have the appropriate SQL database user and Active Directory account.
- The WebLogic Server authenticator is configured to use the default Java authenticator (-DUseSunHttpHandler).
- The SharePoint Central Administration web application must be using the Network LAN Manager (NTLM) authentication mode.
- The WebCenter Content Server system user does not have permissions to the SharePoint Server.

Note: The System User through whom the WebCenter Content server is running should not have permission to the SharePoint Server. Otherwise, when the NTLM authentication happens between the two systems, it would be done using the System User credentials instead of the SharePoint service account credentials provided for connection configuration, and this will eventually result in an error.

2.2.1 Remote Blob Storage

Before installing the connector, you must install and enable RBS on each SharePoint content database for which you want to use the connector.

For information about how to install RBS, see:
http://technet.microsoft.com/en-us/library/ff629463(v=office.14).aspx#Section3

For information about how to enable RBS, see:

http://technet.microsoft.com/en-us/library/ff629463(v=office.14).aspx#enableRBS

2.2.2 SQL User and Active Directory Accounts

Before installing the connector, you must ensure that you have the appropriate SQL database user and Active Directory account.

2.2.2.1 Database User on the SQL Server

You must have a database user on the SharePoint instance of the SQL server. You must also ensure that:

- This database user has the dbCreator, sysadmin, and serveradmin permissions.
- This database user does not have password policies enforced.
- On the Server Properties page of the SQL server SharePoint instance, SQL Server and Windows Authentication mode is enabled.

2.2.2.2 Active Directory Account with Farm Administrative Privileges

You must have an Active Directory account that the connector can use while interacting with SharePoint and WebCenter Content. This Active Directory account

must be a part of the SharePoint Farm Administrators group on the SharePoint Central Administration site.

> **Note:** Ensure the separate Active Directory account is used for configuring the connection to SharePoint. Using SharePoint farm account i.e., System account, for the connection to SharePoint may result in an authentication or invalid user error.

2.3 Installing the Connector on SharePoint

This section covers the following topic:

- Section 2.3.1, "Extracting the Contents of the Connector Package for SharePoint"
- Section 2.3.2, "Deploying and Installing the Connector"
- Section 2.3.3, "Registering the WebCenter Content RBS Provider"

2.3.1 Extracting the Contents of the Connector Package for SharePoint

You must extract the contents of the connector package for SharePoint on the SharePoint server. If you have a multi-server SharePoint farm environment, you must extract the contents of the package on each server in the SharePoint farm.

After you extract the contents of the connector package for SharePoint, you must have the following files:

- DeploySolution.ps1
- RetractSolution.ps1
- WCCConnector.wsp
- WCCConnectorInstaller.exe
- WCCRBSProvider.config

2.3.2 Deploying and Installing the Connector

You must deploy and install connector on only one server in the SharePoint farm. It is recommended to deploy and install the connector on the SharePoint server that hosts the Central Administration web application.

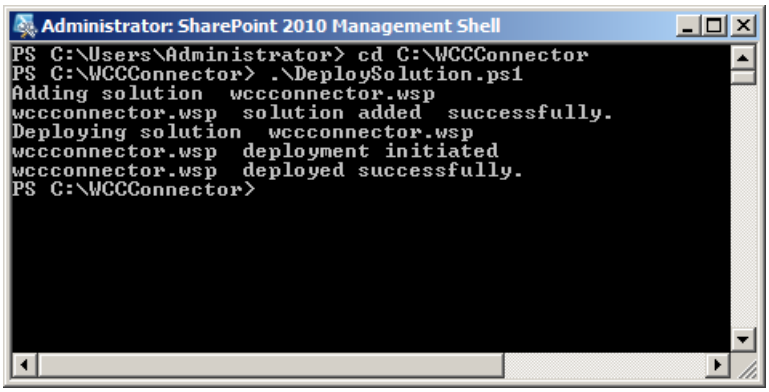
To deploy and install the connector in the SharePoint farm:

> **Note:** Before performing this procedure, you must ensure that the user who is logged in to the SharePoint Server has farm administrative and system administrative rights.

1. On the SharePoint server where you want to deploy and install the connector, open SharePoint 2010 Management Shell as an administrator.
2. Change the directory to the location where you extracted the WCCConnector.zip package. For more information, see Section 2.3.1.
3. To deploy the WCCConnector Web Solution Package (WSP) on the SharePoint farm, use the following command:

```
.\DeploySolution.ps1
```

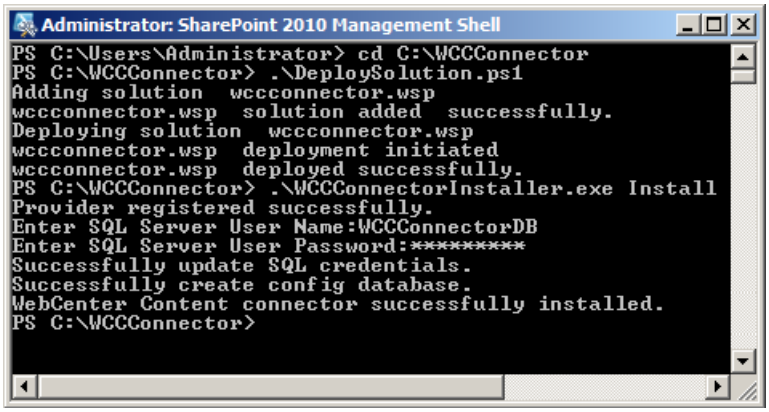
Figure 2–1 Deploy Solution Command and Output



4. To install the connector in the SharePoint farm, use the following command:

.\WCCConnectorInstaller.exe Install

Figure 2–2 Install Command and Output

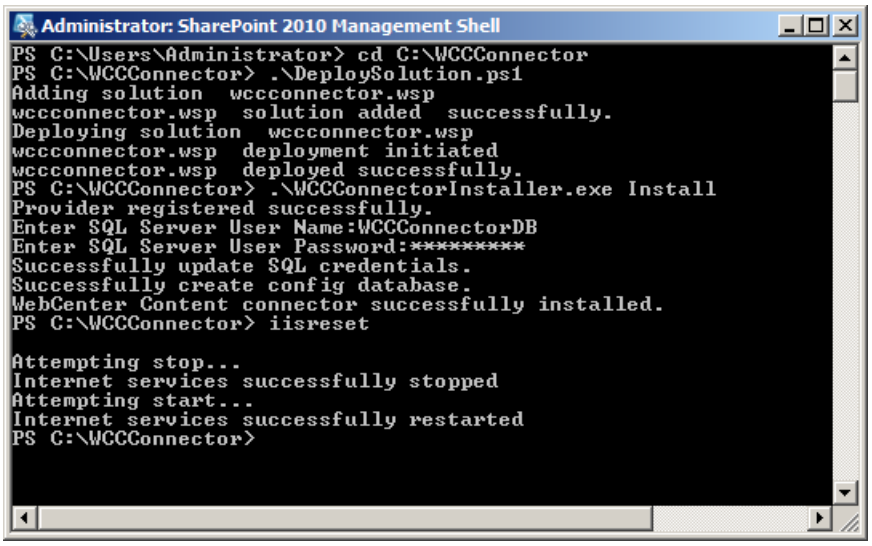


5. When the system prompts you for credentials, enter the credentials of the database user on the SharePoint instance of the SQL server. For more information, see Section 2.2.2.1.

6. Restart the IIS server using the following command:

```
iisreset
```

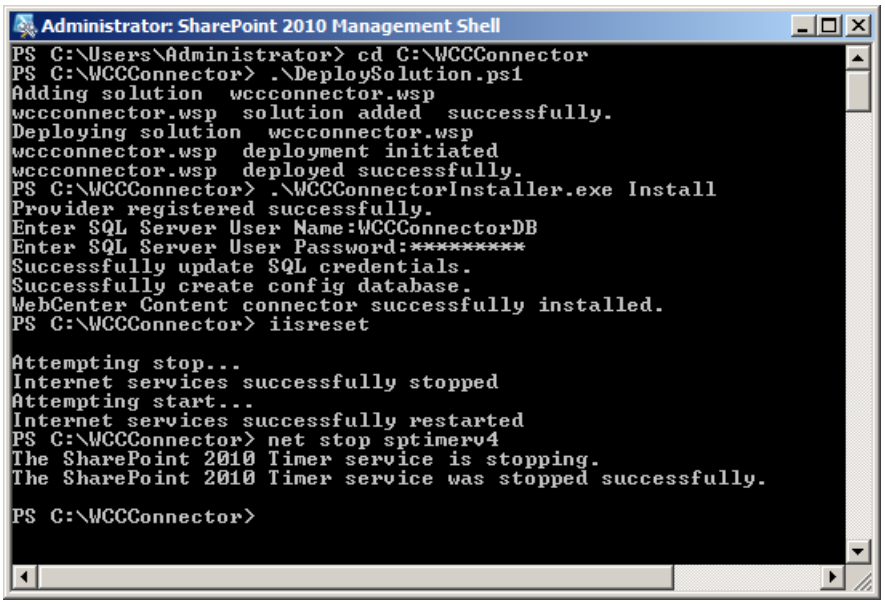
Figure 2–3 IIS Reset Command and Output



7. To restart the SharePoint Timer Services, use the following commands:

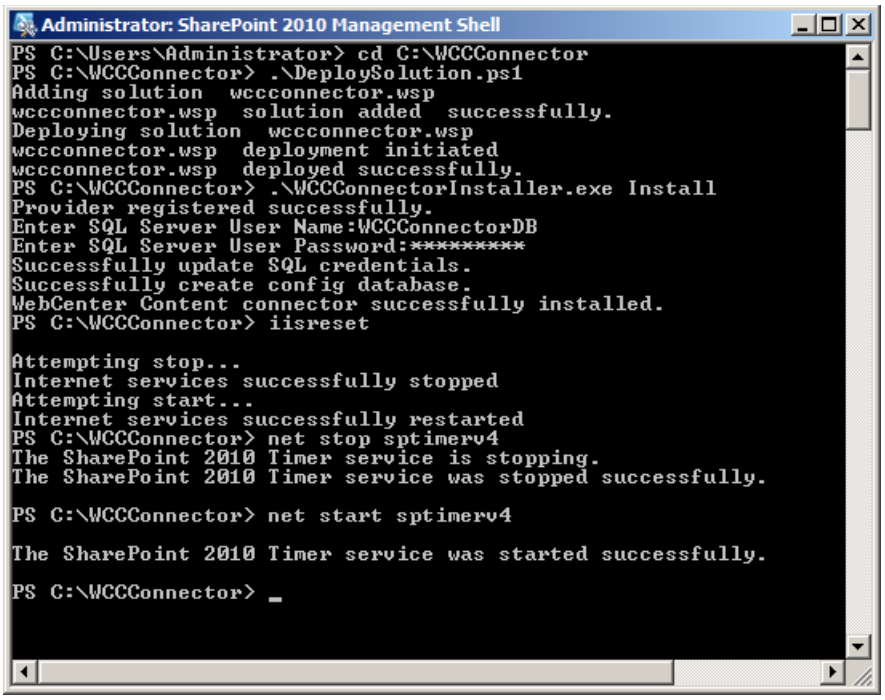
```
net stop sptimerv4
```

Figure 2–4 Stop SharePoint Timer Services Command and Output




```
net start sptimerv4
```

Figure 2–5 Start SharePoint Timer Services Command and Output



2.3.3 Registering the WebCenter Content RBS Provider

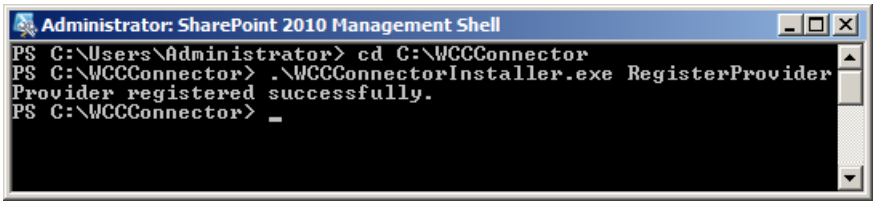
Apart from the server where you deployed and installed the connector, you must register the WebCenter Content RBS provider for each server in the SharePoint farm. If you have a single-server SharePoint farm environment, you do not need to perform this step.

To register the WebCenter Content RBS provider in the SharePoint farm:

1. On the SharePoint server where you want register the WebCenter Content RBS provider, open SharePoint 2010 Management Shell as an administrator.
2. Change the directory to the location where you extracted the WCCConnector.zip package. For more information, see Section 2.3.1.
3. To register the WebCenter Content RBS provider, use the following command:

   ```
   .\WCCConnectorInstaller.exe RegisterProvider
   ```

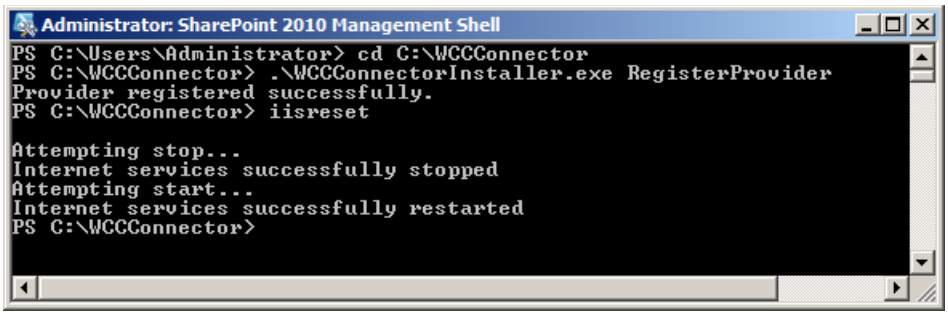
Figure 2–6 Register Provider Command and Output



4. To restart the IIS server, use the following command:

   ```
   iisreset
   ```

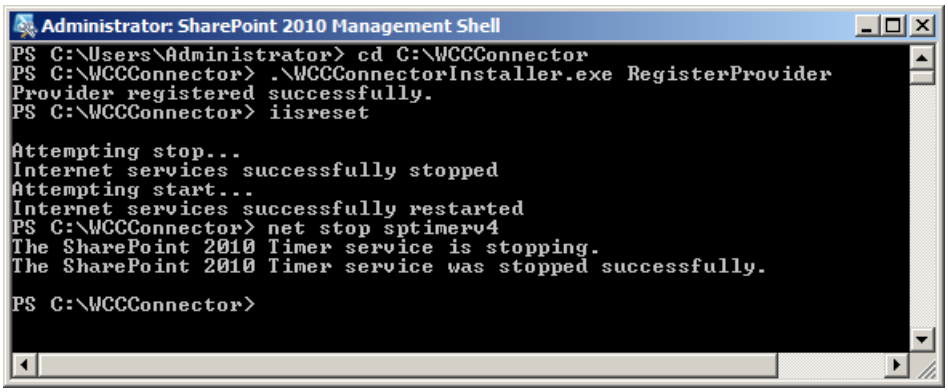
Figure 2–7 IIS Reset Command and Output



5. To restart the SharePoint Timer Services, use the following commands:

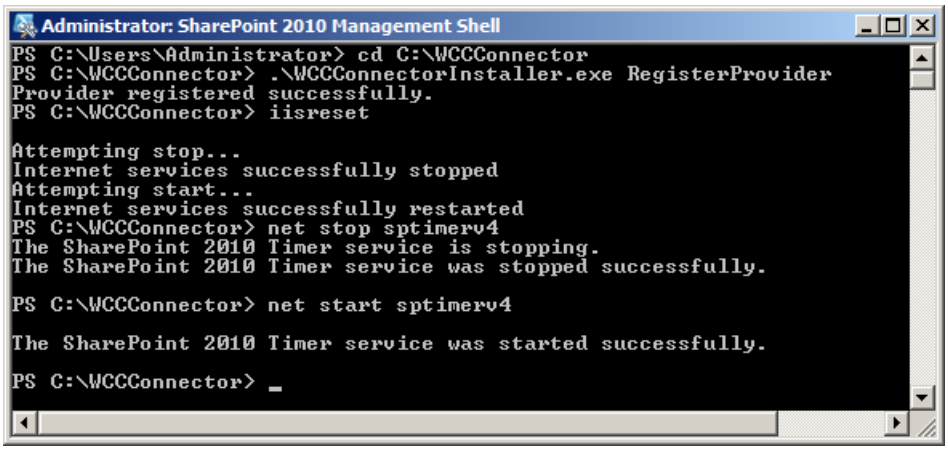
```
net stop sptimerv4
```

Figure 2–8 Stop SharePoint Timer Services Command and Output




```
net start sptimerv4
```

Figure 2–9 Start SharePoint Timer Services Command and Output



2.4 Installing the Connector on the WebCenter Content Server

This section covers the following topics:

- Section 2.4.1, "Installing the SharePointConnector Component"
- Section 2.4.2, "Enabling the SharePointConnector"
- Section 2.4.3, "Creating a WebCenter Content User"
- Section 2.4.4, "Creating the SPConnectorServices Wsdl"
- Section 2.4.5, "WebCenter Content cluster environment settings"
- Section 2.4.6, "Stubs Deployment"

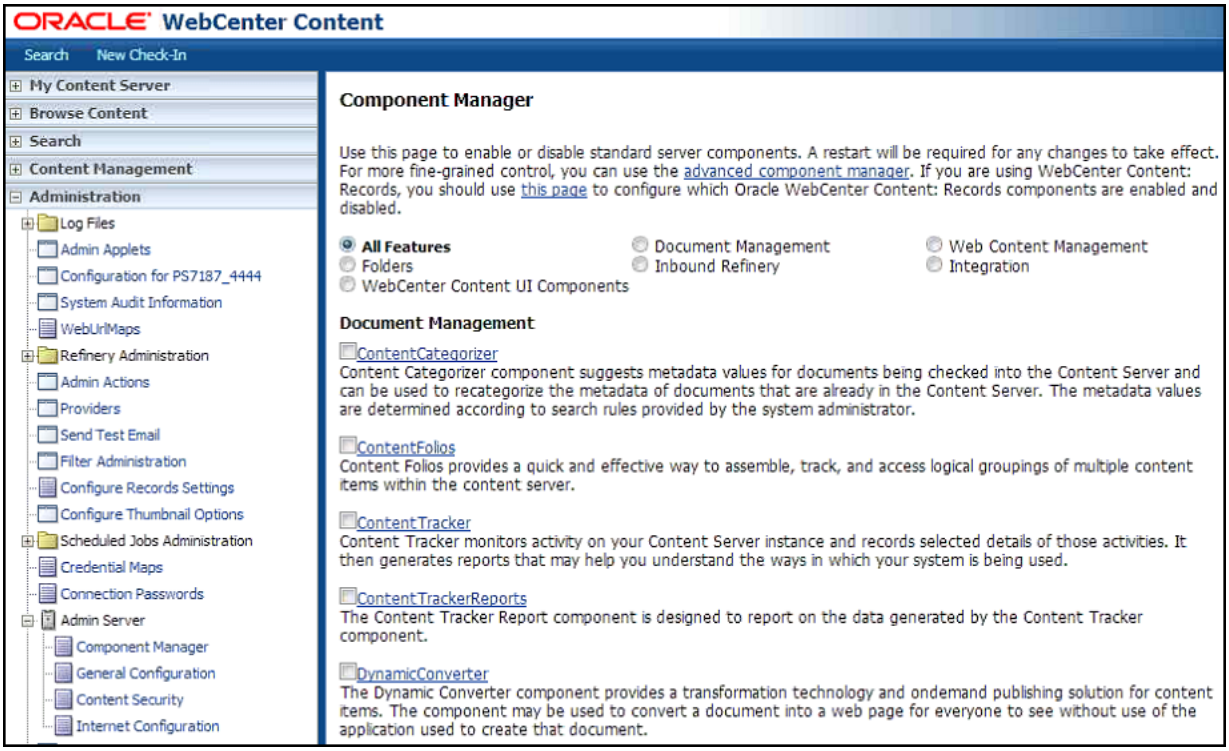
2.4.1 Installing the SharePointConnector Component

Note: If you already installed the SharePointConnector you can skip this procedure and proceed to enable these components. For more information, see Section 2.4.2.

To install the SharePointConnector component:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager.** The Component Manager page opens with a list of component categories and a list of component names.

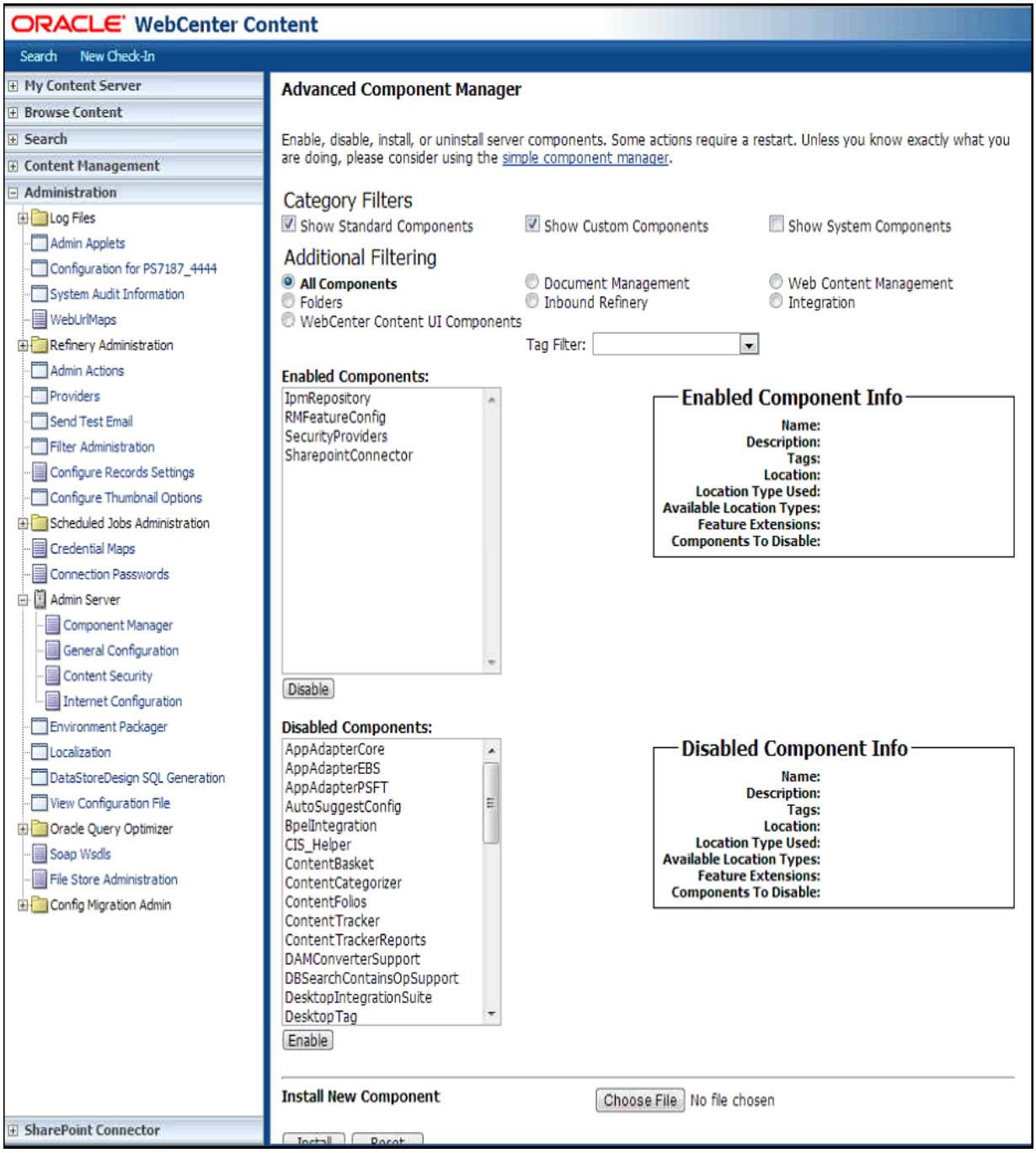
Figure 2–10 Component Manager Page



3. Click the **Advanced Component Manager** link. The Advanced Component Manager page appears.

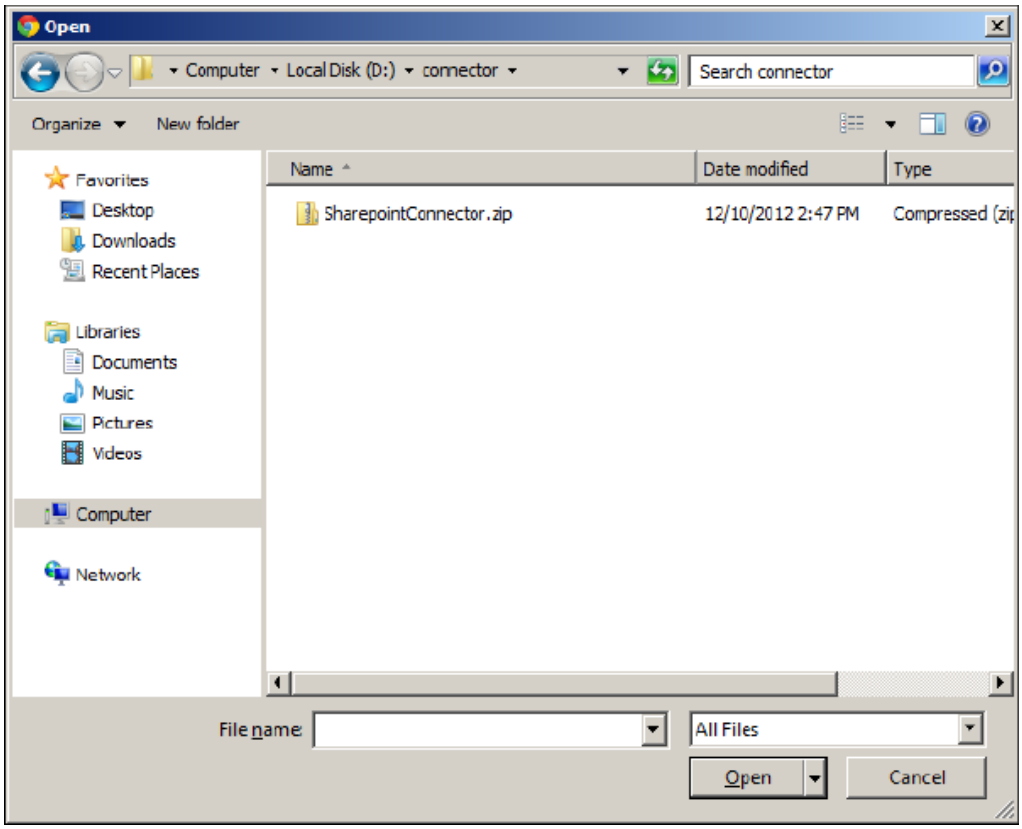
Note: For more information on using the Component Manager, refer to the chapter "Managing Components" in the *Oracle Fusion Middleware Administering Oracle WebCenter Content* guide.

Figure 2–11 Advanced Component Manager Page



4. In the Install New Component region, click **Choose File**. The Choose File to Upload dialog box appears.

Figure 2–12 Choose File to Upload Dialog Box



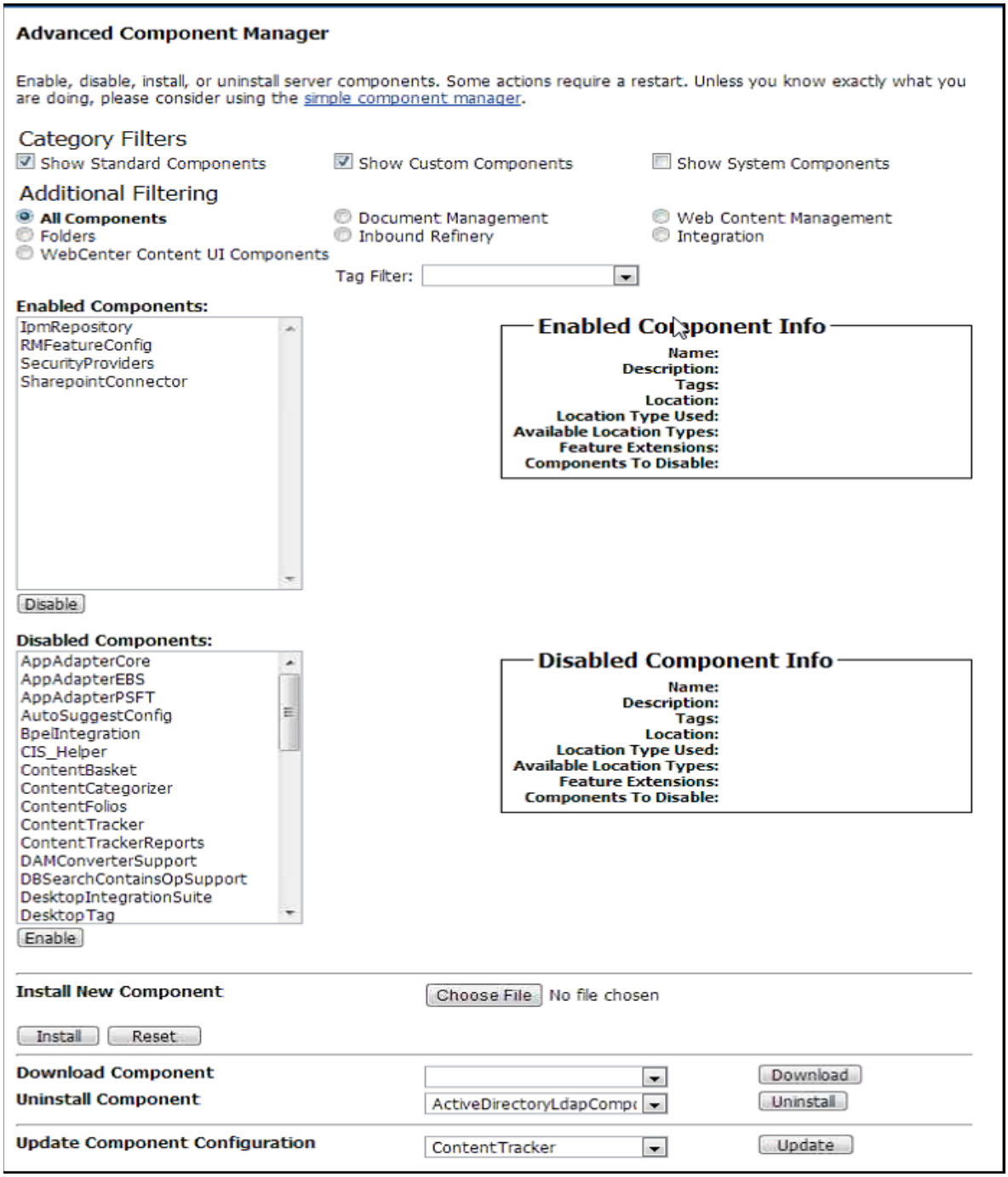
5. Select the SharePointConnector.zip file, and then click **Open**.
6. In the Advanced Component Manager page, click **Install**.
7. In the next page, which displays the items that will be installed, click **Continue**. The Content Server Message page appears, which displays a message that WebCenter Content successfully uploaded and installed the component.

2.4.2 Enabling the SharePointConnector

To enable the SharePointConnector components:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager.** The Component Manager page opens.
3. Click the **Advanced Component Manager** link. The Advanced Component Manager page appears.

Figure 2–13 Advanced Component Manager Page



4. In the Disabled Components list, select SharepointConnector, and then click **Enable**. If the SharepointConnector component does not appear in the Disabled Components list, you must install the SharePointConnector component. For more information, see Section 2.4.1.

   You must restart the Content Server instance for any configuration changes to take effect.

   For more information, see "Using Fusion Middleware Control to Restart Content Server" in *Oracle Fusion Middleware Administering Oracle WebCenter Content* guide.

2.4.3 Creating a WebCenter Content User

You must create a WebCenter Content user that the connector can use while interacting with SharePoint. This user must have administrative privileges, having permissions to all WebCenter Content security groups and accounts to which SharePoint content will be mapped. This user must also have permissions over core WebCenter Content Server services that SharePoint uses to connect to WebCenter Content.

2.4.4 Creating the SPConnectorServices Wsdl

To create the SPConnectorServices Wsdl:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, choose **Administration**, then click **Soap Wsdls**. The Wsdl Information page appears.
3. Create a Wsdl named SPConnectorServices.
4. Add the following services for the SPConnectorServices Wsdl, and then update the response and request parameters for each service.
5. Generate Wsdls.

Table 2–1 Services for the SPConnectorServices Wsdl

Service Name	IdcService	Response Parameter Name	Response Parameter Type	Request Parameter Name	Request Parameter Type
CheckInArchive	CHECKIN_ARCHIVE	diD	Int	dID	Int
				dDocName	String
				dDocTitle	String
				IsNative	Boolean
				dDocAuthor	String
				dSecurityGroup	String
				Action	String
				primaryFile	File
CheckInNewDocument	CHECKIN_NEW	dID	String	dDocType	String
				dDocTitle	String
				dDocAuthor	String
				dSecurityGroup	String
				primaryFile	File
				dDocName	String
CheckInSelectedDocument	CHECKIN_SEL	diD	String	dID	Int
				dDocName	String
				dDocTitle	String
				dDocType	String
				dDocAuthor	String
				dSecurityGroup	String
				dDocAccount	String
				dRevLabel	String
				primaryFile	File
CheckOutDocument	CHECKOUT	None	None	dID	Int
DeleteDocument	DELETE_DOC	None	None	dID	String
				dDocName	String

Table 2–1 (Cont.) Services for the SPConnectorServices Wsdl

Service Name	IdcService	Response Parameter Name	Response Parameter Type	Request Parameter Name	Request Parameter Type
DeleteDocumentByRev	DELETE_REV	None	None	dID	Int
DiscardCheckOut	UNDO_CHECKOUT	None	None	dID	Int
GetDocFileByID	GET_FILE	downloadFile	File	diD	Int
PingServer	PING_SERVER	dUser	String	None	None
		StatusMessage	String		
UpdateDocumentInfo	UPDATE_DOCINFO	diD	String	dDocName	String
				dID	String
				dSecurityGroup	String
				dDocAuthor	String

2.4.5 WebCenter Content cluster environment settings

To install the SharePoint connector on WebCenter Content cluster environment, the settings mentioned in Section 2.4.5.1 and Section 2.4.5.2 need to be done.

2.4.5.1 Accessing SharePoint services from WebCenter Content with Connector Component

To access the SharePoint services, you will need to set the managed server starting parameters through the weblogic server admin console. To do this, follow the steps below:

1. Login to the WLS admin console.
2. Click **Lock & Edit** to enable the edit mode.
3. Click **Environment** then select Servers.
4. Click a managed server name (UCM Sever 1).
5. Click the **Configuration tab**, and in second row of tabs, select the Server Start tab.
6. In the Arguments box, type the starting parameter:

   ```
   DUseSunHttpHandler=true
   ```

7. Click **Save** to save the configuration changes.
8. In case of cluster set up repeat step 4 to 8 for each node in the cluster.
9. Click **Activate Changes.**
10. Stop and start both UCM manage server using the Admin console.

2.4.5.2 Accessing WebCenter Content services from SharePoint with Connector Component

Accessing WebCenter Content services require configuring the web root in OHS. To do this, follow the steps below:

1. Open the mod_wl_ohs.conf file from the following location:

   ```
   OHS_HOME/instances/ohs_instance1/config/OHS/ohs1/mod_wl_ohs.conf
   ```

2. Add a location for the context URL /_dav by adding the following line to file mod_wl_ohs.conf:

```
#DAV
<Location /_dav>
WebLogicCluster ecmhost1:16200, ecmhost2:16200
SetHandler weblogic-handler
WLCookieName JSESSIONID
</Location>
```

3. Restart OHS services.

2.4.6 Stubs Deployment

If the SharePoint connector feature is installed in an Oracle WebCenter Content product, stubs.jar library needs to be added manually from the Oracle WebLogic administration console after a domain is created. A reference to the library must be added to the weblogic-application.xml file of the Oracle WebCenter Content EAR file before the managed server is started for the first time.

To add stubs.jar to the WebLogic WebCenter Content domain, follow these steps:

1. After a domain is created, start the Admin Server. If a managed WebCenter Content server has already been started, then the administrator will have to perform additional steps to add reference to the deployed WebCenter Content server instance later.
2. Open the WebLogic console in a browser. Click **Deployments** in the left pane. Browse the pages to check if there is already a stubs.jar file in the WebLogic administration console. If it is already present, then no more steps need to be performed.
3. If no stubs.jar file is present, click **Install** on the Deployments display. A file selection dialog opens. Browse the available file system and select stubs.jar in the following path:

   FMW_HOME/Oracle_ECM1/ucm/idc/components/SharePointConnector/lib/stubs.jar
4. Click **Next**. The option page to select the file as library opens. Select "Install this deployment as a library" and click **Next**.
5. The Target Selection Screen opens. Select all targets and click **Next**.
6. The Deployment Name screen opens. In the Security section, select "DD Only: Use only roles and policies that are defined in the deployment descriptors." In the Source accessibility section, select "Copy this application onto every target for me" and click **Next**.
7. In the Additional Configuration section, select "Yes, Take me to the deployment's configuration screen" and click **Finish**. The library is now deployed in the environment.

If the managed server has been started at least once after the domain has been created, complete the following:

1. Locate the `weblogic-application.xml` of the Oracle WebCenter Content enterprise application in the deployed WebCenter Content domain at a path similar to the following example:

   FMW_HOME/domain_path/servers/managed_server_name/tmp/_WL_user/Oracle Universal Content Management - Content Server/k6ggd/META-INF/weblogic-application.xml

2. Modify the META-INF/weblogic-application.xml and add the following line for library reference:

```
<library-ref>

  <library-name>stubs</library-name>

</library-ref>
```

3. If the `UCM_server1` Managed Server is not available in */FMW_HOME/domain path/servers/*, then this step is not needed, as the managed server has not been started, which would have deployed the `UCM_server1` at this location.

3 Configuration

This chapter provides information about different settings that you must configure to use the WebCenter Content Storage Connector for Microsoft SharePoint 2010.

This chapter covers the following topics:

- Section 3.1, "Configuring Farm-level Settings"
- Section 3.2, "Activating and Configuring the Connector"

3.1 Configuring Farm-level Settings

This section provides information on how you can configure connection settings, configure security settings at the farm level, and map WebCenter Content fields with SharePoint metadata at the farm level.

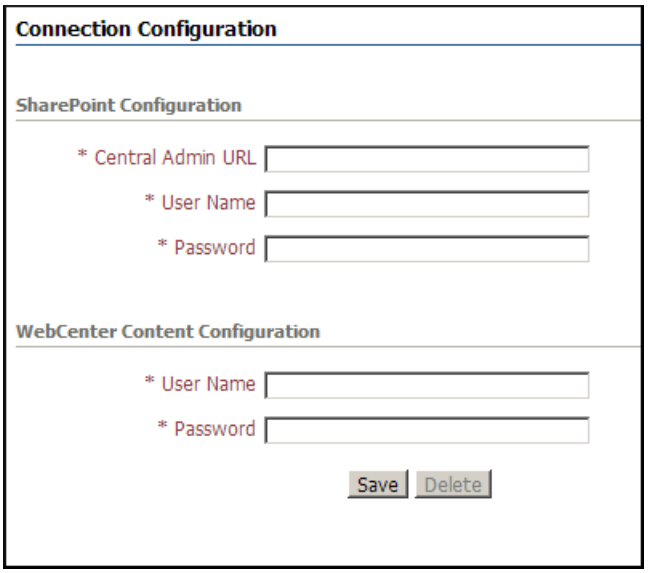
3.1.1 Configuring Connection Settings

To establish the connectivity between WebCenter Content and a SharePoint farm, you must configure the connection settings.

To configure the connection settings:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Connection Configuration**. The Connection Configuration page appears.

Figure 3–1 Connection Configuration Page



3. Enter the applicable information in each field.

   The following table lists each field in the SharePoint Configuration region and the action associated with each field.

Field	Description
SharePoint Central Admin URL	Enter the URL of the Microsoft SharePoint farm that you want to connect to WebCenter Content.
User Name	Enter the user name that you use to access Microsoft SharePoint 2010. This user must be a part of the SharePoint Farm Administrators group on the SharePoint Central Administration site. For more information, see Section 2.2.2.2.
Password	Enter the password for the user name that you use to access Microsoft SharePoint 2010.

   The following table lists each field in the WebCenter Content Configuration region and the action associated with each field.

Field	Description
User Name	Enter the administrator user name for WebCenter Content. This user must have administrative privileges, having permissions to all WebCenter Content security groups, accounts, and services. For more information, see Section 2.4.3.
Password	Enter the password for this user name.

4. Click **Save**. The connection between WebCenter Content and the SharePoint farm is established. If the connection is not established, an error message appears.

> **Note:** Before you change user name, password, or both for SharePoint or WebCenter Content, you must restart the UCM server.

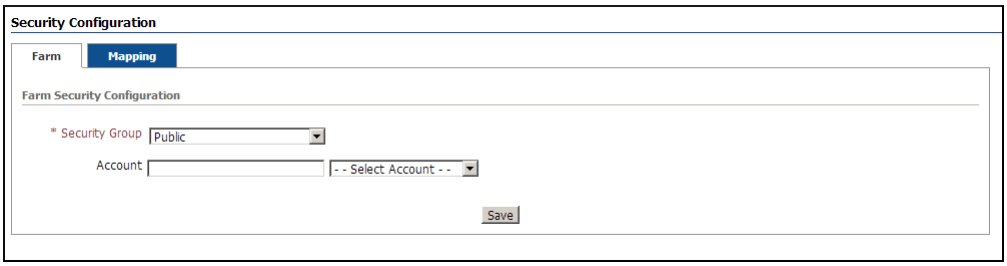
3.1.2 Configuring Security Settings at the Farm Level

To enable the storage of files in WebCenter Content, you must configure security settings at the farm level. By default, all the elements under the hierarchy of a farm inherit the global security settings.

To configure the global security settings:

1. In the Content Server portal, open the SharePoint Connector tray, and then click **Security Configuration**. The Security Configuration page appears.

Figure 3–2 Farm Tab on the Security Configuration Page



2. Click the **Farm tab**.
3. From the Security Group drop-down list, select the security group that you want to configure for the farm. The Security Group drop-down list displays all security groups that are available in WebCenter Content.

> **Note:** The administrator must configure only those security groups to which the service account user has permissions.

4. (Optional) From the Select Account drop-down list, select the security account that you want to configure for the farm.

   The security account that you select appears in the Account field. You can edit the account name in the Account field, if required.
5. Click **Save**. The security settings are applied at the farm level.

3.1.3 Mapping WebCenter Content Fields with SharePoint Metadata at the Farm Level

Metadata mapping allows you to map WebCenter Content fields with SharePoint metadata. After you map the metadata, when a SharePoint document is checked in or when the metadata is updated for a SharePoint document that is stored in WebCenter Content, the metadata is updated for the corresponding WebCenter Content fields.

After a file is stored on WebCenter Content, you can view the metadata for that file on the Content Information page. If the metadata mapping fails, SharePoint files do not get transferred to WebCenter Content.

You can map SharePoint metadata only at the farm level and document library level. Document library level metadata mapping takes precedence over the farm level metadata mapping. If you add a new document library to SharePoint, the document library inherits the default metadata mapping at the farm level.

You must map metadata for all required WebCenter Content fields. If you do not map metadata for any required WebCenter Content field, the connector does not transfer the SharePoint document to WebCenter Content.

You can map SharePoint metadata with WebCenter Content standard fields or custom fields. The following table displays the compatibility of the WebCenter Content supported field types with SharePoint supported metadata.

WebCenter Content Field Data Type	SharePoint Metadata Type
LongText (200 characters)	Any type
Memo (2000 characters)	Any type
Date	DateTime
Text (30 characters)	Any type
Integer	Integer, Counter
Decimal	Number

Note: If the SharePoint metadata content is larger than the WebCenter Content Data Type limitation, the SharePoint metadata is trimmed.

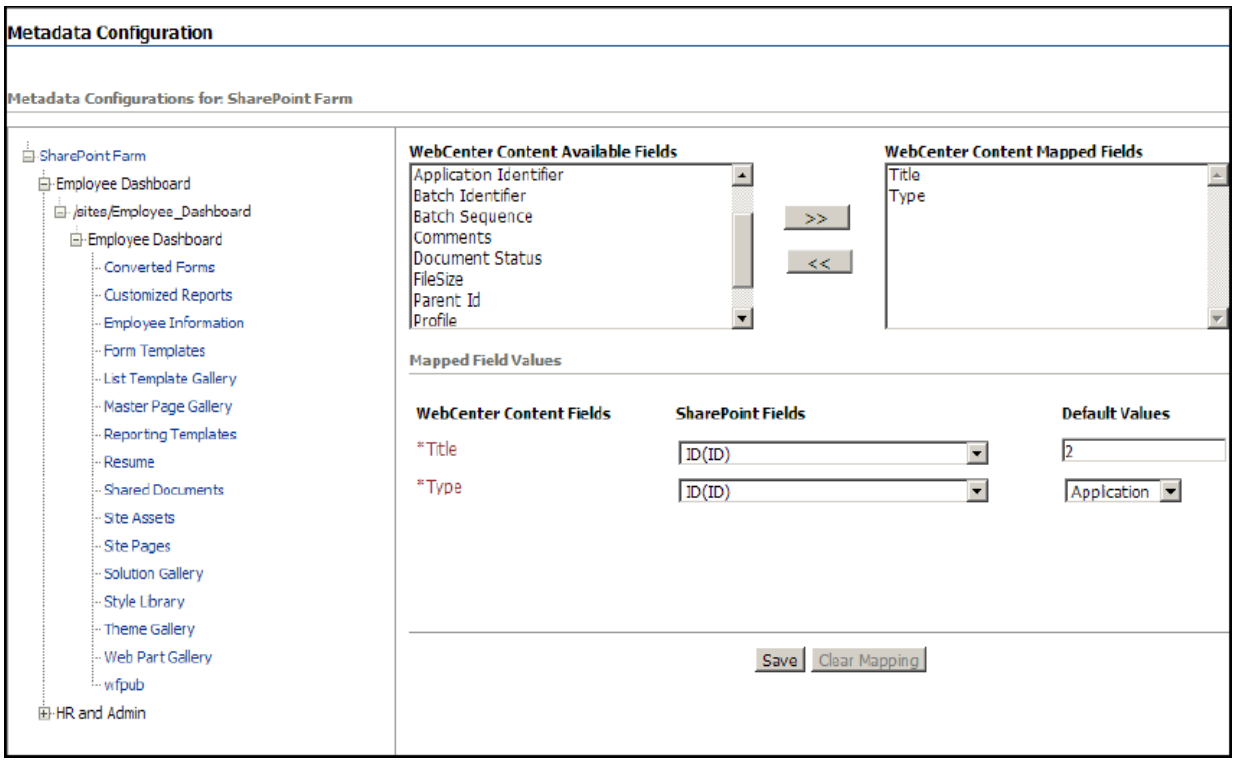
To map SharePoint metadata with WebCenter Content fields at farm level:

Note: If you add a new custom field in WebCenter Content and configure it as a required field, you must update the WebCenter Content database before mapping SharePoint metadata with WebCenter Content fields.

For more information, refer to "Customizing Repository Fields and Metadata" chapter in the *Oracle Fusion Middleware Managing Oracle WebCenter Content* guide.

1. In the Content Server portal, choose the SharePoint Connector tray, then **Metadata Configuration**, then **SharePoint farm**. The metadata mapping for the farm appears in the right pane.

Figure 3–3 Metadata Configuration Page



2. By default, the **WebCenter Content Mapped Fields** group and Mapped Field Values region display the fields for which you must map SharePoint metadata. The fields for which you must map metadata are highlighted in red and are marked with an asterisk (*).

   Note: Title and Type are mandatory fields.

   (Optional) You can add additional fields with which you want to map SharePoint metadata. From the **WebCenter Content Available Fields** group, select the fields that you want to add, and then click the right arrow. The fields that you select appear in the **Mapped Field Values** region.

3. From the **SharePoint Fields** list, select the SharePoint metadata that you want to map with the WebCenter Content field.

4. In the **Default Value** field, enter a default value for the WebCenter Content mandatory field. When the SharePoint field does not contain any metadata, this default value is set as the value in the WebCenter Content field. If you do not enter a default value for a WebCenter Content mandatory field, an error message appears.

5. Click **Ok**. The SharePoint metadata is mapped with the WebCenter Content fields. The message Metadata mapping is successful for the selected SharePoint entity! appears.

3.2 Activating and Configuring the Connector

This section provides information on how you can activate the connector for a SharePoint content database, configure scope rules and conditions, configure security

settings for locations, and map WebCenter Content fields with SharePoint metadata at the document library level.

3.2.1 Activating the Connector for a SharePoint Content Database

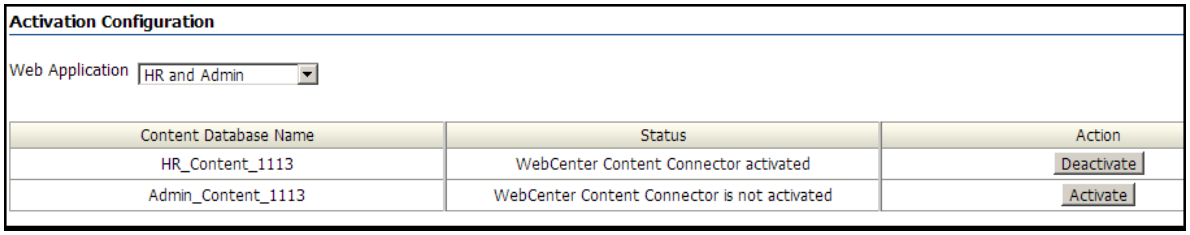
Before you activate a SharePoint content database, you must configure metadata and security mapping at farm level. For more information, see Section 3.1.3.

After you activate the connector for a SharePoint content database, the connector externalizes the documents created or updated in the site collections that belong to this SharePoint content database. When the connector externalizes a document from SharePoint, the connector verifies whether the document complies with the scope configuration rules. If the document complies with the scope configuration rules, it is stored in WebCenter Content. If the document does not comply with the scope configuration rules or if network connectivity issues occur, it is stored in the connector custom database. For more information, see Section 3.2.2.

To activate the connector for a SharePoint content database:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Activation Configuration.** The Activation Configuration page appears.

Figure 3–4 Activation Configuration Page



3. From the Web Application drop-down list, select the SharePoint application that you want to associate with WebCenter Content. The list of content databases that are associated with the application that you selected appears.
4. In the Action column, click **Activate**. The connector is activated on the applicable SharePoint content database. If the Activate button appears grayed, you must install and enable RBS for the content database. For more information, see Section 2.2.1.

> **Note:** After activating the connector on a SharePoint content database, you must not delete the user, which you configured during the connection configuration, from the user policy of the Web Application.

3.2.2 Configuring Scope Rules and Conditions

Documents are transferred to WebCenter Content only if they comply with the scope configuration rules and conditions. When the connector transfers a document from SharePoint, the connector verifies whether the document complies with the scope configuration rules and conditions. If the document complies with the scope configuration rules and conditions, the document is stored in WebCenter Content. If the document does not comply with the scope configuration rules and conditions or if network connectivity issues occur, the document is stored in the connector custom

database. You can configure one scope configuration rule for each site collection, site, or document library. The child elements of a farm inherit the scope configuration rules of the parent elements.

You can configure scope configuration rules based on the following parameters:

- Location where you want to apply this rule. You can configure the rule for site collections, sites, or document libraries.
- File size
- File type

Consider the following SharePoint site collection hierarchy:

- Site collection 1
  - Site A
    - Document Library 1
    - Document Library 2

Consider the following scope configuration rules:

- Scope Rule 1
  - Location: Site Collection 1
  - Condition 1:
    - Type = PDF
    - Size >=0
  - Condition 2:
    - Type = DOC
    - Size >=0
- Scope Rule 2
  - Location: Document Library 1
  - Condition 1:
    - Type = DOC
    - Size >=1 MB
  - Condition 2:
    - Type = XLS
    - Size >=1 MB
- There are no scope configuration rules for Site A and Document Library 2.

Given this SharePoint Site Collection hierarchy and scope configuration rules, consider the following scenarios and their results.

Scenario	Result
You upload a PDF file to Document Library 2.	The connector transfers this document to WebCenter Content. This scenario complies with Rule 1, Condition 1 (file type=PDF, file size>=0), which was configured for Site Collection 1. Although there was no rule set for Document Library 2, it inherits scope rules from Site Collection 1.
You upload a DOC file to Document Library 2.	The connector transfers this document to WebCenter Content. This scenario complies with Rule 1, Condition 2 (file type=DOC, file size>=0), which was configured for Site Collection 1. Although there was no rule set for Document Library 2, it inherits scope rules from Site Collection 1.
You upload an XLS file to Document Library 2.	The connector does not transfer this document to WebCenter Content. There is no scope rule configured for XLS files on Document Library 2 or any of its parent elements.
You upload a PDF file to Document Library 1.	The connector transfers this document to WebCenter Content. This scenario complies with scope rule 1, Condition 1 (file type=PDF, file size>=0), which was configured for Site Collection 1. Although there was no scope rule configured for a PDF file type on Document Library 1, it inherits scope rules from Site Collection 1.
You upload a 2 MB DOC file to Document Library 1.	The connector transfers this document to WebCenter Content. This scenario complies with Rule 2, Condition 1 (file type=DOC, file size>=1 MB), which was configured for Document Library 1.
You upload a 1 MB XLS file to Document Library 1.	The connector transfers this document to WebCenter Content. This scenario complies with Rule 2, Condition 2 (file type=XLS, file size>=1 MB), which was configured for Document Library 1.
You upload a .5 MB DOC file to Document Library 1.	The connector transfers this document to WebCenter Content. Although this scenario does not comply with scope rule 2, condition 1 (file type DOC, file size >=1 MB) that was configured for Document Library 1, it complies with scope rule 1, Condition 1 (file type DOC, file size >=0), which was configured for Site Collection 1. Document Library 1 inherits scope rules from Site Collection 1.

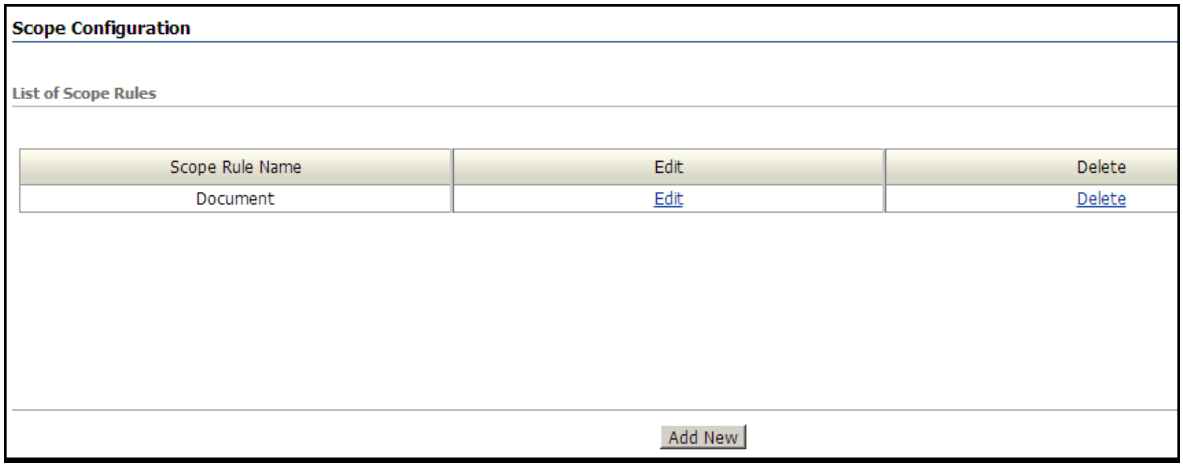
Scenario	Result
You upload a .5 MB XLS file to Document Library 1.	The connector does not transfer this document to WebCenter Content. This scenario does not comply with any scope rules configured for Document Library 1. The file size of the XLS file that you uploaded is less than 1 MB whereas scope configuration rule 2 has a condition where the file size is set to greater than or equal to 1 MB. There are no other scope rules configured for XLS files on the parent elements of Document Library 1.

3.2.2.1 Adding a Scope Configuration Rule

To add a scope configuration rule:

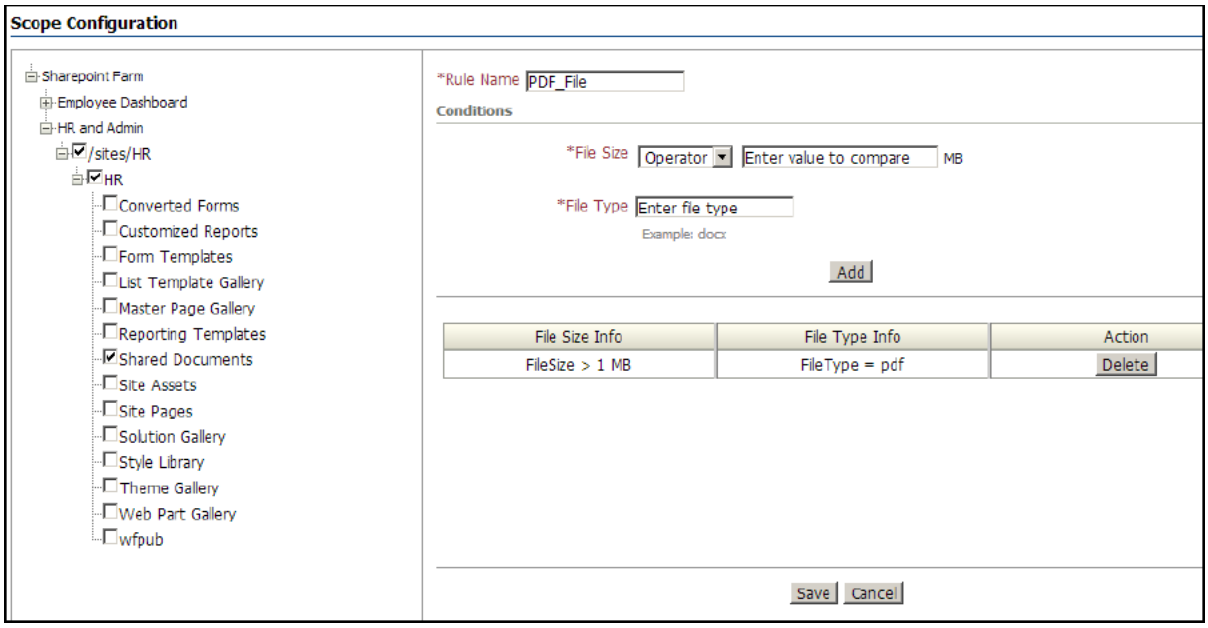
1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Scope Configuration**. The Scope Configuration page appears.

Figure 3–5 Scope Configuration Home Page



3. In the List of Scope Rules region, click **Add New**. The Scope Configuration page, where you can add a new scope configuration rule, appears.

Figure 3–6 Scope Configuration Page



4. In the left pane of the Scope Configuration page, select the site collection, site, or document library for which you want to configure the scope configuration rule.
5. In the Rule Name field, enter a name for the scope configuration rule.

   Note: This is a mandatory field.

6. Add a condition to a rule.
   a. In the Conditions region, select an operator from the **File Size** drop-down list.
   b. In the File Size field, select an operator and enter a file size value.

      Note: This is a mandatory field. You must enter an integer value. The value that you enter must comply with the SharePoint limitations on document upload size.

   c. In the File Type field, enter the type of file that the connector must transfer from SharePoint to WebCenter Content. If you want to transfer all types of files from SharePoint to WebCenter Content, type all.

      Note: This is a mandatory field.

      You must not add a dot before the file type. For example, you must use pdf instead of .pdf.

      The file type is not case-sensitive. For example, you can use pdf or PDF to transfer PDF file types.

      You can enter only one file type at a time. You must add a separate condition for each file type that you want to transfer to WebCenter Content in this rule. If you want to transfer all types of files from SharePoint to WebCenter Content, type all.

d. Click **Add**. The condition is added to this rule. To add another condition to this rule, repeat steps a to d.

7. Click **Save**. The scope configuration rule is added for the site collection, site, or document library that you selected.

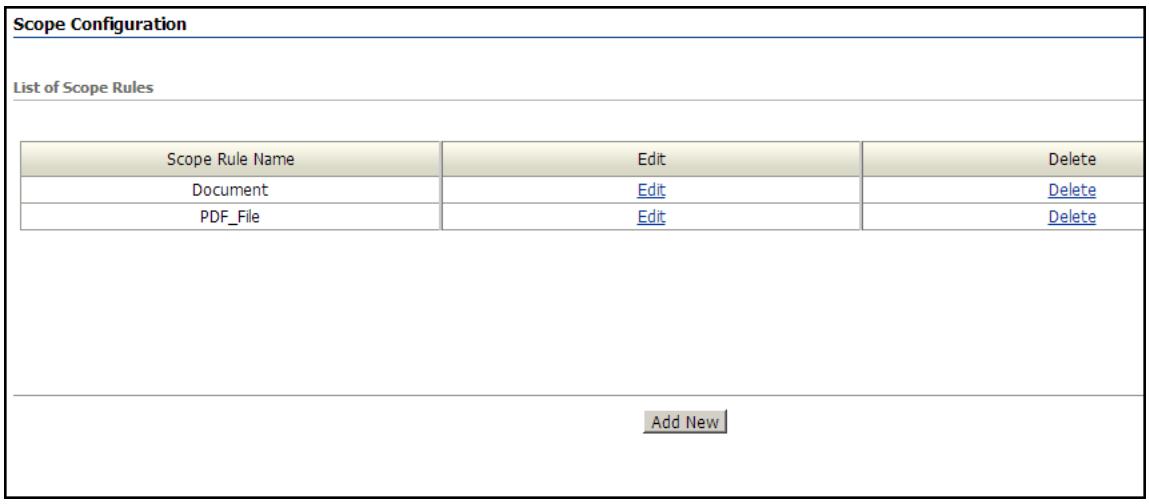
3.2.2.2 Updating a Scope Configuration Rule

The List of Scope Rules table on the Scope Configuration home page displays the rules that you configured for site collections, sites, or document libraries. You can update a scope configuration rule by adding new conditions or deleting existing conditions.

To update a scope configuration rule:

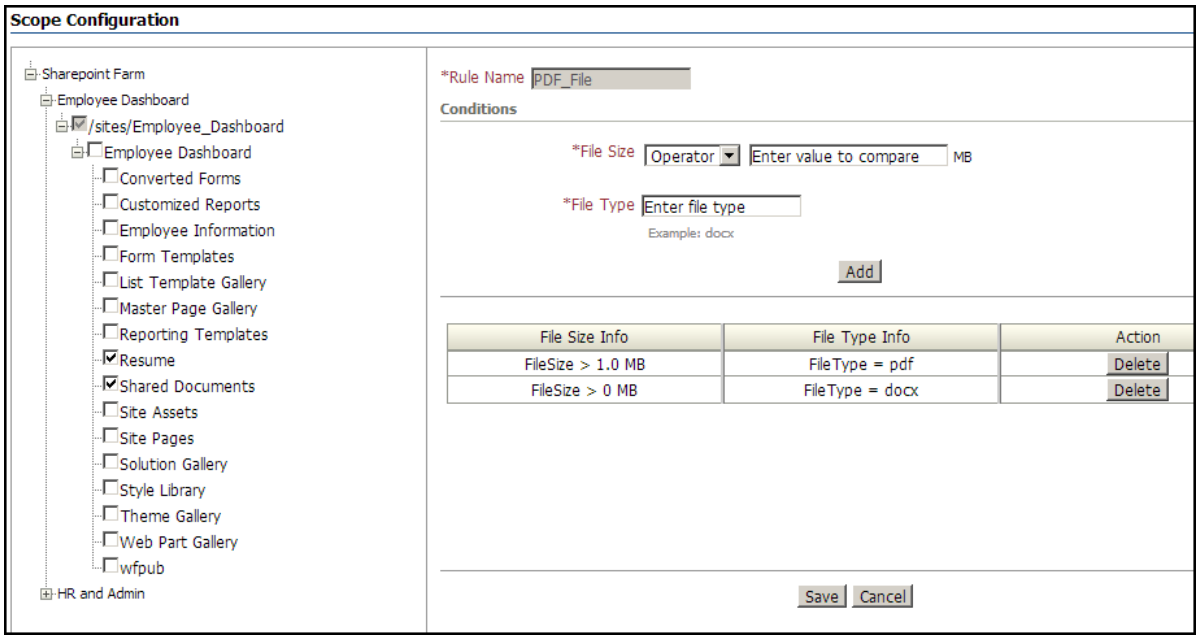
1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Scope Configuration**. The Scope Configuration page appears and displays the list of existing scope configuration rules.

Figure 3–7 Scope Configuration Home Page



3. In the List of Scope Rules region, click **Edit** in the row of the rule that you want to update. The Scope Rule Configuration page, where you can edit a rule, appears.

Figure 3–8 Scope Configuration Page



4. In the left pane of the Scope Configuration page, select the site collection, site, or document library for which you want to configure the scope configuration rule.
5. (Optional) Add a new condition to the scope configuration rule.
   a. In the Conditions region, select an operator from the **File Size** drop-down list.
   b. In the File Size field, select an operator and enter a file size value.

      Note: This is a mandatory field. You must enter an integer value. The value that you enter must comply with the SharePoint limitations on document upload size.

   c. In the File Type field, enter the type of file that the connector must transfer from SharePoint to WebCenter Content. If you want to transfer all types of files from SharePoint to WebCenter Content, type all.

      Note: This is a mandatory field.

      You must not add a dot before the file type. For example, you must use pdf instead of .pdf.

      The file type is not case-sensitive. For example, you can use pdf or PDF to transfer PDF file types.

      You can enter only one file type at a time. You must add a separate condition for each file type that you want to transfer to WebCenter Content in this rule. If you want to transfer all types of files from SharePoint to WebCenter Content, type all.

   d. Click **Add**. The condition is added to this rule. To add another condition to this rule, repeat steps a to d.

6. (Optional) Delete a condition from the scope configuration rule. To delete a condition from a scope configuration rule, in the Conditions region, click **Delete** in the row of the condition that you want to delete.
7. Click **Save**. The scope configuration rule is updated.

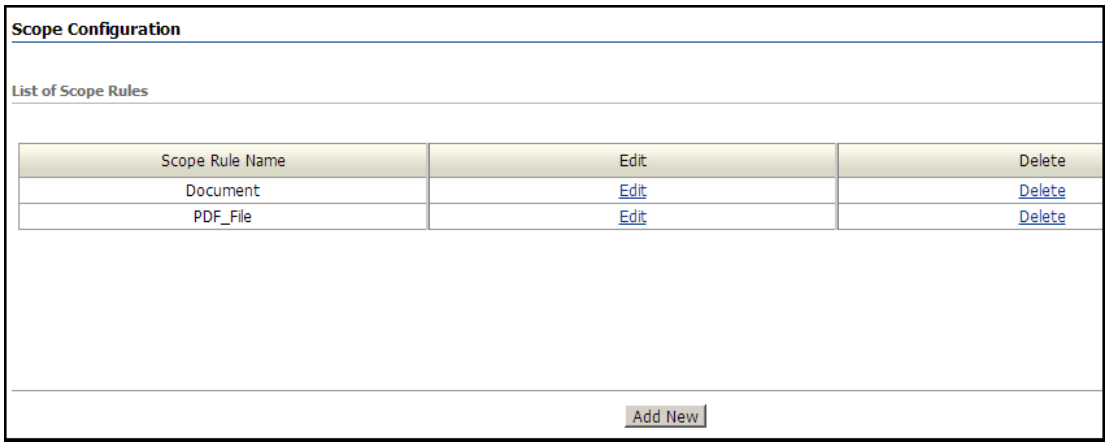
3.2.2.3 Deleting a Scope Configuration Rule

You can delete a scope configuration rule that you configured for a site collection, site, or document library. After you delete a scope configuration rule, the documents that the connector transferred to WebCenter Content remain in WebCenter Content. If these documents are updated in SharePoint, the connector continues to update them in WebCenter Content. However, for new documents in SharePoint, even if they meet the scope configuration rule that you deleted, the connector does not transfer to WebCenter Content.

To delete a scope configuration rule:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Scope Configuration**. The Scope Configuration page appears and displays a list of existing scope configuration rules.

Figure 3–9 Scope Configuration Home Page

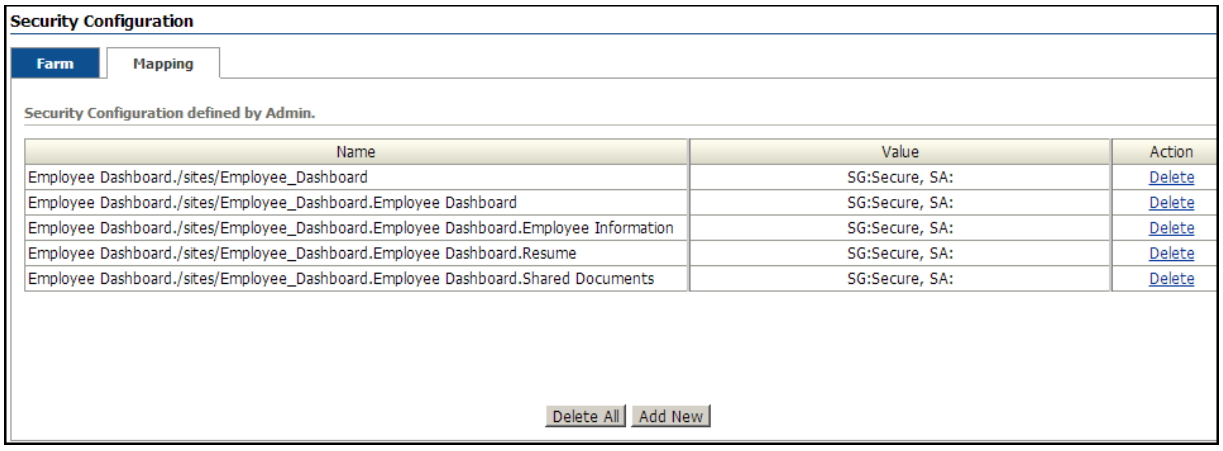


3. In the List of Scope Rules region, click **Delete** in the row of the rule that you want to delete. The scope configuration rule is deleted.

3.2.3 Configuring Security Settings for Locations (Optional)

You can configure the security settings for locations, such as site collections, sites, and document libraries. The Mapped Security Configuration page lists each location for which security settings are configured.

Figure 3–10 Mapping Tab on the Security Configuration Page



The following table describes the fields that appear on the Mapping tab.

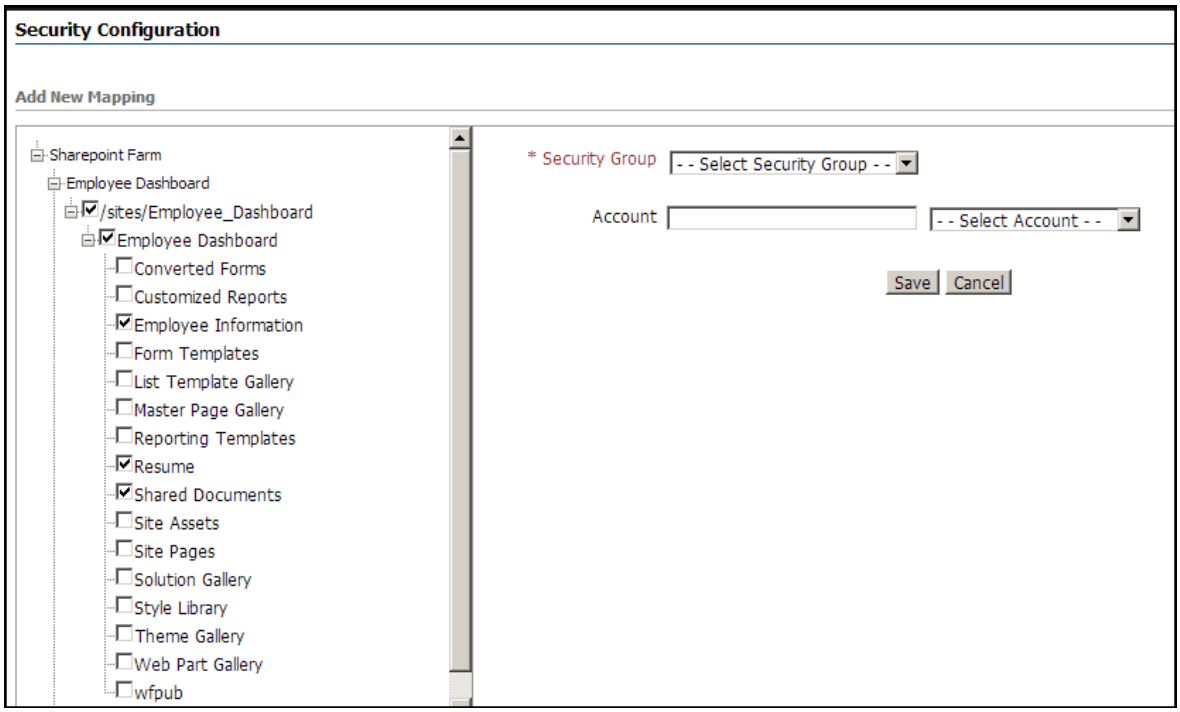
Element	Description
Name	Displays the site collection, site, or document library for which the security settings are configured.
Value	Displays the security group and security account that you configured for the site collection, site, or document library.
Action	Click **Delete** to delete the security settings that are configured for the site collection, site, or document library. For more information, see Section 3.2.3.2.
Delete All	Click **Delete** All to delete the security settings configured for all site collections, sites, and document libraries in the grid. For more information, see Section 3.2.3.2.
Add Mappings	Click **Add Mappings** to configure security settings for a site collection, site, or document library. For more information, see Section 3.2.3.1.

3.2.3.1 Configuring Security Settings for a Site Collection, Site, or Document Library

To configure security settings:

1. On the Mapping tab, click **Add Mapping**. The Add New Mapping page appears.

Figure 3–11 Add New Mapping Page



2. From Sharepoint Farm select the location, such as a site collection, site, or document library, for which you want to configure security settings.

   Note: You can configure security settings for multiple site collections, sites, and document libraries simultaneously.

3. From the **Security Group** drop-down list, select the security group that you want to configure for the locations that you selected.

   Note: The administrator must configure only those security groups to which the service account user has permissions.

4. (Optional) From the Select Account drop-down list, select the security account that you want to configure for the location that you selected. The security account that you select appears in the Account field. You can edit the account name in the Account field, if required.

5. Click **Save**. The grid displays the site collection, site, or document library for which the security settings are configured.

3.2.3.2 Deleting Security Settings for a Site Collection, Site, or Document Library

You can delete the security settings that you configured for a location, such as site collection, site, or document library. On the Mapping tab, click **Delete** in the row of the location for which you want to delete the security settings. After you delete the security settings for a location, this location automatically inherits the security settings that are configured for the immediate parent location.

You can also delete the security settings that you configured for all the site collections, sites, or document libraries that appear on the Mapped Security Configuration page.

On the Mapping tab, click **Delete All.** After you delete all the security settings that you configured for all locations, these locations automatically inherit the security settings that are configured at the farm level.

3.2.4 Mapping WebCenter Content Fields with SharePoint Metadata at the Document Library Level (Optional)

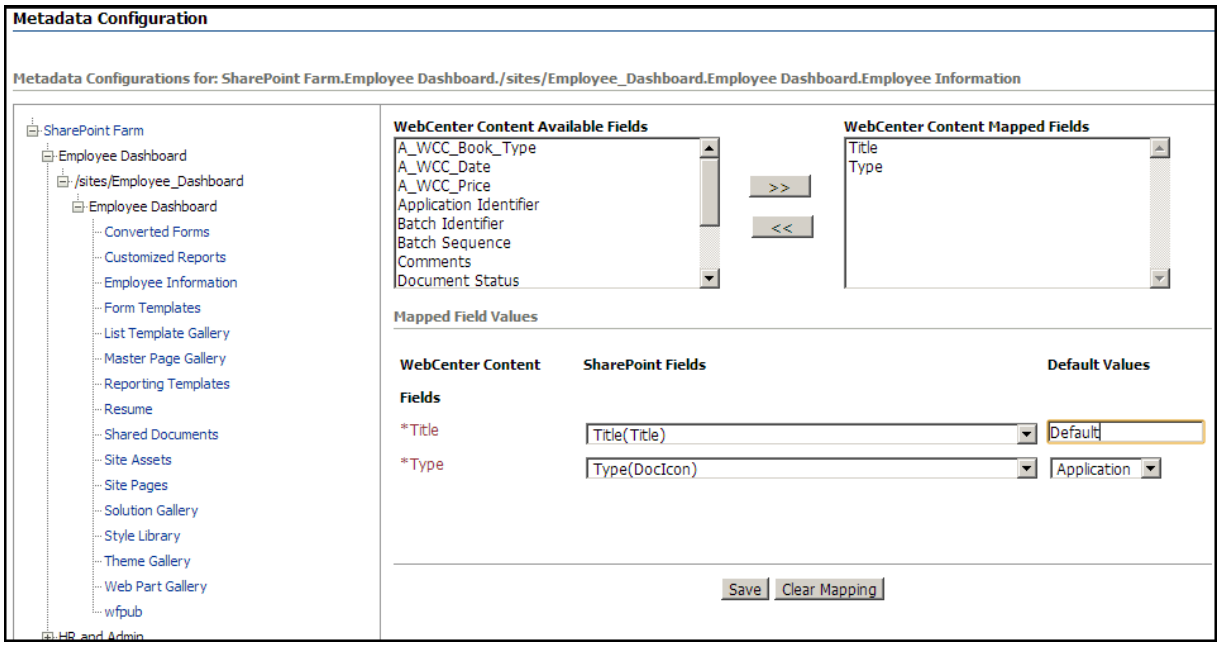
You can also map WebCenter Content fields with SharePoint metadata at the document library level. Document library level metadata mapping takes precedence over the farm level metadata mapping. If you add a new document library to SharePoint, the document library inherits the default metadata mapping at the farm level.

To map SharePoint metadata with WebCenter Content fields at the document library level:

> **Note:** If you add a new custom field in WebCenter Content and configure it as a required field, you must update the WebCenter Content database before mapping SharePoint metadata with WebCenter Content fields. If you do not update the database, the system displays an error message.

1. In the Content Server portal, open the SharePoint Connector tray, and then click **Metadata Configuration**. The Metadata Configuration page appears.

Figure 3–12 Metadata Configuration Page



2. On the navigation tree, expand the SharePoint farm, and then select the appropriate document library. The metadata mapping for the document library that you select appears in the right pane.
3. By default, the **WebCenter Content Mapped Fields** group and Mapped Field Values region display the fields for which you must map SharePoint metadata. The fields for which you must map metadata appear red in color and are marked

with an asterisk (*). The fields that you select appear in the **Mapped Field Values** region.

Note: Title and Type are mandatory fields.

(Optional) You can add additional fields with which you want to map SharePoint metadata. From the **WebCenter Content Available Fields** group, select the fields that you want to add, and then click the right arrow.

4. From the **SharePoint Fields** list, select the SharePoint metadata that you want to map with the WebCenter Content field.
5. In the **Default Value** field, enter a default value for the WebCenter Content mandatory field. When the SharePoint field does not contain any metadata, this default value is set as the value in the WebCenter Content field. If you do not enter a default value for a WebCenter Content mandatory field, an error message appears.
6. Click **Ok**. The SharePoint metadata is mapped with the WebCenter Content fields. The message Metadata mapping is successful for the selected SharePoint entity! appears.

Note: Click **Reset** to clear fields. The page enables you to map SharePoint metadata with WebCenter Content fields again.

4 Migration

Migration configuration allows you to transfer documents that are stored in the SharePoint content database to WebCenter Content.

Conversely, you can also copy the documents that are stored in WebCenter Content back to the SharePoint content database. The documents stored in SharePoint content database are first externalized to the connector custom database. Depending on the scope configuration rules, the documents are then transferred to WebCenter Content.

The Migration Configuration home page displays the migration history in a table.

The Migration Configuration page has a one-minute auto-refresh functionality that updates the status of the ongoing migration job.

A migration job can have one of the following status:

- When you initiate a migration job, the status of the job appears as Initiated. The Initiated status implies that the initiation of the migration process is completed, but the migration of documents is yet to start.
- When you initiate a migration job and the connector starts the migration process, the status of the job appears as In Progress.
- When a migration job is complete, the status of the job appears as Completed.
- If the migration process did not complete successfully, the status of the migration job appears as Aborted.

> **Note:** You can initiate only one migration job at a time.

This chapter covers the following topics:

- Section 4.1, "Externalization Migration"
- Section 4.2, "Scope-based Migration"

4.1 Externalization Migration

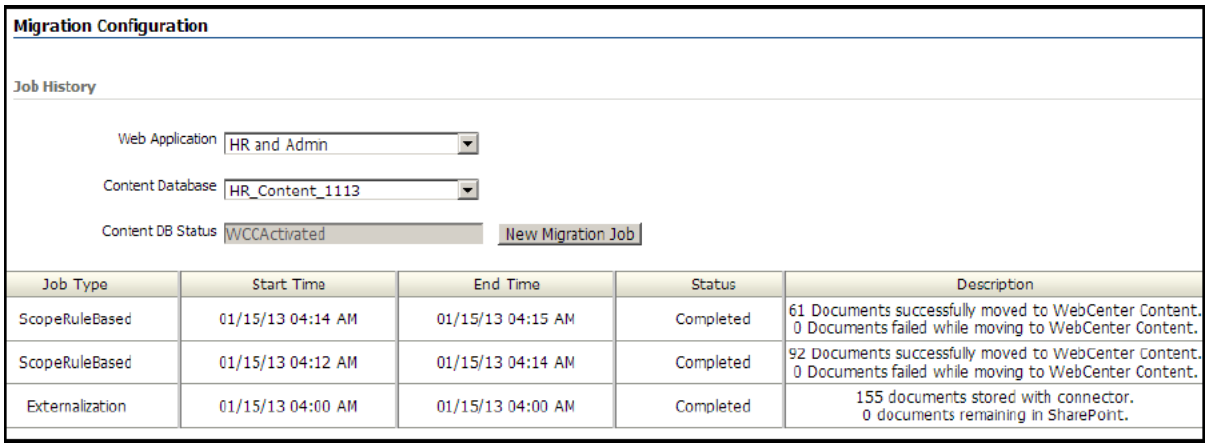
With externalization migration, documents that are stored in the SharePoint content database are externalized to the connector custom database. Before you initiate an externalization migration job for a content database, you must ensure that there is no other migration job scheduled or running.

To initiate externalization migration:

1. Log on to WebCenter Content as an administrator.

2. In the Content Server portal, open the SharePoint Connector tray, and then click **Migration Configuration**. The Migration Configuration page appears.

Figure 4–1 Migration Configuration Home Page

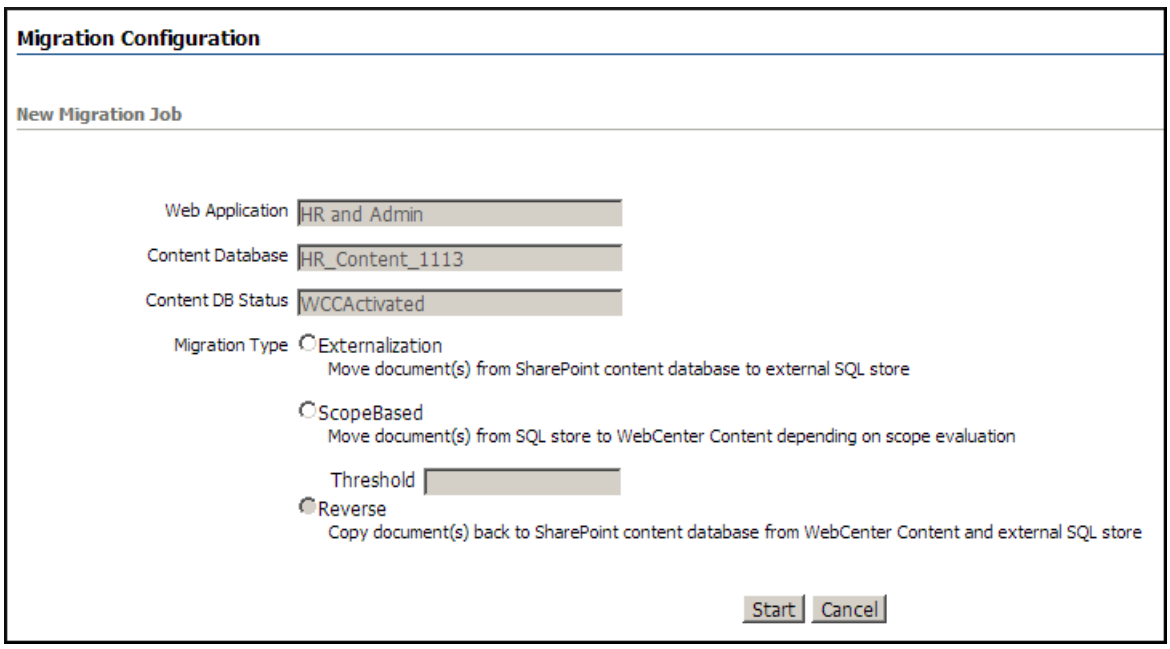


3. From the Web Application drop-down list, select a SharePoint web application.
4. From the Content Database drop-down list, select a content database whose contents you want to migrate to the connector custom database. The status of the content database that you selected appears in the Content DB Status field.

> **Note:** The content database that you selected must be in the WCCActivated status.

5. Click **New Migration Job**. The New Migration job page appears.

Figure 4–2 New Migration Job Page



Note: The New Migration Job button is available only if the status of the content database is WCCActivated or WCCDeactivated.

6. In the Migration Type options group, select Externalization.
7. Click **Start**. The connector initiates externalization migration process for the content database that you selected. You can view the status of the migration task in the Job History table on the Migration Configuration home page.

4.2 Scope-based Migration

With Scope-based migration, you can transfer documents from the connector custom database to WebCenter Content depending on whether the documents comply with scope configuration rules. The scope-based migration also allows you to set a failure threshold value. During the scope-based migration, when the document failure count reaches the threshold, the migration process is aborted.

Note: If the documents are added to the SharePoint content database before activation, you must externalize the documents before proceeding with the scope-based migration. For more information, see Section 4.1

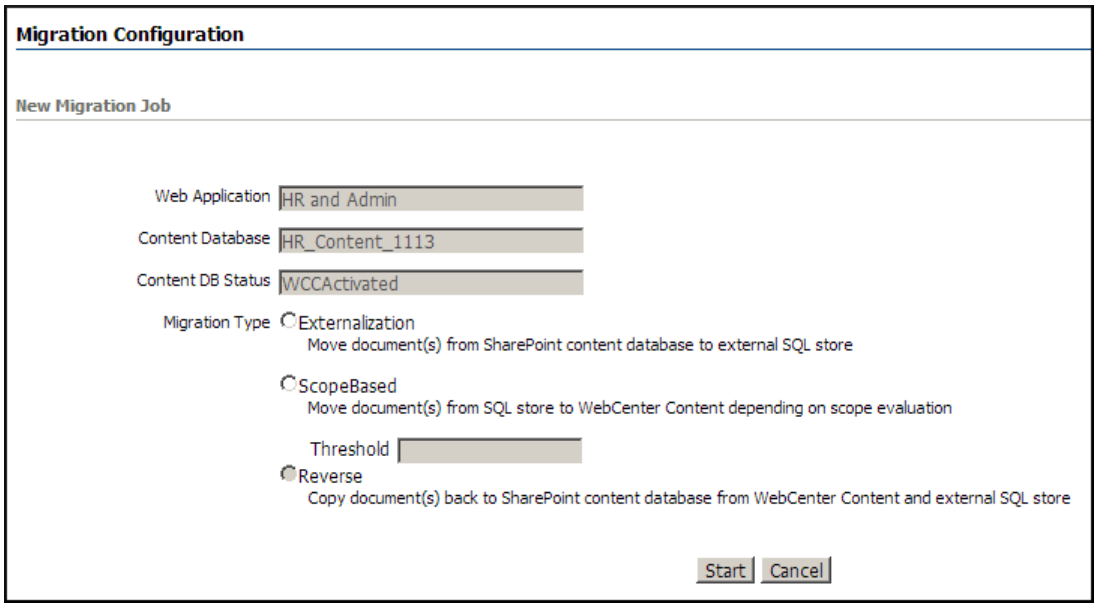
To initiate scope-based migration:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Migration Configuration**. The Migration Configuration page appears. See Figure 4–1.
3. From the Web Application drop-down list, select a SharePoint web application.
4. From the Content Database drop-down list, select a content database whose documents you want to migrate to WebCenter Content from the connector custom database. The status of the content database that you selected appears in the Content DB Status field.

Note: The content database that you selected must be in the WCCActivated status.

5. Click **New Migration Job**. The New Migration Job page appears.

Figure 4–3 New Migration Job Page



Note: The New Migration Job button is available only if the status of the content database is WCCActivated or WCCDeactivated.

6. In the Migration Type options group, select ScopeBased.
7. In the Threshold field, enter a document failure count. If the number of documents that failed to be migrated reaches this threshold count, the migration is stopped. The status of the migration job appears as Aborted.
8. Click **Start**. The connector initiates scope-based migration process for the content database that you selected. You can view the status of the migration task in the Job History table on the Migration Configuration home page.

5

Document Storage and Operations

This chapter deals with document storage and operations while using the Oracle WebCenter Content Storage Connector for Microsoft SharePoint 2010.

When a SharePoint user creates or updates a document, the document is stored in WebCenter Content or the connector custom database. When the connector transfers a document from SharePoint, the connector verifies whether the document complies with the scope configuration rules. If the document complies with the scope configuration rules, it is stored in WebCenter Content. If the document does not comply with the scope configuration rules or if network connectivity issues occur, it is stored in the connector custom database. For more information, see Section 3.2.2.

Note:

- WebCenter Content Workflow processing is not applicable for any SharePoint document.
- System account used for establishing connection between SharePoint and WebCenter Content should not be used for any kind of document operations on WebCenter Content. It must be solely dedicated to connector operations.

This chapter covers the following topics:

- Section 5.1, "Document Storage in WebCenter Content When Creating or Updating Documents in SharePoint"
- Section 5.2, "Document Retrieval from WebCenter Content When Reading or Downloading Documents in SharePoint"
- Section 5.3, "Document Deletion from WebCenter Content"
- Section 5.4, "Document Operations in WebCenter Content"

5.1 Document Storage in WebCenter Content When Creating or Updating Documents in SharePoint

When a user creates or updates a document or metadata on SharePoint, the following scenarios can occur.

Scenario	Result
Major versioning is enabled in SharePoint.	A new major version of the document is created in WebCenter Content.

Scenario	Result
Major and minor versioning is enabled in SharePoint.	A new version of the document is created in WebCenter Content. The document version is based on the major and minor version settings configured at SharePoint and WebCenter Content.
Versioning is not enabled in SharePoint.	The updated version of the document overwrites the existing version in SharePoint and WebCenter Content.
The document complies with the scope configuration rules configured in WebCenter Content.	The document is stored in WebCenter Content.
The document does not comply with the scope configuration rules configured in WebCenter Content.	The document is stored in the connector custom database.
Connectivity, transfer failure, or metadata mapping issues occur.	The document is stored in the connector custom database.

5.2 Document Retrieval from WebCenter Content When Reading or Downloading Documents in SharePoint

A SharePoint user can read or download documents from a SharePoint document library. When the user opens a document for reading, the system retrieves the document from WebCenter Content or from connector custom database and displays it in the SharePoint native application.

5.3 Document Deletion from WebCenter Content

When a user deletes documents from the SharePoint document library or the recycle bin, these documents are not automatically deleted from WebCenter Content. You can delete documents from WebCenter Content only if the documents are deleted from the SharePoint document library and both SharePoint recycle bins. To delete documents from WebCenter Content, run the RBS Maintainer utility. For more information, see http://technet.microsoft.com/en-us/library/ff943565(v=office.14).aspx.

5.4 Document Operations in WebCenter Content

A WebCenter Content user can perform the following operations in WebCenter Content for SharePoint documents that are stored in WebCenter Content:

- Download a document for which the WebCenter Content user has privileges.
- View SharePoint document metadata and content information in WebCenter Content.
- Update the document metadata for non-mapped WebCenter Content fields.

> **Note:** You cannot update document metadata for mapped WebCenter Content fields.

- Subscribe to a document.

6 Log Information

This chapter provides information on how you view log information and update log settings on SharePoint and on WebCenter Content.

This chapter covers the following topics:

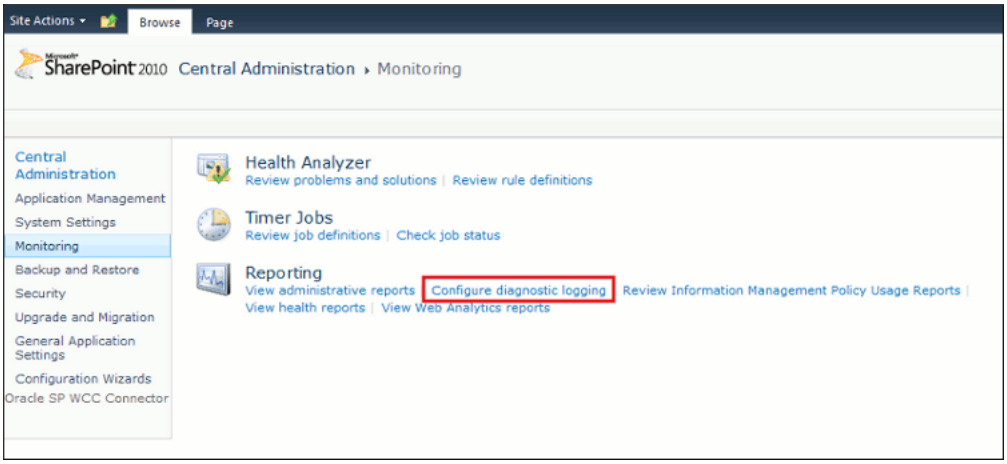
- Section 6.1, "Modifying Log Settings in SharePoint"
- Section 6.2, "Viewing Logs in SharePoint"
- Section 6.3, "Modifying Log Settings in WebCenter Content"
- Section 6.4, "Viewing Event Logs in WebCenter Content"

6.1 Modifying Log Settings in SharePoint

By default, SharePoint generates trace logs and event logs. You can modify the log settings and change logging levels. To modify log settings in SharePoint:

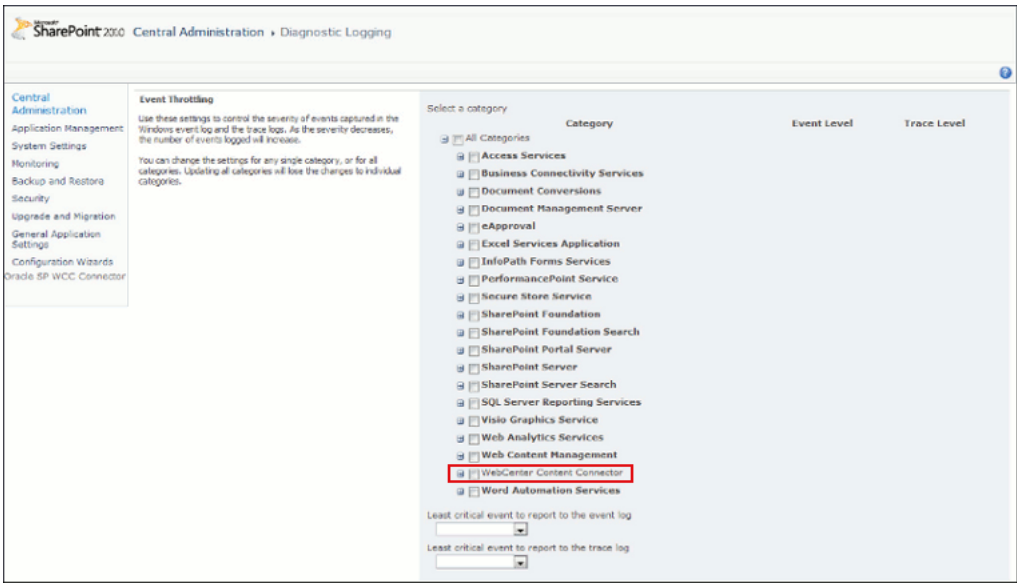
1. Log on to SharePoint Central Administration as an administrator.
2. In the left navigation pane of the SharePoint Central Administration, click **Monitoring**. The Monitoring page appears.

Figure 6–1 Monitoring Page



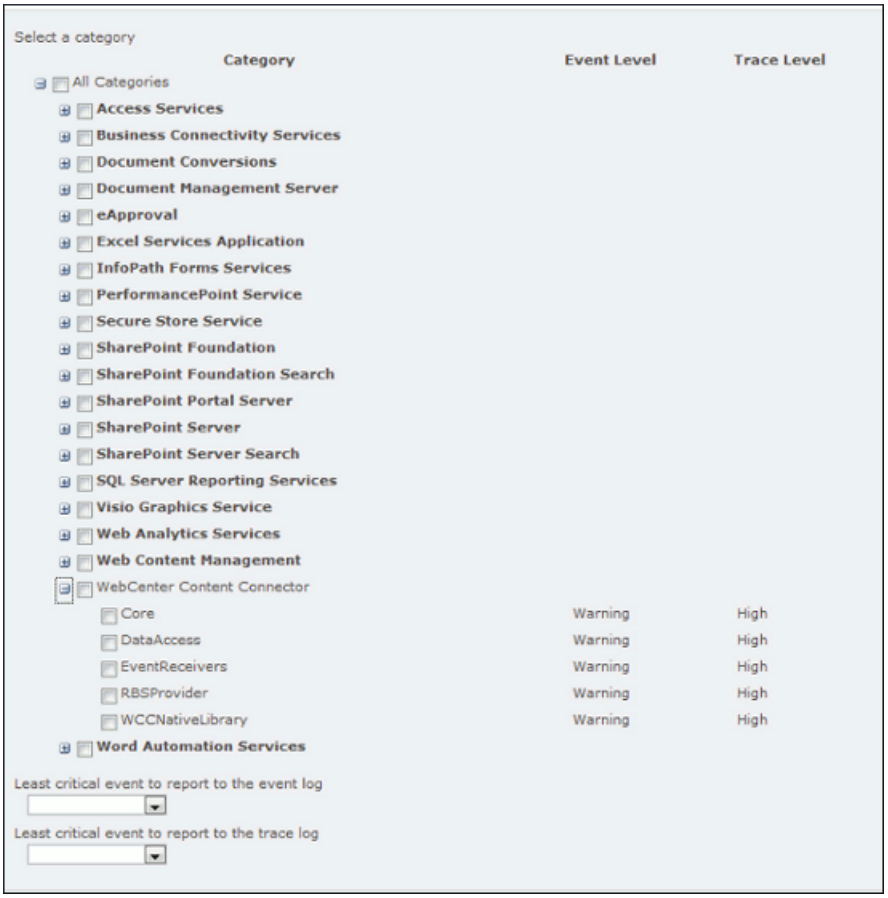
3. Under Reporting, click **Configure Diagnostic Logging**. The Diagnostic Logging page appears.

Figure 6–2 Diagnostic Logging Page



4. From the Category list, select WebCenter Content Connector, and then select the WebCenter Content Connector areas for which you want to modify the log settings.

Figure 6–3 WebCenter Content Connector Categories



5. From the Least critical event to report to the event log drop-down list, select a level for event logs.

   Note: Event logs are Windows logs. By default, SharePoint generates warning and above level event logs.

6. From the Least critical event to report to the trace log drop-down list, select a level for trace logs.

   Note: Trace logs are SharePoint logs. By default, SharePoint generates high and above level trace logs.

   The following table describes the log levels.

Log Level	Description
Critical and Unexpected	When a critical error occurs during a function and the connector fails to handle the error, SharePoint generates critical and unexpected logs.
Warning and High	When a critical error occurs during execution, the connector continues with the functionality and Windows generates warning and high logs.
Verbose	These are informative messages and logs.

6.2 Viewing Logs in SharePoint

You can view the logs that the system generated at the levels you configured.

To view event logs:

1. On the Windows system, click **Start**.
2. In the Search programs and files field, enter **Event Viewer**, and press **Enter**. The Event Viewer page appears and displays the event logs.

To view trace logs, navigate to the following path:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS
```

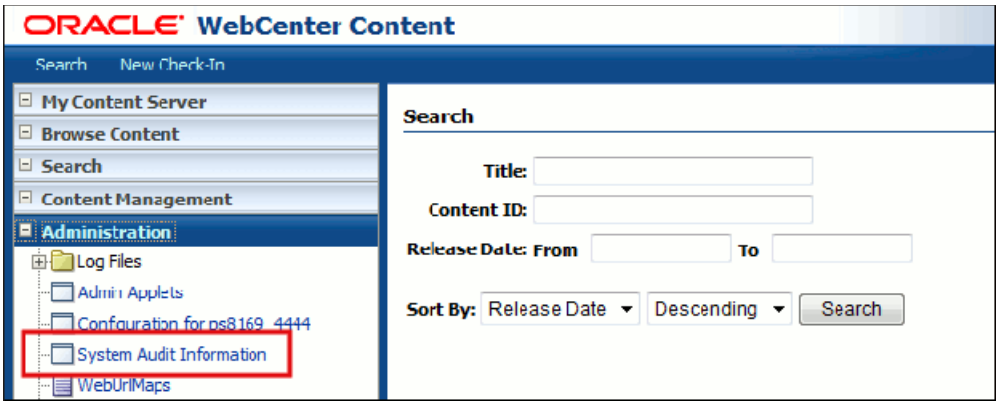
6.3 Modifying Log Settings in WebCenter Content

By default, WebCenter Content generates logs for all levels except the information level. You can modify settings and enable verbose logs.

To modify log settings in WebCenter Content:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, choose Administration, then **System Audit Information**. The System Audit Information page appears.

Figure 6–4 WebCenter Content Home Page



3. (Optional) To enable verbose level logs, in the Tracing Sections Information region, select **Full Verbose Tracing**.
4. In the Active Sections field, enter **SharePointConnector**, and then click **Update**. The modified log settings are saved.

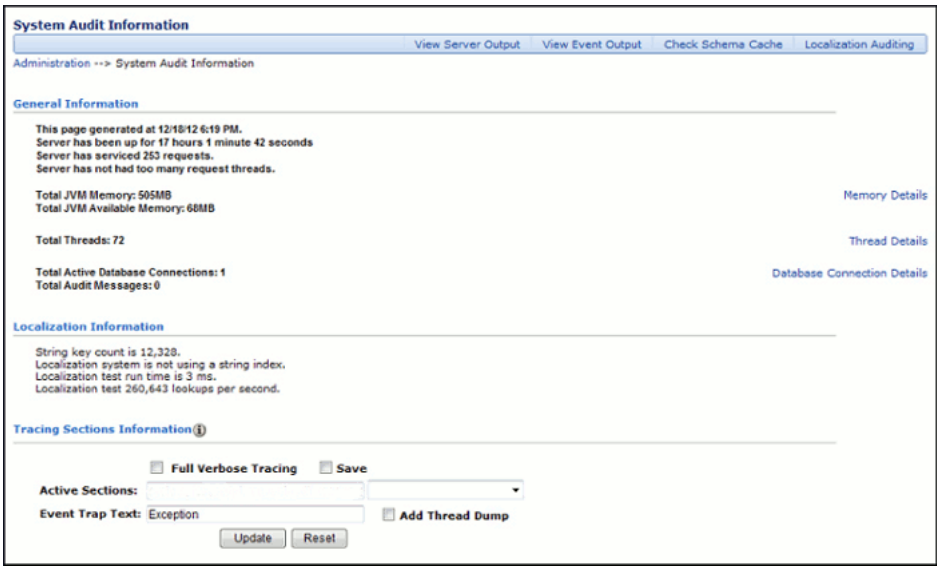
   See *Oracle Fusion Middleware Administering Oracle WebCenter Content* for more information on log settings.

6.4 Viewing Event Logs in WebCenter Content

To view event logs in WebCenter Content:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, choose Administration, select Log Files and then click **System Audit Information**. The System Audit Information page appears.

Figure 6–5 System Audit Information Page



3. In the top navigation pane, click **View Server Output**. The logs appear.

7

Connector Deactivation and Uninstallation

This chapter provides information on how you can deactivate and uninstall the WebCenter Content Storage Connector for Microsoft SharePoint 2010.

This chapter covers the following topics:

- Section 7.1, "Deactivating and Cleaning Up the Connector for a SharePoint Content Database"
- Section 7.2, "Deleting the Connection between SharePoint and WebCenter Content"
- Section 7.3, "Uninstallation"

7.1 Deactivating and Cleaning Up the Connector for a SharePoint Content Database

This section provides information on how you can deactivate the connector on a SharePoint content database, perform reverse migration, run the RBS Maintainer utility, and clean up the connector for a SharePoint content database.

7.1.1 Deactivating the Connector on a SharePoint Content Database

Deactivating the connector on a SharePoint content database removes the security, metadata, and scope configuration settings that you configured for the SharePoint content database. After you deactivate the connector for a SharePoint content database, the connector does not externalize the documents created or updated in the site collections that belong to this SharePoint content database. These documents are stored in the SharePoint content database. However, the documents that were already externalized before you deactivated the connector remain in the connector custom database or in WebCenter Content.

To deactivate the connector on a SharePoint content database:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Activation Configuration**. The Activation Configuration page appears. See Figure 3–4.
3. From the Web Application drop-down list, select the SharePoint web application that contains the content database that you want to deactivate. The list of content databases for the Web Application that you selected appears.
4. In the Action column, click **Deactivate** for the appropriate SharePoint content database.

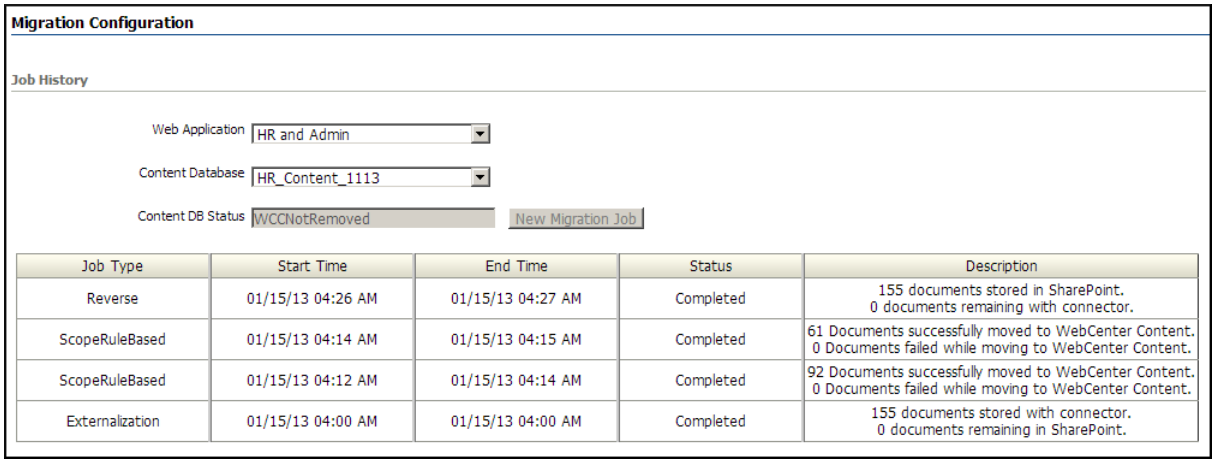
7.1.2 Performing Reverse Migration

With reverse migration, you can copy the documents that are stored in WebCenter Content and the connector custom database to the SharePoint content database.

To initiate reverse migration:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Migration Configuration**. The Migration Configuration page appears.

Figure 7–1 Migration Configuration Home Page

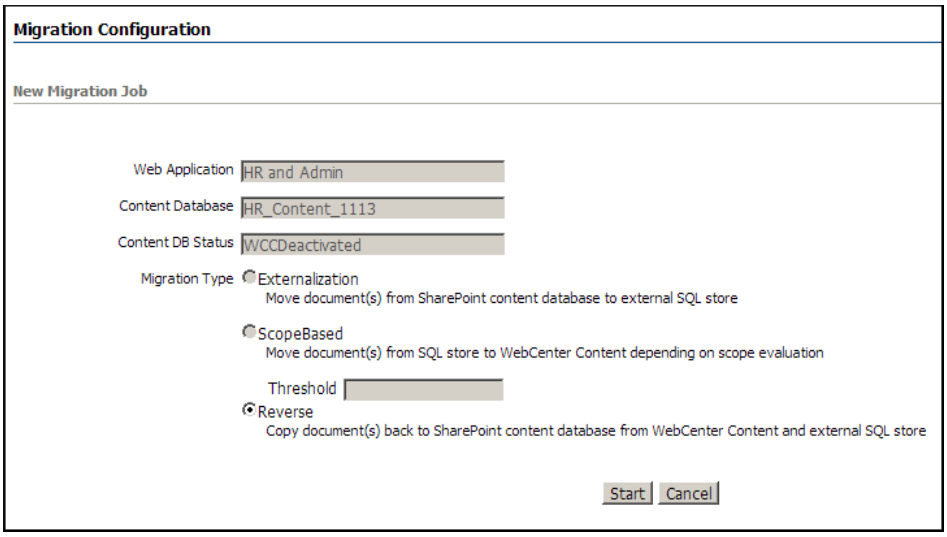


3. From the Web Application drop-down list, select a SharePoint web application.
4. From the Content Database drop-down list, select a content database whose contents you want to copy to the SharePoint content database from WebCenter Content and the connector custom database. The status of the content database that you selected appears in the Content DB Status field.

> **Note:** The content database that you selected must be in the WCCDeactivated status.

5. Click **New Migration Job**. The New Migration Job page appears.

Figure 7–2 New Migration Job Page



Note: The New Migration Job button is enabled only if the status of the content database is WCCActivated or WCCDeactivated.

6. In the Migration Type options group, select Reverse.
7. Click **Start**. The connector initiates reverse migration process for the content database that you selected. You can view the status of the migration task in the Job History table on the Migration Configuration home page.

7.1.3 Running the RBS Maintainer Utility

To delete documents from WebCenter Content and perform other RBS Maintainer operations, you must run the RBS Maintainer utility. For more information, see Section 5.3.

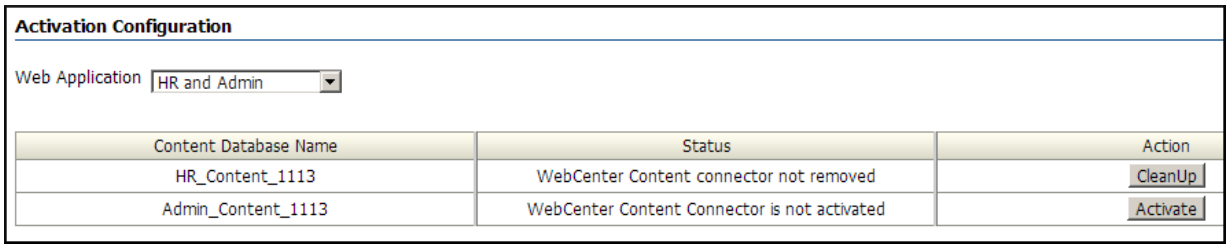
7.1.4 Cleaning Up the Connector for a SharePoint Content Database

Before cleaning up the connector for a SharePoint content database, you must run the the RBS Maintainer. For more information, see Section 7.1.3.

To clean up the connector for a SharePoint content database:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, open the SharePoint Connector tray, and then click **Activation Configuration**. The Activation Configuration page appears.

Figure 7–3 Activation Configuration Page



3. From the Web Application drop-down list, select the SharePoint web application that contains the content database that you want to clean up. The list of content databases for the Web Application that you selected appears.
4. Click **CleanUp**.

7.2 Deleting the Connection between SharePoint and WebCenter Content

Before you delete the connection between SharePoint and WebCenter Content, you must perform the deactivation and cleanup process for all the SharePoint content databases that you connected with WebCenter Content. For more information, see Section 7.1.1.

After you deactivate all the content databases, click **Delete** on the Connection Configuration page.

7.3 Uninstallation

This section provides information on how you can uninstall the WebCenter Content Storage Connector for Microsoft SharePoint 2010 from the SharePoint environment and the WebCenter Content environment.

7.3.1 Uninstalling the Connector from the SharePoint Environment

This section provides information on how you can uninstall and retract the connector, and unregister the WebCenter Content RBS provider.

7.3.1.1 Uninstalling and Retracting the Connector

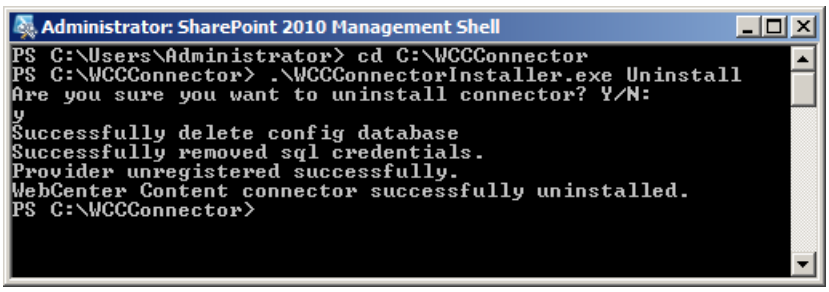
Before uninstalling the connector, you must delete the connection that is configured between SharePoint and WebCenter Content. For more information, see Section 7.2.

To uninstall the connector from the SharePoint farm:

1. On the SharePoint server from where you want to uninstall the connector, open SharePoint 2010 Management Shell as an administrator.
2. Change the directory to the location where you extracted the WCCConnector.zip package. For more information, see Section 2.3.1.
3. To uninstall the connector from the SharePoint farm, use the following command:

```
.\WCCConnectorInstaller.exe Uninstall
```

Figure 7–4 Uninstall Command and Output

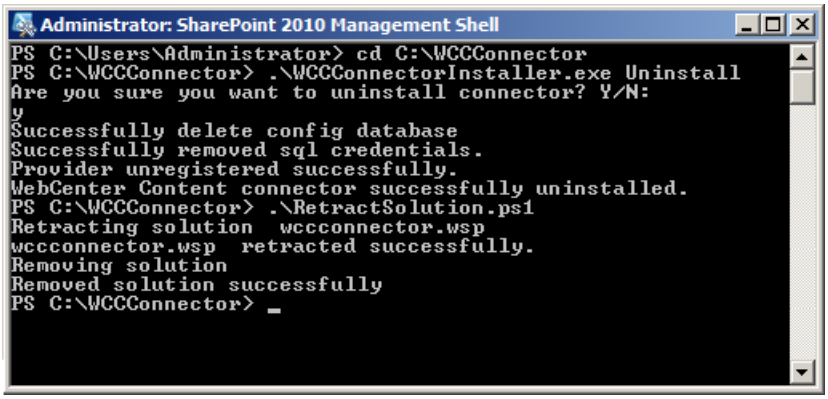


4. When the system prompts you whether you want to uninstall the connector, press Y, and then press Enter.

5. To retract the WCCConnector WSP from the SharePoint farm, use the following command:

```
.\RetractSolution.ps1
```

Figure 7–5 Retract Solution Command and Output



7.3.1.2 Unregistering the WebCenter Content RBS Provider

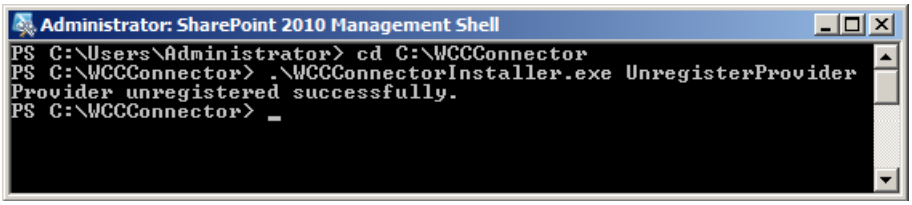
Apart from the server where you uninstalled the connector, you must unregister the WebCenter Content RBS provider from each server in the SharePoint farm. If you have a single-server SharePoint farm environment, you do not need to perform this step.

To unregister the WebCenter Content RBS provider from the SharePoint farm:

1. On the SharePoint server where you want unregister the WebCenter Content RBS provider, open SharePoint 2010 Management Shell as an administrator.
2. Change the directory to the location where you extracted the WCCConnector.zip package. For more information, see Section 2.3.1.
3. Use the following command:

```
.\WCCConnectorInstaller.exe UnregisterProvider
```

Figure 7–6 Unregister Provider Command and Output



7.3.2 Disabling the Connector from WebCenter Content

To disable the connector from WebCenter Content:

1. Log on to WebCenter Content as an administrator.
2. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager.** The Component Manager page opens. See Figure 2–10.
3. Click the **Advanced Component Manager** link. The Advanced Component Manager page appears. See Figure 2–11.

4. In the Enabled Components list, select SharepointConnector, and then click **Disable**.
5. From the Uninstall Component drop-down list, select SharepointConnector, and then click **Uninstall**.

A

Troubleshooting

This appendix describes common problems that you might encounter when using the WebCenter Content Storage Connector for Microsoft SharePoint 2010 and explains how to solve them.

This appendix includes the following sections:

- Section A.1, "Introduction to Troubleshooting"
- Section A.2, "Resolving Common Problems"
- Section A.3, "Frequently Asked Questions"
- Section A.4, "Using My Oracle Support for Additional Troubleshooting Information"

In addition to this appendix, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

A.1 Introduction to Troubleshooting

This section provides guidelines and a process for using the information in this chapter. Using the following guidelines and process will focus and minimize the time you spend resolving problems.

Guidelines

When using the information in this chapter, Oracle recommends:

- After performing any of the solution procedures in this chapter, immediately retrying the failed task that led you to this troubleshooting information. If the task still fails when you retry it, perform a different solution procedure in this chapter and then try the failed task again. Repeat this process until you resolve the problem.
- Making notes about the solution procedures you perform, symptoms you see, and data you collect while troubleshooting. If you cannot resolve the problem using the information in this chapter and you must log a service request, the notes you make will expedite the process of solving the problem.

Process

Follow the process outlined in Table A–1 when using the information in this chapter. If the information in a particular section does not resolve your problem, proceed to the next step in this process.

Table A–1 Process for Using the Information in this Chapter

Step	Section to Use	Purpose
1	Section A.2	Perform problem-specific troubleshooting procedures for WebCenter Content Storage Connector for Microsoft SharePoint 2010. This section describes: ■ Possible causes of the problems ■ Solution procedures corresponding to each of the possible causes
2	Section A.3	Use this section to view frequently asked questions and their answers.
3	Section A.4	Use My Oracle Support to get additional troubleshooting information about Oracle Fusion Applications or Oracle BI. My Oracle Support provides access to several useful troubleshooting resources, including Knowledge Base articles and Community Forums and Discussions.
4	Section A.4	Log a service request if the information in this chapter and My Oracle Support does not resolve your problem. You can log a service request using My Oracle Support at `https://support.oracle.com`.

A.2 Resolving Common Problems

This section describes common problems and solutions. It contains the following topics:

- Section A.2.1, "No Execution Notifications while Installing RBS"
- Section A.2.2, "RBS Installation Failed"
- Section A.2.3, "The Error "WCCConnector solution is already added/deployed" Appears when Deploying the WebCenter Content Connector Web Solution Package on SharePoint"
- Section A.2.4, "The Error "Login failed for user 'username'" Appears while Installing the WebCenter Content Connector on SharePoint"
- Section A.2.5, "SQL Authentication Issues"
- Section A.2.6, "On WebCenter Content, the Connection Configuration Page Displays an Error"
- Section A.2.7, "On WebCenter Content, the Metadata, Security, or Add Scope Rule Page Displays an Error"
- Section A.2.8, "SQL Authentication Issues"

Note: The solutions provided in this section are based on general observations. The solutions may vary depending on your environment. You might also find other solutions to these issues.

A.2.1 No Execution Notifications while Installing RBS

While installing RBS, you do not see any execution notifications.

Cause

The RBS installation command runs the installation in the background.

Solution

The RBS installation command creates a log file, named rbs_install_log.txt, in the same folder that contains the RBS.msi file. You can view notifications in this log file.

A.2.2 RBS Installation Failed

Cause 1

Invalid installation command.

Solution 1

Verify the command that you used to install RBS. For information about how to install RBS, see

http://technet.microsoft.com/en-us/library/ff629463(v=office.14).aspx#Section3

You must also ensure that you replace the following variables of the RBS installation command with valid values:

- RBS

  If the current path of the command prompt is the same as the path of the RBS installation file, you must replace the RBS variable with the name of the MSI file. If the current path of the command prompt is not the same as the path of the RBS installation file, you must provide the complete path for the file.

- DBInstanceName

  You must replace the DBInstanceName variable with the SQL server instance name where the database, for which you want to install RBS, exists. You must also verify that this SQL server instance is accessible by using the server instance name.

- WSS_Content

  You must replace this variable with the database name for which you want to install RBS. You must also verify that this database exists on the SQL server instance that is provided as the DBInstanceName.

Cause 2

Master key does not exist in the database.

Solution 2

The database for which you want to install RBS must contain the DatabaseMasterKey.

To create the DatabaseMasterKey:

1. Replace the variable WSS_Content with the name of the database for which you want to install RBS.
2. Use the following command:

```
use [WSS_Content]

if not exists

(select * from sys.symmetric_keys where name = N'##MS_DatabaseMasterKey##')

create master key encryption by password = N'Admin Key Password !2#4'
```

Cause 3

Authentication issue.

Solution 3

This error occurs when you try to install RBS without appropriate permissions. You must install RBS as a user with sufficient permissions or as a user SharePoint Farm account for this installation.

A.2.3 The Error "WCCConnector solution is already added/deployed" Appears when Deploying the WebCenter Content Connector Web Solution Package on SharePoint

Cause 1

WCCConnector solution package is already added or deployed.

Solution 1

When deploying the ABC package, the error WCCConnector solution is already added/deployed might appear.

This means that the connector is already present in the SharePoint environment. If you are reinstalling the solution, validate that you uninstalled and retracted the connector properly.

Cause 2

The DeploySolution.ps1 file is not digitally signed.

Solution 2

If the environment supports only digitally-signed scripts, follow the standard mechanism to deploy the WSP solution on the SharePoint environment. You must add or deploy WCCConnector.wsp on the SharePoint farm.

A.2.4 The Error "Login failed for user 'username'" Appears while Installing the WebCenter Content Connector on SharePoint

Cause

Invalid SQL Credentials provided during Connector Installation

Solution

Enter valid user credentials for the SQL user.

A.2.5 SQL Authentication Issues

Cause

Invalid or outdated SQL credentials

Solution

To update the SQL credentials:

1. Run the command prompt as an administrator.
2. Change the path to the folder that contains the WCCConnectorInstaller.exe file.
3. Use the following command:

```
WCCConnectorInstaller.exe UpdateSQLCred
```

4. Provide the SQL credentials that the connector must use.

A.2.6 On WebCenter Content, the Connection Configuration Page Displays an Error

Cause

The WebLogic Server authenticator was not configured to use the default Java authenticator (-DUseSunHttpHandler).

The following error appears:

```
http://{doamin}:{port}/_vti_adm/WCCConnector/ConfigurationService.svc with
the supplied Domain/Username/Password. Runtime error:
com.sun.xml.ws.wsdl.parser.InaccessibleWSDLException: 2 counts of
InaccessibleWSDLException.
```

Solution

To ensure that WebCenter Content uses the Java authenticator:

1. Navigate to the following path:

   ```
   $domain_home\bin
   ```

   $domain_home is the domain home directory where WebCenter Content is installed.

2. Open the startManagedWebLogic.cmd file in edit mode.
3. Search for JAVA_OPTIONS.
4. Append the following line to JAVA_OPTIONS:

   ```
   -DUseSunHttpHandler=true
   ```

A.2.7 On WebCenter Content, the Metadata, Security, or Add Scope Rule Page Displays an Error

Cause

The system user of the WebCenter Content Server has permissions on the SharePoint Server.

The following error appears:

```
Getting Runtime error:
com.sun.xml.ws.protocol.soap.MessageCreationException: Couldn't create
SOAP message due to exception: XML reader error:
com.ctc.wstx.exc.WstxUnexpectedCharException: Unexpected character '4'
(code 52) in prolog; expected '<' ?
```

Solution

You must ensure that the system user of the WebCenter Content server does not have the permission to access the SharePoint server. If the system user has the permission, remove the permission, restart the WebLogic server, and then try again.

A.2.8 SQL Authentication Issues

Cause

Invalid or outdated SQL credentials

Solution

To update the SQL credentials:

1. Run the command prompt as an administrator.
2. Change the path to the folder that contains the `WCCConnectorInstaller.exe` file.
3. Use the following command:

   ```
   WCCConnectorInstaller.exe UpdateSQLCred
   ```

4. Provide the SQL credentials that the connector must use.

A.3 Frequently Asked Questions

Question 1

On which database do I need to install and enable RBS?

Answer 1

To find the database where you must install and enable RBS:

1. Identify the site collection on which you want to enable the connector.
2. Open SharePoint 2010 Central Administration.
3. Click **Application Management**. The Application Management page appears.
4. In the Site Collection region, click **View All Site Collections**. The Site Collection List page appears.
5. Select the web application where the site collection exists. The list of site collections for the web application that you selected appears.
6. Select the site collection for which you want to enable the connector. The site collection details appear on the right region. These details contain the name of the database in which the site collection exists. You must install RBS on this database

Question 2

How do I verify whether the RBS installation is successful?

Answer 2

RBS installation has two types of installation, one of the first Web server and the other on all additional Web and Application servers. The validation for both the scenarios is different.

To verify whether RBS is successfully installed on the First Web server:

- Verify the RBS Installation Logs.

  The RBS installation command creates a log file, named rbs_install_log.txt, in the same folder that contains the RBS.msi file. Open the log file by using a text editor and scroll down to the bottom of the file. You must see the following notification in the last few lines of the log file:

```
Product: SQL Remote Blob Storage - Installation completed successfully.
```

> **Note:** This notification does not indicate that the installation is successful. If you see this notification, you must proceed with the database verification task.

- Database Verification.

  On the SQL Server, verify that the RBS tables exist in the SharePoint content database. You must see several tables under the SharePoint content database. These tables have names that are preceded by the letters mssqlrbs.

To verify whether RBS is successfully installed on all additional Web and Application servers:

- Verify the RBS Installation Logs.

  The RBS installation command creates a log file, named rbs_install_log.txt, in the same folder that contains the RBS.msi file. Open the log file by using a text editor and scroll down to the bottom of the file. You must see the following notification in the last few lines of the log file:

  ```
  Product: SQL Remote Blob Storage - Installation completed successfully.
  ```

  > **Note:** This notification does not indicate that the installation is successful. If you see this notification, you must proceed with the database verification task.

- Verify the RBS folder content.

  Verify whether the path C:\Program Files\Microsoft SQL Remote Blob Storage 10.50 contains the following directories:

  – 1033
  – Client Library
  – Documentation
  – Maintainer
  – Provider Libraries
  – Server

A.4 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems. My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles
- Community forums and discussions
- Patches and upgrades
- Certification information

Note: You can also use My Oracle Support to log a service request.

You can access My Oracle Support at https://support.oracle.com.